Citrix DaaS

Contents

Overview

February 19, 2024

Introduction

Citrix DaaS is a service that provides app and desktop virtualization, giving IT control of on-prem or cloud-hosted virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface.

Using Citrix DaaS, you can deliver secure virtual apps and desktops to any device, leaving most of the installation, setup, and upgrades to Citrix. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.

Citrix DaaS allows you to manage on-premises data center and public cloud workloads together in a hybrid deployment. You can connect to public clouds Microsoft Azure, Amazon Web Services (AWS), and Google Cloud, plus on-premises hypervisors such as XenServer, Microsoft Hyper-V, Nutanix AHV, and VMware vSphere. The hybrid, multi-cloud approach gives you the flexibility to deploy different applications in different resource locations worldwide.

Citrix DaaS offers several ways to deliver apps and desktops.

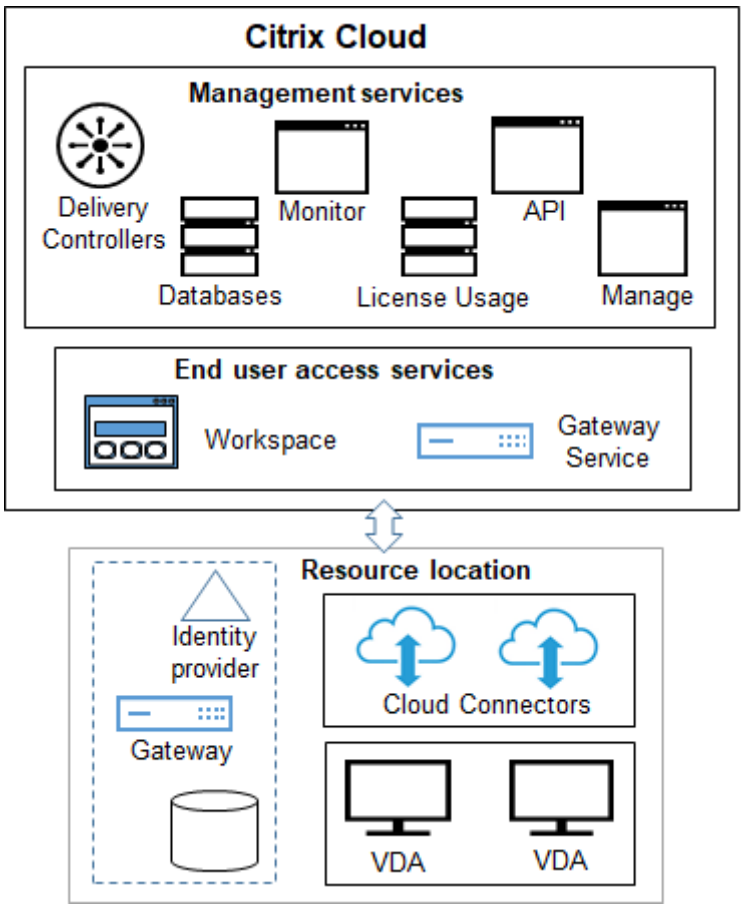
- Delivery methods describes the primary ways, with use-cases and pros/cons.
- Delivery models lists more choices, and also offers VDI model comparisons.

Citrix Managed Azure further simplifies the deployment of virtual apps and desktops. With Citrix Managed Azure, Citrix also manages the hosting of Azure workloads.

Learn more about the advantages of using this service.

Site overview

The following graphic shows the services and components that Citrix administrators work with in a Citrix DaaS production deployment (also known as a site).



As shown in the graphic, Citrix manages the user access and management services and components in Citrix Cloud. The applications and desktops that you deliver to users reside on machines in one or more resource locations. In a Citrix DaaS deployment, a resource location contains components from the access layer and resource layers. Each resource location is considered a zone.

If you recently migrated from Citrix Virtual Apps and Desktops, you'll see that Citrix DaaS eliminates most of the component setup work required in an on-premises deployment.

Components and services managed by Citrix

- **Delivery Controllers:** Citrix DaaS provides the functionality to load balance applications and desktops, authenticate users, and broker or prioritize connections directly from the cloud, without the need to manage Delivery Controllers, as with Citrix Virtual Apps and Desktops.
- **Databases:** Site configuration, monitoring, and configuration logging data is stored by the cloud service, eliminating the SQL database requirement of the on-premises Citrix Virtual Apps and Desktops product.
- **Licensing:** Manages licenses and provides usage statistics.

- **Management interfaces:** See Management interfaces. Many tasks are also available in service APIs.
- **Monitor interface:** The Monitor interface enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become critical, and perform support tasks for end users. Displays include:
  - Real-time session data from the Broker Service in the Controller, which includes data from the broker agent in the Virtual Deliver Agent (VDA).
  - Historical data from the Monitor Service in the Controller.
  - Data about HDX traffic (also known as ICA traffic).
- **Cloud Connectors:** A Cloud Connector is the communications channel between the components in the Citrix Cloud and components in the resource location. In the resource location, the Cloud Connector acts as a proxy for the Delivery Controller in Citrix Cloud.

  Every resource location contains at least one Cloud Connector. Two or more Cloud Connectors are recommended for redundancy.
  - When using Full Configuration to provision machines, you first install Cloud Connectors from the Citrix Cloud console. For details, see Cloud Connectors.
  - When using Quick Deploy to provision Azure machines, Citrix creates the resource location and Cloud Connectors for you when you create a catalog.

  After Cloud Connectors are installed, Citrix manages and updates them. The only tasks handled by the customer are Cloud Connector Windows updates and patching.

Management interfaces

From the **Manage** tab of Citrix DaaS, you can select the following interfaces.

Full Configuration

From the **Manage > Full Configuration** interface, you can:

- Get an overview of your Citrix DaaS deployment and the latest features from the Home page.
- Create and manage connections to hosts.
- Create and manage catalogs of machines that contain apps and desktops you deliver to your users.
- Create and manage delivery groups (and optionally, application groups.

- Create and manage Citrix policies that affect the use and behavior of HDX technologies and features, plus site-level management. This includes policy settings for sessions, adaptive transport, devices, graphics, multimedia, content redirection, and VDAs.
- Customize delegated administration to create role-based administrators who have specific scopes of authority.
- Manage the Autoscale feature to proactively power manage machines that deliver apps and desktops.
- Load balance machines
- Run health checks on your VDAs to identify potential issues and fix suggestions.
- Display configuration log content to see when configuration changes and other administrative activities occurred, and who initiated them.

Quick Deploy

From the **Manage > Quick Deploy** interface, you can easily deploy and manage Microsoft Azure workloads that use either a Citrix Managed Azure subscription or your own Azure subscription. For more information, see Quick Deploy and Citrix Managed Azure. From Quick Deploy, you can:

- Create and manage catalogs.
- Create and customize images, either from various Citrix prepared images, or from images you import from your Azure subscription.

For more information, see Quick Deploy.

Environment Management

From the **Environment Management** interface, you can use intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times. For more information, see Workspace Environment Management.

Components and technologies managed by the customer

- **Citrix Gateway:** When users connect from outside the corporate firewall, Citrix DaaS can use Citrix Gateway technology to secure these connections with TLS. The Citrix Gateway or VPX virtual appliance is an SSL VPN appliance deployed in the DMZ. It provides a single secure point of access through the corporate firewall.

  Citrix installs and manages the Citrix Gateway service in Citrix Cloud. You can also optionally install Citrix Gateway in resource locations.

- **Active Directory:** Active Directory is used for authentication and authorization. It authenticates users and ensures that they are getting access to appropriate resources. A subscriber's identity defines the services to which they have access in Citrix Cloud. This identity comes from Active Directory domain accounts provided from the domains within the resource location.
- **Identity Provider (IdP):** The IdP is the final authority for the user's identity. Supported IdPs include: on-premises Active Directory, Active Directory plus token, Azure Active Directory, Citrix Gateway, and Okta. For more information, see:
  - Workspace Identity
  - Identity and access management
- **Virtual Delivery Agents (VDAs):** Each physical or virtual machine that delivers resources (applications and desktops) must have a Citrix VDA installed on it. VDAs establish and manage the connection between the machine on which it's installed and the user device, and apply policies that are configured for the session.

  The VDA registers with a Delivery Controller, using a Cloud Connector in the resource location as a proxy.

  Several VDA types are available:
  - VDAs for Windows multi-session operating systems allow multiple users to connect to the machine at one time. This VDA type is usually installed on Windows servers.
  - VDAs for Windows single-session operating systems allow one user to connect to a machine at a time. This VDA type is usually used for VDI.

    A core version of this VDA type is available for use with the Remote PC Access feature. It contains a subset of the features in the full single-session VDA.
  - Linux VDAs support virtual apps and desktops based on an RHEL, CentOS, SUSE, or Ubuntu distribution.

  Throughout this service's documentation, "VDA"often refers to the agent and the machine on which it is installed.
- **Hypervisors and cloud services:** In most production sites, the app and desktop instances (workloads) that you make available (publish) to your users are "hosted"by a supported hypervisor or cloud service. (The Remote PC Access feature is usually used with physical machines. Therefore, it does not use hypervisors or cloud services for machine provisioning.)
  - When using the Full Configuration interface, you create a connection to a supported host hypervisor or cloud service. Then from Full Configuration, you use an image (created through that host) to create a catalog of machines that contain the app and desktop instances. Then you create a delivery group. Citrix provides many tools to simplify and facilitate how these session hosts are built and maintained.

  - When using Quick Deploy to deliver Azure workloads, you only need to create the catalog. Although you can use your own Azure subscription when creating the catalog, using a Citrix Managed Azure subscription eliminates your need to manage the host, too.

  The app and desktop instances that you publish can be on-premises, hosted in public clouds, or in a hybrid mixture of both.

- **Citrix StoreFront:** Citrix StoreFront is the predecessor to the cloud-hosted Citrix Workspace. It is used as the web interface for access to applications and desktops.

  You can optionally install StoreFront servers in resource locations. Having local stores can help deliver apps and desktops during network outages. The Local Host Cache feature requires a customer-managed StoreFront in each resource location.

  See User access for considerations for using StoreFront in a service environment.

Objects you configure to deliver desktops and applications

You configure the following items to deliver apps and desktops in a production environment.

- **Host connection:** A host connection (mentioned earlier) helps enable communication between components in the control plane (Citrix Cloud) and VDAs in a resource location. Connection specifications include:

  - The address and credentials to access the host
  - The storage method to use, and the machines to use for storage
  - Which network the VMs can use

  Remember: When using Quick Deploy, you don't have to create a connection. And if you use Citrix Managed Azure, Citrix manages the hosting, as well.

- **Catalog:** In the Full Configuration and Monitor interfaces, catalogs are called "machine catalogs."
  A catalog is a collection of virtual or physical machines that have the same operating system type (for example, Windows multi-session, Ubuntu single-session).

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

After the image is ready, you create the catalog.

- For VMs, MCS creates the machines and the catalog.
- For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

For more information about MCS, see Image management.

- **Delivery group:** A delivery group specifies:
  - One or more machines from a catalog.
  - Users who are allowed to access those machines.
  - The applications and desktops that users can access through Workspace.

  When using Quick Deploy, a delivery group is created automatically. (It appears only in the Full Configuration interface.)
- **Application group:** Application groups let you manage collections of applications. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups. Application groups are optional.

Citrix Managed Azure

Citrix Managed Azure is an option available in several Citrix DaaS editions. Using Citrix Managed Azure simplifies the deployment of virtual apps and desktops from Azure. Citrix manages the infrastructure for hosting Azure workloads.

With Citrix Managed Azure, you get a dedicated Citrix-managed Azure subscription and resource location. In that Azure subscription, you create a catalog of VMs. You can:

- Deploy single-session and multi-session Windows OS machines or Linux OS machines, from various supported versions.
- Choose from a curated list of compute types and storage options in select regions.
- Provision persistent or non-persistent workloads on those machines.
- Choose from several Citrix provided images that have the latest VDA installed. Then, from the Citrix interface, you build your own image from that template, and customize it. You can also import and use images from your own Azure subscriptions.

Even though Citrix manages Azure capacity, if you want to communicate with existing resources on your own Azure subscription, you can use Azure VNet peering to connect resources. You can also use Citrix SD-WAN to connect to your on-premises resources directly.

For information about security and responsibilities when using Citrix Managed Azure, see Technical security overview for Citrix Managed Azure.

Ordering Citrix Managed Azure

To get a Citrix Managed Azure subscription, you must subscribe to a supported Citrix service offering, and then order Citrix Managed Azure Consumption Funds. You can order Citrix DaaS and consumption funds through Citrix or from Azure Marketplace.
Citrix Managed Azure is supported on the following service offerings:

- Citrix Workspace Premium Plus
- Citrix DaaS, Advanced, Advanced Plus, and Premium editions
- Citrix DaaS Standard for Azure edition

For details, see Sign up for Citrix DaaS.

Citrix Managed Azure benefits summary

Using Citrix Managed Azure offers several benefits:

- Fastest path to hybrid-cloud benefits.
- Offloads IT management of infrastructure. Provides an administration experience that puts IT in control without the management and maintenance challenges.
- Enables you to rapidly scale work solutions.
- Provides a separate Azure subscription that is managed and maintained by Citrix. This Isolates activity from your other Azure subscriptions.
- You retain the flexibility to create and manage workloads using your own Azure subscriptions. Your deployment can include workloads that use the Citrix Managed Azure subscription, and workloads that use your own (customer-managed) Azure subscriptions.
- Uses a true consumption-based Infrastructure as a Service (IaaS) model.
- Several technologies are available to create connections to your own on-premises networks (such as Azure VNet peering and SD-WAN). This allows your users to access your network's resources, such as file servers.

Deploying and managing Citrix Managed Azure from this service uses the Quick Deploymanagement interface.

For more information, contact your Citrix representative.

Delivering applications and desktops to users

Citrix Workspace

Subscribers (users) access their desktops and apps through Citrix Workspace.

After installing and configuring Citrix DaaS, you're provided with a workspace URL link. The workspace URL is posted in two places:

- From the Citrix Cloud console, select **Workspace Configuration** from the menu in the upper left corner. The **Access** tab contains the Workspace URL.
- From the Citrix DaaS **Welcome** page, the workspace URL appears at the bottom of the page.

Test and then share the workspace URL link with your subscribers (users) to give them access to their apps and desktops. Your subscribers can access the workspace URL without any additional configuration.

You configure workspaces from Citrix Cloud.

- Specify which services are integrated with Citrix Workspace.
- Customize the URL that your subscribers use to access their workspace.
- Customize the appearance of subscribers' workspaces, such as logos, color, and preferences.
- Specify how subscribers authenticate to their workspace, such as using Active Directory or Azure Active Directory.
- Specify external connectivity for resource locations used by your subscribers.

For more information, see Citrix Workspace.

Citrix Workspace app

From the user side, Citrix Workspace app is installed on user devices and other endpoints, such as virtual desktops. Citrix Workspace app provides users with secure, self-service access to documents, applications, and desktops from any device, including smartphones, tablets, and PCs. Citrix Workspace app provides on-demand access to Windows, web, and Software as a Service (SaaS) applications.

For devices that cannot install Citrix Workspace app software, Citrix Workspace app for HTML5 provides a connection through a HTML5-compatible web browser.

Citrix Workspace app is available for various operating systems. For details, see Citrix Workspace app.

Service Level Agreement

Citrix DaaS is designed using industry best practices to achieve cloud scale and a high degree of service availability.

For complete details about Citrix's commitment for availability of Citrix Cloud services, see the Service Level Agreement.

Performance against this goal can be monitored on an ongoing basis at https://status.cloud.com.

Limitations

The calculation of this Service Level Goal will not include loss of availability from the following causes:

- Customer failure to follow configuration requirements for Citrix DaaS documented in the product documentation on https://docs.citrix.com.
- Caused by any component not managed by Citrix including, but not limited to, customer controlled physical and virtual machines, customer installed and maintained operating systems, customer installed and controlled networking equipment or other hardware; customer defined and controlled security settings, group policies and other configuration policies; public cloud provider failures, Internet Service Provider failures or other external to Citrix control.
- Service disruption due to reasons beyond Citrix control, including natural disaster, war or acts of terrorism, government action.

More information

- Citrix DaaS diagrams
- Citrix DaaS Reference Architecture and Deployment Methods
- Technical security overview
- Network ports
- Third-party notices
- System requirements
- Features
  - An introduction to HDX technologies, plus details about Devices, Graphics, and Multimedia.
  - Remote PC Access: Allow users to log on remotely from anywhere to a physical PC in the office. You can configure Remote PC Access from Full Configuration or Quick Deploy.
  - Publish content: Publish an application that is simply a URL or UNC path to a resource.
  - Server VDI: Deliver a desktop from a server operating system for a single user.
- For Citrix DaaS Standard for Azure, see its dedicated product documentation.

- To learn about feature availability in the Citrix DaaS products and editions, see the Citrix DaaS feature matrix.
- The Citrix Cloud Learning Series offers education course to get you up and running with Citrix Cloud and its services. You can sequentially view all of the modules, from introductions through planning and building services. You can also choose individual modules or task-specific segments within a module. See Cloud Learning Series.

Get started

To learn how to set up your deployment, start with Plan and build a deployment. That summary guides you through the major steps in the process, and provides links to more information and detailed procedures.

What's new

July 2, 2024

A goal of Citrix is to deliver new features and product updates to Citrix DaaS customers when they are available. New releases provide more value, so there's no reason to delay updates. Rolling updates to Citrix DaaS are released approximately every three weeks.

This process is transparent to you. Initial updates are applied to Citrix internal sites only and are then applied to customer environments gradually. Delivering updates incrementally in waves helps ensure product quality and maximize availability.

It is possible that the updates mentioned in this documentation are being rolled out and are not accessible to all customers at the same time.

For details about the Service Level Agreement for cloud scale and service availability, see Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

Virtual Delivery Agents (VDAs)

VDAs for Windows machines generally are released at the same time as the Citrix Virtual Apps and Desktops product.

- For information about new VDA and HDX features, see the What's new and Known issues articles for the current Citrix Virtual Apps and Desktops release.

- For information about VDA platforms and features that are no longer supported, see Deprecation. That article also includes platforms and features that will not be supported in a future release (such as which operating systems support VDA installation).

> **Important:**
>
> If the Personal vDisk (PvD) component was ever installed on a VDA, that VDA cannot be upgraded to version 1912 LTSR or later. To use the new VDA, you must uninstall the current VDA and then install the new VDA. (This instruction applies even if you installed PvD but never used it.) For details, see If the VDA has Personal vDisk installed.

July 2024

New and enhanced features

Option to update write-back cache settings post creation for Machine Creation Service (MCS) catalogs in the hypervisors. You now have the option to update the memory and disk cache size of the write-back cache, when Machine Creation Service (MCS) Storage Optimization (MCSIO) is enabled, after the catalog is created for MCS catalogs in the hypervisors.

For more information, see:

- Create a machine catalog using a machine profile
- Create a catalog with a machine profile
- Create a machine profile-based machine catalog using PowerShell

Enhancement to Session Performance tab. The **Session Topology** section of the **Session Performance** tab is enhanced to include the following endpoint metrics which exists in the Citrix Workspace app for Windows:

- WIFI signal strength
- Throughput incoming and outgoing
- Network interface type
- Link speed

This enhancement helps to troubleshoot issues with respect to sessions quickly.

Diagnose historical user sessions [Preview]. Citrix Monitor now displays the details of sessions in active, disconnected, or in terminated state. Previously, you could see the details of active sessions only. With this feature, helpdesk admins can troubleshoot issues with a session that was ended or in terminated state. The session details are available for last 24 hours and last 2 days. You can view the following details of an ended or terminated session:

- Machine Details panel - Displays the available details of the machine where the selected session was launched.

- Session Details panel - Displays the available details of the selected session.
- Session logon duration - Displays the information on the logon duration taken for the selected session. You can view the chart on time taken for brokering, machine start-up, hdx connection, authentication, GPOs, logon scripts, profile load on disk, and interactive session.

For more information, see Diagnose historical user sessions.

Machine uptime alert. The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alert, Machine uptime alert based on the uptime of a power managed machine in a delivery group. For every delivery group, for which the machines crossed the threshold, you will get an attachment or webhook alert for that delivery group alone.

The new alert condition allows you to configure alert thresholds as the number of hours per day, hours per week, or hours per month for a machine is turned on in a delivery group.

For more information, see Machine uptime alert.

Published desktop name. Citrix Monitor now displays the published desktop name in the UI. This new field allows you differentiate among user groups within the same delivery group. You can also generate custom reports for these user groups. This new field is added to **Filters**, **Custom Reports**, or to **Machine Details** section of Citrix Monitor UI.

Infrastructure rightsizing. The **Infrastructure Rightsizing** page helps you to analyze the provisioning and sizing aspects of your delivery group based on the resources utilization. Based on this analysis, you can optimize the machine provisioning and sizing to match the utilization pattern. You can optimize your infrastructure cost by reducing spending on the unused resources. You can also choose to opt for lower CPU and memory specifications machines if the resource utilization is consistently lower than provisioned. You can optimize for performance by opting for a higher CPU and memory specifications machines if the resource utilization is consistency higher and see evidence of it impacting the session experience such as *Logon and ICARTT* metrics.

You can filter the Infrastructure rightsizing using the following:

- Delivery Group - You can filter for single session OS or multi session OS delivery groups
- Tags - Tags are the tag names applied to the machine. So, you can filter machines with the same tags. You can select multiple tags up to five tags. When you select multiple tags, you can filter for all the machines which have at least one of those selected machine tags applied.
- Time period - You can filter the data for last 24 hours, 7 days, and 30 days.

The Infrastructure rightsizing page offers:

- Insight in to the utilization details
- Summary of the resource utilization
- Trends on the resource utilization

Click the **Cost Optimization** tab from the left menu on the Home page. And then, click the **Infrastructure rightsizing** tab to access the **Infrastructure rightsizing** page.

You can also click the **Rightsize this delivery group link** from the **Infrastructure details** section in the **Cost Optimization** tab > **Cost savings** to access the **Infrastructure rightsizing** page.

For more information, see Infrastructure rightsizing.

Local Host Cache activity dashboard. The new Local Host Cache dashboard under the **Trends tab** provides detailed information on user sessions and machines available during an outage on any Resource location or Zone. Administrators can use the details around number of machine registrations, reconnected sessions, and new sessions brokered to evaluate and audit activities while in Local Host Cache mode. The default selected data is for last 24 hours and for all zone and cloud connectors, with the ability to filter on time period, zone, and cloud connector. The Local Host Cache data is available for last 2 hours, 24 hours, 7 days, 1 month, and up to 90 days. For more information, see Available trends.

Specify CMEK global and regional keys from all projects. In Google Cloud environments, previously, you could only use customer-managed encryption key (CMEK) from within the same GCP project and the same region in which the hosting connection is created.

With this feature, you can now browse and use global or regional CMEK from all projects that are accessible to the service account. This feature enhances the flexibility to manage encryption keys. This feature requires extra permission for the following two service accounts:

- The service account of the current project with which the hosting connection is created.
- The Compute Engine Service Agent of the current project.

For more information, see Specify CMEK global and regional keys.

June 2024

New and enhanced features

Full Configuration: Support for provisioning VMWare VMs using machine profile. When provisioning VMWare VMs using Machine Creation Services (MCS), you can now select an existing template as the machine profile, letting the VMs within the catalog inherit settings from the selected template.

The inherited settings include:

- Tags placed on the template
- Custom attributes
- vSAN Storage policies
- Virtual hardware version

- vSphere Virtual TPM (vTPM)
- CPU count and core per socket
- NIC count

Create delivery groups exclusively for suspend-capable VMs using Full Configuration. We've introduced a new option in **Full Configuration > Create Delivery Group**, **Make suspend capability required for this delivery group**. This option enables you to create delivery groups that contain only suspend-capable VMs, facilitating your machine power management at the delivery group level. Note that this feature applies only to single-session OS VMs.

For more information, see Create delivery groups.

Enhanced Performance Metrics panel. The **Performance Metrics** panel has an enhanced visualization of the historical data metrics. When you click the **Session Performance** tab, along with the real time data, you can view the last 15 minutes data without waiting for the page load time. This enhancement helps to reduce mean time for resolution by enabling admins to be able to correlate multiple component performance metrics in a single view. For more information, see Performance Metrics.

Improved Session Logon view. - The new **Machine Start-up** option with the following sub-sections on the **Session Logon** tab on the **Filters** -> **User Details** page provides breakdown of the time taken to start a virtual machine during different phases:

- **Power on** - Displays the time taken to power on a virtual machine
- **Boot-up and registration** - Displays the time taken to boot up and register a virtual machine

The newly introduced collapsible button on the **Session Logon** page helps to collapse or expand the options on the **Machine Start-up** and the **Interactive Session**.

Along with the default **Logon Duration Phases** table options, which are **Session Logon Phase** and **Duration**, you can also choose the following columns on the **Session Logon** page:

- Start time
- End time
- Delivery Group's 7 Day Avg (sec)
- User's 7 Day Avg (sec)

You can also export the preceding data to a .CSV file.

The newly added columns **Power on** and **Boot up and registration** can be added to the **Logon Duration by User Session** table in the **Trends** -> **Logon Performance** > **Choose Columns**. You can also export the reports on the **Logon Performance** screen.

This enhancement helps to understand and easily troubleshoot issues related to logon duration. For more information, see Diagnose user logon issues.

Unregistered machines alert. The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alert, **Unregistered Machines (in %)** based on the percentage of unregistered machines in a delivery group. The new alert condition allows you to configure warning and critical threshold values as a percentage of unregistered machines in a delivery group. For more information, see Unregistered Machines (in %) section in the Alerts article.

Shared or Dedicated directory connections. You can now create directory connections using dedicated or shared tenancies. If dedicated tenancy is selected while adding a directory connection then the workspaces created are for single session desktops. If shared tenancy is selected while adding a directory connection then the workspaces created are shared. For more information, see:
Shared or Dedicated directory connections. You can now create directory connections using dedicated or shared tenancies:

- If you select dedicated tenancy while adding a directory connection then the workspaces created are for single session desktops.
- If you select shared tenancy while adding a directory connection then the workspaces created are shared. For more information, see:
  - Create a directory connection
  - Import an image
  - Create a deployment

Contextual App Protection. With this feature, the administrators can apply **App Protection Anti-Screen Capture** and **Anti-keylogging** control on devices and users contextually instead of having the controls always enabled or always disabled. This implementation helps you to enforce **App Protection Anti-Screen Capture** and **Anti-keylogging** only when required. For more information, see Step 7. App Protection and Manage app protection.

Enhanced default view settings for machine catalogs, delivery groups, and applications. We've introduced new default view options for Machine Catalogs, Delivery Groups, and Applications, offering greater flexibility and customization:

- **Default view selection.** Previously, those nodes defaulted to a folder view, which was suitable for organizations using folder-based management structures. With the introduction of a **Folder** icon on the action bar, you can now switch between folder view and list view as your preferred default view.
- **Improved folder view.** The **View all** toggle now retains your last selection when you sign back in. If previously turned off, it will remain off, with the root folder selected and the first-level sub-folders expanded.

Data caching for the StoreFront node. We've introduced data caching for the **StoreFront** node. This enhancement significantly reduces the page load time when you navigate to the **StoreFront** node, improving the overall user experience.

Improved user name search in machine catalog creation. We've enhanced the functionality for searching for administrators by user names during machine catalog creation. Key enhancements to the **Machine Catalog Setup > Enter Credentials** page include:

- **Domain specification:** A new option, **Domain**, is now available on that page, enabling you to narrow the search by entering the domain name or SID.
- **SamName search optimization:** Searches using SamName are now confined to the specified domain.

These enhancements make user searches faster and more efficient.

Simplified subnet updates for machine catalogs. Previously, to change the subnet settings of a machine catalog, you had to delete and recreate it. With this feature, you can now achieve the same functionality by editing the catalog. Note that only new virtual machines created under the catalog will be on the newly associated subnets. This enhancement reduces the need for catalog deletion and associated tasks. For more information, see Edit a catalog.

Support for creating resource groups during Azure catalog creation (for PVS). Previously, when creating Azure catalogs using Full Configuration, you had to create the resource groups using PowerShell commands. With this feature, you can now seamlessly create a resource group as part of catalog creation in Web Studio. This enhancement simplifies the overall creation workflow. For more information, see Create a Citrix Provisioning catalog using the Full Configuration Interface.

May 2024

New and enhanced features

Secure HDX (Preview). You can now use this feature to prevent any network elements in the traffic path from being able to inspect the HDX traffic. For more information, see Secure HDX.

Azure GPU hibernation support (Preview). You now have the option to support hibernation for Azure machine SKUs that support GPU.
For more information on supported VM sizes, see the Microsoft documentation.

Citrix Provisioning catalogs support for hybrid Azure AD join extended to Full Configuration. When you create a Citrix Provisioning catalog, the **Hybrid Azure Active Directory joined** identity type is now available on the **Machine Catalog Setup > Machine Identities** page. With this new option, you can create hybrid Azure AD joined machines through Citrix Provisioning. For more information, see this Citrix Provisioning article.

Enhancements to Full Configuration contextual help. We've redesigned the help panel to provide a more informative experience, offering targeted information for each node within Full Configuration. By clicking the Help icon on any node, you can now access a comprehensive set of resources aimed at providing a one-stop learning experience, helping you better understand related features:

- Access key documents specifically related to the selected node.
- Stay informed about service updates including Citrix Roadmap, Known issues, Limits, System requirements, and What's new features.
- Access expanded resources such as Citrix Blogs, Citrix Community, Citrix Feature Explained, Citrix Product Documentation, Citrix Support, and Developer Documentation.

Enhanced configuration logging: tracking membership changes for delivery groups. With this enhancement, configuration logging now captures and displays user and group IDs added to or removed from delivery groups. To view configuration logs, go to **Full Configuration > Logging > Events**.

Customize the tab order on the Search node. You can now customize the order of tabs on the **Search** node according to your usage patterns, enhancing the browsing experience. To do so, click the three-dot icon next to the tabs, drag the tabs to your preferred order, and then click **Apply**.

Data caching for the Machine Catalogs node. We've introduced data caching for the Citrix DaaS **Machine Catalogs** node. This enhancement significantly reduces the page load times when you navigate to the **Machine Catalogs** node, improving the overall user experience.

Support for creating Citrix Provisioning catalogs using MCS PowerShell commands in VMware. You can now create Citrix Provisioning catalogs using MCS PowerShell commands in VMware.

This implementation provides you the following advantages:

- A single unified API to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning, and so on.

For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

Failure Detection and Mitigation in VDA Upgrade Service During the VDA upgrade process (Preview). Our service now incorporates advanced detection mechanisms. If any issues are detected that could potentially lead to the failure of the VDA IPU, rendering the VDA unusable, the service will take proactive measures. It will cease to update additional machines and gracefully exit the current workflow. This proactive approach aims to minimize the impact and ensure a smooth experience, even in the event of unexpected challenges, reducing the potential blast radius of any issues encountered. For more information, see Failure Detection and Mitigation in VDA Upgrade Service

Support VDA Updates from a local file share that VDAs have access (Preview). With Enhanced VDA Installer Access Control, you can now have greater flexibility and control over which VDAs can connect and retrieve necessary download MSIs without worrying about granting network access for VDAs to fetch updates from the Citrix Managed Azure CDN. This allows you to enforce stricter network rules while ensuring seamless access to essential updates. For more information, see Support VDA Updates from a local file share that VDAs have access

Full Configuration support for delivering packaged applications to single-session static desktops and office PCs. With this enhancement, you can now deliver packaged applications to all types of desktops using Full Configuration. Benefits of delivering packaged applications to *single-session static* desktops include:

- Applications are available on the VDA at sign-in and not staged on demand through Workspace or StoreFront.
- Improved launch time when accessing the packaged applications.
- Facilitates maintenance of the packaged applications independently, separate from the VDA's base image.

To deliver packaged applications to desktops, add those applications to the delivery groups using these ways:

- Add applications during delivery group creation.
- Add applications to an existing delivery group using one of these entries: **Delivery Groups > Add Applications > Applications**, **Applications > Properties > Groups**, or **App Packages > Packages > Add Delivery Groups**.

For more information, see Create delivery groups, Manage delivery groups, and Add applications to delivery groups.

Full Configuration support for delivering packaged applications in FlexApp format. In **Full Configuration > App Packages**, you can now upload FlexApp packaged applications to Citrix Cloud, and deliver them to your users. For more information, see App packages.

OData pagination. Monitor enhances the limit of OData pagination. All OData v4 endpoints return a maximum of 1000 records per page with a link to the next 1000 records in the response. Because every page returns large data sets, you can get the same amount of total data with lesser OData queries. Thus this feature reduces time to get total data and thus improves the user experience. For more information, see Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud documentation.

Support for creating and managing Azure confidential VMs using Full Configuration. Azure confidential VMs provide a strong, hardware-enforced boundary to help meet your security needs. With the Full Configuration user interface, you can now create and manage confidential VMs on Azure. For more information, see Azure confidential VMs (Preview).

Support for displaying client IPs in configuration logs. In **Full Configuration > Logging > Events**, you can now view IP address details in logs, facilitating tracking of action origins. To show the IP address column in the main view, click the **Columns to Display** icon in the top right of the logs, and then select **Client IP**. For more information, see View configuration log content.

Support for capturing additional properties using machine profile source in AWS. In AWS environments, with this enhancement, you can now create or update a machine profile-based catalog to

include the following:

- Capture CPU options, tenancy type, and hibernation capability from the machine profile source while creating an MCS machine catalog.
- Change the tenancy type of the machine profile source while editing an MCS machine catalog. This functionality is applicable only to the new VMs added to the catalog.
- Change the hibernation capability of the machine profile source while editing an MCS machine catalog. This functionality is applicable only to the new VMs added to the catalog.

The machine profile source can be a VM or launch template version. This feature is applicable to both persistent and non-persistent catalogs.

For more information, see Create a machine profile-based machine catalog using PowerShell.

Repair the identity information of active computer accounts in AWS. In AWS environments, you can now reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent MCS machine catalogs. Currently, the feature is supported only for AWS, Azure and VMware virtualization environments. For more information, see Repair the identity information of active computer accounts.

Support for encrypting ID disk of an MCS machine catalog VMs in AWS. Previously, in AWS environments, MCS allowed the encryption of only the OS disk of the provisioned VMs. With this feature, you can now encrypt the ID disk in addition to the OS disk. This functionality allows you to use AWS KMS keys (Customer managed key and AWS managed key) to perform cryptographic operations on the disks attached to a VM.

For encryption of OS and ID disks, configure one of the following:

- Use a master image that is encrypted (for example, an AMI created from an instance or snapshot that contains a root volume encrypted with KMS key)
- Use a machine profile source (VM or launch template) that contains an encrypted root volume.

For more information, see Encrypt OS and ID disks.

Configure security groups per network interface in AWS. When editing a host connection for AWS environments, you can now configure the maximum number of security groups allowed per elastic network interface (ENI) using a PowerShell command. Therefore, if you increase your security groups per network interface quota, you can configure the same value for the hosting connection. For information on configuration, see Configure security groups per network interface.

Cost optimization [Preview]. The **Cost Optimization** page provides a visual representation of infrastructure savings accrued over a selected period and forecasts expected savings for the remaining days. By analyzing machine usage and sessions, this page helps you to identify achieved savings and opportunities for cost reduction. This page offers:

- Insight into the optimization of infrastructure costs
- The amount saved
- Information on a range of scenarios that might result in exceeding projected costs
- Potential opportunities for identification and strategic planning to realize infrastructure cost savings

The **Cost Optimization page** includes **Estimated savings** and **Autoscale savings report**.

The **Estimated savings** helps to evaluate the efficient utilization of infrastructure resources. The cost savings are displayed in either US dollars or as a percentage of the cost incurred. You can view the results for the last 3, 6, and 12 months. The **Estimated savings** graph displays the following:

- Estimated savings - Displays the amount of savings achieved in infrastructure for the selected duration
- Power managed machines - Displays the total number of power-managed machines.
- Projected savings - Displays how much infrastructure savings can be done for the remaining duration

The **Autoscale savings report** displays information about the delivery group for which the Autoscale is configured and enabled. This report is applicable only for power-managed machines. For more information, see the Cost Optimization page.

Inspect machines with recent power actions. You can now inspect machines with the status of the success and failed power actions. This feature helps you to analyze the following:

- Power on failure which causes user issues
- Power off failure which increases cost

> **Note:**
>
> Data is available only for the power-managed machine. Data is not available for the power actions taken before the feature was supported.

You can view the power action status of the machines using the following ways:

- From **Filters** -> **Machines** tab. In this case, by default the **Power Action Time** and the **Power Action Result** columns are visible. You can also select the columns that you want to visible.
- From **Cost Optimization** tab. In this case, the default filter is **Power Action Triggered By** is set to *Autoscale* and the **Power Action Result** is set to *Failed*.

With this feature, you can view the details of the power action controls. For example, you can view who triggered the action, which action changed the power state, the reason for failure, and the time when the action is completed. You can also export these details.

For more information, see Inspect machines with recent power actions.

April 2024

New and enhanced features

Support for newer version of Microsoft Teams. Citrix Monitor now supports Microsoft Teams version 2.1 or earlier.

Change disk encryption in Azure. With this feature, you can now change the disk encryption in Azure virtualization environments. You can do the following:

- Create an MCS machine catalog with a disk encryption set (DES) that is different from the master image DES.
- Change the disk encryption type from one DES key to another DES key of an existing MCS machine catalog and existing VMs.
- Update an MCS machine catalog and VM that was not previously CMEK enabled to have customer-managed encryption key (CMEK) encryption (DES), disk encryption at host, or double encryption.
- Update an existing MCS machine catalog and VM to be non-encrypted that was previously encrypted.
- Enable disk encryption with private endpoint (an MCS machine catalog that used a host connection enabled with `ProxyHypervisorTrafficThroughConnector`).

For more information, see Change disk encryption.

Support for modifying the page file settings. With this feature, you can modify the page file settings of the newly added VMs to an existing catalog without updating the master image. Currently, this feature is applicable to only Azure environments.

To modify the page file settings, you need VDA version 2311 or later. You can modify the page file settings using the PowerShell commands. For more information on modifying the page file settings, see Modify page file settings.

Check for multiple NICs in VMware. In VMware environments, we have introduced various pre-flight checks when the hosting unit and machine profile template have multiple networks, and the `-NetworkMapping` parameter is used in the `New-ProvScheme` and `Set-ProvScheme` commands. For more information on the pre-flight checklist for multiple NICs, see Check for multiple NICs.

Support for creating Windows 11 VMs in GCP. You can now create Windows 11 VMs in GCP. If you install Windows 11 on the master image, then you must enable vTPM during the master image creation process. Also, you must enable vTPM on the machine profile source (VM or instance template).

This feature is applicable to:

- Persistent and Non-persistent MCS machine catalogs.

- Only sole-tenant node group.

For information on creating Windows 11 VMs on the sole-tenant node, see Create Windows 11 VMs on the sole-tenant node.

Virtual channel allow list support for environment variables.
You can now use system environment variables in the trusted processes' path. For more information, see Using system environment variables.

Deprecated features in Full Configuration. The following features and settings have been deprecated in Full Configuration:

Support for HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops. Monitor now supports HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops (AVD). For more information, see Troubleshoot Machines.

Cloud Build Service Account Change. GCP is introducing changes to Cloud Build Services's default behavior and use of service accounts in new projects created after April 29, 2024. For more information, see Cloud Build Service Account Change. However, your existing Google projects and Citrix catalogs are not affected by this change. For more information, see:

- Configure and update service accounts
- Required GCP permissions

Support for HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops. Monitor now supports HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops (AVD). For more information, see Troubleshoot Machines.

VDA environments with proxies for internet and URL filtering (Preview). You can now use the VDA Upgrade Service to update VDAs when you have proxies for internet connectivity and web filtering. The proxy configured in policy takes precedence over the proxy configured in registry. For more information, see Install VDAs. Also, refer to the list of urls that need to be white listed in the proxy.

Cloud Build Service Account Change. GCP is introducing changes to Cloud Build Services's default behavior and use of service accounts in new projects created after April 29, 2024. For more information, see Cloud Build Service Account Change. However, your existing Google projects and Citrix catalogs are not affected by this change. For more information, see:

- Configure and update service accounts
- Required GCP permissions

March 2024

New and enhanced features

Dynamic Session Recording. You can now record the current active session using the Session Recording controls from the **User Details** screen without the need to re-establish the session. This feature enables quicker and effective troubleshooting of session experience-related issues faced by users. This is useful to debug issues that are difficult to reproduce.

For more information about Dynamic Session Recording, see the Session Recording service article.

Enrollment tool to register VDAs using WebSockets to machine catalogs. You can now use this enrollment tool to securely register your non-domain joined VDAs to machine catalogs. This feature provides the benefits of using only the TLS port 443 for communication from VDA to the Delivery Controller and removing port 80 traffic. For more information, see Enroll machines to catalogs using the WebSocket VDA enrollment tool.

Full Configuration: Support for updating more Azure VM settings using machine profiles. With Full Configuration, you can now update a wider range of settings for MCS-provisioned Azure VMs through machine profiles, which include:

- Machine size
- License type
- Availability Zone
- Dedicated Host Group ID

After you update the machine profile, Full Configuration compares the current settings with the new ones. If differences exist, you'll be prompted to confirm which to apply. This design ensures transparent and efficient VM setting updates.

Full Configuration: Support for Changing write-back cache properties for MCS-provisioned Azure VMs. For Azure VMs provisioned using Machine Creation Services (MCS), you can now change their write-back cache (WBC) properties using Full Configuration, such as **Disk cache size**, **Memory cache size**, and **Enable storage cost saving**. In addition, when you select a new machine size or machine profile for those VMs, Full Configuration validates WBC settings to prevent conflicts, such as exceeding the memory limit of the new selection. If conflicts occur, you'll be prompted to re-configure WBC settings.

February 2024

New and enhanced features

Suspend VMs from the Workspace interface. You can now suspend persistent VMs with active sessions from the Workspace user interface. This enhancement offers the following benefits:

- Resume the system from where you left off.
- Faster launch time compared to a stopped deallocated machine.
- Cost-effective and energy efficient.
- Efficient resource allocation using the Autoscale feature.

New Machine Creation Services (MCS) Storage Optimization (MCSIO) support: You now have the option for the Image Portability Service to add or remove MCSIO when you prepare an image for the MCS provisioning.
For more information, see Automate VDA configuration.

Probes Overview enhancements: A summary of the Probe Metrics and the Probe Failure Stages in now available in the **Probe** > **Overview** page. The Probe Metrics shows the count of Scheduled, Failed, Skipped, and Successful runs. The graphical representation of the failure stages helps analyze the stages in which most failures have occurred. This information helps to quickly troubleshoot the probe results. For more information, see the Application and Desktop Probing article.

Image information on the Machine Catalogs page. You can now view the following image information through the **Template Properties** of the machine catalog:

- Operating system
- Machine identity service
- Machine Creation Service storage
- Filepath for `pagefile.sys` for Azure deployments

This enhancement provides better clarity on the image information and ensures that the administrators have all the information about the machine catalog in one place.

Full Configuration support for VDA enrollment token management. Token-based VDA enrollment reduces the load on Cloud Connectors and decreases potential failure points, ideal for the use cases where you prepare the machines using non-Citrix Provisioning technology. With Full Configuration, you can now generate and manage enrollment tokens for non-Citrix-provisioned VDAs, streamlining enrollment token-based deployments. For more information, see Generate and manage enrollment tokens.

PowerShell logging. In Full Configuration, you can now view the PowerShell commands corresponding to your daily UI actions. This feature helps you gain insights into the underlying PowerShell commands for learning purposes. To view the PowerShell logs, go to **Logging > PowerShell**. For more information, see Configuration logging.

Enable Local Host Cache (LHC) for single-session pooled VDAs using Full Configuration. By default, single-session pooled VDAs provisioned using MCS or Citrix Provisioning are unavailable when in LHC mode. With Full Configuration, you can now override this default behavior on a per delivery group basis, making those VDAs available for new connections during LHC. For more information, see Create delivery groups and Manage delivery groups.

Citrix Hypervisor rebranded to XenServer in Full Configuration. In line with our rebranding strategy, we've updated all instances of Citrix Hypervisor within Full Configuration to XenServer.

End-to-end Network Hop view. End-to-end network hop view is the next step towards enhancing troubleshooting workflows in Citrix Monitor. The **User Details** > **Session Performance** > **Session Topology** section provides a visual representation of the end-to-end network hop view for connected HDX sessions. The in-session path helps understand the components involved in the session path with their metadata, the link between the components, and the applications published on the VDA. The Session Topology helps the data flows and to identify the specific hop that might be bringing in performance issues.

In addition, ICA Latency and ICA RTT measurements are displayed for the session when it is in a connected state. For more information, see End-to-end Network Hop view.

Use Disk Encryption Set ID (DES ID) of the master image to encrypt all the disks of catalog VMs. In Azure environments, previously, the Disk Encryption Set ID (DES ID) of an MCS machine catalog was derived from a machine profile or custom properties. With this feature, a machine catalog can also derive the DES ID from the master image to encrypt all the disks of the VMS in a catalog.

Update MCS tags to detect orphaned resources after migration. When you migrate from on-premises configuration to a cloud site, or from your cloud configuration to another cloud site, the orphaned resources aren't detected correctly because of the old site id tag. With this feature, using a PowerShell command, you can update the MCS site id tags of a persistent catalog, after migration so that orphaned resources can be detected correctly. Currently, this feature is applicable to Azure. For more information, see Update MCS tags to detect orphaned resources after migration.

Validate configuration before creating an MCS machine catalog. With this feature, you can now validate configuration settings before creating an MCS machine catalog using the parameter `-validate` in `New-ProvScheme` command. After you run this PowerShell command with the parameter, you get an appropriate error message if there's an incorrect parameter used or a parameter has conflict with another parameter. You can then use the error message to resolve the issue and successfully create an MCS machine catalog using PowerShell.

Currently, this feature is applicable to Azure, GCP, and VMware virtualization environments. For more information, see Validate configuration before creating an MCS machine catalog.

Support for copying tags from a machine profile source to a VM in AWS. With this feature, in AWS virtualization environments, you can copy tags on NICs, and disks (Identity disk, write back cache disk, and OS disk) that are specified in the machine profile to newly created VMs in an MCS machine catalog. You can specify these tags in any of the machine profile sources (AWS EC2 instance or AWS launch template version). This feature is applicable to persistent and non-persistent machine catalogs and VMs. For more information, see Copy tags on VMs.

SCVMM support for machine profile. With this feature, you can now use a machine profile to create and update an MCS machine catalog in System Center Virtual Machine Manager (SCVMM) envi-

ronments. You can also enable nested virtualization and vTPM. For more information, see Create a catalog with a machine profile.

Azure support for using spot VMs with MCS. Azure Spot VMs allow you to take advantage of Azure's unused computing capacity at a significant cost savings. However, due to its eviction policy, Azure Spot VMs are good for only some non-critical applications and desktops.

With this feature, you can create an MCS machine catalog of Azure Spot VMs using a machine profile (VM or template spec). You can update an existing catalog to have Azure Spot VMs as the newly created VMs or switch to have standard Azure VMs. You can also update existing VMs to be Azure Spot VMs. For more information, see Create a catalog using Azure Spot VMs.

Support for capturing diagnostic settings from a machine profile. In Azure environments, MCS now supports capturing of diagnostic settings on VMs and NICs from a machine profile while creating or updating an MCS machine catalog, or updating existing VMs. Therefore, with this implementation, the diagnostic data can be seamlessly transmitted to designated Azure destination endpoints, such as Log Analytics workspaces or Event Hubs, for in-depth analysis and visualization. For more information, see Capture diagnostic settings on VMs and NICs from a machine profile.

MCS support for managing different versions of a machine catalog. With this feature, you can manage the configuration versions of a machine catalog using PowerShell commands. Each configuration change using the `Set-ProvScheme` results in a new configuration version. You can:

- See the list of versions.
- Use any previous version to update a machine catalog.
- Manually delete a version if it isn't used by a VM.
- Change the number of maximum versions to be retained by a machine catalog.

For more information, see Manage versions of a machine catalog.

Publish App-V, MSIX and MSIX app attach packaged applications on single-session and shared desktop VDAs. You can now access packaged applications, for example, App-V, MSIX, and MSIX app attach on the single-session and shared desktop VDAs. This enhancement ensures that the packaged applications are readily available to use when you sign in. This feature facilitates faster launch of packaged applications and improves your experience significantly by bringing it closer to accessing a locally installed application. For more information, see Publish packaged applications on single-session or shared desktop VDAs.

Play back live and recorded sessions: Citrix Monitor now supports playing back recorded and live user sessions that are recorded using the Session Recording service. You can quickly understand the session-related issues encountered by the user from the replay. With this feature, you get ready access to recordings along with session-related metrics within the Monitor console. It helps corelate the issues discovered in the recordings with the performance metrics. It eliminates the requirement of searching for recordings across multiple session recording servers or looking for third-party apps to view the recordings.

This feature requires VDA and the Session Recording server version 2308 or later.

Monitor stores the recordings in a centralized repository and displays them on the **Session Selector** modal. The **Sessions with recordings** link displays the recordings of sessions that were active during the last 24 hours or the last 2 days. The recording is played back on a new tab using the Citrix Session Recording playback server.

For more information, see Record sessions.

Microsoft Teams Optimization: Monitor displays the status of HDX optimization available for Microsoft Teams. The new **Microsoft Teams Optimization** can be viewed in the **User Details** page > **Session Details** panel. Monitor displays the status of the Microsoft Teams optimization only if Microsoft Teams is run as a published app or inside a published desktop. This enhancement provides administrators with visibility to enable troubleshooting of session performance issues on Microsoft Teams reported by users. For more information, see Troubleshoot user issues.

User interface improvements: The Citrix Monitor user interface is now refreshed with a modern look and feel. The new and improved user interface provides easier navigation and better data representation. The improved experience is intuitive and designed to easily comprehend the data required to monitor and troubleshoot a Citrix session.

Optimal screen resolution: The recommended optimal screen resolution for viewing the Citrix Monitor is updated to 1440 x 1024.

January 2024

New and enhanced features

Enhanced bidirectional content redirection configuration Previously, configuring bidirectional content redirection involved managing three distinct policies: Allow bidirectional content redirection, Allow redirection of URLs to VDA, and Allow redirection of URLs to the Client. These policies require configurations on both the server side (configured in **DaaS > Full Configuration**) and the client side (configured through Group Policies). Starting with this release, we have consolidated all three policies into a single, unified policy. It not only simplifies and enhances the configuration process but also eliminates the requirement for client-side configurations. For more information, see Bidirectional content redirection configuration.

Support for restarting and shutting down single-session machines from the Search node's Sessions tab. On the **Sessions** tab of the **Search** node, you can now search for user sessions in an unhealthy state and seamlessly restart or shut down the associated single-session machines within the same tab. This feature enhances efficiency, enabling prompt action on identified session issues within a single interface.

Support for accessing Global App Configuration Service from Full Configuration. We've provided action items in the Full Configuration interface to link you to the Global App Configuration Service. With this integration, you can easily access Global App Configuration for managing end-user settings through Full Configuration.

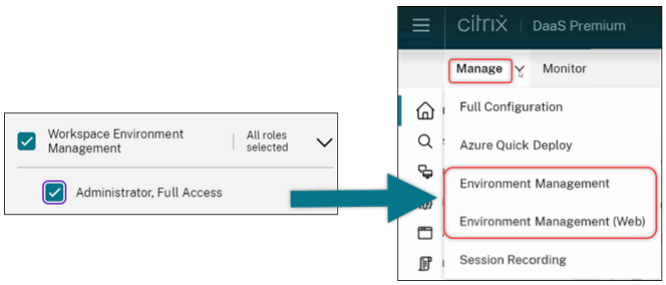
To access this service from Full Configuration, you have two options:

- Select the **StoreFront** node, click a server record, and then select **Configure Client Settings** in the action bar.
- Select the **Policies** node and then select **Configure Client Settings** in the action bar.

Support for managing user assignments for Citrix Cloud-managed delivery groups using Full Configuration. As part of our plan to migrate user assignment management from Cloud Library to Full Configuration, you can now manage user assignments for Citrix Cloud-managed delivery groups through Full Configuration. To accomplish this task, edit a target delivery group in **Full Configuration > Delivery Groups** and designate users permitted to use desktops or applications through one of these menus: **Desktops** (or **Desktop Assignment Rules**) or **Application Assignment Rule**. For more information, see Manage delivery groups.

Updates made in one portal seamlessly synchronize with the other, ensuring consistent updates across both portals.

Limit WEM console access to the WEM Full Access Administrator role. We've enabled access control for the Workspace Environment Management (WEM) consoles to prevent unauthorized entry. Only users with the **Workspace Environment Management Full Access Administrator** role can now use **DaaS > Manage** to access the WEM consoles.



Full Configuration: Azure catalogs support for inheriting DES settings from master images. Previously, Full Configuration set the Azure catalogs' default DES settings only based on machine profiles. We've now expanded this capability. With this enhancement, in the following cases, Full Configuration sets an Azure catalog's default DES settings directly based on the master image:

- If a machine profile isn't selected
- If the profile specifies a Platform Managed Key (PMK)

For more information, see Create a machine catalog using an Azure Resource Manager image in the Full Configuration interface.

Enhanced search: More filters for enhanced precision. We've enhanced the search on the Search node to include two new filters, Zone and Provisioning Type, for enhanced precision and improved usability.

Full Configuration: Support for selecting Google Cloud machine type for GCP machine catalogs. With this feature, administrators have the flexibility to select the required memory and processor configurations for provisioned GCP VMs, tailoring them to meet specific operational requirements. For more information, see Create a machine catalog using the Full Configuration interface.

Support for global and regional customer-managed encryption keys (CMEK) for provisioning GCP VMs. You can now use global and regional CMEK keys for provisioning VMs from any provisioning project. This enhancement provides greater flexibility in key selection for provisioning VMs and improving VM security.

December 2023

New and enhanced features

Send Message progress. You can now view the progress of the **Send Message** operation available in **Monitor** > **Filters**. This operation helps send bulk messages to all connected sessions on your Site. The progress of the operation is displayed in percentage. Once the operation is completed, the system displays the number of messages that were sent and the number that have failed. Send message status is helpful when you are administering large sites. It helps understand if the message needs to be resent to certain users. Sending messages can fail if the machines are unregistered or if the sessions are faulty. For more information about Send Message, see Send messages to users.

Citrix Probe Agent authentication support via Citrix Gateway with domain credentials and Multi-factor authentication.

Citrix Probe Agent for application and desktop probing now supports authentication via Citrix Gateway with domain credentials and Multi-factor authentication. This feature helps to run the Probe Agent on machines that are connected to StoreFront via Citrix Gateway. The comprehensive probe results available on Monitor help troubleshoot issues related to the applications, hosting machine, or connection before the users experience them. Support for Citrix Gateway with Multi-factor authentication is available only for Citrix Gateway that is configured with LDAP and Native OTP using Single Login Schema. For more information, see Application and Desktop Probing

Redesigned Access Policy UI for more flexible resource access control. We've redesigned the **Edit Delivery group > Access Policy** UI to give you more flexibility in managing resource access for delivery groups. The following are the key features available with the new design:

- **Support for adding policies.** You can now add access policies to restrict resource access based on attributes of user connections. A policy can consist of two types of criteria:

  - **Inclusion criteria.** Let you specify user connections that are allowed to access the delivery group.
  - **Exclusion criteria.** Let you specify user connections that are prohibited from accessing the delivery group.

- **Expanded filter support.** You can now define inclusion and exclusion criteria using a range of SmartAccess filters. Those filters include Workspace filters such as `Citrix.Workspace.UsingDomain` and `Citrix-Via-Workspace`, as well as filters for network location-based adaptive access.
- **Match All logic support for included criteria.** The new logic enables you to achieve a high level of precision and control when specifying allowed user connections for delivery groups.

For more information, see Restrict access to resources in a delivery group.

November 2023

New and enhanced features

Support for creating Citrix Provisioning catalogs using Full Configuration interface. To create a Citrix Provisioning catalog, you had to use the Citrix Virtual Apps and Desktops Setup Wizard. With this feature, you can now create a Citrix Provisioning catalog using the Full Configuration interface and PowerShell.

This implementation provides you the following advantages:

- A single unified console to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning and so on.

Currently, this feature is available only for Azure workloads. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

Introducing search for Application Groups. We have introduced the search functionality for application groups in the **Applications** node. With this enhancement, you can now directly search for an application group inside any application folder. For more information, see Search for Application Groups.

Modified configuration limits. The following table describes the modifications made to the DaaS configuration limits to improve the performance and provide cost-effectiveness.

Resource	Old limit	New limit
Active Directory domains	85	100

Resource	Old limit	New limit
Catalogs	1000	2000
Delivery Groups	1000	2000
Resource location	85	100
Resource location -> Total sessions	20,000	25,000

For more information, see Limits.

A single option to retain VM and system disk during power cycles. Starting an existing VM on Azure is now faster than launching a new one, making it a more efficient choice to retain VMs across power cycles. In response to this change, we've combined the options **Retain VMs across power cycles** and **Retain system disk during power cycles** into a single option **Retain VM and system disk during power cycles**. This means that when you select this option to reduce VM restart times by retaining system disks, your VMs are retained as well.

New capability in Full Configuration to filter machine sizes based on *Encryption at Host property* in machine profiles (Azure VMs specific). Once you choose a machine profile with *Encryption at Host* enabled during Azure machine catalog creation or management, only machine sizes that support this feature are displayed.

Restrict backup and restore actions to Full Administrator role. We've enhanced access control for the backup and restore actions. Only users with the Full Administrator role can now access the **Backup + Restore** node, preventing unauthorized actions.

Data caching for the Search node. We have introduced data caching for the Citrix DaaS **Search** node. This enhancement improves the performance of the search and the following lists the use cases that ease your regular tasks:

- Quick display of search results after they are retrieved for the first time.
- Retains pagination results after navigating out and back to the **Search** node.

Image information on the Machine Catalogs page. You can now view the following image information through the **Template Properties** of the machine catalog:

- Operating system
- Machine identity service
- Machine Creation Service storage
- Filepath for `pagefile.sys` for Azure deployments.

This enhancement provides better clarity on the image information and ensures that the administrators have all the information about the machine catalog in one place.

Support for pinning search filters. To provide a quick search experience, Full Configuration enables a facility to pin your search filters. Filter pins allow you to keep the frequently used search filters accessible on the page. This enhancement is available in the search panels of the following nodes:

- **Search**
- **Machine Catalogs**
- **Delivery Groups**
- **Applications**

For more information, Use Search in the Full Configuration management interface.

Support for associating metadata with configuration logs. Using this enhancement, you can now attach metadata with the configuration logs by associating a `name-value` pair on the high-level operations. For more information, see Associate metadata with configuration logs.

Ignore orphaned resources with specific tag. In Azure environments, a customer-managed resource tagged with all Citrix tags is detected as an orphaned resource. With this feature, if you add another tag `CitrixDetectIgnore` with value as true to that resource, then the resource is ignored while detecting orphaned resources.

Solution for SCCM duplicated GUID issue. After creating multiple VMs using MCS, the System Center Configuration Manager (SCCM) displayed only one VM on its console because of duplicated GUIDs. This issue is now resolved by adding a step in the image preparation. This step deletes the existing certificates and GUID information within the master image. The step is enabled by default.

Repair the identity information of active computer accounts. With this feature, you can reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent machine catalogs. Currently, the feature is supported only for Azure and VMware virtualization environments. For more information, see Repair the identity information of active computer accounts.

Get encryption at host information associated with a machine profile. In Azure environments, with this feature, you can now know whether encryption at host is enabled for a machine profile input (VM or template spec) using PowerShell commands. For more information, see Retrieve encryption at host information from a machine profile.

Repair the user certificates of hybrid Azure AD joined machine identities. With this feature, you can use Powershell command to repair the user certificates of hybrid Azure AD joined machine identities if they corrupt or expire. For more information, see Create Hybrid Azure Active Directory joined catalogs.

Certificate expiry warning support for Hybrid Azure AD joined machine catalogs. Full Configuration now provides one-month advance warnings for user certificate expiration on Hybrid Azure AD joined machine catalogs. This enhancement aims to reduce the risk of service interruptions resulting

from certificate expiration. To view the details and recommended actions, go to the **Machine Catalogs** node, select the machine catalog, and then click the **Troubleshoot** tab.

You can run the `Get-ProvScheme` command to get information about the user certificate expiration date of a hybrid Azure AD joined machine catalog.

Support for Azure confidential VMs (Preview). Azure confidential computing VMs ensure that your virtual desktop is encrypted in memory and protected in use. With this feature, you can now use MCS to create a catalog with Azure confidential VMs. You must use the machine profile workflow to create such a catalog. You can use both VM and ARM template spec as a machine profile input. For more information, see Azure confidential VMs (Preview).

Support for converting a non-machine profile-based machine catalog to machine profile-based machine catalog in AWS environment. In an AWS environment, you can now use a VM or launch template as a machine profile input to convert a non-machine profile-based machine catalog to machine profile-based machine catalog. New VMs added to the catalog take property values from the machine profile. For more information, see Convert a non-machine profile-based machine catalog to machine profile-based machine catalog.

Support for Citrix-managed HPE Moonshot plug-in (Preview). Previously, you used HPE-managed Moonshot plug-in (HPE Moonshot Machine Manager) maintained by Hewlett Packard Enterprise (HPE) to perform the power management actions on HPE Moonshot chassis. The plug-in was based on legacy APIs that made MCS infrastructure projects difficult. With this feature, a Citrix-managed HPE Moonshot plug-in (HPE Moonshot) is introduced. With this plug-in, you can create connections to your HPE Moonshot chassis, create catalogs, and power manage machines in the catalog using Full Configuration interface and PowerShell commands. For more information, see:

- HPE Moonshot virtualization environments (Preview)
- Connection to HPE Moonshot (Preview)
- Create an HPE Moonshot machine catalog (Preview)
- Manage an HPE Moonshot catalog (Preview)

Ability to change memory and disk cache size. With this feature, you can now change the memory and disk cache size of the Write-back cache (when MCSIO is enabled) using a PowerShell command without creating a new machine catalog. This implementation helps you to have the optimized cache configuration that is suitable for your business needs. This feature is applicable to:

- GCP and Microsoft Azure environments, and
- a non-persistent catalog with MCSIO enabled

For more information, see Change cache configuration on an existing machine catalog.

Support for creating a customer-managed encryption key enabled catalog. In Azure environments, you can now create a Citrix Provisioning catalog enabled with customer-managed encryption

key (CMEK) using the Full Configuration interface and PowerShell commands. For more information, see Create a customer-managed encryption key enabled catalog.

Ability to copy tags on all resources in Azure. With this feature, in Azure environment, you can now copy tags specified in a machine profile to all the resources such as, multiple NICs and disks (OS disk, Identity disk, and write-back cache disk) of a new VM or an existing VM in a machine catalog.

The machine profile source can be a VM or an ARM template spec. For more information, see Copy tags on all resources.

Session state updated to disconnected after the machine is suspended. Previously, after you suspended a VM, the session was still shown as **Active**. With this enhancement, after you suspend a VM, the associated session's state is now shown as **Disconnected**.

Support for creating AWS VMs that support hibernation. You can now create machine catalogs that support VM hibernation in your AWS environments, enhancing the overall cost-effectiveness of your deployment. You can also edit a catalog to include hibernation-capable VMs if the associated machine profile supports this capability. For more information, see Power Manage AWS VMs.

Support for configuring load-balancing methods at the delivery group level (Preview). This feature allows you to choose the **Vertical Load Balancing** method at a delivery group level. With this feature, each machine is aligned to the maximum load index before the next machine is powered on. Autoscale and Vertical Load Balancing determine when the next machine is powered on. This feature achieves maximum utilization for each machine and cost savings in public clouds. This feature offers more flexibility in managing the load balancing strategies for machines.

You can configure a delivery group to either inherit the load balancing method from the site-level settings or override the site-level load balancing method and instead choose one of the vertical or horizontal load balancing methods. For more information, see Step 2. Load balancing.

Support for hibernation-capable VMs in Azure (Preview). In Azure environments, you can create an MCS machine catalog that supports hibernation. Using this feature, you can suspend a VM, and then reconnect to the previous state of the VM when a user signs in again. For more information, see Create hibernation-capable VMs (Preview).

DaaS get-started guide. We've launched a new guide to streamline and simplify DaaS deployment and configuration for both new and experienced administrators. It offers these key benefits:

- **Easy to get started.** Using a step-by-step questionnaire-based approach, this guide helps new administrators set up their deployments quickly. Contextual help info throughout the guide aids in understanding essential concepts and terminology.
- **Simplify complex configurations.** This guide includes pre-configured settings where applicable and provides access to the Full Configuration UI for advanced setup. Experienced admins can use it as a foundation for more complex configurations.

For more information, see Use DaaS get-started guide.

Assign drive letters to write-back cache disks using Full Configuration. Previously, you could assign a specific drive letter to the write-back cache disk only by using a PowerShell cmdlet. You can now accomplish the same task using Full Configuration. For more information, see Create machine catalogs.

Support for changing various Azure machine properties using Full Configuration. For Machine Creation Services-provisioned Azure machines, you can now change the following property settings using Full Configuration:

- Storage type
- Dedicated host group
- Azure Compute Gallery settings

When you change any of these settings, Full Configuration automatically identifies related settings and provides automatic synchronization or prompt messages requesting you to reselect related settings. This capability ensures consistent changes across associated settings, preventing potential configuration errors. For more information, see Edit a catalog.

Use existing identity pools to create identities for MCS-provisioned machines. When creating AD-joined catalogs or adding machines to them using Full Configuration, you can now use an existing identity pool to allocate machine identities. This feature allows you to apply a consistent machine account naming scheme across multiple catalogs. For more information, see Machine identities.

Session Topology. The Session Topology view is the next step towards enhancing troubleshooting workflows in Monitor. The Session Topology view provides a visual representation of the in-session path for connected HDX sessions. You can access the topology view from the **User Details > Session Performance**.

The Session Topology view for an HDX connected session shows the components involved in the session path with their metadata, the link between the components, and the applications published on the VDA. In addition, ICA Latency and ICA RTT measurements are displayed for the session when it is in a connected state.

Use the Session Topology view to understand the components through which the session data flows and to identify the specific hop that might be bringing in performance issues. For more information see Session Topology.

October 2023

New and enhanced features

Refine your Autoscale settings using historical usage. A new Autoscale settings tab called **Autoscale Insights**, offers a comprehensive graph that visually compares your Autoscale settings and

machine usage data from the previous week. With this graph, you can gain insights into the effectiveness of Autoscale settings:

- **Not cost-effective**. Financial waste exists due to the over-provisioning of capacity.
- **Poor user experience**. User experience is negatively impacted due to the under-provisioning of capacity.
- **Good balance between user experience and cost**. The capacity provisioned is aligned with the historical usage.

For more information, see Analyze the effectiveness of Autoscale settings.

Multiple NICs support for Azure VMs. With Full Configuration, you can now create Azure VMs with multiple NICs. A VM's maximum NIC count is determined by the machine size setting while its actual NIC count allowed is defined by the machine profile setting. For more information, see Create machine catalogs.

For creating or updating a catalog with multiple NICs per VM using PowerShell commands, see Create or update a catalog with multiple NICs per VM.

Trends for Session Performance metrics. Monitor is introducing a new **User Details > Session Performance** tab with enhanced troubleshooting workflows starting with the ability to correlate real-time metrics in identifying issues within user sessions. Session Experience now contains trends of session metrics like ICARTT, ICA Latency, Frames Per Second, Output Bandwidth Available, and Output Bandwidth Consumed. This feature helps reduce the mean time for resolution by enabling you to correlate multiple performance metrics in a single view. For more information see the User Issues article.

Support VDA version on settings page of create/edit policy. As part of creating a policy, when configuring the settings, the system provides an option to view the settings type. You can view the following settings type:

- All settings - View all settings for all VDA versions
- Current settings only - View settings for only the current VDA versions
- Legacy settings only - View settings for only the deprecated VDA versions

For more information, see Create policies

Limit application visibility only supported for Active Directory accounts. The capability to limit the application visibility is available only for the Active Directory user accounts, and not for Azure Active Directory and Okta accounts. Note that to aid this feature, on the application setting workflow, on the Select Users or Groups page, **Azure Active Directory**, and **Okta** options in the **Select Identity type** field are disabled.

New UI option to delete VM records only from the Citrix site database. When catalog and VM deletion fails due to an unreachable hypervisor, you can now opt to only delete VM records from the Citrix site database, leaving the VMs intact on the host. For more information, see Delete a catalog.

Support for creating empty machine catalogs for non-MCS-provisioned machines. Creating empty machine catalogs now extends to non-MCS-provisioned machines, including:

- Virtual or blade machines provisioned using technologies other than Machine Creation Services.
- Physical machines not power managed by Citrix DaaS
- Remote PC Access machines

With this feature, you can now create machine catalogs without the need to add machines to them during catalog creation.

Image Refresh enhancements. Previously, when refreshing images, all images in the image tree were updated, irrespective of whether a specific node in the tree was selected. With the latest enhancement, if you've selected a node, only images in this node are refreshed. This enhancement ensures a more targeted refresh process, significantly improving the image refresh speed. Additionally, you can now clear a selected node in the image tree by holding CTRL and clicking the node. For more information, see Master image.

Peak Autoscale Assigned PowerOn. When persistent desktops are powered on but remain unused or if no user logs on, the administrators can define the wait time to take actions like, no action, suspend, or shutdown.

For assigned machines, where it is powered on but a session has not been connected to it within the set time after the start of peak time, then you can add a policy to the delivery group level to turn off the machine.

For assigned machines, where it is in resumed state but a session has not been connected to it within the set time after the start of peak time, then you can add a policy to the delivery group level to suspend the machine.

This feature is helpful if there is an end user who is on PTO, or has not logged on, or if a company has a long weekend, then you can set the wait time and machine disconnection actions to take to help reduce the Azure consumption cost. For more information, see Single-session OS random delivery groups and Single-session OS static delivery groups

Monitor multiple Citrix DaaS instances (Preview). You can now use Citrix Monitor to monitor and troubleshoot issues across multiple Citrix DaaS instances. Citrix DaaS allows customers to aggregate multiple service instances using a hub and spoke model. With this configuration, administrators can perform helpdesk search on all configured DaaS instances from a single Monitor console. For more information regarding the configuration required to aggregate the spoke service instances to a hub, see Aggregate multiple Citrix Virtual Apps and Desktops service instances. Monitor supports the aggregation of up to four DaaS tenants (spokes) under a single DaaS tenant (hub).
To have unified monitoring across all DaaS tenants, use bi-directional enumeration of the hub and spoke instances. For more information, see Aggregated Search across multiple DaaS instances (Preview).

Support for vSAN 8.0. You can now use MCS to provision VMs in the vSAN 8.0 environment.

Preserve NIC settings on provisioned VMs. Previously, the NIC settings of the master image were not retained in the provisioned VMs. For example, if you configured the DNS settings on the master image, the provisioned VMs did not retain the configured DNS settings of the master image. With this feature, the provisioned VMs can now retain the NIC settings of the master image. The settings are retained even after a Windows update. The filter driver is automatically installed if you do a fresh installation of VDA version 2308 or later on a Hyper-V deployed machine through the MCS master image installations. However, currently, if you upgrade from an older version of VDA (version less than 2308) and want to install the filter driver, then you must select the checkbox **Citrix HyperV Filter Driver** on the **Additional Components** page while upgrading the VDA. For more information, see Install additional components.

This feature is applicable to:

- Hyper-V VMs (including Azure and SCVMM)
- Persistent and non-persistent MCS machine catalogs
- Non-persistent MCS machine catalogs with MCSIO
- Master image with multiple NICs

Detect Orphaned Azure resources. With this feature, you can now detect the orphaned resources in your Azure deployment, enabling efficient resource management. After the orphaned resources are identified, you can take further action, bringing in more productivity and cost reduction. For more information, see Detect Orphaned Azure resources in your deployment.

New image update status. When monitoring image update statuses for catalogs in Full Configuration, you can now view a new status **Preparing image**, in addition to the existing ones **Fully updated**, **Partially updated**, and **Pending update**. For more information, see Change the master image.

PowerShell commands to create Auto-tags (Preview). With this feature you can now create tags automatically by using the PowerShell command. For more information, see Auto Tags.

Notification sign is shown to user or delivery group. While creating or modifying a policy and configuring the settings, if all delivery groups are disabled, the system displays a warning that - None of the elements in this filter is enabled. If at least one delivery group is enabled, the system does not display the warning sign. For more information, see Policy settings

September 2023

New and enhanced features

PowerShell commands to manage Local Host Cache (LHC). You can now use PowerShell commands to manage LHC on Citrix Cloud Connectors. For more information, see Local Host Cache PowerShell commands.

Support for creating empty machine catalogs. In Full Configuration, you can now create a machine catalog without immediate VM creation. With this feature, you can postpone VM creation until back-end hosts are fully prepared or VM provisioning is completed, gaining more flexibility in creating catalogs. Currently, this feature applies only to Machine Creation Services-provisioned catalogs. For more information, see Create machine catalogs.

Data caching for the Home node. We've introduced data caching for the Citrix DaaS **Home** node. This enhancement improves the user experience by reducing the page load times when you navigate to the **Home** node.

Search enhancements for applications. We've revamped the search functionality in the **Applications** node to align with the new design introduced in the **Search** node. This new feature improves your application search experience and maintains a consistent search experience across DaaS. The keyword **Application Name** in the filter expression is renamed to **Name**, while retaining its original meaning. For more information, see Use Search in the Full Configuration management interface.

Enhanced scope management: showing objects in folder view. On the scope creation and management pages, machine catalogs, delivery groups, and application groups are now displayed in folder structures that align with their management in DaaS. This folder view simplifies the process of selecting objects for scope creation and management, making your choices more intuitive and straightforward. For more information, see Create and manage scopes.

Removed the Leave user management to Citrix Cloud option. When creating a delivery group in Manage > Full Configuration, on the Users page, the support for this option is removed. For delivery groups where user assignments were handled through Citrix Cloud, continue to manage user assignments within the Citrix Cloud library.

Removed the Azure Germany option. In line with the closure of Microsoft Cloud Deutschland on October 29, 2021, we've removed the **Azure Germany** option from the host connection creation page.

Proactive service alerts in Full Configuration. Alerts come at two levels —site-wide alerts shown in Home (flag icon) and zone-related alerts shown on the Troubleshoot tab of each zone. Currently, this feature gives you proactive warnings and alerts to make sure that your Local Host Cache and zones are configured correctly so that when an outage occurs, Local Host Cache works and your users are not impacted. For more information, see Service health alerts and Zones.

August 2023

New and enhanced features

Full Configuration: Support for provisioning AWS and GCP VMs using machine profiles. When provisioning AWS or GCP VMs using Machine Creation Services (MCS), you can now select an existing VM as the machine profile, letting VMs within the catalog inherit settings from the selected VM.

- For GCP VMs, the inherited settings include Disk Encryption Set ID, Machine size, Storage type, and Zone.
- For AWS VMs, the inherited settings vary based on the stage:
  - During catalog creation: Machine size, Tenancy type, Security group, and the number of NICs.
  - During catalog editing: Machine size and Security group.

For more information, see Create a machine catalog.

Introducing search functionality in Machine Catalogs and Delivery Groups nodes. You can now directly search and locate machine catalogs and delivery groups within the **Machine Catalogs** and **Delivery Groups** nodes. The search functionality in these nodes provides the same interface as the **Search** node, providing seamless search experience across DaaS. For more information, see Use Search in the Full Configuration management interface.

View endpoint device status in Session Launch Diagnostics using Device Posture. The Session Launch Diagnostics feature in Monitor helps narrow down to the exact component and stage where a session failure occurred. This helps identify the exact reason for a session launch failure and take the recommended action.

As the next step in making this check comprehensive across all the components involved in the session launch sequence, you can now view the endpoint device scan results. Clicking **Endpoint Device** in the list of components shows the Device Posture scan status. Device Posture Service scans the endpoint device for compliance based on policies defined by the administrator.

Ensure that the Device Posture service is configured with DaaS as described in the Device Posture article. Errors logged by Device Posture are described in Device Posture Error Logs.

For more information, see Steps to diagnose session launch failure

New options in Full Configuration to route API requests to Azure and GCP through Citrix Cloud Connectors. Previously, API requests to Azure and GCP could be routed only through public endpoints. With a new option in **Full Configuration > Add Connection and Resources**, you can now opt for a more secure approach by routing them through Citrix Cloud Connectors. For more information, see Create a service principal and connection using Full Configuration.

Search and filter enhancements. We've made the following enhancements to improve your search experience:

- **Simplified search**: Performing a search without filters now removes search recommendations, providing a clean and straightforward search experience.
- **AND/OR operator update**: "Match all(AND operator)"and "Match any(OR operator)"options are now available in the filters panel, accessible with a single click the filters icon.
- **Streamlined filter configuration**: You can now specify and apply multiple filters seamlessly with the filters panel.

- **Cleaner interface**: The "filter pinning"ability has been removed, reducing UI clutter and making your search experience more intuitive.
- **Quick filter addition**: After applying filters, you can now use the plus sign to quickly add one more filter.
- **Delete saved filter sets**: You can now easily delete saved filter sets right within the search menu, without navigating to **Manage filter sets**.

For more information, see Use Search in the Full Configuration management interface.

VDA upgrade support for Azure Quick Deploy-created machine catalogs. With Full Configuration, you can now enable **VDA Upgrade** for machine catalogs created through Azure Quick Deploy and then perform **Upgrade VDA** on them for immediate or scheduled upgrades. For more information, see Upgrade VDAs using the Full Configuration interface.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog in SCVMM. You can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS. Currently, this feature is applicable to Azure, Citrix Hypervisor, SCVMM, and VMware virtualization environments. For more information on using the PowerShell command to reset the OS disk, see Reset OS disk.

Update properties of individual VMs. You can now update properties of individual VMs in a persistent MCS machine catalog using a PowerShell command. This implementation helps you to manage individual VMs efficiently without updating the entire machine catalog. Currently, this feature is applicable only to the Azure environment. For more information, see Update properties of individual VMs.

Restrict upload and download of managed disks. As per Azure policy, you cannot upload or download more than five disks or snapshots at the same time with the same disk access object. With this feature, the limit of five concurrent uploads or downloads is not enforced if you:

- Configure `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`, and
- Do not configure Azure policy to create Disk Accesses automatically for each new disk to use private endpoints.

Support for assigning a specific drive letter to MCS I/O write-back cache disk. Previously, the Windows operating system automatically assigned a drive letter to MCS I/O write-back cache disk. With this feature, you can now assign a specific drive letter to an MCS I/O write-back cache disk. This implementation helps you to avoid conflicts between the drive letter of any applications that you use and the drive letter of MCS I/O write-back cache disk. This feature is applicable to only Windows operating system. For more information, see Assign a specific drive letter to MCS I/O write-back cache disk.

Support for machine profile in Citrix Hypervisor. In Citrix Hypervisor, you can now create an MCS machine catalog using a machine profile. The source of the machine profile input is a VM. The machine profile captures the hardware properties from a VM template and applies them to the newly provisioned VMs in the catalog. For more information, see Create a machine catalog using a machine profile.

Retry creating catalog after failure. When catalog creation fails, you can now retry creating the catalog. To ensure successful creation, check the troubleshooting information and resolve the issues. The information describes the issues found and provides recommendations for resolving them. Failed catalogs are marked with an error icon. To see the details, go to the **Troubleshoot** tab of each catalog. For more information, see Manage machine catalogs.

Permission for managing configuration sets. To enable more precise control over WEM configuration set management, we've introduced a new permission called **Manage configuration sets** to the **Machine catalogs** permission set. This permission grants exclusive access to users who can perform tasks such as binding or unbinding a configuration set and switching to a different configuration set for catalogs. For more information, see Manage configuration set for a catalog.

New option in Full Configuration to enable cleanup of stale Azure AD joined devices. We've introduced an option in Full Configuration to simplify the cleanup of stale Azure AD joined devices in Citrix DaaS. Previously, you had to run a custom PowerShell script to perform the task. Enabling this option grants host connections permission to automatically clean stale Azure AD joined devices. For more information, see Azure host connections.

Monitor image update status for catalogs using Full Configuration. You can now monitor image update statuses for non-persistent machine catalogs using a new column, **Image Update**. This column indicates whether images of a catalog are **Fully updated**, **Partially updated**, or **Pending update**.

To show the column in the **Machine Catalogs** table, follow these steps:

1. In the **Machine Catalogs** node, select the **Columns to Display** icon in the action bar.
2. Select **Machine Catalog > Image Status**.
3. Click **Save**.

Displaying the **Image update** column might degrade the console performance. We recommend displaying it only when necessary.

Secure environment for GCP-managed traffic. With this feature, you can now allow only private Google access to your Google Cloud projects. This implementation enhances security to handle sensitive data. To do this, add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` in case of Citrix Cloud deployment. If you are using a private worker pool, add `UsePrivateWorkerPool` in `CustomProperties`. For more information, see Create a secure environment for GCP managed traffic.

July 2023

New and enhanced features

Support for getting a list of orphaned resources on Azure. In Azure environments, you can now get a list of orphaned resources that are created by MCS but are no longer used by MCS. This feature helps to avoid extra costs. For more information, see Retrieve a list of orphaned resources.

Support for creating persistent multi-session machines using Full Configuration. When creating a catalog of multi-session machines, you can now specify whether to make them persistent. For persistent multi-session machines, keep in mind that changes users make to the desktops are saved and accessible to all authorized users. For more information, see Create machine catalogs.

New capability in Full Configuration to filter the AWS AMI inventory. When selecting machine templates during AWS catalog creation, you can now filter the AWS AMI inventory for a target template using these search criteria:

- Image name
- Image ID
- Image tags

The machine template list loads dynamically as you scroll down the list - 25 items are initially loaded and more loaded as you scroll.

Support for deleting Azure AD devices. With this feature, stale Azure AD devices can be consistently deleted by assigning the Cloud Device Administrator role to the service principal and modifying the custom property of the hosting connection. If you do not delete the Azure stale AD devices, then the corresponding non-persistent VM stays in the initializing state until you manually remove it from the Azure AD portal. For more information, see Create Azure Active Directory joined catalogs.

Support for machine profile in AWS environment. When you create a catalog to provision machines using Machine Creation Services (MCS) in AWS, you can now use a machine profile to capture the hardware properties from an EC2 instance (VM) or launch template version and apply them to the provisioned machines. Properties that are captured can include, for example, EBS volume properties, instance type, EBS optimization, and other supported AWS configurations. When editing the catalog, the machine profile of the provisioned machines can be changed by providing a different VM or launch template. For more information, see Create a catalog using a machine profile.

Export limit on search results extended to 30,000 from 10,000. We've extended the export limit on search results. Previously restricted to 10,000 items, you can now export up to 30,000 items to a CSV file. For more information, see Export search results to a CSV file.

Image refresh option. When selecting master images for machine catalogs, you can now quickly get the most up-to-date master image list using the **Refresh** option at the top right. Note that the **Re-**

fresh option is not available for AWS catalogs. Additionally, a **Refresh** option is available for machine profiles and host groups in Azure catalogs.

June 2023

New and enhanced features

Support for getting custom properties from the machine profile input in GCP. Previously, in GCP environments, while creating an MCS machine catalog using a machine profile input, you had to explicitly specify the custom properties. The action forced an extra effort. With this feature, you can now derive the following custom properties without explicitly defining them:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

When you run `New-ProvScheme` and `Set-ProvScheme` commands and do not explicitly specify the custom properties, then the values of the properties are derived from the machine profile input.

For example, `New-ProvScheme -MachineProfile` writes the machine profile's machine type to the provisioning scheme's `ServiceOffering` property unless you specify `ServiceOffering` in the `New-ProvScheme` command. If you run `Set-ProvVMScheme` twice, then the most recent command takes effect.

Remove tags in AWS environments. Previously, `Remove-ProvVM` and `Remove-ProvScheme` PowerShell commands with `ForgetVM` parameter removed the VMs and machine catalogs from the Citrix database. However, the commands didn't remove the tags. You had to individually manage the VMs and machine catalogs that weren't removed entirely from all the resources. With this feature, you can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and tags from a single VM or a list of VMs from a machine catalog.
- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and resources from a machine catalog.

This implementation helps in:

- Identifying leaked resources
- Removing the additional cost of maintaining the resources that are not required

This feature is only applicable to persistent VMs. For more information, see Remove tags.

Ability to get historical errors and warnings associated with an MCS machine catalog. Previously, you only got the latest warnings and errors associated with a machine catalog. With this feature, you

can now get a list of the historical warnings and errors of an MCS machine catalog. This list helps you to understand any issues with your MCS machine catalog and fix those issues.

For more information, see Retrieve warnings and errors associated with a catalog.

Increased capacity with improved performance for Citrix in Google Cloud. Citrix can now support catalogs containing up to 3,000 VDAs in a single Google Cloud project. This update brings performance improvements to both provisioning and power management operations.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog in Google Cloud and AWS environment. You can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS. Currently, this feature is applicable to AWS, Azure, Citrix Hypervisor, Google Cloud, and VMware virtualization environments. For more information on using the PowerShell command to reset the OS disk, see Reset OS disk.

Support for changing disk related custom properties of an existing catalog and existing VMs in GCP. Previously, in GCP environments, you could add the custom properties only when you created the MCS machine catalog. With this feature, you can now change the following disk-related custom properties of an existing catalog and existing VMs of the catalog.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

This implementation helps you to select different storage types for different disks even after you create a catalog and thus, balance pricing associated with different storage types. For more information, see Change disk related custom properties of an existing catalog.

Dynamic session timeout support extended to VDA version 2203 LTSR CU3 or later. For single-session OS delivery groups, this feature now applies to VDAs of version 2206 CR or later, or 2203 LTSR CU3 or later. For more information, see Dynamic session timeouts.

Improved host connection creation experience in Full Configuration. After you select a resource location, the **Connection type** drop-down list now displays all Citrix-supported hypervisors and cloud services, and their availabilities depend on:

- For a resource location without accessible Cloud Connectors, only hypervisors and cloud services that support connectorless deployments are available.
- For a resource location with accessible Cloud Connectors, only hypervisors and cloud services that have their plug-ins properly installed on those connectors are available.

For more information, see Create and manage connections.

Additional component selection in VDA upgrade. You can now select which additional components to upgrade or install while upgrading a VDA. For more information, see Configure auto-upgrade for VDAs.

> **Important:**
>
> To use the additional components feature, make sure that your VDA Upgrade Agent is version 7.34 or later, which is included in the VDA installer version 2206 or later.

Full Configuration now preconfigures certain settings for Azure machines based on machine profiles. When you provision Azure VMs, Full Configuration now preconfigures the following settings based on the selected machine profile:

- Host group
- Disk Encryption Set
- Availability Zone
- License Type

Support for AWS instance hibernation. You can now launch AWS instances, set them as desired, and hibernate them. The hibernation process stores the in-memory state of the instance, along with its private and elastic IP addresses, allowing it to pick up exactly where it left off. For more information on creating VMs that support hibernation, see Instance Hibernation.

Support for optimizing AWS throttling. You can now power on and off a large number of machines in an AWS catalog without encountering throttling issues. Throttling issues occur when the number of requests sent to AWS exceeds the number of requests that the server can handle. This feature increases efficiency by reducing the number of AWS calls to power machines on and off in bulk. It also significantly reduces the time taken to power on and off machines in persistent catalogs.

Secure environment for Azure managed traffic. Previously, you relied on the public internet to let your Azure endpoints interact with resources in your environment. As a result, security concerns were raised because the public internet was accessed. With this feature, MCS enables network traffic to be routed through Citrix Cloud Connectors in your environment. This makes the environment safe because now all Azure managed traffic originates from your own environment. To do this, add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`. For more information, see Create a secure environment for Azure managed traffic.

After you set the custom properties, you can configure Azure policies to have private disk access to Azure managed disks.

Support for provisioning catalog VMs with Azure Monitor Agent. Azure Monitor Agent (AMA) collects monitoring data and delivers it to Azure Monitor. With this feature, you can provision MCS machine catalog VMs (persistent and non-persistent) with AMA installed as an extension. This implemen-

tation enables monitoring by uniquely identifying the VMs in monitoring data. For more information on AMA, see Azure Monitor Agent overview.

Currently, MCS supports only the machine profile workflow for this feature. For more information on provisioning machine catalog VMs with AMA enabled, see Provision catalog VMs with Azure Monitor Agent installed.

Enable restart schedule for an MCS catalog. Previously, you could schedule image updates by waiting for the next restart or by triggering an immediate restart of all VMs. With this feature, you can now create a one-time restart schedule for a catalog to be triggered on a desired date and time to facilitate MCS image updates. To create a restart schedule, use the `BrokerCatalogRebootSchedule` command. For more information, see Change the master image.

Manage expired client secrets in Azure Quick Deploy. In Azure Quick Deploy, you can now stay informed with alerts when client secrets expire, and easily update them to ensure continuous access to Azure resources. For more information, see Update expired client secrets.

May 2023

New and enhanced features

Search enhancements. This feature enhances visuals and interactions for filters, bringing you a better search experience. For more information, see Use Search in the Full Configuration management interface.

New user exclusions policy where you can define directory paths that are not redirected to the user layer. User exclusions apply to the user personalization layer (UPL), but not to the session host. Logoff.txt now contains all active user exclusions. For more information, see User personalization layer.

Support for updating hardware version of new VMs added in an MCS machine catalog. In VMware environments, you can now update the hardware version of the newly added VMs in an existing MCS machine catalog using a machine profile source. You do not have to create a new machine catalog to update the hardware version of the VMs added to a catalog. You must use the machine profile workflow to use this feature.

Support for filtering AWS VM instances. Previously, when you used an AWS VM instance as a machine profile input to create an MCS machine catalog, the catalog sometimes did not create or function correctly because of invalid machine profile input. With this feature, you can now list the AWS VM instances that can be used as valid machine profile VMs. To do this, use the `Get-HypInventoryItem` command. For more information, see Filtering VM instances.

Support for converting a non-machine profile-based machine catalog to machine profile-based machine catalog in Azure environment. In the Azure environment, you can now use a VM or tem-

plate spec as a machine profile input to convert a non-machine profile-based machine catalog to machine profile-based machine catalog. Existing VMs and new VMs added to the catalog take property values from the machine profile unless overwritten by explicit custom properties. For more information, see Convert a non-machine profile-based machine catalog to machine profile-based machine catalog.

Support for double encryption on managed disk in Azure environment. In Azure environment, you can now create an MCS machine catalog with double encryption. Double encryption is platform-side encryption (default) and customer-managed encryption (CMEK). Therefore, if you are a high security sensitive customer who is concerned about the risk associated with any encryption algorithm, implementation, or a compromised key, you can opt for this double encryption. Persistent OS and data disks, snapshots, and images are all encrypted at rest with double encryption. For more information, see Double encryption on managed disk.

Support for machine profile in VMware. In VMware environments, you can now create an MCS machine catalog using a machine profile. The source of the machine profile input is a VMware template. The machine profile captures the hardware properties from a VMware template and applies them to the newly provisioned VMs in the catalog. For more information, see Create a machine catalog using a machine profile.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog in Azure and Citrix Hypervisor. You can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS. Currently, this feature is applicable to Azure, Citrix Hypervisor, and VMware virtualization environments. For more information on using the PowerShell command to reset the OS disk, see Reset OS disk.

Improved host connection creation experience. You can now get the following information while you create a host connection:

- List of all Citrix supported hypervisor plug-ins, including third party plugins
- Availability of hypervisor plug-in. If the availability status is false, possible reason might be that Cloud Connector is not installed

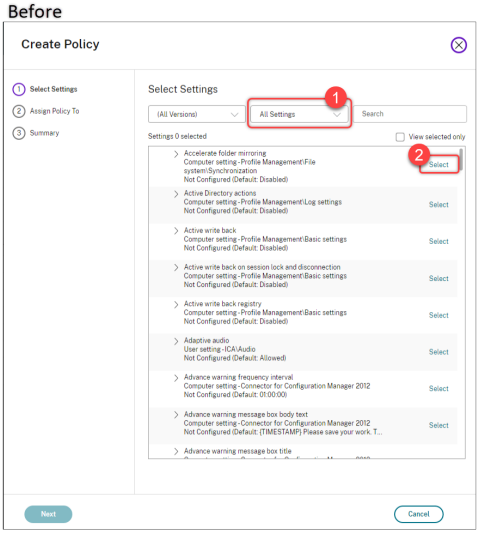
This feature helps you to correctly set-up a resource location and thus, create a host connection. For more information, see Step 1. Connection.

User experience improvements for the Policies node. To improve the user experience and make policy management more efficient, we've implemented the following improvements to the **Full Configuration > Policies** node:

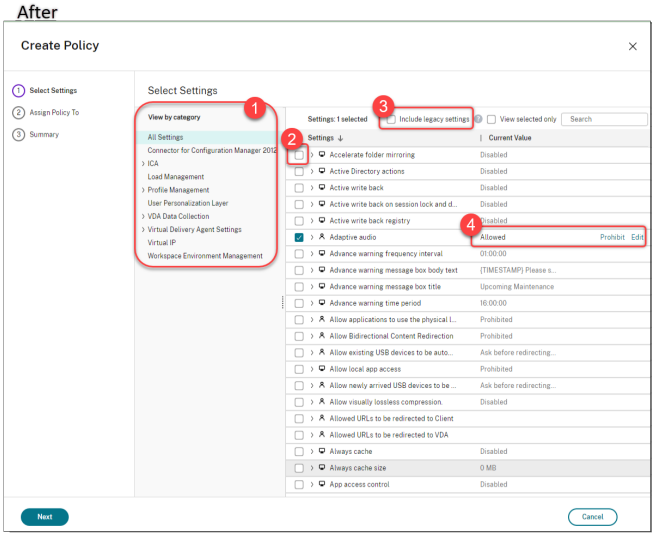
- New UI design for the **Create Policy** and **Create Template** actions:

- Expandable folder view for policy settings. On the **Select Settings** page, all settings are displayed by category in an expandable tree view, making it easier to find a setting.
- To select a setting, you simply click a check box instead of using the **Select** button.
- Legacy settings have been hidden by default so that only the most relevant settings are shown. If legacy settings are needed, select **Include legacy settings**.
- An action button has been added next to a Boolean setting, enabling you to change its value directly in the settings list.

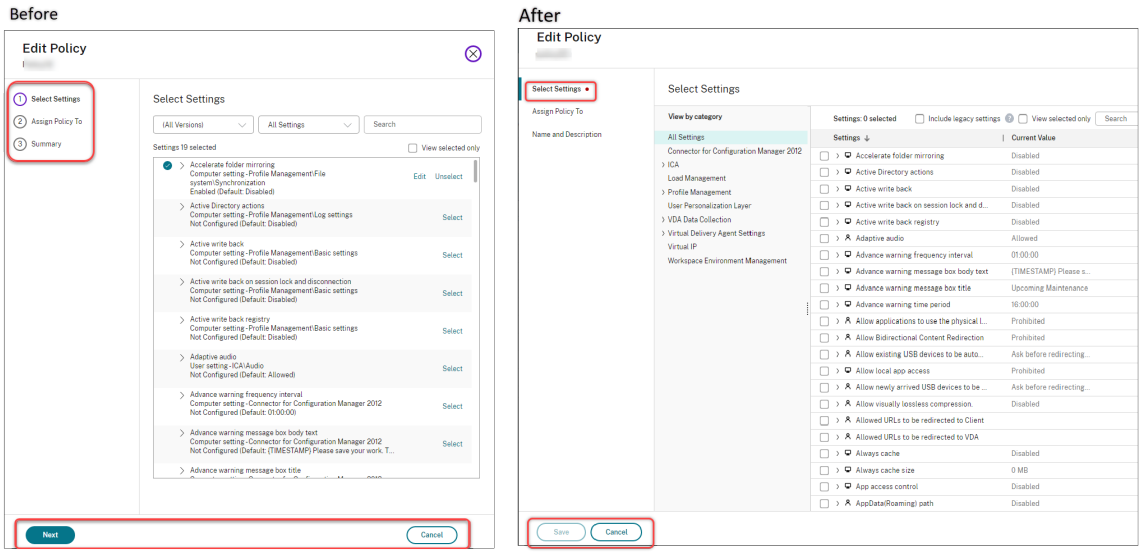
Before



After



- New UI design for the **Edit Policy** action:
  - The navigation menu has been updated to an unordered list. Each item in the list now includes a **Save** button on its page. With this new design, you can save changes made to an item without having to navigate through all items in the navigation menu. These improvements make policy management more efficient and streamlined.
  - Red dots appear next to the navigation items to indicate setting errors.



- Drag to reprioritize policies. In the priority list, you can now change the priority of a policy by dragging it to a desired position.

New option to turn off forced user logoff for AutoScale. A new option, **Neither notify nor force user logoff**, is now available on the **Manage Autoscale > User Logoff Notification** page. With the option selected, Autoscale will neither force users to log off from machines in drain state nor notify users to log off and log on to a different machine. For more information, see User logoff notifications.

Ability to restart Windows 365 Cloud PCs. You can now use Citrix DaaS to restart Windows 365 Cloud PCs.

More session details. When you view a session in **Full Configuration > Search > Sessions**, the session view (in the lower pane) now includes more session details to help you troubleshoot and identify client issues:

- **Reconnect time.** The time when a session reconnected after being disconnected.
- **Client platform.** The platform used to launch the session.
- **Client version.** The version of the client platform used to launch the session.
- **Remote host IP.** The IP address of the remote host where Citrix Workspace is being hosted.

Support for renaming Azure AD security groups for VMs. For VMs added to an Azure AD security group through Citrix DaaS, you can now rename the security group using **Full Configuration > Edit Machine Catalog**. Renaming occurs after you save the change.

Default domain selection for machine accounts. When you create a catalog, the domain where the resource (connection) resides is selected by default for machine accounts.

Ability to display the Azure AD assigned security groups for VMs to join. In Full Configuration, when you create Azure Active Directory joined VMs, an option, **Join an assigned security group as a member**, is now available, letting you add the Azure AD security group where the VMs reside to an

assigned security group. For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for changing networks for connections. In Full Configuration, you can now change networks for a connection. You can't unassociate networks from a connection if they are in use. For more information, see Edit network.

Ability to remove tags in Azure environments. Previously, `Remove-ProvVM` and `Remove-ProvScheme` PowerShell commands with `ForgetVM` parameter removed the VMs and machine catalogs from the Citrix database. However, the commands didn't remove the tags from the resources. You had to individually manage the VMs and machine catalogs that weren't deleted entirely from all the resources. With this feature, you can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and tags created on the resources from a single VM or a list of VMs from a machine catalog.
- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and tags created on the resources from an entire machine catalog.

This implementation helps in identifying orphaned resources that are created by MCS but no longer used by MCS.

This feature is only applicable to persistent VMs. For more information, see Remove tags.

Failed Machines alert.The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alert, Failed Machines (in %) based on the percentage of failed machines in a delivery group. The new alert condition, allows you to configure alert thresholds as a percentage of failed machines in a delivery group. For more information, see Failed Machines section in the Alerts article.

April 2023

New and enhanced features

Publishing with specific cloud platforms using Citrix Provisioning in Image Portability Service. Specific workflows for using Image Portability Service to publish in AWS, Azure, and Google Cloud are now available. In addition, the required permissions for Azure and networking have been updated. For more details, see Migrate workloads to public cloud.

Support for identifying why a machine is in maintenance mode. Previously, PowerShell was your only choice to identify why a machine was in maintenance mode. You can now achieve that in Full Configuration:

1. Use Search to locate the machine.
2. Check **Maintenance Reason** on the **Details** tab in the lower pane. Or hover over the **Maintenance Mode** column. The following information can appear:

- By Administrator: Put into maintenance mode by administrator.
- Maximum Failed Registrations: Put into maintenance mode as machine exceeded maximum allowed registration attempts.

Also, a filter, **Maintenance Reason**, is now available. You can use it to identify the target machines.

The feature is useful for administrators to troubleshoot issues with machines in maintenance mode.

Use variables to notify users of remaining time before they are logged off. When forcing user logoff, you can now use %s% or %m% as variables to indicate the specified time in the notification message. To express the time in seconds, use %s%. To express the time in minutes, use %m%. For more information, see User logoff notifications.

Support for customizing power on behavior at storage type change failure. At power-on, the storage type of a managed disk might fail to change to the desired type due to a failure on Azure. Previously, in these scenarios, the VM would remain off with a failure message sent to you. With this feature, you can either choose to power on the VM even when storage cannot be restored to its configured type or choose to keep the VM powered off. For more information, see Customize power on behavior at storage type change failure.

Support for MAK activation. You can now provision persistent and non-persistent machine catalogs with VMs activated through the Multiple Activation Key (MAK). With this feature, now MCS can also communicate with provisioned VMs. This implementation helps in activating the Windows system without losing activation counts. For more information, see Volume licensing activation.

Support for Azure disk encryption at host. With this feature, you can now create an MCS machine catalog with encryption at host capability. Currently, MCS supports only the machine profile workflow for this feature. You can use a VM or a template spec as an input for a machine profile. For more information, see Azure disk encryption at host.

In this type of encryption, the server hosting the VM encrypts the data and then the encrypted data flows through the Azure storage server. Therefore, this method of encryption encrypts data end to end. For more information, see Encryption at host - End-to-end encryption for your VM data.

Support for GCP instance template as an input for machine profile. With this feature, you can now select a GCP instance template as an input for the machine profile. Instance templates are lightweight resources in GCP, therefore are very cost effective. To do this, use PowerShell commands. For more information on using PowerShell commands to create and update machine catalogs by selecting a GCP instance template, see Create a machine catalog with machine profile as an instance template.

Support for modifying Azure AD dynamic security group name. You can modify or delete an Azure AD dynamic security group name from Azure portal. This action can make the Azure AD dynamic security group name out-of-sync with the dynamic security group associated with a machine catalog. With this feature, you can now modify the Azure AD dynamic security group name associated with a machine catalog.

This modification helps you to make the Azure AD dynamic security group information stored in Azure AD identity pool object to be consistent with the information stored in Azure portal. For more information, see Modify Azure AD dynamic security group name.

Added permissions required in GCP. The permissions required to do the following are now added:

- Create host connection
- Do power management of VMs
- Provision catalogs

For more information, see About GCP permissions.

Credential handling. For enhanced security, by default, credentials are not forwarded to the cloud for users who are not in the same domain as their VDAs. Login attempts fail when all of the following conditions are met:

- The user is in a domain different from the VDA
- No trust exists between the domains
- StoreFront is installed in the same domain as the VDA

Previously under these conditions, the user couldn't be authenticated to StoreFront. So, the Cloud Connector forwarded user credentials to the cloud to route the authentication request to the correct destination for that user. This behavior can still be configured if needed. For more information, see the `CredentialForwardingToCloudAllowed` parameter of Set-Brokersite in the DaaS PowerShell SDK.

March 2023

New and enhanced features

Support for configuring role and scope for administrators. Citrix Cloud now supports a higher degree of flexibility and customization when configuring access for an administrator. Previously, you could only select predefined pairs of roles and scopes. With this enhancement, you can select a role and then pair it with the scope of your choice.

For more information, see Configure custom access for an administrator.

Support for creating dynamic security group under existing assigned security group. Previously, you could create Azure AD dynamic security groups for a machine catalog. With this feature, you can also add an Azure AD dynamic security group under an existing Azure AD assigned security group. You can do the following:

- Get security group information.
- Get all Azure AD assigned security groups that are synced from on-premises AD server or the assigned security groups to which Azure AD roles can be assigned.

- Get all Azure AD dynamic security groups.
- Add Azure AD dynamic security group as a member of Azure AD assigned group.
- Remove the membership between Azure AD dynamic security group and Azure AD assigned security group when Azure AD dynamic security group is deleted along with the machine catalog.

For more information, see Create an Azure AD dynamic security group under an existing Azure AD assigned security group.

Support for Azure AD dynamic security group for Azure AD joined VM. Citrix now supports dynamic security group for a catalog while creating an MCS machine catalog. Dynamic security group rules place the VMs in the catalog to a dynamic security group based on the naming scheme of the machine catalog. This is useful when you want to manage the VMs by Azure Active Directory (Azure AD). This is also useful when you want to apply Conditional Access policies or distribute apps from Intune by filtering the VMs with Azure AD dynamic security group. When you delete a catalog, the dynamic security group is also deleted. For more information, see Azure Active Directory dynamic security group.

For more information on license requirement for using dynamic security groups, see the Microsoft document Create or update a dynamic group in Azure Active Directory.

Support for adding VMs to Azure AD security groups through Full Configuration. An option, **Azure AD security group**, is now available when you create Azure AD joined VMs. The option lets you add the VMs to an Azure AD security group based on their naming scheme. For more information, see Create a Microsoft Azure catalog.

Support for changing the storage type of existing VMs to a lower tier on shutdown in Azure environments. In Azure environments, you can now save storage costs by changing the storage type of existing VMs to a lower tier when the VMs are shut down. To do this, use the StorageTypeAtShutdown custom property. For more information, see Change the storage type of existing VMs to a lower tier on shutdown.

Support for allowing security identifiers while creating virtual machines. Previously, while creating new virtual machines with the configuration specified by a provisioning scheme, you could not add a security identifier (`ADAccountSid`) to the `NewProvVM` command. With this feature, you can now add the parameter `ADAccountSid` to uniquely identify the machines while creating new virtual machines. For more information, see Add SIDs while creating virtual machines.

Ability to get warnings associated with MCS catalogs. Previously, you did not get any information indicating that there are issues with your machine catalog. With this feature, you can now get warnings to understand issues with your MCS catalogs and fix those issues.

Warnings, unlike errors, do not cause an initiated provisioning task to fail.

To get warnings, use PowerShell commands. For more information, see Retrieve warnings associated with a catalog.

Shared tenants for connections. You can now add tenants and subscriptions that share the Azure

Compute Gallery with the subscription of the connection. As a result, when creating or updating catalogs, you can select shared images from those tenants and subscriptions. For more information, see Edit connection settings.

Removed support for changing the OS type for Azure catalogs. When changing catalog images, only images with the same OS type as the image in use are shown. With this enhancement, Citrix DaaS no longer supports changing the OS type for Azure catalogs after catalog creation such as, changing from Windows OS type to Linux and vice versa.

February 2023

New and enhanced features

Support for sharing images across different Azure tenants. Previously, in Azure environments, you could share images only with shared subscriptions using Azure Compute Gallery. With this feature, you can now select an image in Azure Compute Gallery that belongs to a different shared subscription in a different tenant to create and update an MCS catalog. For more information, see Image sharing across Azure tenants.

Policy modeling. The policy modeling feature is now generally available. You can simulate policies for planning and testing purposes. For more information, see Use the Policy Modeling wizard.

Ability to turn preview features on or off. In Full Configuration > Home, as a Citrix Cloud administrator with full access, you can now turn preview features on or off without contacting Citrix. For more information, see Home page for the Full Configuration interface.

Search Session Diagnostics with user name. This feature enables the use of Session Launch Diagnostics starting with the user name if you don't have the transaction id. This feature is specifically useful for help desk administrators to triage a failed session if the end user hasn't captured the transaction id.
You can search for a user name, and select a session to triage from a list of failed sessions that the user attempted to launch over the last 48 hours. The Session Launch Diagnostics page shows the details of the failed session. It lists the exact component and stage where the failure occurred. For more information, see the Session Launch Diagnostics article.

Deploy secure web and SaaS apps with Secure Private Access. On the **Full Configuration > Applications > Applications** tab, a new option, **Add Web/SaaS Applications**, is now available in the action bar. The option lets you deploy secure web and SaaS apps with Secure Private Access. Citrix Secure Private Access provides an easy, flexible way for remote users to access web, SaaS, and client-server based apps using a Zero-Trust approach. It enables single sign-on to web and SaaS apps, along with granular security controls such as watermarking and copy/paste controls, among other security features. With Citrix Secure Private Access, you can combine all your virtualized and non-virtualized apps in one place and enhance the user experience for your users. See Citrix Secure Private Access.

Filter log content for a specific time duration. A new option, **Custom**, is now available in the time duration list in **Full Configuration > Logging > Events**. Use it to specify a period of the events for which you want to filter your search. For more information, see Configuration logging.

Updates for Autoscale. We've updated the **Control when Autoscale starts powering on tagged machines** option to make it easy to understand. The option controls when Autoscale starts powering on tagged machines based on the percentage of the remaining capacity of untagged machines. When the percentage falls below the threshold (default, 10%), Autoscale starts powering on tagged machines. When the percentage exceeds the threshold, Autoscale goes into power-off mode. For more information, see Autoscaling tagged machines (cloud burst).

App protection policies. You can now enable app protection when creating or editing a delivery group. The feature provides anti-keylogging and anti-screen-capturing capabilities for client sessions. For more information, see Create delivery groups and Manage delivery groups.

Real-time GPU Utilization available for AMD GPUs. You can now see GPU Utilization of AMD Radeon Instinct MI25 GPUs and AMD EPYC 7V12(Rome) CPUs on Monitor. Monitor already supports the NVIDIA Tesla M60 GPUs. GPU Utilization displays graphs with real-time percentage utilization of the GPU, the GPU memory, and of the Encoder and the Decoder to troubleshoot GPU-related issues on multi-session and single-session OS VDAs. The AMD GPU Utilization graphs are available only for VDAs running 64-bit Windows and Citrix Virtual Apps and Desktops 7 2212 or later. For more information, see GPU Utilization.

Support for scheduling configuration updates in Azure. In Azure environments, you can now schedule a time slot for the configuration updates of the existing MCS provisioned machines using the PowerShell command `Schedule-ProvVMUpdate`. Any power on or restart during the scheduled time slot applies a scheduled provisioning scheme update to a machine. You can also cancel the configuration update before the scheduled time using `Cancel-ProvVMUpdate`.

You can schedule and cancel the configuration update of:

- A single or multiple VMs
- An entire catalog

For more information, see Schedule configuration updates.

Support for using Citrix ready images directly from Google Cloud Marketplace. You can now browse and select images offered by Citrix on the Google Cloud Marketplace to create MCS catalogs. Currently, MCS supports only the machine profile workflow for this feature. For more information, see Google Cloud Marketplace.

Limit host groups scope in SCVMM Host Connection. Previously, host connection to SCVMM required the admin to have a single top level host group configured. This implies that the admin had visibility to all host groups, clusters, or hosts beneath the single top level host group. With this feature, in large deployments where a single SCVMM manages multiple clusters in different data centers, you

can now limit the host groups scope of the admins. To do this, you can use the Delegated Admin role in the Microsoft System Center Virtual Machine Manager (VMM) console to select the host groups to which an admin must have access. For more information, see Install and configure a hypervisor.

Support for zone-redundant storage in Azure. Previously, MCS offered only locally-redundant storage. With this feature, zone-redundant storage is now an option in Azure, allowing you to select a storage type depending on what type of redundancy you want to use. Zone-redundant storage replicates your Azure managed disk across multiple availability zones, which allows you to recover from a failure in one zone by utilizing the redundancy in others. For more information see, Enable zone-redundant storage.

January 2023

New and enhanced features

Option to downgrade storage disk to Standard HDD when VMs shut down. A new option, **Enable storage cost saving**, is now available on the **Disk Settings** page when you create or update Azure catalogs. The option saves storage costs by downgrading to Standard HDD for the storage disk and the write-back cache disk when the VM shuts down. The VM switches to its original settings on restart. For more information, see Create a Microsoft Azure catalog.

Support for configuring session roaming in Full Configuration. Previously, PowerShell was your only choice to configure session roaming for applications and desktops. You can now do that in **Full Configuration**. For more information, see Manage delivery groups.

Renamed some actions to better align with their actual meanings. We've renamed the following actions in **Full Configuration > Machine Catalogs** and **Full Configuration > Delivery Groups**. The workflows for performing those actions remain unchanged.

- **Update Machines** renamed to **Change Master Image**
- **Rollback Machine** Update renamed to **Roll Back Master Image**
- **Upgrade Catalog** renamed to **Change Functional Level**
- **Upgrade Delivery Group** renamed to **Change Functional Level**
- **Undo Upgrade Catalog** renamed to **Undo Functional Level Change**
- **Undo Upgrade Delivery Group** renamed to **Undo Functional Level Change**

Support for organizing application groups using folders. You can now create nested folders to organize application groups for easy access. For more information, see Organize application groups using folders.

Restriction enhancements for delivery groups. Previously, when restricting the use of apps or desktops for a delivery group, you could specify only users and user groups that were allowed to use them

in a delivery group. You can now also add users and user groups that you want to block. This enhancement is useful when you add a group of users to an allow list and at the same time want to block a subset of users in the allow list. For more information, see Create delivery groups.

Access Citrix Analytics for Performance - Session Details from Monitor. The Session Details page from Citrix Analytics for Performance is now integrated in Monitor. Click **View Session Timeline** in the Sessions page in Monitor to view the Sessions Details page from Citrix Analytics for Performance within Monitor. This requires you to have a valid Citrix Analytics for Performance entitlement. The Session Details are available for sessions that are categorized as Excellent, Fair, or Poor in Citrix Analytics for Performance.

You can view a trend of the session experience for the session for up to the last three days along with the factors contributing to the experience. This information complements the live data available in Monitor, used by the helpdesk admin while troubleshooting issues related to session experience.

For more information, see the Site Analytics article.

Non-persistent VMs are deleted from hypervisors or cloud services when you delete them or their machine catalogs in Full Configuration. The option to retain VMs in hypervisors or cloud services is now available only to persistent VMs. For more information, see Manage machine catalogs.

December 2022

New and enhanced features

Support for creating Azure AD joined, Hybrid Azure AD joined, and Microsoft Intune enabled catalogs with Azure AD joined master VMs. You can now create Azure AD joined, Hybrid Azure AD joined, and Microsoft Intune enabled catalogs with Azure AD joined, Hybrid Azure AD joined, and non-domain-joined master VMs. If you want to manage a master VM by Microsoft Intune, use VDA version 2212 or later, and do not skip image preparation while creating or updating machine catalogs.

For more information on machine identities, see Azure Active Directory joined, Microsoft Intune, and Hybrid Azure Active Directory joined.

Support in MCS for deleting VM objects without accessing the hypervisor. You can now delete VM objects in MCS without having access to the hypervisor. When deleting a VM or provisioning scheme, MCS needs to remove tags so that the resources are no longer tracked or identified. Previously, if the hypervisor could not be accessed, the tag removal failures were ignored. With this feature, if the hypervisor is not accessible while using the `Remove-ProvVM` command the tag removal will fail, but by using the `PurgeDBOnly` option, you can still delete the VM resource object from the database. For more information, see Delete machines without hypervisor access.

November 2022

New and enhanced features

Support for delivering MSIX and MSIX app attach apps. In **Full Configuration > App Packages**, you can now upload MSIX and MSIX app attach packaged apps to Citrix Cloud, and deliver them to your users. For more information, see App packages.

Prompt for unsupported VDA versions and functional levels. The Full Configuration interface now alerts you about unsupported VDA versions and functional levels. To avoid potential issues:

- If a machine runs an unsupported VDA version, you are prompted to upgrade to a supported version.
- If the functional level of a catalog or delivery group is not supported, you are prompted to set it to a higher level.

> **Tip:**
>
> VDAs are covered by the CR and LTSR lifecycles of Citrix Virtual Apps and Desktops.

Ability to annotate master images extended to catalog creation. When creating an MCS catalog in **Full Configuration**, you can now annotate its master image. For more information, see Master image.

Support for exporting desktop assignment data through Full Configuration. When viewing desktop assignments for a single-session OS delivery group, you can now export the assignment data into a CSV file for auditing purposes. To do so, select such a delivery group in **Full Configuration > Delivery Groups**, go to the **Desktops** tab, and then click **Export** in the upper-left corner on the tab.

All Applications and Application Folders tabs consolidated into one. In **Full Configuration > Applications**, the **All Applications** and **Application Folders** tabs have been consolidated into one tab, **Applications**. This change unifies the user experience of folder view management across Full Configuration nodes.

Support for changing the storage type to a lower tier when a VM is shut down in Azure environments. In Azure environments, you can now save storage costs by switching the storage type of a managed disk to a lower tier when you shut down a VM. To do this, use the `StorageTypeAtShutdown` custom property. The storage type of the disk changes to a lower tier (as specified in the `StorageTypeAtShutdown` custom property) when you shut down the VM. After you power on the VM, the storage type changes back to the original storage type (as specified in `StorageType` or `WBCDiskStorageType` custom property). For more information, see Change the storage type to a lower tier when a VM is shut down.

Updates in Filters View. The Filters page in Monitor is updated to include separate Saved and Default filters lists for better visualization and accessibility to the filters. You can select a view from among

Machines, sessions, Connections, or Application Instances. Then, you can select a filter from the list of Saved filters or Default filters to view the filtered list of data. You can use the drop-down lists to refine the filter criteria or edit existing criteria. You can save your filter in the Saved Filter list. For more information, see the Filters article.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog. In VMware virtualization environments, you can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS.

For more information on using PowerShell command to reset the OS disk, see Reset OS disk.

Support for updating machine profile and additional custom properties of MCS provisioned machines in Azure environments. Previously, in Azure environments, you could use `Request-ProvVMUpdate` to update `ServiceOffering` custom property of an MCS provisioned machine. Now, you can also update the machine profile and the following custom properties:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

For more information, see Update provisioned machines to current provisioning scheme state.

Support for machine profile in GCP. When you create a catalog to provision machines using Machine Creation Services (MCS) in Google Cloud Platform (GCP) environments, you can now use a machine profile to capture the hardware properties from a virtual machine and apply them to the newly provisioned VMs in the catalog. When `MachineProfile` parameter is not used, the hardware properties are captured from the master image VM or snapshot.

Machine profiles work with both Linux and Windows operating systems.

For information on how to create a machine catalog with a machine profile, see Create a machine catalog using a machine profile.

Support for updating MCS provisioned machines in GCP environments. In GCP environments, `Set-ProvScheme` changes the template (provisioning scheme) and does not affect existing machines. Using the PowerShell command `Request-ProvVMUpdate`, you can now apply the current provisioning scheme to an existing machine (or set of machines). Currently, in GCP, the property

update supported by this feature is machine profile. For more information, see Update provisioned machines using PowerShell.

October 2022

New and enhanced features

Support for using machine profiles and host groups at the same time. When creating a catalog using an Azure Resource Manager master image, you can now use a machine profile and a host group at the same time. This is useful in scenarios where you want to use trusted launch for improved security and at the same time run the machines on dedicated hosts. For more information, see Microsoft Azure Resource Manager virtualization environments.

Support for organizing delivery groups using folders. You can now create a folder tree to organize delivery groups for easy access. For more information, see Organize delivery groups using folders.

Support for scheduling a one-time restart for machines through Full Configuration. A new option, **Once**, is now available when you create restart schedules for delivery groups. With this option, you can schedule machines in a delivery group to restart once, at a specified date and time. For more information, see Create a restart schedule.

Advanced Probe Scheduling. Improved scheduling of Application and Desktop Probes can now be done from Monitor. Using this feature, Citrix Probe Agent can be configured to run the probe tasks on specific days of the week and repeated at specified intervals during the day. This allows you to schedule a single probe task to repeat at specific times of the day and the week. You can now proactively check your site health with probes set to run regularly at suitable times. This feature simplifies probe setup and management in Monitor. For more information, see Application and Desktop Probing.

September 2022

New and enhanced features

Older versions of the Remote PowerShell SDK are now deprecated. If you are using a deprecated version, the SDK stops working and you see an error message prompting you to download the current version. If this happens, download the latest Remote PowerShell SDK from the Citrix website.

Machine catalogs with Trusted launch in Azure. In Azure environments, you can create machine catalogs enabled with Trusted launch, and use the `SupportsTrustedLaunch` property of the VM inventory to determine the VM sizes that support Trusted launch.

Trusted launch is a seamless way to improve the security of Generation 2 VMs. Trusted launch protects against advanced and persistent attack techniques. For more information, see Machine catalogs with Trusted launch.

Support for identifying Microsoft System Center Virtual Machine Manager resources created by MCS. You can now identify Microsoft System Center Virtual Machine Manager (SCVMM) resources created by MCS using tags. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for identifying VMware resources created by MCS. You can now identify VMware resources created by MCS using tags. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for optimizing AWS Workspace throttling. You can now power on and off a large number of machines in an AWS Workspace without encountering throttling issues. Throttling issues occur when the number of requests sent to AWS Workspace exceeds the number of requests that the server can handle. Therefore, Citrix now groups multiple requests into one single request before sending it to the AWS Workspace SDK.

Ability to check machine details when viewing machine counts in Home. When viewing machine counts by availability state in **Home**, you can now click a state to view details of machines in that state. For more information, see Home page for the Full Configuration interface.

Support for machine catalog creation using an image from a different subscription in the same Azure tenant. Previously, in Azure environments, you could only select an image within your subscription to create a machine catalog. With this feature, you can now select an image in Azure Compute Gallery (formerly Shared Imaged Gallery) that belongs to a different shared subscription to create and update MCS catalogs.

For more information on creating a catalog, see Create a machine catalog using an Azure Resource Manager image.

For information on sharing image with another service principal in the same tenant, see Image sharing with another service principal in the same tenant.

For information on PowerShell commands to select an image from a different subscription, see Using PowerShell to select an image from a different subscription.

For more information on Azure Compute Gallery, see Azure Shared Image Gallery.

August 2022

New and enhanced features

Support for identifying Citrix hypervisor resources created by MCS. You can now identify Citrix hypervisor resources created by MCS using tags. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for using host groups and Azure availability zones at the same time. In Azure environments, there is now a pre-flight check to assess whether the creation of a machine catalog will be

successful based on the Azure availability zone specified in the custom property and the host group's zone. Catalog creation fails if the availability zone custom property does not match the host group's zone.

A host group is a resource that represents a collection of dedicated hosts. A dedicated host is a service that provides physical servers that host one or more virtual machines.
Azure availability zones are physically separate locations within each Azure region that are tolerant to local failures.

For more information on the various combinations of availability zone and host group zone that result in successful or failed the machine catalog creation, see Using host groups and Azure availability zones at the same time.

Support for updating the folder ID of a machine catalog in VMware. In VMware virtualization environments, you can now update the folder ID of an MCS machine catalog using the custom property `FolderID` in `Set-ProvScheme`. The VMs created after updating the folder ID are created under this new folder ID. If this property is not specified in `CustomProperties`, then VMs are created under the folder where the master image is located. For more information on updating the folder ID, see Update the folder ID of a machine catalog.

Time zone setup. You can now configure the date and time format of the interface to suit your preferences using the **Date and time** setting. For more information, see Time zone setup.

Image Portability Service (IPS) now supports Amazon Web Services (AWS). By configuring the required permissions and components for AWS, IPS workflows can be used with an AWS account. See Migrate workloads to public cloud for more details.

Page file setting during image preparation in Azure environments. In Azure environments, you can now avoid potential confusion with the page file location. To that end, MCS now determines the page file location when you create the provisioning scheme during image preparation. This calculation is based on certain rules. Features like ephemeral OS disk (EOS) and MCS I/O have their own, expected page file location, and are exclusive to each other. Also, if you decouple image preparation from provisioning scheme creation, MCS correctly determines the page file location. For more information on page file location, see Page file location.

Support for updating page file setting in Azure environments. While creating a catalog in an Azure environment, you can now specify the page file setting, including its location and the size, using PowerShell commands. This overrides the page file setting determined by MCS. You can do this by running the `New-ProvScheme` command with the following custom properties:

- `PageFileDiskDriveLetterOverride`: Page file location disk drive letter
- `InitialPageFileSizeInMB`: Initial page file size in MB
- `MaxPageFileSizeInMB`: Maximum page file size in MB

For more information on updating the page file setting, see Update page file setting.

Updates to the Home page. The Get Started widget now has a new look and feel. Other updates to the Home page include:

- The newly added Refresh and Help icons in the upper right corner.
- Clickable resource counts, providing quick access to relevant resource pages.
- Enhancement to the Dislike icon. If you dislike a recommendation, the recommendation disappears. If you dislike the recommendation widget, the widget disappears.

For more information, see Home page.

Support for enabling Azure VM extensions. When using an ARM template spec as a machine profile to create a machine catalog, you can now add Azure VM extensions to the VMs in the catalog, view the list of supported extensions, and remove extensions you added. Azure VM extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a VM requires software installation, antivirus protection, or the ability to run a script inside it, you can use a VM extension. For more information on how to enable Azure VM extensions, see Use PowerShell to enable Azure VM extensions.

Trusted launch support for ephemeral OS disk. You can now create provisioning schemes using ephemeral OS disk on Windows with trusted launch. Trusted launch is a seamless way to improve the security of generation 2 VMs. It protects against advanced and persistent attack techniques by combining technologies that can be independently enabled like secure boot and virtualized version of trusted platform module (vTPM). For more information on creating a machine catalog, see Create a machine catalog using an Azure Resource Manager image.

July 2022

New and enhanced features

Dynamic session timeouts for single-session OS machines. Dynamic session timeouts now support single-session OS machines. A delivery group with at least one VDA of version 2206 or later is required. Ensure that those VDAs have registered with Citrix Cloud at least once. For more information, go to Dynamic session timeouts.

Send logoff reminders without forcing user logoff in Autoscale. A new feature is now available in **User Logoff Notifications** (formerly **Force User Logoff**) in Autoscale. The feature lets you send logoff reminders to users without forcing them to log off. Doing that avoids potential data loss caused by forcing users to log off from their sessions. See User logoff notifications for details.

Ability to set the Linux OS license type when creating Linux VM catalogs in Azure. Using the Full Configuration interface, you can now choose the Linux OS license type when creating Linux VM catalogs in Azure. You have two choices for bring-your-own Linux licenses: Red Hat Enterprise Linux and

SUSE Linux Enterprise Server. For more information, see Create a machine catalog using an Azure Resource Manager image.

Enhanced search experience in Full Configuration. The Search node provides the following new features and enhancements:

- **Ability to export search results**. You can now export search results. To do that, click the export icon in the upper right corner.
- **New filter available**. A filter, Pending Power Action, is now available for use. Use the filter to refine your search.
- **"Does not contain"search support for certain items**. Items such as machine names and tags now support "Does not contain"search criteria.
- **Support for searching for objects when adding filters**. When adding filters for the following objects, you can now search for them: connections, machine catalogs, delivery groups, application groups, and tags.

For more information, see Use Search in the Full Configuration management interface.

Support for VMware Storage Profiles. When you create a machine catalog using a master image on a vSAN Datastore, you can now copy the storage policy such as the RAID-1 or RAID-5 information from the master image to the created target devices. For existing catalogs, the storage policy remains unchanged even if you update the catalog.

Support for RestrictedKrbHost SPN registration. All the Citrix MCS created computer accounts are now registered with `RestrictedKrbHost` Service Principal Names (SPN). This avoids the requirement to run the `setspn` command to register the SPN for the computer accounts after MCS creates them.

App Packages in Full Configuration for delivering Microsoft packaged applications. The App-V node is renamed to App Packages and redesigned to accommodate more types of Microsoft packaged apps. Previously, you had to use the discovery module to add App-V packaged apps to your environment for delivery. You can now add and deliver the apps in one place by using the App Packages node. For more information, see App packages.

Support for using ARM template specs as machine profiles. Previously, you could use only VMs as machine profiles. You can now use ARM template specs as machine profiles as well when creating Azure machine catalogs. This feature lets you take advantage of Azure ARM template features such as versioning. To ensure that the selected spec is configured correctly and contains required configurations, we perform validation on it. If the validation fails, you are prompted to select a different machine profile. For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for validating ARM template spec. You can now validate the ARM template spec to make sure that it can be used as a machine profile to create a machine catalog. There are two ways to validate the ARM template spec:

- Using the Full Configuration management interface.
- Using the PowerShell command.

For more information on validating the ARM template spec, see Create a machine catalog using an Azure Resource Manager image.

June 2022

New and enhanced features

Restart schedule support for single-session OS machines. Previously, the restart schedule feature was available only for multi-session OS machines. It's now also available for single-session OS machines. You can now create restart schedules for delivery groups containing single-session OS machines. For more information, see Create and manage restart schedules for machines in a delivery group.

Option to perform user name pre-checks. An option, **Check name**, is now available when you enter domain credentials. With the option, you can check whether the user name is valid or unique. The option is useful, for example, when:

- The same user name exists in multiple domains. You are prompted to select the desired user.
- You can't remember the domain name. You can enter the user name without specifying the domain name. If the check passes, the domain name populates automatically.

For more information, see Domain credentials.

Ability to change the network setting for an existing provisioning scheme. You can now change the network setting for an existing provisioning scheme so that the new VMs are created on the new subnetwork. Use the parameter `-NetworkMapping` in the `Set-ProvScheme` command to change the network setting. Only the newly provisioned VMs from the scheme will have the new subnetwork settings. You must also make sure that the subnetworks are under the same hosting unit. For more information, see Change the network setting for an existing provisioning scheme.

Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM template. You can now display the region name information for an Azure VM, managed disks, snapshots, Azure VHD, and ARM template. This information is displayed for the resources on the master image when a machine catalog is assigned. For more information, see Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM template.

Ability to use machine profile property values in Azure environment. While creating an Azure catalog with a machine profile, you can now set the property values from the ARM template spec or VM, whichever is used as a machine profile, if the values are not explicitly defined in the custom properties. The properties affected by this feature are:

- Availability zone
- Dedicated Host Group Id
- Disk Encryption Set Id
- OS type
- License type
- Service Offering
- Storage type

If some of the properties are missing from the machine profile and not defined in the custom properties, then the default value of the properties takes place wherever applicable. For more information, see Use machine profile property values.

Extended support for VDA upgrade. Using the Full Configuration interface, you can now upgrade MCS-provisioned persistent machines. You can upgrade them on a per-catalog or a per-machine basis. For more information, see Upgrade VDAs using the Full Configuration interface.

Citrix Probe Agent in Citrix Cloud Japan and Citrix Cloud Government Control Planes. Citrix Probe Agent now supports sites hosted on Citrix Cloud Japan and Citrix Cloud Government Control Planes. To use the probing agent in these planes, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region"to 2 for Japan and 3 for the Government region. Citrix Probe Agent automates the process of checking the health of virtual apps and desktops that are published in a site. For more information, see Application and Desktop Probing.

Customize the port used for communication between VDAs and Cloud Connectors. You can now customize the port that the VDA uses to communicate with Cloud Connectors based on your specific security requirements. This feature is useful if your security team doesn't allow the default port (port 80) to be open or if the default port is already in use. For more information, see Customize the port for communicating with Cloud Connectors.

Support for organizing machine catalogs using folders. You can now create nested folders to organize machine catalogs for easy access. For more information, see Organize catalogs using folders.

Support for SCVMM 2022. Citrix DaaS now supports Microsoft's System Center Virtual Machine Manager (SCVMM) 2022. SCVMM provides a range of services to include maintaining the resources you need to deploy VMs. For more information about the new features supported in SCVMM 2022, see What's new in System Center Virtual Machine Manager.

Support for configuring maximum concurrent provisioning operations parameter on AWS. Citrix DaaS now supports `MaximumConcurrentProvisioningOperations` as a configurable custom property for MCS on AWS. `MaximumConcurrentProvisioningOperations` is the property that determines the number of VMs you can create or delete simultaneously. While MCS supports 100 maximum concurrent provisioning operations by default, you can now enter PowerShell commands to customize this value. You can enter a range from 1-1000. Setting this property to your

preferred value allows you to control the number of parallel tasks you can perform when creating or deleting VMs. For details about configuring the maximum concurrent provisioning operations, see Host Connection Default Values.

May 2022

New and enhanced features

Enhanced Session launch diagnostics. Citrix DaaS now supports detailed session launch failure diagnostics. You can now view the components involved in the session launch sequence. The components which failed with last generated error codes are highlighted. This helps identify the exact reason for a session launch failure and take the recommended action.

The Transaction page is extended with the Transaction Details panel that contains a list of components indicating the error occurrence. Clicking on the component name displays the Component Details and the Last Known Failure Details. The Failure Reason and Error Code are displayed. Clicking the Learn more link leads to the specific code on Error codes containing a detailed description and recommended action. For more information, see Session Diagnostics.

Support for using Set-ProvServiceConfigurationData in Remote PowerShell SDK. You can now run `Set-ProvServiceConfigurationData` using Remote PowerShell SDK to do the settings on all applicable parameters. You can also skip enabling DHCP during image preparation using this command. Following is the list of settings that is supported with `Set-ProvServiceConfigurationData`:

- Change Image Preparation Timeout: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- Skip Enable DHCP: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Ex -Value EnableDHCP`
- Skip Microsoft Windows KMS Rearm: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Skip Microsoft Office KMS Rearm: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`
- Disable preparation VM auto shutdown: `Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown –Value true`
- Disable domain injection: `Set-ProvServiceConfigurationData –Name DisableDomainInjection –Value true`

Ability to set the Linux license type when creating Linux machine catalogs using PowerShell commands. Using PowerShell commands, you can set the Linux license type when creating Linux machine catalogs. You have two choices for bring-your-own Linux licenses: RHEL_BYOS and SLES_BYOS. The setting defaults to Azure Linux licensing. For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for identifying all Azure resources created by MCS. You can now identify all Azure resources created by MCS such as Image, ID disk, OS disk, NIC, VM, and so on that are associated with a ProvScheme using a tag called `provschemeID`. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for Azure Stack HCI provisioning through SCVMM. MCS now supports Azure Stack HCI provisioning through Microsoft System Center Virtual Machine Manager (SCVMM). You can manage the Azure stack HCI cluster with your existing tools including SCVMM. For more information, see Microsoft System Center Virtual Machine Manager virtualization environments.

Support for adding non-Active Directory users manually. Using the Full Configuration management interface, you can now enter a semicolon-separated list of user names when adding non-Active Directory users for a catalog. Consider the format when adding users that reside in different directories. For example, if the users are in Active Directory, enter the names directly. If not, enter the names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`. For more information, see Create machine catalog.

April 2022

New and enhanced features

Home page for the Full Configuration interface. Full Configuration now has a home page, which provides an overview of your Citrix DaaS deployment and workloads along with information that helps you get the most from your subscription. The page comprises the following parts:

- **Service overview**. Provides an overview of your Citrix DaaS deployment and workloads.
- **Recommendations**. Recommends features that are available with your subscription and collects your feedback.
- **What's new**. Shows the latest features.
- **Preview features**. Shows features that are currently in preview.
- **Get started**. Shows steps to guide you through the initial setup.

For more information, see Home page.

Show the progress of catalog creation and updates. Full Configuration now lets you stay up to date on catalog creation and updates. You can gain an overview of the creation and update process, view

the history of steps performed, and monitor the progress and running time of the current step. For more information, see Start creating the catalog.

Display available hypervisors and cloud services based on the selected zone. In Full Configuration, when creating hosting connections, you're required to select a zone before selecting a connection type. The Connection type drop-down list displays hypervisors and cloud services available with the zone. Previously, to ensure the Connection type list shows a required hypervisor or cloud service, you had to install its plug-in in every zone. With this new configuration sequence, you can now install the plug-in only in the required zone.

You can also use PowerShell command to get the list of hypervisor plug-in available with the selected zone. For more information, see Create a connection and resources.

Support for non-on-premises-AD-joined users in Full Configuration. A new field, **Select identity type**, is available in the interfaces where you assign users to provisioned desktops or apps, delivery groups, or application groups. With the field, you can now select user accounts from any of the following identity providers to which your Citrix Cloud is connected:

- Active Directory
- Azure Active Directory
- Okta

Ability to reject invalid custom properties in Google Cloud Platform (GCP) and Azure environments. You can now avoid potential confusion if custom properties set at `New-ProvScheme` and `Set-ProvScheme` do not take effect. If you specify non-existing custom property or properties, you get an error message. For more information, see Important consideration about setting custom properties.

Support for creating Azure Active Directory joined machines. In **Full Configuration**, when you create a catalog, an **Azure Active Directory joined** identity type, is now available in **Machine Identities**. With that identity type, you can use MCS to create machines that are joined to Azure Active Directory. You also have an extra option, **Enroll the machines in Microsoft Intune**, to enroll the machines in Microsoft Intune for management.

For information about creating Azure Active Directory joined catalogs, see Create machine catalogs. For information about requirements and considerations related to Azure Active Directory join, see Azure Active Directory joined.

Support for creating hybrid Azure Active Directory joined machines. In **Full Configuration**, when you create a catalog, a **Hybrid Azure Active Directory joined** identity type, is now available in **Machine Identities**. With that identity type, you can use MCS to create hybrid Azure Active Directory joined machines. Those machines are owned by an organization and signed into with an Active Directory Domain Services account that belongs to that organization.

For information about creating hybrid Azure Active Directory joined catalogs, see Create machine cata-

logs. For information about requirements and considerations related to hybrid Azure Active Directory join, see Hybrid Azure Active Directory joined.

Azure trusted launch support for snapshots. In addition to images, Azure trusted launch is now available for snapshots as well. If you select a snapshot with trusted launch enabled, using a machine profile is mandatory. Also, you must select a machine profile with trusted launch enabled. For more information, see Microsoft Azure Resource Manager cloud environments.

Export machines. You can now export machines listed on the **Machines** page of the **Machine Catalog Setup** wizard to a CSV file, to be used as a template when adding machines to a catalog in bulk. For more information, see Export machines from a catalog.

Option to access Workspace Environment Management web console. An option, Environment Management (Web), is now available in the menu of the **Manage** tab. The option takes you to the new, web-based Workspace Environment Management console. To access the legacy console, use **Environment Management**. We are in the process of migrating the full set of functionalities from the legacy console to the web console. The web console generally responds faster than the legacy console. For more information, see Workspace Environment Management service.

Ability to manage ProvScheme parameters. When you use MCS to create a catalog, you will now get an error if you set the `New-ProvScheme` parameters in unsupported hypervisors during machine catalog creation or update `Set-ProvScheme` parameters after machine catalog is created. For more information, see Create machine catalogs.

Increased resource location limits. Resource location limits for single-session VDAs and multi-session VDAs are now increased to 10000 and 1000 respectively. For more information, see Limits.

Support for restarting non-power managed machines after draining all sessions. Citrix DaaS now allows you to create restart schedules for machines that are not power managed after all sessions are drained from the machines. In the Full Configuration interface, select **Restart all machines after draining all sessions** as the **Restart duration**. For more information, see Create a restart schedule.

Support for upgrading VDA machines (preview). Using the Full Configuration interface, you can now upgrade VDA machines for your Citrix DaaS deployment. You can upgrade them on a per-catalog or a per-machine basis. The feature applies to machines that are not created using MCS (for example, physical machines). For more information, see Upgrade VDAs using the Full Configuration interface.

Machines are not shut down during outages. Citrix DaaS now prevent virtual machines from being shut down by the broker when the zone that the machines are in experiences an outage. The machines automatically become available for connections when the outage ends. You don't have to take any action to make the machines available after the outage.

Session launch diagnostics. Citrix DaaS now supports enhanced session launch failure diagnostics. Use the Citrix Workspace app-generated 32-digit (8-4-4-4-12) Transaction ID from inside Citrix Monitor (that is, Citrix Director service) to narrow down to the exact component and stage where the problem

occurred and apply the recommended actions to resolve the issue. For more information, see Session launch diagnostics.

Option to access the Session Recording service. An option, Session Recording, is now available in the menu of the **Manage** tab. The introduction of the Session Recording service provides centralized management of policies, playback, and server configurations. It eases the burden on IT administrators by providing a unified entry point to manage and observe the distributed objects across your organization. For more information, see Session Recording service (preview).

Rebranded Citrix Virtual Apps and Desktops service. **Citrix Virtual Apps and Desktops service** has been renamed to **Citrix DaaS**. Learn more about the name change at our announcement on our blog.

The following offerings of Citrix Virtual Apps and Desktops service have been renamed.

- **Citrix Virtual Apps service Advanced** renamed to **Citrix DaaS Advanced**.
- **Citrix Virtual Apps service Premium** renamed to **Citrix DaaS Premium**.
- **Citrix Virtual Desktops service** renamed to **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Advanced** renamed to **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Premium** now available as **Citrix DaaS Premium and Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard for Azure** renamed to **Citrix DaaS Standard for Azure**.
- **Citrix Virtual Apps and Desktops Standard for Google Cloud** renamed to **Citrix DaaS Standard for Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium for Google Cloud** renamed to **Citrix DaaS Premium for Google Cloud**.

Implementing this transition in our products and their documentation is an ongoing process. Your patience during this transition is appreciated.

- The product UI, in-product content, and the images and instructions in product documentation will be updated in the coming weeks.
- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product documentation might still contain former names.

> **Note:**
>
> The on-premises **Citrix Virtual Apps and Desktops** product name remains the same.

Tenant support in Full Configuration. You can now create configuration partitions within a single Citrix DaaS instance. You achieve that by creating tenant scopes in **Administrators > Scopes** and

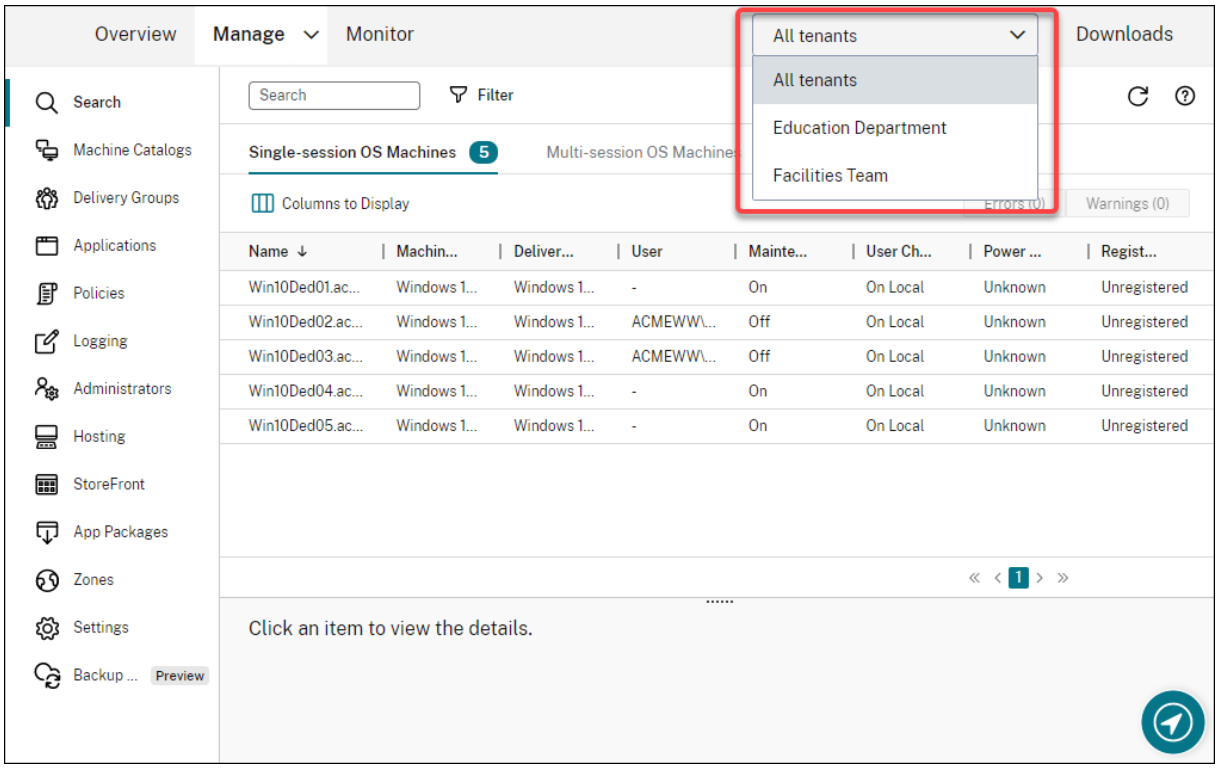
associating related configuration objects, such as machine catalogs and delivery groups, with those tenants. As a result, administrators with access to a tenant can manage only objects that are associated with the tenant. This feature is useful, for example, if your organization:

- Has different business silos (independent divisions or separate IT management teams) or
- Has multiple on-premises sites and wants to maintain the same setup in a single Citrix DaaS instance.

Also, the Full Configuration interface lets you filter tenant customers by name. By default, the interface displays information about all tenants.

The feature is available for both Citrix Service Providers (CSPs) and non-CSPs. The interface in a CSP environment is essentially the same as that in a non-CSP environment except for the method used to create tenants.

- CSPs onboard tenant customers to Citrix DaaS and then configure administrator access to Citrix DaaS. For more information, see Citrix DaaS for Citrix Service Providers.
- Non-CSPs create tenant customers by first creating scopes and then configuring custom access for respective administrators. For more information, see Create and manage scopes.



Updates for Autoscale. We have updated Autoscale with a blade style to bring you a better user experience. The workflows for configuring your settings remain the same. Other updates to Autoscale include:

- Renamed **Restrict Autoscale** to **Autoscaling Tagged Machines** to make it easy to understand.

- Added a new option, **Control when Autoscale starts powering on tagged machines**. The option lets you control when Autoscale starts powering on tagged machines based on the usage of untagged machines.

For more information on autoscaling tagged machines, see Autoscale tagged machines.

License validity checks. The Full Configuration interface now automatically checks the validity of licenses in use by host connections. A host connection is placed into maintenance mode if its license is invalid. As a result, you cannot perform certain operations, such as editing the connection and turning off maintenance mode. A license becomes invalid, for example, when:

- The license has expired. In this case, contact your Citrix sales representative to renew it or to purchase new licenses.
- The license has been deleted from the License Server.

Blade style applied to the Machine Catalogs and Policies nodes. Blade styles are now applied to all nodes of Full Configuration.

Support for updating MCS provisioned machines in Azure environments. `Set-ProvScheme` changes the template (provisioning scheme) and does not affect existing machines. Using RequestProvVMUpdate command, you can now apply the current provisioning scheme to an existing machine (or set of machines). Currently, the property update supported by this feature is `ServiceOffering`. For more information, see Update provisioned machines to current provisioning scheme state.

March 2022

New and enhanced features

Citrix Virtual Apps and Desktops for Google Cloud available on Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium for Google Cloud is now available for purchase on Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium for Google Cloud runs the Citrix Virtual Apps and Desktops service control plane on Google Cloud.

Azure trusted launch support. Azure trusted launch is now available for the Full Configuration management interface. If you choose to select an image with trusted launch enabled, using a machine profile is mandatory. Also, you must select a machine profile with trusted launch enabled. For more information, see Microsoft Azure Resource Manager cloud environments.

Blade style applied to wizards in three more nodes in Full Configuration. The nodes are **Search**, **Delivery Groups**, and **Applications**.

Image Portability Service (IPS) has been released for general availability. IPS simplifies the management of images across platforms. This feature is useful for managing images between an on-premises Resource Location and the public cloud. The Citrix Virtual Apps and Desktops REST APIs

can be used to automate the administration of resources within a Citrix Virtual Apps and Desktops site. For more information, see Migrate workloads to public cloud.

February 2022

New and enhanced features

Azure permissions. There are two sets of permissions required for security requirements and to minimize risk.

- Minimum permissions: This set of permissions gives better security control. However, new features that require additional permissions will fail because of using minimum permissions.
- General permissions: This set of permissions does not block you from getting new enhancement benefit.

For more information, see About Azure permissions.

Support for using VM's temporary disk to host the write-back cache disk in Azure environments. We added an option, **Use non-persistent write-back cache disk**, to the **Machine Catalog Setup > Disk Settings** page of the **Manage > Full Configuration** interface. Select that option if you do not want the write-back cache disk to persist for the provisioned VMs. With the option selected, we use the VM's temporary disk to host the write-back cache disk if the temporary disk has sufficient space. Doing that reduces your costs. For more information, see Microsoft Azure Resource Manager cloud environments.

Updates to AWS host connection default settings. The AWS host connection default setting values are updated to higher values and most likely same for all AWS cloud platform setup. This helps to create host connections in AWS cloud environments, without evaluating and configuring the default setting values according to individual setup. For more information, see Host connection default values.

Added support for different storage tiers in GCP environments. You can now provide the following custom properties in the GCP environments to set the storage type of the disks attached to the newly created VM:

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

For more information, see Citrix Virtual Apps and Desktops Service SDK.

Change certain VM settings after creating Azure VM catalogs. Using the Full Configuration management interface, you can now change the following settings after creating a catalog:

- Machine size

- Availability zones
- Machine profile
- Windows licenses

To do that, on the **Machine Catalogs** node, select the catalog and then select **Edit Machine Catalog** in the action bar. For more information, see Edit a catalog.

Support for storing Azure ephemeral OS disk either on the cache disk or temporary disk. Citrix Virtual Apps and Desktops service now allows you to store the Azure ephemeral OS disk either on cache disk or temporary disk for an Azure-enabled virtual machine. This functionality is useful for Azure environments that require a higher performant SSD disk over a standard HDD disk. For more information, see Microsoft Azure Resource Manager cloud environments.

Support for Nutanix clusters on AWS. Citrix Virtual Apps and Desktops service supports Nutanix Clusters on AWS. Nutanix Clusters simplifies how applications are run on private or multiple public clouds. For more information, see Nutanix clusters on AWS.

Support for VMware cloud on Amazon Web Services (AWS). VMware cloud on Amazon Web Services (AWS) enables you to migrate VMware based on-premises Citrix workloads to AWS cloud and your core Citrix Virtual Apps and Desktops environment to Citrix Virtual Apps and Desktops service. For more information, see VMware cloud on Amazon Web Services (AWS).

Support for configuring write-back cache disk for machines running on Google Cloud Platform (GCP). In the Full Configuration management interface, when provisioning machines on GCP, you can now configure the following write-back cache disk settings:

- Disk size
- Memory allocated to cache
- Disk storage type
- Disk persistence

For more information, see Create a machine catalog in the Google Cloud Platform virtualization environments article.

January 2022

New and enhanced features

Support for Nutanix clusters on AWS. Citrix Virtual Apps and Desktops service now supports Nutanix clusters on AWS. This support provides the same functionality as a Nutanix on-premises cluster. Only a single cluster is supported, *Prism Element*. For more information, see Nutanix virtualization environments.

New features available in Cloud Health Check. Cloud Health Check has been updated to a new version with features including:

- **Automatic fix.** Cloud Health Check now supports automatically detecting and fixing certain issues identified on machines where it is running. There is now a results report to show you what specific actions were taken. For more information, see Automatic fix.
- **Command line support.** Cloud Health Check can now be run from the command line. For more information, see Running Cloud Health Check on the command line.
- **Citrix Universal Injection Driver status.** Cloud Health Check now shows the Citrix UVI driver status and has a related event log check for Citrix UVI drivers.
- **Session launch registry check.** Cloud Health check now checks for session launch registry settings.
- **Updates to check report.** For checked items that have several check points, the final check report now lists all the checks that have been verified to show what actions were performed during the health check.

For more information, see Cloud Health Check.

Troubleshoot VDA registration and session launch issues using Full Configuration. Using the Full Configuration management interface, you can now run checks that gauge the health of VDAs. VDA health checks identify possible causes for common VDA registration and session launch issues. You can run health checks individually and in batches. For more information, see VDA health checks.

Ability to specify the Azure secret expiration date for existing connections. Using the Full Configuration management interface, you can now specify the date after which the application secret expires. For guidance on how to view the expiration date of the secret, see Microsoft Azure Resource Manager cloud environments. When using this feature, consider the following differences:

- For service principals created manually in Azure, you can directly edit the expiration date on the **Edit Connection > Connection Properties** page.
- For first-time edits of the expiration date for service principals created through Full Configuration on your behalf, go to **Edit Connection > Edit settings > Use existing**. You can make subsequent edits on the **Edit Connection > Connection Properties** page.

A button to add administrators. We added a button, **Add Administrator**, to the **Full Configuration > Administrators > Administrators** tab. The button offers a quick way to go to **Identity and Access Management > Administrators**, where you can add (invite) administrators. For more information, see Add an administrator.

New look and feel of wizards in Full Configuration. We have updated the wizards in the following nodes with a new style, including colors, fonts, and other formatting changes, to bring you a better user experience: **Administrators**, **Hosting**, **StoreFront**, **App Packages**, **Zones**, and **Settings**. The new wizards appear in blade views with wider viewports, enabling more content to display. The workflows for configuring your settings remain the same.

Support for retaining system disk when MCS I/O is enabled for machines running on Google Cloud Platform (GCP). In the Full Configuration management interface, when provisioning machines on GCP, you can now retain system disk during power cycles when MCS storage optimization (MCS I/O) is enabled. For more information, see Enabling MCS storage optimization updates.

Support for direct upload or download from EBS on Amazon Web Services (AWS). AWS now provides API to allow direct creation of EBS volume with desired content. You can now use the API to eliminate volume worker requirement for catalog creation and VM addition. For information on AWS permissions required for this functionality, see Amazon Web Services cloud environments.

Ability to identify Amazon Web Services (AWS) resources created by MCS. We added a new tag named `CitrixProvisioningSchemeID` to identify AWS resources created by MCS. For more information, see Identify resources created by MCS.

Ability to configure access to Manage and Monitor. The Full Configuration management interface now provides you with additional options to control whether to grant custom roles access to **Manage** and **Monitor**. For more information, see Create and manage roles.

December 2021

New and enhanced features

Support for Google Cloud VMware Engine. The platform now enables you to migrate VMware based on-premises Citrix workloads to Google Cloud and your core Citrix Virtual Apps and Desktops environment to Citrix Virtual Apps and Desktops service. For more information, see Google Cloud Platform (GCP) VMware Engine support.

Ability to specify what account names start with when specifying a naming scheme. This release introduces an option to the **Machine Catalog Setup > Machine Identities** page of the Full Configuration management interface. The option lets you specify numbers or letters the account names start with, giving you more control over how machine accounts are named during catalog creation. For more information, see Machine identities.

Support for creating Nutanix AHV XI and Nutanix AHV Prism Central (PC) connections. In the Full Configuration management interface, you can now create Nutanix AHV XI and Nutanix AHV PC connections. For more information, see Nutanix virtualization environments.

Support for selecting the storage type for OS disks when provisioning VMs on GCP. In the Full Configuration management interface, when provisioning VMs on GCP, you can now select the storage type for the OS disk. Available storage options on the **Machine Catalog Setup > Storage** page include **Standard persistent disk**, **Balanced persistent disk**, and **SSD persistent disk**. For more information, see Create a machine catalog.

Full Configuration management interface now supports Azure ephemeral disk. Previously, PowerShell was your only choice to create machines that used ephemeral OS disks. We now add an option, **Azure ephemeral OS disk**, to the **Machine Catalog Setup > Storage and License Types** page. Select the option if you want to use the VM's local disk to host the operating system disk. For more information, see Create a machine catalog using an Azure Resource Manager image.

Protect Machine Creation Services (MCS) managed resources from accidental deletion. You can now protect MCS managed resources on the Google Cloud Platform (GCP) by applying GCP's `deletionProtection` flag enabled for the VMs. Using the `compute.instances.setDeletionProtection` permission or the IAM Compute Admin role, you can reset the flag to allow the resource to be deleted. This functionality is applicable for both persistent and non-persistent catalogs. For more information, see Protect accidental machine deletion.

November 2021

New and enhanced features

Annotate an image when updating machines. In the Full Configuration management interface, you can now annotate an image by adding a note for it when updating an MCS-created catalog. Each time you update the catalog, a note-related entry is created whether you add a note. If you update the catalog without adding a note, the entry appears as null (-). To view note history for the image, select the catalog, click **Template Properties** in the lower pane, and then click **View note history**. For more information, see Update a catalog.

Multi-type licensing support. The Full Configuration management interface now supports multi-type licensing, letting you specify which license entitlement you want your site (your deployment of a Citrix Virtual Apps and Desktops service product) or a delivery group to use.

- At the site level, you determine which license to use site wide when users launch an app or a desktop on their devices. The selected license applies to all delivery groups, except those configured with a different license.
- At a delivery group level, you determine which license you want the delivery group to use, enjoying the multi-type licensing flexibility and benefits.

For more information, see Multi-type licensing.

Support for displaying Azure Marketplace purchase plan information. In the Full Configuration management interface, when creating a machine catalog, you can now view purchase plan information for master images originated from Azure Marketplace images.

October 2021

New and enhanced features

Ability to update persistent MCS catalogs. We introduced the **Update Machines** option for persistent MCS catalogs in the Full Configuration management interface. The option lets you manage the image or template the catalog uses. When updating a persistent catalog, consider the following: Only machines you add to the catalog later are created using the new image or template. We do not roll out the update to existing machines in the catalog. For more information, see Update a catalog.

Option to provision VMs on an Azure dedicated host. We added an option, **Use a host group**, to the **Machine Catalog Setup > Master Image** page of the Full Configuration management interface. The option lets you specify which host group you want to use when provisioning VMs in Azure environments. For more information, see Create a machine catalog using an Azure Resource Manager image.

Improve performance by preserving a provisioned VM when power cycling. We added a setting, **Retain VMs across power cycles**, to the **Machine Catalog Setup > Disk Settings** page of the Full Configuration management interface. The setting lets you preserve a provisioned VM when power cycling in Azure environments. For more information, see MCS storage optimization. Alternatively, you can configure the feature by using PowerShell. For more information, see Preserving a provisioned virtual machine when power cycling.

Bind a machine catalog to a Workspace Environment Management configuration set. When creating a machine catalog, you can now bind it to a Workspace Environment Management configuration set. Doing so lets you use Workspace Environment Management service to deliver the best possible workspace experience to your users. You can also choose to bind the catalog after you create the catalog. For more information, see Create machine catalogs and Manage machine catalogs.

September 2021

New and enhanced features

Add informative description for image updates. You can now add informative descriptions about changes related to image updates for machine catalogs. This functionality is useful for administrators who want to add descriptive labels when updating an image used by a catalog, for example, *Office 365 installed*. Using PowerShell commands, you can create and view these messages. For details, see Adding descriptions to an image.

Azure VMware Solution (AVS) integration. Citrix Virtual Apps and Desktops service supports AVS, the Azure VMware Solution. AVS provides cloud infrastructure containing vSphere clusters created by Azure. Leverage the Citrix Virtual Apps and Desktops service to use AVS for provisioning your VDA

workload in the same way that you would using vSphere in on-premises environments. For more information, see Azure VMware Solution Integration.

Same resource group for multiple catalogs. You can now use the same resource group for updating and creating catalogs in Citrix Virtual Apps and Desktops service. This process:

- applies to any resource group that contains one or more machine catalogs.
- supports resource groups that are not created by Machine Creation Services.
- creates the VM and associated resources.
- deletes resources in the resource group when the VM or the catalog is removed.

For more information, see Azure Resource groups.

Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition. You can display information for an Azure VM, OS disk, snapshot, and gallery image definition. This information is displayed for resources on the master image when a machine catalog is assigned. Use this functionality to view and select either a Linux or Windows image. For more information, see Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition.

New update for Automated Configuration. Automated Configuration has been updated to a new version with features including:

- Machines Creation Services (MCS) support - Automated Configuration now supports MCS catalogs. For more information, see Understanding migrating Machine Creation Services provisioned catalogs.

Other updates to Automated Configuration include:

- Enhanced Zone support by pre-populating the ZoneMapping.yml file with the names of on-premises zones during export and cloud Resource Locations when backing up.
- StoreFront has been made a top level manageable component. Prior to this, StoreFront was managed as part of Delivery Groups. This separation better facilitates site merging.
- Changed `AddMachinesOnly` to `MergeMachines` to match the pattern for current and new merge options.
- Added the use of the SecurityClient.csv file to import the ClientId and Secret when creating and updating the CustomerInfo.yml when using the support cmdlets.
- Added User Zone Preferences migration.
- Fixed support for the Japanese Control Plane.
- Other fixes and improvements.

Download Automated Configuration at Citrix Downloads. For more information on Automated Configuration, see Migrate configuration to Citrix Cloud.

More scheduling options available with restart schedules. The Full Configuration management interface now provides you with additional options to control when scheduled restarts occur. In addi-

tion to the daily recurring restart schedules, you can now set weekly and monthly recurrence patterns. For more information, see Create a restart schedule.

Preserve custom columns that degrade performance. Previously, on the **Search** node of the Full Configuration management interface, custom columns that degraded performance disappeared after you refreshed the browser window or signed out of the console and then signed in. You can now control whether to preserve those custom columns. For more information, see Use Search in the Full Configuration management interface.

Use the Automated Configuration tool to back up and restore. We added a node, **Backup and Restore**, to the Full Configuration management interface. That node aggregates all resources related to the Automated Configuration tool, including information about:

- Scheduling automated backups of your Citrix Virtual Apps and Desktops configuration using a single command
- Restoring from a previous backup if necessary
- Performing backups and restores granularly
- Other use cases supported

For more information, see the Automated Configuration documentation.

Support for non-domain-joined catalogs. We added an identity type, **Non-domain-joined**, to the **Machine Catalog Setup > Machine Identities** page of the Full Configuration management interface. With that identity type, you can use MCS to create machines that are not joined to any domain. For more information, see Create machine catalogs.

Support for using a machine profile. We added an option, **Use a machine profile**, to the **Machine Catalog Setup > Master Image** page of the Full Configuration management interface. The option lets you specify which machine profile you want the VMs to inherit configurations from when creating VMs in Azure environments. The VMs in the catalog can then inherit configurations from the selected machine profile. Examples of configurations include:

- Accelerated networking
- Boot diagnostics
- Host disk caching (relating to OS and MCSIO disks)
- Machine size (unless otherwise specified)
- Tags placed on the VM

For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for Windows Server 2022. Requires minimum VDA 2106.

August 2021

New and enhanced features

Extend the number of sortable items from 500 to 5,000. On the **Search** node of the Full Configuration management interface, you can now sort up to 5,000 items by any column header. When the number of items exceeds 5,000, use filters to reduce the number of items to 5,000 or fewer to enable sorting. For more information, see Use Search in the Full Configuration management interface.

Support for additional Azure storage types. You can now select different storage types for virtual machines in Azure environments using MCS. For details, see Storage types.

Support for selecting the storage type for write-back cache disks. In the Full Configuration management interface, when creating an MCS catalog, you can now select the storage type for the write-back cache disk. Available storage types include: Premium SSD, Standard SSD, and Standard HDD. For more information, see Create machine catalogs.

Shut down suspended machines. In the **Manage > Full Configuration** interface, we added an option, **When no reconnection in (minutes)**, to the **Load-based Settings** page of the Manage Autoscale user interface for single-session OS delivery groups. The option becomes available after you select **Suspend**, letting you specify when to shut down the suspended machines. Suspended machines remain available to disconnected users when they reconnect but are not available for new users. Shutting the machines down makes them available again to handle all workloads. For more information, see Autoscale.

Extended support for using CSV files to bulk add machines to a catalog. In the **Manage > Full Configuration** interface, you can now use a CSV file to bulk add machines already in your data center to a catalog where those machines are power managed. For more information, see Create machine catalogs and Manage machine catalogs.

July 2021

New and enhanced features

Configuration logging. The **Logging** user interface has changed in **Manage > Full Configuration**. The following three tabs comprise the interface:

- **Events** (formerly, configuration logging). This tab lets you track configuration changes and administrative activities.
- **Tasks**. This tab lets you view tasks related to machine catalog operations.
- **APIs**. This tab lets you view REST API requests made during a certain time period.

For more information, see Configuration logging.

Autoscale now provides you with dynamic session timeout options. You can configure disconnected and idle session timeouts for your peak and off-peak usage times to achieve faster machine draining and cost savings. For more information, see Dynamic session timeouts.

Support for Google Cloud Platform (GCP) Customer Managed Encryption Keys (CMEK). You can now use Google's CMEK with MCS catalogs. CMEK provides greater control over keys used to encrypt data within a Google Cloud project. For more information, see Customer-managed encryption keys (CMEK). To configure this feature, see Using Customer Managed Encryption Keys (CMEK). The feature is available on the **Machine Catalog Setup > Disk Settings** page of the **Manage > Full Configuration** interface.

> **Note:**
>
> This feature is available as a preview.

Updates to the Manage tab. We have updated options in the menu of the **Manage** tab:

- **Full Configuration**: Previously, this option took you to the legacy console. It now takes you to the new, web-based console (Web Studio). The web-based console has full parity with the legacy console and includes several enhancements. We recommend that you start using it now.
- **Legacy Configuration**: This option takes you to the legacy console, which is scheduled for removal in September 2021. After that, **Full Configuration** will be the only interface that offers access to the full range of configuration and management actions.

Web Studio now supports choosing a power management connection for a Remote PC Access catalog. Previously, you were able to use Studio to create a Wake on LAN host connection to your resource location (selecting **Remote PC Wake on LAN** as the connection type). However, PowerShell was your only choice to associate that connection with a Remote PC Access catalog. You can now use Studio to achieve that. For more information, see Configure Wake on LAN in the Full Configuration interface.

June 2021

New and enhanced features

Access Azure Shared Image Gallery images. When creating a machine catalog, you can now access images from the Azure Shared Image Gallery on the Master Image screen. For details, see Access images from Azure Shared Image Gallery.

Support shielded virtual machines on Google Cloud Platform (GCP). You can provision shielded virtual machines on GCP. A shielded virtual machine is hardened by a set of security controls that provide verifiable integrity of your Compute Engine instances, using advanced platform security capabilities like secure boot, a virtual trusted platform module, UEFI firmware and integrity monitoring. For more information, see Shield VMs.

Enforce either HTTPS or HTTP. Use registry settings to enforce HTTPS or HTTP traffic through the XML service.

Always use standard SSD for an identity disk to reduce cost in Azure environments. Machine catalogs use the standard SSD storage type for identity disks. Azure standard SSDs are a cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels. For more information about storage types, see Azure Resource Manager master image.

> **Note:**
>
> For more information about Azure managed disk pricing, see Managed Disks pricing.

New feature available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports authenticating to Azure to create a service principal**. You can now establish a host connection to Azure by authenticating to Azure to create a service principal. This support eliminates the need to manually create a service principal in your Azure subscription before creating a connection in Studio. For more information, see Microsoft Azure Resource Manager virtualization environments.
- **Studio now supports cloning of existing machine catalogs**. This feature enables you to clone an existing machine catalog to use as a template for a new one, eliminating the need to create a similar catalog from scratch. When cloning a catalog, you cannot change settings associated with operating system and machine management. The cloned catalog inherits those settings from the original. For more information, see Clone a catalog.
- **A new node called Settings now available in the Studio navigation pane**. The **Settings** node lets you configure settings that apply to the entire site (your deployment of a Citrix Virtual Apps and Desktops service product). The following settings are available:
  - **Load balance multi-session catalogs**. Select the load balancing option that meets your needs. This setting applies to all your catalogs. Previously, you accessed this feature by clicking the gear icon in the upper right corner of the console. For more information, see Load balance machines.
- **Enhanced search experience in Studio**. This release enhances your Studio search experience. When you use filters to perform an advanced search, the Add filters window appears in the foreground, leaving the background view unchanged. For more information, see Use Search in the Full Configuration management interface.
- **Ability to suspend and resume Google Cloud VMs in MCS**. You can now suspend and resume Google Cloud VMs in MCS as you would any VM. For details, see Manage delivery groups. To enable this ability, set the `compute.instances.suspend` and `compute.instances.resume` permissions in the Google Cloud service account. The Compute Admin role comes with these permissions.

In Citrix Virtual Apps and Desktops, you can also use the `New-BrokerHostingPowerAction` PowerShell command to suspend and resume the VMs. For details, see New-Brokerhostingpoweraction.

Google Cloud enforces some limitations on the type and configuration of instances that can be suspended. For additional information, refer to Suspending and resuming an instance on the Google Cloud site.

May 2021

New and enhanced features

Session reconnection after disconnect from machine in maintenance mode. Previously, when pooled (random) single-session desktop (VDI) users were disconnected from a machine in maintenance mode, session reconnection was not allowed to any machine in the pool. Multi-session and static single-session machines always allowed session reconnection in that circumstance.

Now, using PowerShell, you can control at the delivery group level whether session reconnection is allowed after a disconnect occurs on a machine in maintenance mode. This applies to all VDAs in the group (single-session and multi-session).

For details, see Control session reconnection when disconnected from machine in maintenance mode.

Application probing and Desktop probing support in all Citrix Virtual Apps and Desktops Service editions. In addition to the existing **Premium** edition support, Application probing and Desktop probing are now available in **Citrix Virtual Apps Advanced Service** and **Citrix Virtual Apps and Desktops Advanced Service** editions.

New feature available in Web Studio. The following feature is now available in the web-based console:

- **Studio now supports selecting Azure Availability Zones**. Previously, PowerShell was your only choice to provision machines into a specific Availability Zone in Azure environments. When using Studio to create a machine catalog, you can now select one or more Availability Zones into which you want to provision machines. If no zones are specified, Machine Creation Services (MCS) lets Azure place the machines within the region. If more than one zone is specified, MCS randomly distributes the machines across them. For more information, see Provision machines into specified availability zones.

Azure emphemeral disk. Citrix Virtual Apps and Desktops service supports Azure ephemeral disk. An ephemeral disk allows you to repurpose the cache disk to store the OS disk for an Azure-enabled virtual machine. This functionality is useful for Azure environments that require a higher performant SSD disk over a standard HDD disk.

> **Note:**
>
> Persistent catalogs do not support ephemeral OS disks. Also, when using this feature, consider that the extra performant disk incurs an extra cost. It's beneficial to reuse the cache disk to store the OS disk instead of paying for an extra managed disk.

Ephemeral OS disks require that your provisioning scheme use managed disks and a Shared Image Gallery. For more information, see Azure ephemeral disks.

Improved performance for MCS managed VDAs on Azure. The Citrix Virtual Apps and Desktops service improves performance for VDAs managed with Machine Creation Services (MCS) on Azure. This enhancement changes the default values for *Absolute Simultaneous actions* for the hosting connection to 500, and *Maximum new actions per minute* for the hosting connection to 2,000. No manual configuration tasks are required to take advantage of this enhancement. For details, see Azure throttling.

New features available in Cloud Health Check. Cloud Health Check has been updated to a new version with features including:

- **Automatically discovering VDA machines**. Cloud Health Check can now automatically discover and retrieve VDAs from your Citrix Virtual Apps and Desktops service deployments. For more information, see Retrieve VDA machines.
- **Scheduling health checks**. Cloud Health Check now lets you set up schedules for performing periodic health checks. For more information, see Cloud Health Check scheduler.
- **Cloud Health Check version information**. You can now check which version of Cloud Health Check you are using. To view version information, click the gear icon in the upper right corner of the Cloud Health Check main window.
- **Automatic fix**. Cloud Health Check now supports automatically detecting and fixing certain issues identified on machines where it is running. For more information, see Automatic fix.

  > **Note:**
  >
  > Automatic fix is available as a preview.

April 2021

New and enhanced features

Retreive dynamic instances using AWS API. The Citrix Virtual Apps and Desktops service now queries AWS to retrieve instance types dynamically. This functionality removes the need to create a custom `InstanceTypes.xml` file for those customers wishing to use machine sizes beyond

those defined in Citrix Virtual Apps and Desktops service. This information was previously supplied by the `InstanceTypes.xml` file. To facilitate this dynamic access to the available AWS instance types, users must update the permissions on their service principals to include `ec2:DescribeInstanceTypes` permissions. To support backward compatibility for customers who choose not to update their service principal permissions, the AWS instance types listed in the `InstanceTypes.xml` are used. This process generates a warning message to the MCS CDF log.

> **Note:**
>
> Citrix Studio does not display the warning message contained in the CDF log.

For more information about permissions, see Defining IAM permissions and About AWS permissions.

New feature available in Web Studio. The following feature is now available in the web-based console:

- **Studio now displays date and time of your time zone**. Previously, Studio displayed only date and time based on the system clock and time zone. Studio now supports displaying date and time local to your time zone when you hover the mouse pointer over an event item. The time is expressed in UTC.

MCS I/O support for Azure VMs without temporary storage. MCS I/O now supports machine catalog creation for VMs that do not have temporary disks or attached storage. With this support:

- The snapshot (managed disk) is retrieved from the source VM *without* temporary storage. The VMs in the machine catalog have no temporary storage.
- The snapshot (managed disk) is retrieved from the source VM *with* temporary storage. The VMs in the machine catalog have temporary storage.

For more information, see Machine Creation Services (MCS) storage optimization

New feature available in Web Studio. The following feature is now available in the web-based console:

- **Force log off**. Autoscale now lets you log off sessions existing on machines by force when the established grace period is reached, making the machine eligible for shutdown. Doing that enables Autoscale to power off machines much faster, thus reducing costs. You can send notifications to users before they are logged off. For more information, see Autoscale.

New update for Automated Configuration. Automated Configuration has been updated to a new version with features including:

- **Merging multiple sites** –you can merge multiple sites into a single site while avoiding name collisions using prefixes and suffixes. For more information, see Merging multiple sites into a single site.

- **Site activation** –you can select whether your on-premises or cloud deployment controls resources such as reboot schedules and power schemes. For more information, see Activating sites.

Other updates to Automated Configuration include:

- The ability to migrate administrator roles and scopes.
- A `Quiet` parameter for select cmdlets to suppress console logging.
- A `SecurityFileFolder` parameter to allow placing of the CvadAcSecurity.yml file in a secure network file share that requires authentication.
- The ability to filter by machine name in machine catalogs and delivery groups.
- Improvements to component selection parameters to use the switch parameter method, eliminating the need to add a `$true` after the component name.
- A new cmdlet (`New-CvadAcZipInfoForSupport`) to zip all your log files to send to Citrix for support.

Download Automated Configuration at Citrix Downloads. For more information on Automated Configuration, see Migrating to cloud.

Preserve GCP instances across power cycles. Non-persistent Google Cloud Platform (GCP) instances are no longer deleted when powering off. Instead, the instances are preserved across power cycles. When a non-persistent instance is powered off, the OS disk is detached and deleted. When the instance is powered on, the OS disk is recreated from the base disk, and attached to the existing instance.

Support for Azure Gen2 images. You can now provision a Gen2 VM catalog by using either a Gen2 snapshot or a Gen 2 managed disk to improve boot time performance. For more information, see Create machine catalogs. The following operating systems are supported for Azure Gen2 images:

- Windows Server 2019, 2016, 2012 and 2012 R2
- Windows 10

> **Note:**
>
> Creating a Gen2 machine catalog using a Gen1 snapshot, or managed disk, is not supported. Similarly, creating a Gen1 machine catalog using a Gen2 snapshot, or managed disk, is also not supported. For more information, see Support for generation 2 VMs on Azure.

Disabling table storage accounts. Machine Creation Services (MCS) no longer creates table storage accounts for catalogs that use managed disks when provisioning VDAs on Azure. For more information, see Azure table storage.

Eliminating locks in storage accounts. When creating a catalog in Azure using a managed disk, a storage account is no longer created. Storage accounts created for existing catalogs remain unchanged. This change is applicable for managed disks only. For unmanaged disks, there is no change in the existing behavior. Machine Creation Services (MCS) continues creating storage accounts and locks.

New features available in Web Studio. The following features are now available in the web-based console:

- **Use a customer-managed encryption key to encrypt data on machines**. Studio now adds a setting called **Customer-managed encryption key** to the **Machine Catalog Setup > Disk Settings** page. The setting lets you choose whether to encrypt data on the machines to be provisioned in the catalog. For more information, see Customer-managed encryption key.
- **Studio now supports restricting Autoscale to tagged machines**. Previously, you had to use PowerShell to restrict Autoscale to certain machines in a delivery group. You can now also use Studio. For more information, see Restrict Autoscale to certain machines in a delivery group.

March 2021

New and enhanced features

Azure dedicated hosts. Azure dedicated hosts allow you to provision virtual machines on hardware dedicated to a single customer. While using a dedicated host, Azure ensures that your virtual machines would be the only machines running on that host. This provides more control and visibility to customers thereby ensuring they meet their regulatory or internal security requirements. A pre-configured Azure host group, in the region of the hosting unit, is required when using the `HostGroupId` parameter. Also, Azure auto-placement is required. For more information, see Azure dedicated hosts.

> **Tip:**
>
> When using Azure dedicated hosts, selecting the **Azure Availability Zone** has no effect. The virtual machine is placed by the Azure auto-placement process.

Support for Azure server side encryption. Citrix Virtual Apps and Desktops service supports customer-managed encryption keys for Azure managed disks. With this support you can manage your organizational and compliance requirements by encrypting the managed disks of your machine catalog using your own encryption key. For more information, see Azure server side encryption.

Provision machines into specified availability zones on Azure. You can now provision machines into a specific availability zone in Azure environments. With this functionality:

- You can specify one or multiple Availability Zones on Azure. Machines are nominally equally distributed across all provided zones if more than one zone is provided.

- The virtual machine and the corresponding disk are placed in the specified zone (or zones).
- You can browse Availability Zones for a given service offering or region. Valid Availability Zones are displayed using PowerShell commands. View service offering inventory items using `Get-Item`.

For more information, see Provision machines into specified availability zones on Azure.

New features available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports associating apps with custom icons**. Previously, you had to use PowerShell to add custom icons for use with published applications. You can now also use Studio to do that. For more information, see Manage application groups.
- **Studio now supports applying tags to machine catalogs**. Previously, you might use Studio to create or delete tags for use with a catalog. However, you had to use PowerShell to apply tags to the catalog. You can now also use Studio to apply or remove a tag to or from a catalog as you do with delivery groups. For more information, see Apply tags to machine catalogs.
- **Studio now supports switching between "horizontal load balancing"and "vertical load balancing"modes**. Previously, PowerShell was your only choice to switch between horizontal and vertical load balancing modes. Studio now gives you more flexibility to control how to load balance multi-session OS machines. For more information, see Load balance machines.
- **Studio now supports including machines in maintenance mode in restart schedules**. Previously, PowerShell was your only choice to configure scheduled restarts for machines in maintenance mode. You can now also use Studio to control whether to include those machines in a restart schedule. For more information, see Create a restart schedule.
- **Studio now supports configuring Wake on LAN for Remote PC Access**. Previously, you had to use PowerShell to configure Wake on LAN for Remote PC Access. You can now also use Studio to configure the feature. For more information, see Configure Wake on LAN.
- **Studio now supports applying AWS instance properties and tagging operational resources**. When creating a catalog to provision machines in AWS by using MCS, you can specify whether to apply the IAM role and tag properties to those machines. You can also specify whether to apply machine tags to operational resources. You have the following two options:

  - **Apply machine template properties to virtual machines**
  - **Apply machine tags to operational resources**

  For more information, see Applying AWS instance properties and tagging operational resources.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops service supports Azure Shared Image Gallery as a published image repository for MCS provisioned machines in Azure. Administrators have the option of storing an image in the gallery to accelerate the creation and hydration of OS disks. This

process improves the boot and application launch times for non-persistent VMs. For details about this feature, see Azure shared image gallery.

> **Note:**
>
> Shared Image Gallery functionality is compatible with managed disks. It is not available for legacy machine catalogs.

Storage buckets created in same Google Cloud Platform region as the machine catalog. In previous releases, MCS created temporary storage buckets during provisioning as part of the disk upload process. These buckets spanned multiple regions, which Google defines as a large geographic area containing two or more geographic places. These temporary buckets resided in the United States geographic location, no matter where the catalog was provisioned. MCS now creates storage buckets in the same region where you provision your catalogs. Storage buckets are no longer temporary; they remain in your Google Cloud Platform project after you complete the provisioning process. Future provisioning operations use the existing storage bucket, if one exists in that region. A new storage bucket is created if one does not exist in the specified region.

February 2021

New and enhanced features

Support for Azure Gen2 images. You can now provision managed disks using Gen2 VMs in Azure environments to improve boot time performance. The following operating systems are supported:

- Windows Server 2019, 2016, 2012 and 2012 R2
- Windows 10

> **Note:**
>
> With this support, only a subset of VMs is supported. For example, some VMs can be both Gen1 and Gen2 types, while other VMs can only be Gen1. For more information, see Support for generation 2 VMs on Azure.

Machine restart schedules. Citrix Studio now adds an option called **Restart all machines after draining sessions** to the **Restart duration** menu. The option lets you choose whether to restart all machines after draining all sessions. When the restart time is reached, machines are put into the drain state and restarted when all sessions are logged off. For more information, see Create a restart schedule.

New features available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports using CSV files to bulk add machines to a catalog**. This feature enables you to use a CSV file to:
  - Bulk add machines to a multi-session or single-session OS catalog where machines are not power managed through Studio.
  - Bulk add machines to a Remote PC Access catalog. Previously, you had to choose OUs to bulk add machines to a Remote PC Access catalog. Doing that, however, is not easy in scenarios with OU structure restrictions. The feature gives you more flexibility to bulk add machines. You can add only machines (for use with user auto-assignments) or add machines along with user assignments.

  For more information, see Create machine catalogs and Manage machine catalogs.
- **Extended support for Citrix Managed Azure.** Citrix Managed Azure is now available in the following Citrix Virtual Apps and Desktops service editions: Standard for Azure, Advanced, Premium, and Workspace Premium Plus.
- **Support for placing master images in Azure Shared Image Gallery**. Studio now provides you an option to place master images in Azure Shared Image Gallery (SIG). SIG is a repository for managing and sharing images. It lets you make your images available throughout your organization. We recommend that you store a master image in SIG when creating large non-persistent machine catalogs because doing that enables faster reset of VDA OS disks. For more information, see Microsoft Azure Resource Manager virtualization environments.
- **Retain system disk for MCS machine catalogs in Azure**. Studio now lets you control whether to retain system disks for VDAs during power cycles. Ordinarily, the system disk is deleted on shutdown and recreated on startup. This ensures that the disk is always in a clean state but results in longer VM restart times. If system writes are redirected to the cache and written back to the cache disk, the system disk remains unchanged. To avoid unnecessary disk recreation, use the **Retain system disk during power cycles** option, available on the **Machine Catalog Setup > Disk Settings** page. Enabling the option reduces VM restart times but increases your storage costs. The option can be useful in scenarios where an environment contains workloads with sensitive restart times. For more information, see MCS storage optimization.
- **Studio now supports creating MCS machine catalogs with persistent write-back cache disk**. Previously, PowerShell was your only choice to create a catalog with persistent write-back cache disk. You can now use Studio to control whether the write-back cache disk persists for the provisioned VMs in Azure when you are creating a catalog. If disabled, the write-back cache disk is deleted during each power cycle to save storage costs, causing any data redirected to the disk to be lost. To retain the data, enable the **Use persistent write-back cache disk** option, available on the **Machine Catalog Setup > Disk Settings** page. For more information, see MCS storage optimization.

Support for App protection for Citrix Virtual Apps and Desktops Service with StoreFront. For

more information, see the App protection.

January 2021

New features available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports associating apps with custom icons**. Previously, you had to use PowerShell to add custom icons for use with published applications. You can now also use Studio to do that. For more information, see Manage application groups.
- **Studio now supports applying tags to machine catalogs**. Previously, you might use Studio to create or delete tags for use with a catalog. However, you had to use PowerShell to apply tags to the catalog. You can now also use Studio to apply or remove a tag to or from a catalog as you do with delivery groups. For more information, see Apply tags to machine catalogs.
- **Studio now supports switching between "horizontal load balancing"and "vertical load balancing"modes**. Previously, PowerShell was your only choice to switch between horizontal and vertical load balancing modes. Studio now gives you more flexibility to control how to load balance multi-session OS machines. For more information, see Load balance machines.
- **Studio now supports including machines in maintenance mode in restart schedules**. Previously, PowerShell was your only choice to configure scheduled restarts for machines in maintenance mode. You can now also use Studio to control whether to include those machines in a restart schedule. For more information, see Create a restart schedule.
- **Studio now supports configuring Wake on LAN for Remote PC Access**. Previously, you had to use PowerShell to configure Wake on LAN for Remote PC Access. You can now also use Studio to configure the feature. For more information, see Configure Wake on LAN.
- **Studio now supports applying AWS instance properties and tagging operational resources**. When creating a catalog to provision machines in AWS by using MCS, you can specify whether to apply the IAM role and tag properties to those machines. You can also specify whether to apply machine tags to operational resources. You have the following two options:

  - **Apply machine template properties to virtual machines**
  - **Apply machine tags to operational resources**

  For more information, see Applying AWS instance properties and tagging operational resources.
- **AWS dedicated host**. Citrix Studio now adds an option called **Use dedicated host** to the **Machine Catalog Setup > Security** page. This setting is suitable for deployments with licensing restrictions or security requirements that need your use of a dedicated host. With a dedicated host, you own an entire physical host and are billed on an hourly basis. Owning that host lets

you spin up as many EC2 instances as that host permits, without more charges. For more information, see AWS tenancy.

- **Studio now supports running a restart schedule immediately**. Studio now lets you run a restart schedule immediately to restart all applicable machines in the schedule. For more information, see Immediately run a restart schedule.
- **Autoscale**. Autoscale provides the following new features and enhancements:
  - **Studio now supports displaying machines in drain state**. Previously, PowerShell was your only choice to identify machines in drain state. You can now use Studio to identify machines that are in drain state. For more information, see Display machines in drain state.
  - **Studio now supports defining peak times at a granular level of 30 minutes for VDI delivery groups**. Previously, you had to use PowerShell to define the peak times for the days included in a schedule at a granular level of 30 minutes for VDI delivery groups. You can now also use Studio to do that. This support enables you to set the minimum number of machines running in a VDI Delivery Group separately for each half hour of the day.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops service supports Azure Shared Image Gallery as a published image repository for MCS provisioned machines in Azure. Administrators have the option of storing an image in the gallery to accelerate the creation and hydration of OS disks from the master image. This process improves the boot and application launch times for non-persistent VMs.

The gallery contains the following three elements:

- Gallery. Images are stored here. MCS creates one gallery for each machine catalog.
- Gallery Image Definition. This definition includes information (operating system type and state, Azure region) about the master image. MCS creates one image definition for each master image created for the catalog.
- Gallery Image Version. Each image in a Shared Image Gallery can have multiple versions, and each version can have multiple replicas in different regions. Each replica is a full copy of the master image. Citrix Virtual Apps and Desktops service always creates one Standard_LRS image version (version 1.0.0) for each image with the appropriate number of replicas in the catalog's region. This configuration is based on the number of machines in the catalog, the configured replica ratio, and the configured replica maximum.

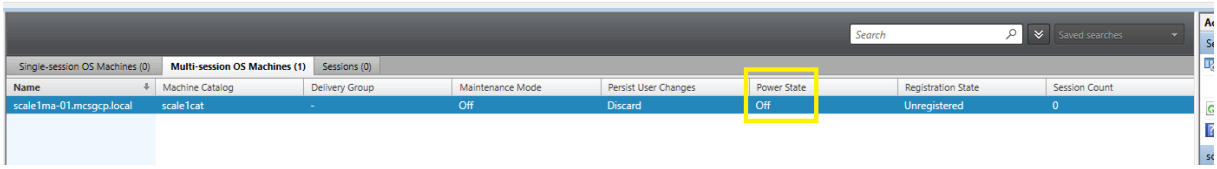
> **Note:**
>
> Shared Image Gallery functionality only works with managed disks. It is not available for legacy machine catalogs.

For details about this feature, see Configure shared image gallery.

Storage buckets created in same Google Cloud Platform region as the machine catalog. In previous releases, MCS created temporary storage buckets during provisioning as part of the disk upload process. These buckets spanned multiple regions, which Google defines as a large geographic area containing two or more geographic places. These temporary buckets resided in the United States geographic location, no matter where the catalog was provisioned. MCS now creates storage buckets in the same region where you provision your catalogs. Storage buckets are no longer temporary; they remain in your Google Cloud Platform project after you complete the provisioning process. Future provisioning operations use the existing storage bucket. If one exists in that region, or a new storage bucket is created if one does not exist in the specified region.

PowerShell option that sets default to re-use pooled VDAs during an outage. A new PowerShell command option (`-DefaultReuseMachinesWithoutShutdownInOutage`) extends the ability to reuse pooled desktop VDAs that haven't been shut down during an outage, by default. See Application and desktop support.

Google Cloud Platform on-demand provisioning. Citrix Virtual Apps and Desktops service updates how the Google Cloud Platform (GCP) provisions machine catalogs. When creating a machine catalog, the corresponding machine instance is not created in GCP and the power state is set to **OFF**. Machines are not provisioned at catalog creation time but rather the first time the machines are powered on. For example, after you create a catalog, the VM power state is set to **Off**:

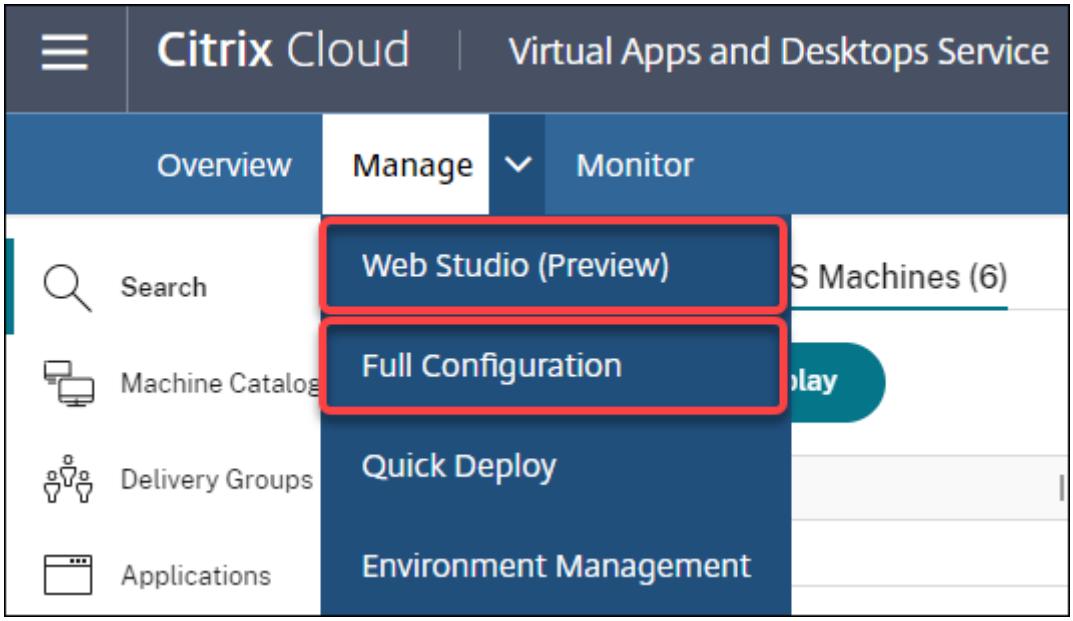


December 2020

New and enhanced features

Web Studio is available as a preview. A new, web-based console is now available. We are in the process of migrating the full set of Studio functionalities from the legacy console to the new, web-based console. The web-based console generally responds faster than the legacy console. By default, you automatically log on to the web-based console. You can easily switch between the web-based console and the legacy console from within the **Manage** tab to perform your configuration or site management tasks. Click the down arrow next to **Manage** and select an option:

- **Web Studio (Preview)**. Takes you to the new, web-based console.
- **Full Configuration**. Takes you to the legacy console.



The following features are available only in the web-based console:

- **Standard SSD disk type support for Azure**. Studio now adds support for standard SSD disk type. Azure standard SSDs are a cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels. For more information, see Create a machine catalog using an Azure Resource Manager master image.
- **Studio now supports configuring the power-off delay for static VDI delivery groups**. Previously, you might configure the power-off delay for static VDI delivery groups only through the PowerShell SDK. Studio now lets you configure the power-off delay in the Autoscale user interface for static VDI delivery groups. For more information, see Autoscale.

October 2020

New and enhanced features

Dismiss multiple hypervisor alerts. Citrix Monitor now supports automatic dismissal of hypervisor alerts older than a day. For more information, see Hypervisor Alerts Monitoring.

Remove external IP address. An external IP address on a temporary virtual machine that is used to prepare a provisioned image in the Google Cloud Platform (GCP) is no longer required. This external IP address enables the temporary virtual machine to access the Google public API to complete the provisioning process.

Enable Private Google Access to permit the VM to access the Google public API directly from the subnet. For more information, see Enable Google Private access.

New model addresses how machine identities are managed. Machine identities used in machine catalogs have been managed and maintained using Active Directory. All machines created by MCS will now be joining Active Directory. The new Citrix Virtual Apps and Desktops service model addresses how machine identities are managed. This model allows the creation of machine catalogs using *workgroup*, or, non-domain joined machines.

> **Tip:**
>
> This functionality supports a new identity service, *FMA trust*, added to Citrix Cloud for non-domain joined machines.

MCS communicates with the new FMA trust service for identity management. Identity information is stored in the identity disk as a pair of GUID and private key pairs, instead of the domain SID and machine account password paradigm used by Active Directory. VDAs using non-domain joined machines use this GUID and private key combination for broker registration. For more information, see Configure support for non-domain joined catalogs.

Use direct upload for Azure managed disks. This release allows you to use direct upload when creating managed disks in an Azure environment. This functionality reduces costs associated with extra storage accounts. You no longer have to stage the VHD into a storage account before converting it to a managed disk. Also, direct upload eliminates the need to attach an empty managed disk to a virtual machine. Directly uploading to an Azure managed disk simplifies the workflow by enabling you to copy an on-premises VHD directly for use as a managed disk. Supported managed disks include Standard HDD, Standard SSD, and Premium SSD.

For more information on this feature, see the Microsoft Azure blog.

For more information about Azure managed disks, see the documentation page.

Single Resource Group in Azure. You can now create and use a single Azure resource group for updating and creating catalogs in Citrix Virtual Apps and Desktops. This enhancement applies to both the full scope and narrow scope service principals.
The previous limit of 240 VMs per 800 managed disks per Azure Resource Group has been removed. There is no longer a limit on the number of virtual machines, managed disks, snapshots, and images per Azure Resource Group.

For more information, see Microsoft Azure Resource Manager virtualization environments.

September 2020

New and enhanced features

Quick Deploy. The new Quick Deploy feature replaces the earlier Azure Quick Deploy. The new feature offers a quick way to get started with the Citrix Virtual Apps and Desktops service using Microsoft Azure. You can use Quick Deploy to deliver desktops and apps, and configure Remote PC Access.

Session Administrator (built-in role). Citrix Studio now adds a new built-in role called **Session Administrator**. The role lets an administrator view delivery groups and manage their associated sessions and machines on the **Filters** page of the **Monitor** tab. With this feature, you can configure access permissions of existing administrators or administrators you invite in a way that aligns with their role in your organization. For more information about the built-in role, see Built-in roles and scopes. For information about how to assign the built-in role to an administrator, see Delegated administration and monitoring.

For a more granular level of control over access to the **Filters** page related to sessions and machines, create a custom role and select one of the following for the Director object: **View Filters page - Machines only**, **View Filters page - Sessions only**. For information about creating a custom role, see Create and manage roles.

Support for a new machine type. This release adds support for the NV v4 and the DA v4 series of AMD machines, when configuring Premium Disks for a machine catalog. For more information, see Create delivery groups.

August 2020

New and enhanced features

Limited access to the Remote PowerShell SDK during an outage. Previously, you might not use PowerShell commands during an outage. Now, Local Host Cache allows limited access to the Remote PowerShell SDK during an outage. See What is unavailable during an outage.

Support for two new Citrix Virtual Apps and Desktops service editions. Citrix Monitor now supports two new Citrix Virtual Apps and Desktops service editions, namely, **Citrix Virtual Apps Advanced service** and **Citrix Virtual Apps and Desktops Advanced service**. For more information, see the Citrix Monitor Feature compatibility matrix.

Support for shared Virtual Private Cloud (VPC) in Google Cloud Platform. The Citrix Virtual Apps and Desktops service supports Shared VPC on Google Cloud Platform as a host resource. You can use Machine Creation Services (MCS) to provision machines in a Shared VPC and manage them using Citrix Studio. For information about Shared VPC, see Shared Virtual Private Cloud.

Zone selection support for Google Cloud Platform. The Citrix Virtual Apps and Desktops service supports zone selection on Google Cloud Platform. This feature allows administrators to specify one or multiple zones within a region for catalog creation.

For sole-tenant type VMs, zone selection provides administrators with the ability to place sole tenant nodes across zones of their choice. For non-sole tenant VMs, zone selection provides the ability to place VMs deterministically across zones of their choice thereby providing flexibility in designing the deployment. For configuration information, see Enable zone selection.

Also:

- Sole tenancy provides exclusive access to a sole tenant node, which is a physical compute engine server dedicated to hosting only your project's VMs. These nodes allow you to group your VMs together on the same hardware or separate your VMs from other project's VMs.
- Sole tenant nodes help you meet dedicated hardware requirements for Bring Your Own License (BYOL) scenarios. They also enable you to comply with network access control policy, security, and privacy requirements such as HIPAA.

> **Note:**
>
> Sole tenancy is the only route to using Windows 10 VDI deployments on Google Cloud. Server VDI also supports this method. A detailed description for sole tenancy can be found on the Google documentation site.

Improved boot performance for Azure system disks. This release supports improved boot performance for Citrix Cloud implementations using Azure when MCSIO is enabled. With this support, you can retain the system disk. This provides the following advantages:

- VMs and applications now boot and launch with performance similar to how the golden image is served.
- Reduction in API quota consumption, deleting and creating the system disk, and state transition delay caused when you delete a VM.

For example, use the PowerShell `PersistOSDisk` custom property in the `New-ProvScheme` command to configure this feature.

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>'
<!--NeedCopy-->
```

For more configuration information, see Improve boot performance.

July 2020

New and enhanced features

Support for granular, role-based access to the Filters page. Citrix Studio now provides more granular control over access to the **Monitor > Filters** page when you create a custom role. Specifically, you can assign permissions to view any combination of **Machines**, **Sessions**, **Connections**, and **Application Instances** to a custom role. The following are four more options for the **Director** object in the **Create Role** window:

- View Filters page - Application Instances only
- View Filters page - Connections only
- View Filters page - Machines only
- View Filters page - Sessions only

For information about creating roles, see Create and manage roles.

Power-off delay support for assigned VDI machines (PowerShell only). In earlier releases, the power-off delay applied only to unassigned machines. Starting with this release, the power-off delay applies to both assigned and unassigned machines. For more information, see How Autoscale power manages machines.

Support for Windows Client licenses. The Citrix Virtual Apps and Desktops service now supports using Windows Client licenses to provision VMs in Azure. To run Windows 10 VMs in Azure, verify that your volume licensing agreement with Microsoft qualifies for this usage. For more information, see Create a machine catalog using an Azure Resource Manager master image.

May 2020

New and enhanced features

Machine restart schedules. You can now indicate whether a restart schedule affects machines that are in maintenance mode. This feature is available only in PowerShell. For details, see Scheduled restarts for machines in maintenance mode.

Resource availability. You can now ensure resource availability during an outage without having to publish resources in every zone (resource location). For details, see Resource availability.

April 2020

New and enhanced features

Enhanced scheduling granularity for VDI Delivery Groups (PowerShell only). Autoscale now supports defining the peak times for the days included in a schedule at a granular level of 30 minutes. You can set the minimum number of machines running in a VDI Delivery Group separately for each half hour of the day. Also, Autoscale can now scale up or down the number of powered-on machines in VDI Delivery Groups on a half-hourly basis instead of on an hourly basis. For more information, see Broker PowerShell SDK commands.

MTU Discovery. The Citrix protocol Enlightened Data Transport (EDT) now has MTU Discovery capabilities. MTU Discovery allows EDT to automatically determine and set the payload size for the session. This feature enables the ICA session to adjust to networks with non-standard Maximum Transmission Unit (MTU) or Maximum Segment Size (MSS) requirements. The ability to adjust avoids packet fragmentation that might result in degraded performance or failure to establish an ICA session. This update requires a minimum of Citrix Workspace app 1911 for Windows. If using Citrix Gateway, the minimum Citrix ADC firmware version required is 13.0.52.24 or 12.1.56.22. For more information, see EDT MTU Discovery.

March 2020

New and enhanced features

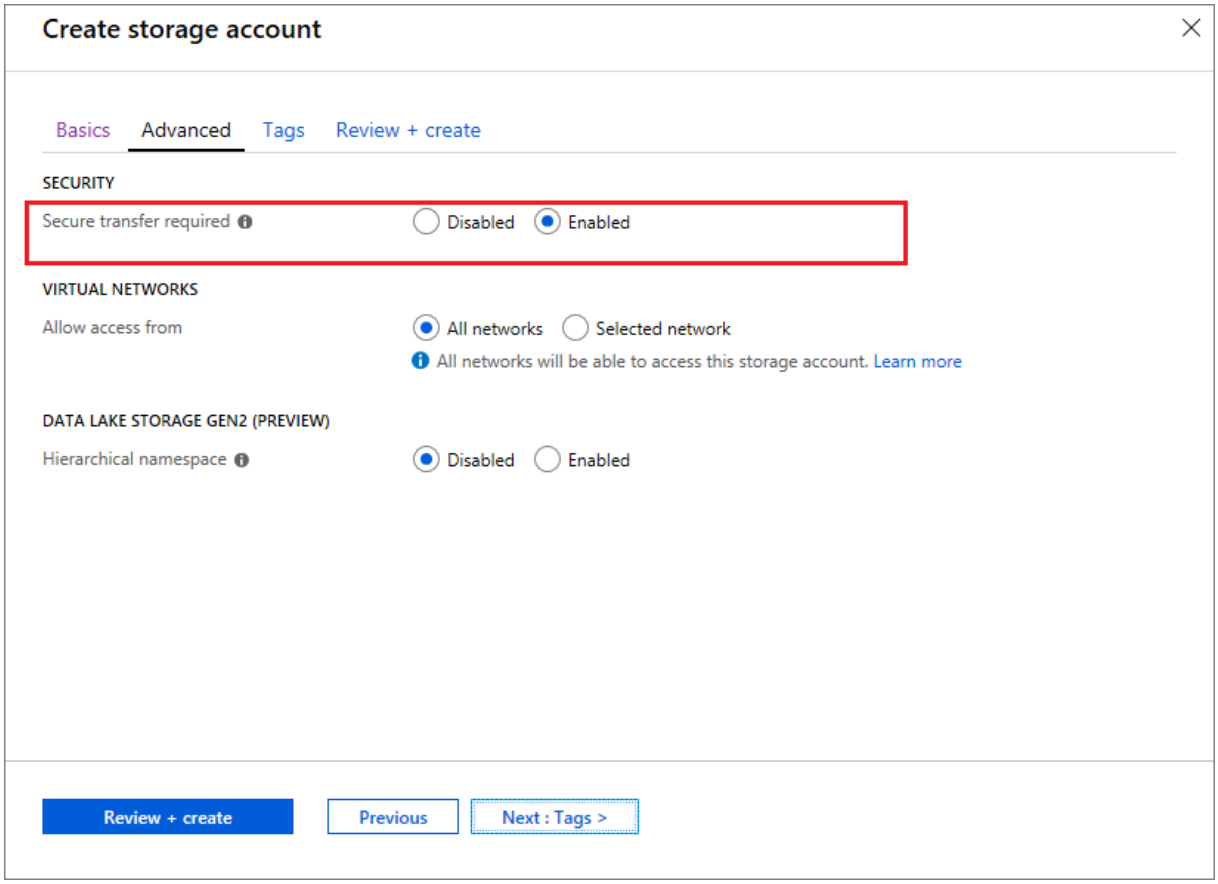
PVS target device metrics. Citrix Monitor now provides a PVS target device metrics panel on the Machine Details page. Use the panel to view the status of Provisioning target devices for single-session and multi-session OS machines. Several metrics for Network, Boot, and Cache are available on this panel. These metrics help you monitor and troubleshoot PVS target devices to ensure that they are up and running. For more information, see PVS target device metrics.

AWS instance property capturing. MCS now reads properties from the instance from which the AMI was taken and applies the IAM role and tags of the machine to the machines provisioned for a given catalog. When using this optional feature, the catalog creation process finds the selected AMI source instance, reading a limited set of properties. These properties are then stored in an AWS Launch Template, which is used to provision machines for that catalog. Any machine in the catalog inherits the captured instance properties. For more information, see AWS instance property capturing.

AWS operational resource tagging. This release introduces an option to tag resources created by Citrix components during provisioning. Each tag represents a label consisting of a customer-defined key and an optional value that improve your ability to manage, search for, and filter resources. For more information, see AWS operational resource tagging.

Secure transfer in Azure storage. Machine Creation Services (MCS) provides an enhancement for storage accounts created by MCS-provisioned catalogs in Azure Resource Manager environments. This enhancement automatically enables the secure transfer required property. This option enhances storage account security by only allowing requests to the account from secure connections. For more information, see Require secure transfer to ensure secure connections on the Microsoft site.

Enable the **Secure transfer required** property when creating a storage account in Azure:



Support for Azure SSD managed disks. Machine Creation Services (MCS) supports standard SSD managed disks for Azure virtual machines. This disk type provides consistent performance, and delivers better availability compared to HDD disks. For more information, see Standard SSD Disks for Azure Virtual machine workloads.

Use the PowerShell `StorageAccountType` custom property in the `New-ProvScheme` command or `Set-ProvScheme` command to configure this feature:

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
<!--NeedCopy-->
```


> **Note:**
>
> This feature is only available when using managed disks, that is, the custom property `UseManagedDisks` is set to **true**. For unmanaged disks only Standard HDD and Premium SSD are supported.

January 2020

New and enhanced features

Language bar in Citrix Studio. Starting with this release, Citrix Studio provides a language bar to facilitate correct keyboard mapping.

- If the language of Citrix Cloud or the display language of your browser is set to **English** or **Japanese**, the language bar does not appear.
- If the language of Citrix Cloud or the display language of your browser is set to **German**, **Spanish**, or **French**, the language bar appears after you log on to Citrix Studio. There are two language options on the language bar list. Select an option that matches the topmost language of your browser.

  > **Tip:**
  >
  > - Settings that you configure for the language bar might not take effect. In this case, log out and log back on.
  > - You might fail to input certain symbols and localized characters by using the language bar. To resolve the issue, you need to configure the language of Citrix Cloud, the display language of your browser, and the local keyboard layout. For more information, see Knowledge Center article CTX310743.

Restart schedule maximum delay timer (PowerShell only). If a scheduled restart of machines in a Delivery Group doesn't begin because of a site database outage, you can specify how long to wait beyond the scheduled start time. If the database connection is restored during that interval, the restarts begin. If the connection isn't restored during that interval, the restarts don't begin. For details, see Scheduled restarts delayed due to database outage.

Vertical load balancing (PowerShell only). Previously, the service used horizontal load balancing for all RDS launches, which assigns incoming load to the least-loaded RDS machine. That remains the default. Now, you can use PowerShell to enable vertical load balancing as a site-wide setting.

When vertical load balancing is enabled, the broker assigns incoming load to the most-loaded machine that has not reached a high watermark. This saturates existing machines before moving on to new machines. As users disconnect and free up existing machines, new load is assigned to those machines.

By default, horizontal load balancing is enabled. To view, enable, or disable vertical load balancing, the `Get-BrokerSite`, and `Set-BrokerSite` cmdlets now support the `UseVerticalScalingForRdsLau` setting. For more information, see Load manage machines in Delivery Groups.

December 2019

New and enhanced features

Service for Citrix Service Providers (CSP). CSPs can now onboard tenant customers to the Virtual Apps and Desktops service, configure customer administrator access to the service, and provide shared or dedicated workspaces to customers' users using federated domains. For more information, see Citrix Virtual Apps and Desktops service for Citrix Service Providers.

Support for determining why a machine is in maintenance mode (PowerShell only). Using PowerShell, you can now determine why a machine is in maintenance mode. To do so, use the parameter `-MaintenanceModeReason`. The feature is useful for administrators to troubleshoot issues with machines in maintenance mode. For details, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/.

Autoscale. Autoscale now provides the capability to create machines and delete them dynamically. You can use the capability by using a PowerShell script. The script helps you dynamically scale up or down the number of machines in the Delivery Group based on the current load conditions. For more information, see Dynamically provision machines with Autoscale.

November 2019

New and enhanced features

GroomStartHour. Monitor now supports **GroomStartHour** - a new configuration that helps administrators to determine the time of the day that grooming should start running. For more information, see the Citrix Virtual Apps and Desktops SDK documentation.

OData Pagination. Monitor now supports **OData pagination**. All OData v4 endpoints return a maximum of 100 records per page with a link to the next 100 records in the response. For more information, see Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.

October 2019

New and enhanced features

App-V. App-V functionality is now available in Citrix Cloud. You can add App-V packages to the Delivery Controller in your Citrix Cloud configuration, in either single- or dual admin mode. The *Virtual Apps*

and Desktops Service App-V package discovery module, available in Citrix Downloads, allows you to import App-V packages and register Microsoft App-V servers. The apps they contain are then available to your users. This PowerShell module allows you to register Microsoft App-V Management and Publishing Servers using DNS URLs, avoiding the need for servers behind load balancing mechanisms to be registered using their actual machine URL. For more information, see Citrix Virtual Apps and Desktops service discovery module for App-V packages and servers.

Google Cloud Platform. Citrix Virtual Apps and Desktops service now adds support for using Machine Creation Services (MCS) to provision machines on the Google Cloud Platform (GCP). For more information, see Google Cloud Platform virtualization environments.

September 2019

New and enhanced features

VDA support for Azure Virtual Desktop. For supported operating systems and VDA versions see VDAs in an Azure Virtual Desktop environment.

Enhanced power policy. In earlier releases, a VDI machine transitioning to a time period where an action (disconnect action="**Suspend**"or "**Shutdown**") was required remained powered on. This scenario occurred if the machine disconnected during a time period (peak or off-peak times) where no action (disconnect action="**Nothing**") was required.

Starting with this release, Autoscale suspends or powers off the machine when the specified disconnection time elapses, depending on the disconnect action configured for the destination time period. For more information, see Power manage VDI machines transitioning to a different time period with disconnected sessions.

Machine catalogs: Tags. You can now use PowerShell to apply tags to machine catalogs. For more information, see Apply tags to machine catalogs.

Session startup duration. Monitor now displays the session startup duration divided into Workspace App Session Startup and VDA Session Startup time periods. This data helps you to understand and troubleshoot high session startup duration. Further, the time duration for each phase involved in the session startup helps in troubleshooting issues associated with individual phases. For example, if the Drive Mapping time is high, you can check if all the valid drives are mapped properly in the GPO or script. This feature is available on VDAs 1903 or later. For more information, see Diagnose session startup issues.

August 2019

New and enhanced features

Session Auto Reconnect. The Sessions page on the Trends tab now includes information about the number of auto reconnects. Auto reconnects are attempted when the Session Reliability or Auto Client Reconnect policies are in effect. The auto reconnect information helps you view and troubleshoot network connections having interruptions, and also analyze networks having a seamless experience.

The drilldown provides additional information like Session Reliability or Auto Client Reconnect, time stamps, Endpoint IP, and Endpoint Name of the machine where the Workspace app is installed. This feature is available for Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Receiver for Windows, and Citrix Receiver for Mac. This feature requires VDAs 1906 or later. For more information, see:

- Sessions
- Auto client reconnect policy settings
- Session reliability policy settings
- Session Auto Reconnect

July 2019

New and enhanced features

Configuration Logging. You can now use the Remote PowerShell SDK to periodically delete Configuration Logging database content. For details, see Schedule periodic data deletion.

Autoscale. Autoscale now provides the flexibility to power manage only a subset of machines in a Delivery Group. This feature can be useful in cloud bursting use cases, where you want to use on-premises resources to handle workloads before cloud-based resources address other demands (that is, burst workloads). For more information, see Restrict Autoscale to certain machines in a Delivery Group.

Local App Access and URL redirection. Citrix Studio now lets you add the Add Local App Access Application option to the Studio user interface for your Site by using the PowerShell SDK. For more information, see Provide access only to published applications.

Operating system name changes. Operating system names on the **Create Machine Catalog > Machine Catalog Setup > Operating System** and the **Monitor** pages have changed:

- Multi-session OS (formerly Server OS): The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session or Linux OS machines.

- Single-session OS (formerly Desktop OS): The single-session OS machine catalog provides VDI desktops ideal for various users.

Citrix Profile Management duration in Profile Load. Monitor now includes profile processing duration in the Profile Load bar of the Logon duration chart. This is the duration Citrix Profile Management takes to process user profiles. This information helps administrators to troubleshoot high profile load durations with greater accuracy. This enhancement is available on VDAs 1903 and later. For more information, see Profile Load.

Desktop probing. Desktop probing is a feature of the Citrix Virtual Apps and Desktops service. It automates health checks of virtual desktops published on a site, which improves user experience. To initiate desktop probing, install and configure the Citrix Probe Agent on one or more endpoints. Desktop probing is available for Premium licensed Sites. This feature requires Citrix Probe Agent 1903 or later. For more information, see Application and Desktop Probing.

> **Note:**
>
> Citrix Probe Agent now supports TLS 1.2.

June 2019

New and enhanced features

Restrict by tags. Tags are strings that identify items such as machines, applications, desktops, Application Groups, and policies. After creating a tag and adding it to an item, you can tailor certain operations to apply to only items that have a specified tag. For more information, see Application Groups and Tags.

Email Notifications. Citrix Virtual Apps and Desktops service sends email notifications related to alerting and probing directly. This eliminates the need to configure the SMTP email server. The **Notification Preferences** box is enabled by default and Citrix Cloud sends alert notifications to the email addresses provided in the **Notification Preferences** section. Ensure that the email address `donotreplynotifications@citrix.com` is white-listed in your email setup.

May 2019

New and enhanced features

Autoscale. Autoscale is a feature of Citrix Virtual Apps and Desktops service that provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience. Autoscale incorporates the deprecated Smart Scale technology into the Studio power management solution. For more information, see Autoscale. You can monitor the metrics of

Autoscale-managed machines from the Trends pages on the **Monitor** tab. For more information, see Monitor Autoscale-managed machines.

February 2019

New and enhanced features

Hypervisor alerts monitoring. Alerts from Citrix Hypervisor and VMware vSphere are now displayed on the **Monitor** > **Alerts** tab to help monitor the following states/parameters of hypervisor health:

- CPU usage
- Memory usage
- Network usage
- Hypervisor connection unavailable
- Disk usage (vSphere only)
- Host connection or power state (vSphere only)

For more information, see the Hypervisor alerts monitoring section in Alerts and Notifications.

Communications over earlier TLS versions. To improve the security of the service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1 as of March 15, 2019, allowing only TLS 1.2 communications. For more information, see TLS versions. For comprehensive guidance, see CTX247067.

Application Groups. Application Groups let you manage collections of applications. You can create Application Groups for applications shared across different Delivery Groups or used by a subset of users within Delivery Groups. For more information, see Create Application Groups.

Logon Performance - Profile Drilldown. The **Logon Duration** panel on the **User Details** page within **Monitor** now includes information on the **Profile load phase** drilldown of the logon process. Profile drilldown provides useful information about user profiles for the current session that can help administrators troubleshoot high profile load issues. A tool tip with the following user profiles information is displayed:

- Number of files
- Profile size
- Number of large files

A detailed drill-down provides information about the individual folders, their size, and the number of files. This feature is available on VDAs 1811 and later. For more information, see Diagnose user logon issues.

Microsoft RDS license health. Monitor the Microsoft RDS (Remote Desktop Services) license status on the **Machine Details** panel on the Machine Details and the User Details page for Server OS machines.

An appropriate message is displayed for the license status. You can hover over the info icon to see further details. For more information, see the Microsoft RDS license health section in Troubleshooting Machines.

Application Probing. This feature automates the assessment of the health of Virtual Apps published in a Site.

To initiate application probing:

- On one or more endpoint machines, install the Citrix Application Probe Agent
- Configure the Citrix Application Probe Agent with the credentials of Citrix Workspace and Citrix Virtual Apps and Desktops service.
- Configure the applications to be probed, the endpoint machines to run the probe on, and the scheduled probe time in **Monitor** > **Configuration** of the Citrix Virtual Apps and Desktops service.

The agent tests the launch of selected applications via Citrix Workspace and reports back the probe results on the **Monitor** tab of Citrix Virtual Apps and Desktops service in:

- the Applications page –the last 24-hours'data and the **Trends** > **Application Probe Results** page
- the historical probe data along with the stage when the probe failure occurred - Workspace Reachability, WorkspaceAuthentication, WorkspaceEnumeration, ICA download, or Application launch

The failure report is emailed to configured email addresses. You can schedule application probes to run during off-peak hours across multiple geographical locations. In that way, you can use the results to proactively troubleshoot issues related to provisioned applications, hosting machines, or connections before the users experience them. For more information, see Application and Desktop Probing.

January 2019

New and enhanced features

Delegated Administration with custom scope. Monitoring now supports custom scope for built-in delegated administrator roles. For more information on the available built-in roles for monitoring and how to assign them, see Delegated administrator roles.

December 2018

New and enhanced features

The date after which Citrix will block communication over Transport Layer Security (TLS) 1.0 and 1.1 has changed from December 31, 2018 to January 31, 2019. For details, see Deprecation of TLS versions.

November 2018

New and enhanced features

Machine historical data available using OData API: Historical data containing machine analytics is now available through the OData API. This data is collected on an hourly basis and rolled up for the day.

- Number of powered on machines (for power managed machines)
- Number of registered machines
- Number of machines in maintenance mode
- Total number of machines

The data is aggregated for the time period during which the Monitoring Service is running. For more information on the usage of the OData API and examples, see Citrix Monitor Service 7 1808. The database schema is available at Monitor Service Schema.

Logon Performance - Interactive session drilldown: The **Logon Duration** panel on the **User and Session Details** view includes information on the **Interactive Session** phase of the logon process. The time taken for each of the three subphases (**Pre-userinit**, **Userinit**, and **Shell**) is displayed on the **Interactive Session** bar as a tooltip. This provides more granular troubleshooting and remediation of this phase of the logon. The cumulative time delay between the subphases and a link to the documentation is also provided. This feature is available on Delivery Controller version 7 1808 and later. The **Interactive Session** drilldown bar shows the time duration for the current session only. For more information, see Diagnose user logon issues.

Logon Performance - GPO drilldown: The **Logon Duration** panel on the **User and Session** details view contains the GPO (Group Policy Objects) duration. This is the total time taken to apply the GPOs on the virtual machine during the logon process. Now, you can see the drilldown of each policy applied as per CSEs (Clients-Side Extension) as a tool tip on the GPO bar. For each policy application, the drilldown displays the status and the time taken. This additional information eases troubleshooting and remediation of issues involving high GPO duration. The time durations in the drilldown represent the CSE processing time only and do not add up to the total GPO time. This feature is available on Delivery Controller version 7 1808 and later. For more information, see Diagnose user logon issues.

Fixes

Custom report queries saved during monitoring are not available after a Cloud upgrade. [DNA-23420]

October 2018

New and enhanced features

Applications: Limit per machine. You can now limit the number of application instances per machine. This limit applies to all machines in the Site. This limit is an addition to the existing application limit for all users in the Delivery Group and the limit per user. This capability is available only through PowerShell, not in Studio. For details, see Configure application limits.

Windows Server 2019. You can now install VDAs for multi-session OS (formerly VDAs for Server OS) on Windows Server 2019 machines, as noted in System requirements.

September 2018

New and enhanced features

Delegated Administration. With Delegated Administration, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization. For details, see Delegated Administration. Monitoring supports allocation of built-in roles. Built-in roles are available with full scope. For more information about built-in roles for monitoring and how to assign them, see Delegated administrator roles.

Configuration Logging. Configuration Logging allows administrators to keep track of configuration changes and administrative activities. For details, see Configuration Logging.

Several PowerShell cmdlets in the Remote PowerShell SDK that were previously disabled are now enabled, for use with Configuration Logging:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Local Host Cache. Local Host Cache is now fully available. Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. For details, see Local Host Cache.

Citrix Provisioning. To provision VDAs, you can now use Citrix Provisioning or the existing Machine Creation Services. For Citrix Provisioning information specific to the cloud environment, see Citrix Provisioning managed by Citrix Cloud.

Fixes

In earlier versions, when using Azure on-demand provisioning, all VMs were deleted when powered-off. Now, only pooled VMs are deleted. Persistent (dedicated) VMs are not deleted when powered-off.

August 2018

- **New product names**

  If you've been a Citrix customer or partner for a while, you'll notice new names in our products and in this product documentation. If you're new to this Citrix product, you might see different names for a product or component.

  The new product and component names stem from the expanding Citrix portfolio and cloud strategy. Articles in this product documentation use the following names.

  - **Citrix Virtual Apps and Desktops:** Citrix Virtual Apps and Desktops offers a virtual app and desktop solution, provided as a cloud service and as an on-premises product, giving employees the freedom to work from anywhere on any device while cutting IT costs. Deliver Windows, Linux, web, and SaaS applications or full virtual desktops from any cloud: public, on-premises, or hybrid. Virtual Apps and Desktops was formerly XenApp and XenDesktop.
  - **Citrix Workspace app:** The Citrix Workspace app incorporates existing Citrix Receiver technology and other Citrix Workspace client technologies. It has been enhanced to deliver more capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they must do their best work. For more information, see this blog post.
  - **Citrix SD-WAN:** NetScaler SD-WAN, a crucial technology for our customers and partners transforming their branch networks and WANs with cloud technology, is now Citrix SD-WAN.
  - **Citrix Secure Web Gateway:** As the Citrix Networking portfolio expands, we're proud to offer our robust Citrix Secure Web Gateway Service, previously known as NetScaler Secure Web Gateway.
  - **Citrix Gateway:** Our robust NetScaler Unified Gateway, which allows secure, contextual access to the apps and data you must do your best work, is now Citrix Gateway.
  - **Citrix Content Collaboration and Citrix Files for Windows:** The advanced access, collaboration, workflows, rights management, and integration features of ShareFile are now

available in the Citrix Content Collaboration component set in our secure, contextual, integrated Citrix Workspace. Citrix Files for Windows allows you to access your Content Collaboration files directly through a mapped drive, providing a native Windows Explorer experience.

- **Citrix Hypervisor**: The technology from XenServer for virtualization infrastructure, based on the XenProject hypervisor, is now Citrix Hypervisor.

Here's a quick recap:

Is	Was
Citrix Virtual Apps and Desktops	XenApp and XenDesktop
Citrix Workspace app	Incorporates Citrix Receiver and extensive enhancements
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files for Windows	ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

Implementing this transition in our products and their documentation is an ongoing process.

- In-product content might still contain former names. For example, you might see instances of earlier names in console text, messages, and directory/file names.
- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product's documentation might still contain former names.
- For Citrix Hypervisor: The new name is used on the Citrix website and in informational product materials from September 2018. You will also see the new name on the administrator consoles of some Citrix products, such as Citrix Virtual Apps and Desktops. The XenServer product release and technical documentation materials continue to use XenServer 7.x until early 2019.

Your patience during this transition is appreciated.

For more detail about our new names, see https://www.citrix.com/about/citrix-product-guide/.

- **Product and component version number changes**

  Citrix installs and manages most of the Citrix Virtual Apps and Desktops components, so you won't be concerned with those version numbers. However, you might see version numbers when installing Cloud Connectors, and when installing or upgrading VDAs in resource locations.

  Citrix Virtual Apps and Desktops product and component version numbers are displayed in the format: **YYMM.*c.m.b***

  - YYMM = Year and month when the product or component released. For example, a September 2018 release appears as 1809.
  - c = Citrix Cloud release number for the month.
  - m = Maintenance version (if applicable).
  - b = Build number. This field is shown only on the About page of the component, and in the OS's feature for removing or changing programs.

  For example, **Citrix Virtual Apps and Desktops 1809.1.0** indicates that the component released in September 2018. It is associated with Citrix Cloud release 1 in that month, and is not a maintenance version. Some displays show only the version's year and month: for example, **Citrix Virtual Apps and Desktops 1809**.

  In earlier releases (7.18 and earlier), version numbers were displayed in the format: 7.*version*, where version incremented by one for each release. For example, the VDA release following XenApp and XenDesktop 7.17 was 7.18. Earlier releases (7.18 and earlier) will not be updated with the new numbering format.

- **Deprecation of TLS versions.** To improve the security of the Citrix Virtual Apps and Desktops service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1, effective December 31, 2018. For details, see Deprecation of TLS versions.

- **Google Cloud Platform virtualization environment.** The Citrix Virtual Apps and Desktops service supports the ability to manually power cycle Virtual Apps and Desktops VMs on the Google Cloud Platform (GCP). For more information, see Google Cloud Platform virtualization environments.

July 2018

- **Export of Filters data.** You can now export real-time monitoring data on the **Monitor** > **Filters** tab to CSV format files. The export feature is available from the Machines, Sessions, Connections, and Application Instances Filters pages. You can select a predefined custom filter or select suitable filter criteria, choose required columns on the table, and export the data. Data of

up to 100,000 records can be exported. The exported CSV files give a comprehensive view of the real-time data, and helps ease analysis of large data sets.

June 2018

- **Azure Resource Manager connections.** In the Studio connection creation wizard, the Azure environment selection on the **Connection** page includes all Azure Clouds that are valid for your Azure subscription. General availability for Azure US Government Cloud and Azure Germany Cloud replaces the preview versions of those two environments in earlier releases.

May 2018

- **Azure Quick Deploy.** When your resource location uses Azure Resource Manager machines to deliver applications and desktops, you can now choose a deployment method:
  - Full Configuration: This existing method uses the Studio management console, which guides you through creating a machine catalog and then creating a Delivery Group.
  - Azure Quick Deploy: This new option offers a simpler interface that offers faster deployment of apps and desktops.
- **Citrix Health Assistant link.** The Machine Details page of an unregistered machine on the Monitoring console now contains a **Health Assistant** button. Currently, the button links to Troubleshoot machines and to the Knowledge Center article, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch where you can download the tool. Citrix Health Assistant is a tool to troubleshoot configuration issues in unregistered VDAs. The tool automates several health checks to identify possible root causes for common VDA registration, session launch, and time zone redirection configuration issues.
- **Interactive Session drilldown.** In the monitoring console, the **User Details view > Logon Duration** panel now includes information on the **Interactive Session** stage of the logon process. To provide more granular troubleshooting and remediation of this phase of the logon, **Interactive Session** now has three subphases: **Pre-userinit**, **Userinit**, and **Shell**. In this release, hovering over **Interactive Session** displays a tooltip showing the subphases and a link to the documentation. For a description of the subphases and how to improve the performance of each phase, see Diagnose user logon issues.

March 2018

- **Application instance prediction (Preview feature).** This is the first monitoring feature based on predictive analytics. Predicting resource usage patterns is important for administrators to

organize resources and the required number of licenses on each resource. The Application instance prediction feature indicates the number of hosted application instances that are likely to be launched per Site or Delivery Group over time. Machine learning algorithms based on data models created with existing historical data are used to do the prediction. Tolerance level indicates the prediction quality.

For more information see Application instance prediction in Director. Submit your feedback regarding the usefulness and usability of this feature in the Citrix Cloud discussion forum.

- **Delivery Groups APIs - Preview**

  The Delivery Groups APIs Preview provides a set of REST APIs that you can use to automate the management of Delivery Groups. The complete set of available APIs can be viewed and tried out in the Citrix Cloud API documentation at https://developer.cloud.com/.

- **Web Studio authentication**

  The service management console on Citrix Cloud now uses a bearer token to authenticate customers. The bearer token is required to authenticate access to the Delivery Groups REST API.

- **Access Monitor Service data using OData Version 4 API (Preview feature)**

  You can create your customized monitoring and reporting dashboards based on the Monitor Service data by using the OData V.4 endpoint. OData V.4 is based on ASP .Net Web API and supports aggregation queries. Use your Citrix Cloud user name and bearer token to access the data with the V4 endpoint. For more information and examples, see Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

  Share your feedback on the utility of this feature in the Citrix Cloud discussion forum.

Fixes

- You can rename, move, and delete application folders. [#STUD-2376]

January 2018

- **RDS license check.** Creation of machine catalogs containing Windows Server OS machines now includes an automatic RDS license check. Any RDS license issues found are displayed, so that you can take the appropriate steps to prevent a gap in service. For details, see Create machine catalogs.
- **Access to machine console from Monitor.** The Machine Details panel from Monitor now provides access to consoles of machines hosted on the XenServer hypervisor version 7.3. You can now troubleshoot issues in VDAs directly from Monitor. For more information, see Machine Console access in Troubleshoot machines.

December 2017

New and enhanced features

- **Citrix Workspace.** Citrix Workspace is now available for **new** XenApp and XenDesktop Service customers. For more information, see Workspace Configuration.
- **Applications Analytics.** You can now analyze and monitor the performance of applications efficiently with the new Application Analytics page available from **Monitor** > **Applications** tab. The page provides a consolidated view of the health and usage of all applications published on your Site. It shows metrics such as the number of instances per application, and faults and errors associated with the published applications. This feature requires VDAs Version 7.15 or later.

  For more information, see Application Analytics section in Monitor.

November 2017

New and enhanced features

- **Local Host Cache.** Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. For details, see Local Host Cache.
- **Azure Managed Disks.** Azure Managed Disks are now used by default for MCS-provisioned VMs in Azure Resource Manager environments. Optionally, you can use conventional storage accounts. For details, see Microsoft Azure Resource Manager virtualization environments.
- **Help desk administrator.** When managing service administrators for a Citrix Cloud customer account, you now have a new choice: Help Desk Administrator. A help desk administrator can access the Monitor functions on the service. For details, see Manage.

Fixes

- You can now use the service management console wizard to create a Remote PC Access machine catalog. In earlier releases, you had to use a PowerShell cmdlet to create a catalog (as documented in CTX220737). Then, you had to return to the management console to create a Delivery Group. Now, you create the catalog and the Delivery Group sequentially on the management console.
- MCS-created catalogs can use existing Active Directory machine accounts. [#DNA-24566]
- When monitoring a deployment, scrolling in a sorted **Trends > Sessions** table displays accurate results. [DNA-51257]

More information

- Known issues.
- For information about third-party software that is included in the service, see Third party notifications.

Known issues

April 16, 2024

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) has the following known issues:

- In a VMware environment hosted on AWS, the MCS machine catalog creation fails if the master image is vTPM enabled. For VMware support, see Get Support. [PMCS-37603]
- Monitor screens might not load if the Pendo URL, `https://citrix-cloud-content.customer.pendo.io/` is blocked.
  [DIR-18482]
- You get an error if you run a command with `XDHyp:\` in the remote PowerShell SDK. To resolve this issue:

  1. Run a command with `Hyp`. For example: `Get-HypServiceStatus`
  2. Run a command with `XDHyp:\`. For example: `Get-ChildItem XDHyp:\Connections\`

  [BRK-13723]
- After changes in the Citrix DaaS architecture in version 2209, the default icons for Windows desktops and for applications deployed before this release have changed to generic PC desktop icons. This change is only applicable to desktops and applications that are pointing to the default icon. If you want to change icons back to the Windows application default icon, run the following script using the Remote PowerShell SDK:
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- In **Manage > Full Configuration**, attempts to change the OS type for Azure catalogs fail with an error message. Changing the OS type for Azure catalogs is no longer supported even if you use PowerShell. [STUD-19819]
- In Microsoft Azure environments, enabling Azure ephemeral OS disk and MCS I/O at the same time fails to create a machine catalog. However, for existing machine catalogs, you can still update a machine catalog, add or delete VMs, and delete a machine catalog. [PMCS-21698]

- The drop-down arrow icon for the Average IOPS, Session Control, and Power Control buttons might not appear on the **User Details** and the **Machine Details** pages. However, the functionality works as expected. To view all the items on the menu, click anywhere on the button. [DIR-11875]
- If you use Azure AD Domain Services: Workspace (or StoreFront) logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.
- When deploying to Azure and creating an MCS catalog version 7.9 or later with write-back cache enabled and the VDA installed on the master image is 1811 or earlier, an error occurs. Also, you cannot create anything related to Personal vDisk for Microsoft Azure. As a workaround, select a different catalog version to deploy to Azure, or disable the write-back cache. To disable write-back cache when you create a catalog, clear the **Memory allocated to cache** and **Disk cache size** checkboxes on the **Machines** page.
- The **Console** link on **Monitor > Machine Details** does not launch the Machine Console in the Microsoft Edge 44 and Firefox 68 ESR browsers. [DIR-8160]
- When you try to use the 'Restart'option in the Workspace App web or desktop, the 'Restarting' dialogue never closes and never reports success. The hypervisor shows that the machine has shut down but has not started. As a workaround, after some time the user can close the 'Restarting'dialogue and launch the desktop and the desktop must start. [BRK-5564]

For issues related to current VDAs, see Known issues.

Deprecation

February 22, 2024

This article gives you advanced notice of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) features that are being phased out, so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when features are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see the Product Lifecycle Support Policy article.

> **Note:**
>
> Citrix Virtual Apps and Desktops deprecations and removals are described in their own Deprecation article.

Deprecations and removals

The following list shows the Citrix DaaS features that are deprecated or removed.

Deprecated items are not removed immediately. Citrix continues to support them but they will be removed in a future release.

Removed items are removed, or no longer supported, in Citrix DaaS. Dates in **bold** face indicate the latest updates.

Item	Deprecation announced in release	Removed in release	Alternative
Support for configuring the write-back cache to include only a disk cache and no memory cache	February 2024		Use the memory cache size configuration option and give a non-zero size.
Support for Azure catalogs created before on-demand provisioning feature (“legacy”catalogs)	February 2024		Recreate Azure legacy catalog VMs. The catalogs are provisioned as on-demand and help to save storage cost.
Support for Citrix Connector 3.1 for System Center Configuration Manager	December 2023		Do image or application update manually.
Support for using a master image in a region different from the region where the catalog is created	December 2023		Use Azure Compute Gallery to replicate the master image to the required region.
Support for AWS volume worker	November 2023		Use Direct disk upload and download. See Direct disk upload and download.

Item	Deprecation announced in release	Removed in release	Alternative
Support for `Leave user management to Citrix Cloud` used in creating delivery groups	September 2023	September 2023	
Support for `AwsCaptureInstanceProperties` used in AWS environments	August 2023		Use a machine profile. See Create a catalog using a machine profile.
Support for VMware vSphere 6.7		June 2023	Use higher versions for VMware vSphere.
`Schedule-ProvVMUpdate` PowerShell command	April 2023		Use `Set-ProvVMUpdateTimeWindow` command.
`Request-ProvVMUpdate` PowerShell command	April 2023		Use `Set-ProvVMUpdateTimeWindow` command with `-StartsNow` and `-DurationInMinutes -1` parameters.
`Cancel-ProvVMUpdate` PowerShell command	April 2023		Use `Clear-ProvVMUpdateTimeWindow` command.
`DedicatedTenancy` parameter used in `New-ProvScheme` command	March 2023		Use `TenancyType` parameter.
Unmanaged disk to create VM in the Azure environment	June 2022		

Item	Deprecation announced in release	Removed in release	Alternative
Support for four AWS specific commands: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress`, and `Grant-HypSecurityGroupIngress`	May 2022		
`StorageAccountType` parameter used in Azure environments	April 2022		Use `StorageType`.
Legacy console (MMC-based console)	July 2021	November 2021	Use **Manage > Full Configuration** to access the full range of configuration and management actions.
Azure Quick Deploy	September 2020		Use Quick Deploy.
Ability to import Citrix Provisioning target devices to create catalogs in Citrix Studio.	August 2020	February 2021	Use the Citrix Provisioning Export Devices Wizard to push Citrix Provisioning VMs into Delivery Controllers/MCS for catalog creation. See Export Devices Wizard.

System requirements

May 28, 2024

Introduction

System requirements for components that are not covered here (such as Citrix Workspace app and Citrix Provisioning) are described in their respective documentation.

Specific recommendations for sizing VMs that deliver desktops and applications cannot be provided because of the complex and dynamic nature of hardware offerings. Every deployment has unique needs. Generally, sizing a VM is based on the hardware and not the user workloads (except for RAM; you need more RAM for applications that consume more.) The Citrix Tech Zone contains the latest guidance on VDA sizing.

> **Important:**
>
> VDA versions mentioned in this article are subject to the Citrix product lifecycle. For more information, see the Product Matrix on the Citrix web site.
>
> For more information about using LTSR VDAs with Citrix DaaS, see CTX205549.

Remember: In a Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment, you don't need to install or manage the core components (Delivery Controllers, the site database, or management and monitoring consoles). For Virtual Delivery Agent (VDA) installation guidance, see:

- Install VDAs
- Install VDAs using the command line.

Cloud Connectors

For details, see Cloud Connector Technical Details.

VDAs in an Azure environment

Supported operating systems:

- Windows 11 multi-session
- Windows 11 single-session
- Windows 10 multi-session
- Windows 10 single-session

- Windows Server 2022 (requires minimum VDA 2106)
- Windows Server 2019
- Windows Server 2016

All VDAs that haven't reached end of life are supported for use with Citrix DaaS. For LTSR VDAs, we recommend using them with the latest Cumulative Update. For more information about the lifecycle of VDAs, see Citrix Product Matrix.

Windows Server 2012 R2 is supported only with VDA 1912 (and later CUs).

Windows Server requires Microsoft RDS licensing.

For information about Azure Virtual Desktop, see the Microsoft documentation.

VDA for single-session OS

The following information applies to the latest VDA release.

Supported operating systems:

- Windows 11
- Windows 10
  - For edition support, see CTX224843. That article also contains links to Citrix known issues with the supported Windows versions.
  - Desktop composition redirection and legacy graphics mode are not supported on Windows 10.

Requirements:

- Microsoft .NET Framework 4.8 is installed automatically, if it (or a later version) is not already installed.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - If the machine contains an earlier version of that runtime (such as 2015-2017), the Citrix installer upgrades it.
  - If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

Remote PC Access uses this VDA, which you install on physical office PCs. This VDA supports Secure Boot for Citrix Virtual Desktops Remote PC Access.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features are not installed and do not work. Do not remove Media Foundation from the machine after installing the Citrix

software. Otherwise, users cannot log on to the machine. On most supported Windows desktop OS editions, Media Foundation support is already installed and cannot be removed. However, N editions do not include certain media-related technologies. You can obtain that software from Microsoft or a third party.

More information:

- For Linux VDA information, see the Linux Virtual Delivery Agent product documentation.
- To use the server VDI feature, you can use the command line interface to install a single-session VDA on a supported Windows Server machine. See Server VDI for guidance.
- For information about installing a VDA on an older machine, see Earlier operating systems.
- See also VDAs in an Azure Virtual Desktop environment.

VDA for multi-session OS

The following information applies to the latest VDA release.

Supported operating systems:

- Windows Server 2022 (requires minimum VDA 2106)
- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows 11
- Windows 10 (64-bit) all supported versions

The installer automatically deploys the following requirements:

- Microsoft .NET Framework 4.8 is installed automatically, if it (or a later version) is not already installed.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - If the machine contains an earlier version of that runtime (such as 2015-2017), the Citrix installer upgrades it.
  - If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled. This triggers a restart.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that the Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features are not installed and do not work. Do not remove Media Foundation from the machine after installing the

Citrix software. Otherwise, users cannot log on to the machine. On most Windows Server versions, the Media Foundation feature is installed through the Server Manager. However, N editions do not include certain media-related technologies. You can obtain that software from Microsoft or a third party.

If Media Foundation is not present on the VDA, these multimedia features do not work:

- Flash Redirection
- Windows Media Redirection
- HTML5 Video Redirection
- HDX RealTime Webcam Redirection

More information:

- For Linux VDA information, see the Linux Virtual Delivery Agent articles.
- For information about installing a VDA on a Windows operating system that is no longer supported, see Earlier operating systems.
- See also VDAs in an Azure Virtual Desktop environment.

Hosts / virtualization resources

The following host/virtualization resources (listed alphabetically) are supported. Where applicable, the *major.minor* versions are supported, including updates to those versions. CTX131239 contains the most current hypervisor version information, plus links to known issues.

- **Amazon Web Services (AWS)**
  - You can provision applications and desktops on supported Windows server operating systems.
  - The Amazon Relational Database Service (RDS) is not supported.

  For more information, see AWS cloud environments.
- **XenServer (formerly Citrix Hypervisor)**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see XenServer virtualization environments.
- **Google Cloud Platform**

  For more information, see Google Cloud environments and Getting Started with Citrix DaaS on Google Cloud.
- **HPE Moonshot**

  For more information, see HPE Moonshot virtualization environments.

- **Microsoft Azure Resource Manager**

  For more information, see Microsoft Azure Resource Manager cloud environments.

- **Microsoft System Center Virtual Machine Manager**

  Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Microsoft System Center Virtual Machine Manager virtualization environments.

- **Nutanix Acropolis**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Nutanix virtualization environments.

- **VMware Cloud on AWS**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see VMware cloud on Amazon Web Services (AWS).

- **Azure VMware Solution (AVS)**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Azure VMware Solution (AVS) integration.

- **Google Cloud VMware Engine**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Google Cloud VMware Engine.

- **VMware vSphere(vCenter + ESXi)**

  No support is provided for vSphere vCenter Linked Mode operation.

  CTX131239 contains current version information, plus links to known issues.

  For more information, see VMware virtualization environments.

> **Note:**
>
> You must not install the VDA software on any Citrix DDC or StoreFront server. The VDA must be a stand-alone system. Installing multiple components on a single VM is only permissible when developing a proof-of-concept or when publishing the Studio admin console to administrators only. In this case you must ensure non-admin users do not have access to DDC/StoreFront VMs.

Active Directory functional levels

The following functional levels for the Active Directory forest and domain are supported:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

For more information about Active Directory, see Active Directory joined.

HDX technologies

For specific HDX feature support and requirements, see HDX.

Universal Print Server

The Universal Print Server comprises client and server components. The UpsClient component is included in the VDA installation. You install the UpsServer component on each print server where shared printers reside that you want to provision with the Citrix Universal Print Driver in user sessions.

The UpsServer component is supported on:

- Windows Server 2019
- Windows Server 2016

Requirements:

- Microsoft .NET Framework 4.8 (minimum)
- Microsoft Visual C++ 2015-2022 Redistributable.
  - If the machine contains an earlier version of that runtime (such as 2015-2017), the Citrix installer upgrades it.
  - If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

For multi-session VDAs, user authentication during printing operations requires the Universal Print Server to be joined to the same domain as the VDA.

Standalone client and server component packages are also available for download.

For more information, see Provision printers.

Service connectivity

See System and Connectivity Requirements for Internet connection information. That information includes requirements that are common to most Citrix Cloud services, plus requirements specific to Citrix DaaS.

Other

- The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the site configuration database. The machine on which you install `CitrixGroupPolicyManagement_x64.msi` must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.
- This product supports PowerShell versions 3 through 5.
- For product components and features that you can install on Windows Servers, Server Core and Nano Server installations are not supported, unless noted.
- For details about resource limits in a deployment, see Limits.
- For supported StoreFront versions, see the StoreFront system requirements.
- For globalization information, see CTX119253.
- For information about ports that Citrix DaaS uses, see Communications Ports Used by Citrix Technologies.
- For information about requirements when using the Quick Deploy management interface, see Requirements.

Limits

July 1, 2024

The values in this article indicate the limits of a single Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) instance. These limits are extensively tested by Citrix and recommended for the best end user and admin experience. These are soft limits and not technically enforced (except the total number of VDAs per resource location). When the number of concurrent users exceeds 125,000, Citrix can scale and combine multiple Citrix DaaS instances, to deliver a unified experience at any scale.

The information in this article is dynamic. Check back frequently for updates. If you have current requirements that the published limits do not address, contact your Citrix representative for assistance as early as possible.

Configuration limits

If policies exceed the limit, Citrix recommends using the Workspace Environment Management service or Active Directory Group Policy Objects (GPOs).

Resource	Limit
Active Directory domains	100
Application folders	1,000
Application Groups	250
Applications	5,000
Catalogs	2,000
Delivery Groups	2,000
Host connections	200
Resource locations	100
Manage console (Full Configuration) policies	200
Tags	10,000
VDAs	100,000

Resource location limits

The following table lists the limits for each resource location.

If your requirements exceed these limits, Citrix recommends using additional resource locations.

Resource	Limit
Total VDAs (hard limit)	10,000
Total sessions	25,000
Active Directory domains	1
Host connections	40

Citrix Cloud Connectors are assigned to resource locations and link workloads to Citrix DaaS. For information about Cloud Connector limits, see Size and scale considerations for Cloud Connectors.

Provisioning limits

The provisioning limits in the following table are the Citrix recommended maximums for a single public provider subscription.

You are likely to reach quota limits from your public cloud vendor at lower levels. In such cases, contact the vendor to raise your subscription quota. For larger-scale deployments, Citrix recommends a hub-and-spoke model, where VDAs are distributed across multiple subscriptions and host connections.

For more information, see the following reference architectures:

- Citrix DaaS on AWS
- Citrix virtualization on Google Cloud
- Citrix DaaS on Azure

Resource	Limit
VDAs per Amazon Web Services account per region	3,000
VDAs per Google Cloud Platform project	3,000
VDA per Microsoft Azure subscription per region	5,000

> **Note:**
>
> The limits are Citrix recommended.

Usage limits

For information about administrator roles and the differences between them, see:

- Manage (Full Configuration) administrators
- Monitor (Director) administrators

Resource	Limit
Concurrent Monitor (Director) full administrators	40
Concurrent Monitor (Director) help desk administrators	200
Concurrent Monitor (Director) session administrators	50

Resource	Limit
Concurrent Manage (Full Configuration) cloud administrators	100
Concurrent Manage (Full Configuration) help desk administrators	60
Concurrent end users	125,000
Resources published to a single user	250
Session launches per minute	3,000

- Monitor (Director) supports aggregation of up to four Citrix DaaS tenants (spokes) under a single tenant (hub).
- A help desk administrator on the hub instance can monitor and troubleshoot users, machines, endpoints, and transactions from all aggregated instances (hub and spokes) as per the Delegated Administration configuration on the specific instance.
- The number of concurrent administrators per Citrix DaaS instance is as per the Usage Limits table.

Limits change log

The following table tracks the configuration limit modification:

Date	Resource	Description
22 Nov 2023	Active Directory domains	Limit increased from 85 to 100.
	Catalogs	Limit increased from 1000 to 2000.
	Delivery Groups	Limit increased from 1000 to 2000.
	Resource locations	Limit increased from 85 to 100.
	Resource location -> Total sessions	Limit increased from 20,000 to 25,000.
07 Dec 2023	Provisioning limits -> VDA per Microsoft Azure subscription per region	Limit increased from 2,500 to 5,000.

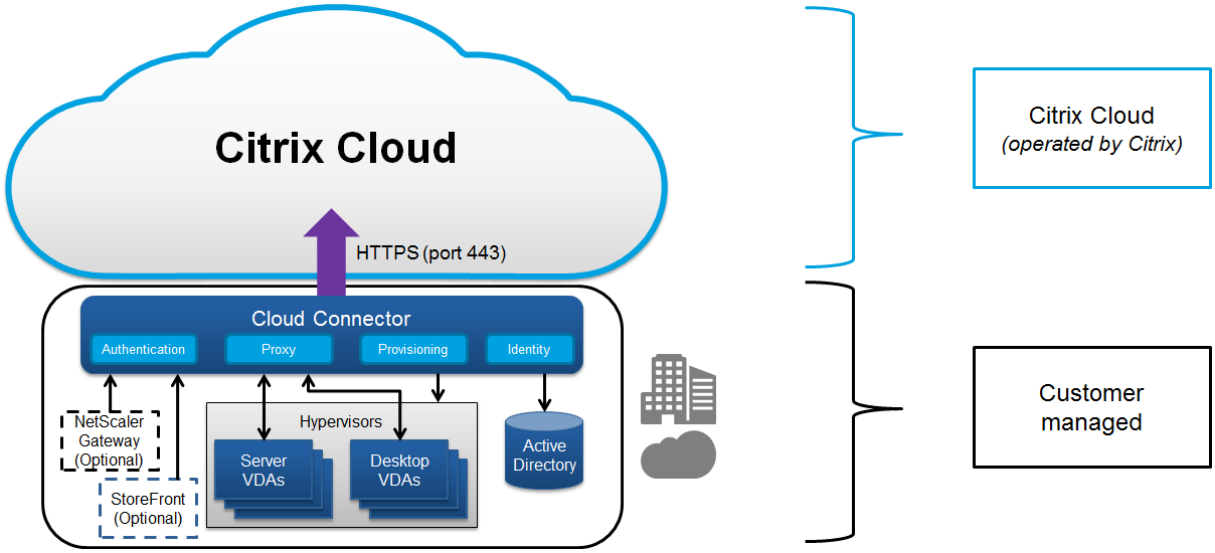
Technical security overview

June 20, 2024

Security overview

This document applies to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) hosted in Citrix Cloud. This information includes Citrix Virtual Apps Essentials and Citrix Virtual Desktops Essentials.

Citrix Cloud manages the operation of the control plane for Citrix DaaS environments. The control plane includes the Delivery Controllers, management consoles, SQL database, license server, and optionally StoreFront and Citrix Gateway (formerly NetScaler Gateway). The Virtual Delivery Agents (VDAs) hosting the apps and desktops remain under the customer's control in the data center of their choice, either cloud or on-premises. These components are connected to the cloud service using an agent called the Citrix Cloud Connector. If customers elect to use Citrix Workspace, they can also choose to use the Citrix Gateway Service instead of running Citrix Gateway within their data center. The following diagram illustrates Citrix DaaS and its security boundaries.



Citrix cloud-based compliance

As of January 2021, the use of Citrix Managed Azure Capacity with various Citrix DaaS editions and Workspace Premium Plus has not been evaluated for Citrix SOC 2 (Type 1 or 2), ISO 27001, HIPAA, or other cloud compliance requirements. Visit the Citrix Trust Center for more information regarding Citrix Cloud Certifications, and check back frequently for updates.

Data flow

Citrix DaaS does not host the VDAs, so the customer's application data and images required for provisioning are always hosted in the customer setup. The control plane has access to metadata, such as user names, machine names, and application shortcuts, restricting access to the customer's Intellectual Property from the control plane.

Data flowing between the cloud and customer premises uses secure TLS connections over port 443.

Data isolation

Citrix DaaS stores only the metadata needed for the brokering and monitoring of the customer's applications and desktops. Sensitive information, including images, user profiles, and other application data remains on the customer premises or in their public cloud vendor's subscription.

Service editions

The capabilities of Citrix DaaS vary by edition. For example, Citrix Virtual Apps Essentials supports only Citrix Gateway service and Citrix Workspace. Consult that product documentation to learn more about supported features.

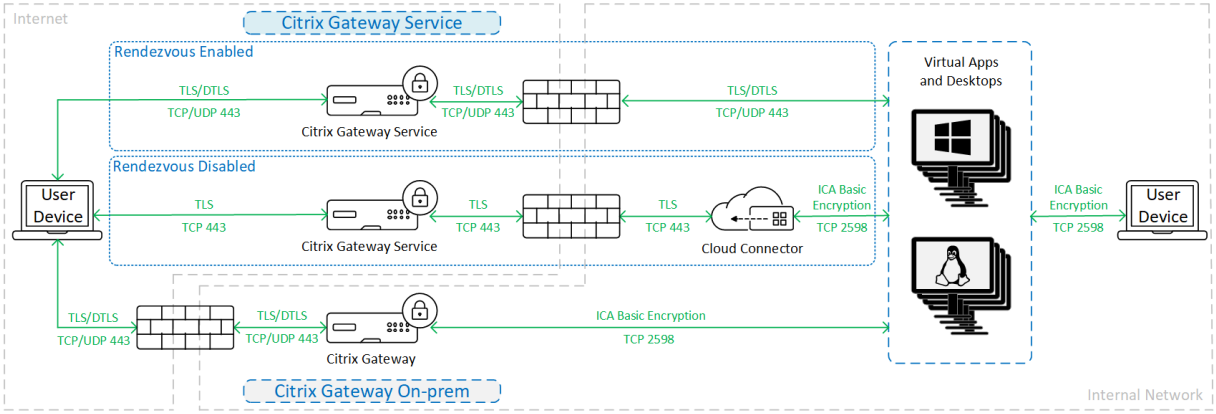
ICA Security

Citrix DaaS provides several options for securing ICA traffic in transit. The following are the options available:

- **Basic encryption:** The default setting.
- **SecureICA:** Allows encrypting session data using RC5 (128-bit) encryption.
- **VDA TLS/DTLS:** Allows using network-level encryption using TLS/DTLS.
- **Rendezvous protocol:** Available only when using the Citrix Gateway Service. When using the Rendezvous protocol, ICA sessions are encrypted end-to-end using TLS/DTLS.

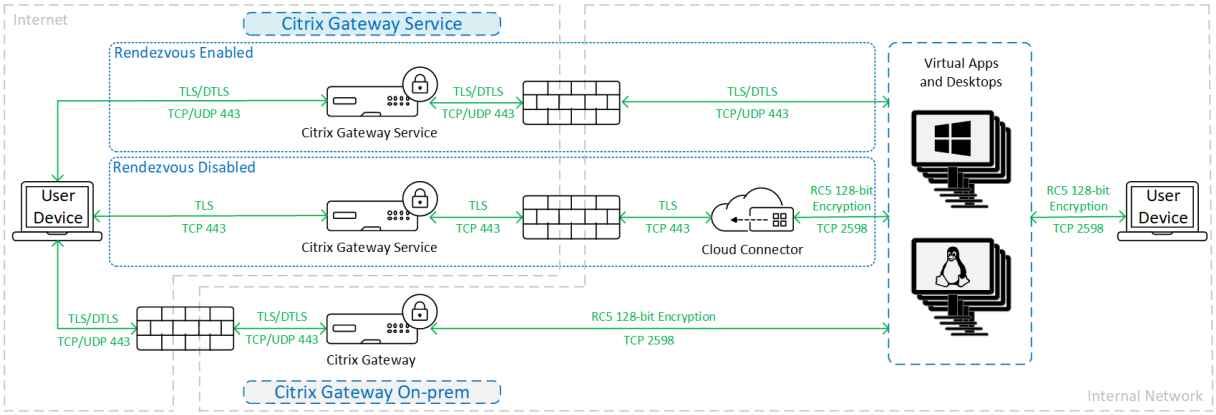
Basic encryption

When using basic encryption, traffic is encrypted as shown in the following graphic.



SecureICA

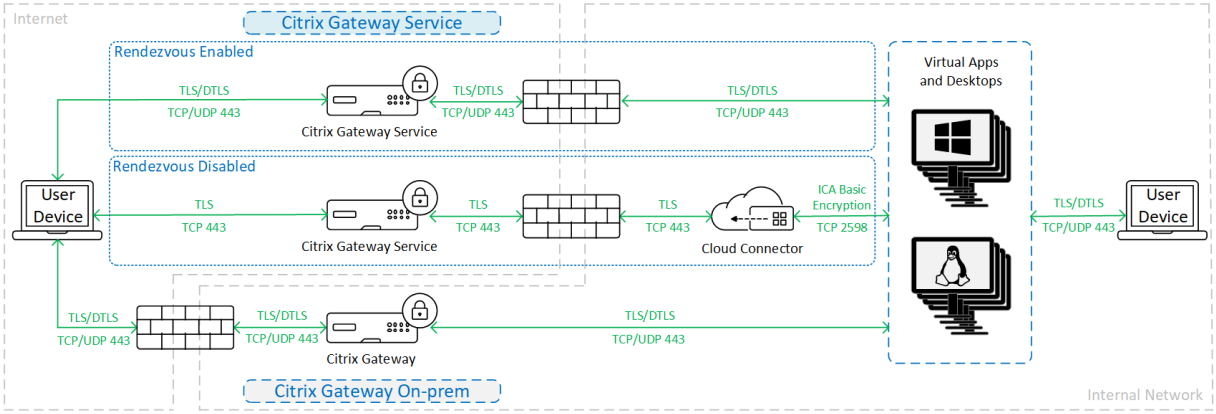
When using SecureICA, traffic is encrypted as shown in the following graphic.



> **Note:**
>
> SecureICA is not supported when using Workspace app for HTML5.

VDA TLS/DTLS

When using VDA TLS/DTLS encryption, traffic is encrypted as shown in the following graphic.



> **Note:**
>
> When using the Gateway Service without Rendezvous, the traffic between the VDA and the Cloud Connector is not TLS encrypted, because the Cloud Connector does not support connecting to the VDA with network-level encryption.

More resources

For more information about the ICA security options and how to configure them, see:

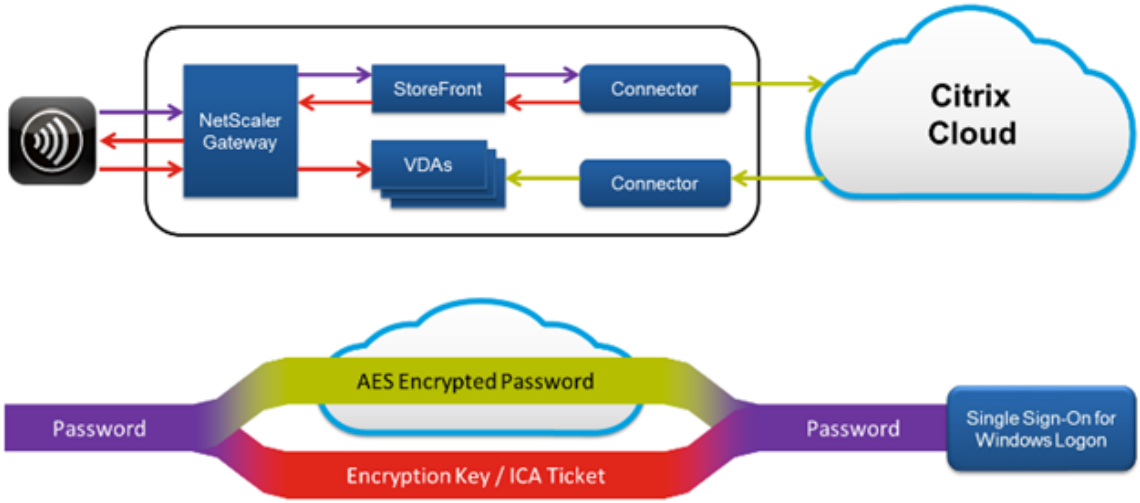
- SecureICA: Security policy settings
- VDA TLS/DTLS: Transport Layer Security
- Rendezvous protocol: Rendezvous protocol

Credential handling

Citrix DaaS handles four types of credentials:

- User Credentials: When using a customer-managed StoreFront, the Cloud Connector encrypts user credentials using AES-256 encryption and a random one-time key generated for each launch. The key is never passed into the cloud, and returned only to Citrix Workspace app. The Citrix Workspace app then passes this key to the VDA to decrypt the user password during session launch for a single sign-on experience. The flow is shown in the following figure.

  By default, user credentials are not forwarded across untrusted domain boundaries. If a VDA and StoreFront are installed in one domain and a user in a different domain attempts to connect to the VDA, the logon attempt fails unless a trust is established between the domains. You can disable this behavior and allow credentials to be forwarded between untrusted domains using the DaaS PowerShell SDK. For more information, see Set-Brokersite.



- Administrator Credentials: Administrators authenticate against Citrix Cloud. Authentication generates a one-time signed JSON Web Token (JWT) which gives the administrator access to Citrix DaaS.
- Hypervisor Passwords: On-premises hypervisors that require a password for authentication have an administrator-generated password that is directly stored encrypted in the SQL database in the cloud. Citrix manages peer keys to ensure that hypervisor credentials are only available to authenticated processes.
- Active Directory (AD) Credentials: Machine Creation Services uses the Cloud Connector for creating machine accounts in a customer's AD. Because the machine account of the Cloud Connector has only read access to AD, the administrator is prompted for credentials for each machine creation or deletion operation. These credentials are stored only in memory, and are held only for a single provisioning event.

Deployment considerations

Citrix recommends that users consult the published best practices documentation for deploying Citrix Gateway applications and VDAs within their environments.

Citrix Cloud Connector network access requirements

The Citrix Cloud Connectors require only port 443 outbound traffic to the internet, and can be hosted behind an HTTP proxy.

- The communication used in Citrix Cloud for HTTPS is TLS. (See Deprecation of TLS versions.)
- Within the internal network, the Cloud Connector needs access to the following for Citrix DaaS:

  - VDAs: Port 80, both inbound and outbound. plus 1494 and 2598 inbound if using Citrix Gateway service
  - StoreFront servers: Port 80 inbound.
  - Citrix Gateways, if configured as a STA: Port 80 inbound.
  - Active Directory domain controllers
  - Hypervisors: Outbound only. See Communications Ports Used by Citrix Technologies for specific ports.

Traffic between the VDAs and Cloud Connectors is encrypted using Kerberos message-level security.

Customer-managed StoreFront

A customer-managed StoreFront offers greater security configuration options and flexibility for deployment architecture, including the ability to maintain user credentials on-premises. The StoreFront can be hosted behind the Citrix Gateway to provide secure remote access, enforce multifactor authentication, and add other security features.

Citrix Gateway service

Using the Citrix Gateway service avoids the need to deploy Citrix Gateway within customer data centers.

For details, see Citrix Gateway service.

All TLS connections between the Cloud Connector and Citrix Cloud are initiated from the Cloud Connector to the Citrix Cloud. No in-bound firewall port mapping is required.

XML trust

This setting is available in **Full Configuration > Settings > Enable XML trust** and is disabled by default. Alternatively, you can use the Citrix DaaS Remote PowerShell SDK to manage XML trust.

XML trust applies to deployments that use:

- An on-premises StoreFront.
- A subscriber (user) authentication technology that does not require passwords. Examples of such technologies are domain pass-through, smart cards, SAML, and Veridium solutions.

Enabling the XML trust setting allows users to successfully authenticate and then start applications. The Delivery Controller trusts the credentials sent from StoreFront. Enable this setting only when you have secured communications between your Delivery Controllers and StoreFront using Security Keys or another mechanism such as firewalls or IPsec.

This setting is disabled by default.

Use the Citrix DaaS Remote PowerShell SDK to manage XML trust.

- To check the XML trust current value, run `Get-BrokerSite` and inspect the value of `TrustRequestsSentToTheXMLServicePort`.
- To enable XML trust, run `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`
- To disable XML trust, run `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`

Enforce HTTPS or HTTP traffic

To enforce either HTTPS or HTTP traffic through the XML Service, configure one of the following registry value sets on each of your Cloud Connectors.

After you configure the settings, restart the Remote Broker Provider Service on each Cloud Connector.

In `HKLM\Software\Citrix\DesktopServer\`:

- To enforce HTTPS (ignore HTTP) traffic: Set `XmlServicesEnableSsl` to `1`, and `XmlServicesEnableNonSsl` to `0`.
- To enforce HTTP (ignore HTTPS) traffic: Set `XmlServicesEnableNonSsl` to `1`, and `XmlServicesEnableSsl` to `0`.

Deprecation of TLS versions

To improve the security of Citrix DaaS, Citrix began blocking any communication over Transport Layer Security (TLS) 1.0 and 1.1 as of March 15, 2019.

All connections to Citrix Cloud services from Citrix Cloud Connectors require TLS 1.2.

To ensure successful connection to Citrix Workspace from user devices, the installed Citrix Receiver version must be equal to or newer than the following versions.

Receiver	Version
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7

Receiver	Version
iOS	7.0
Chrome/HTML5	Latest (browser must support TLS 1.2)

To upgrade to the latest Citrix Receiver version, go to https://www.citrix.com/products/receiver/.

Alternatively, upgrade to the Citrix Workspace app, which uses TLS 1.2. To download the Citrix Workspace app, go to https://www.citrix.com/downloads/workspace-app/.

If you must continue using TLS 1.0 or 1.1 (for example, with a thin client based on an earlier Receiver for Linux version), install a StoreFront in your resource location. Then, have all the Citrix Receivers point to it.

More information

The following resources contain security information:

- Technical security overview for Citrix Managed Azure.
- Citrix security site.
- Security and Compliance Information: The security and compliance center contains security bulletins that can help you stay informed. The center also has documentation about standards and certifications that are important in maintaining a secure and compliant IT environment.
- Secure Deployment Guide for the Citrix Cloud Platform: This guide provides an overview of security best practices when using Citrix Cloud and describes the information Citrix Cloud collects and manages. This guide also contains links to comprehensive information about the Citrix Cloud Connector.
- System and Connectivity Requirements.
- Security considerations and best practices.
- Smart cards.
- Transport Layer Security (TLS).

> **Note:**
>
> This document is intended to provide the reader with an introduction to and overview of the security functionality of Citrix Cloud; and to define the division of responsibility between Citrix and customers with regard to securing the Citrix Cloud deployment. It is not intended to serve

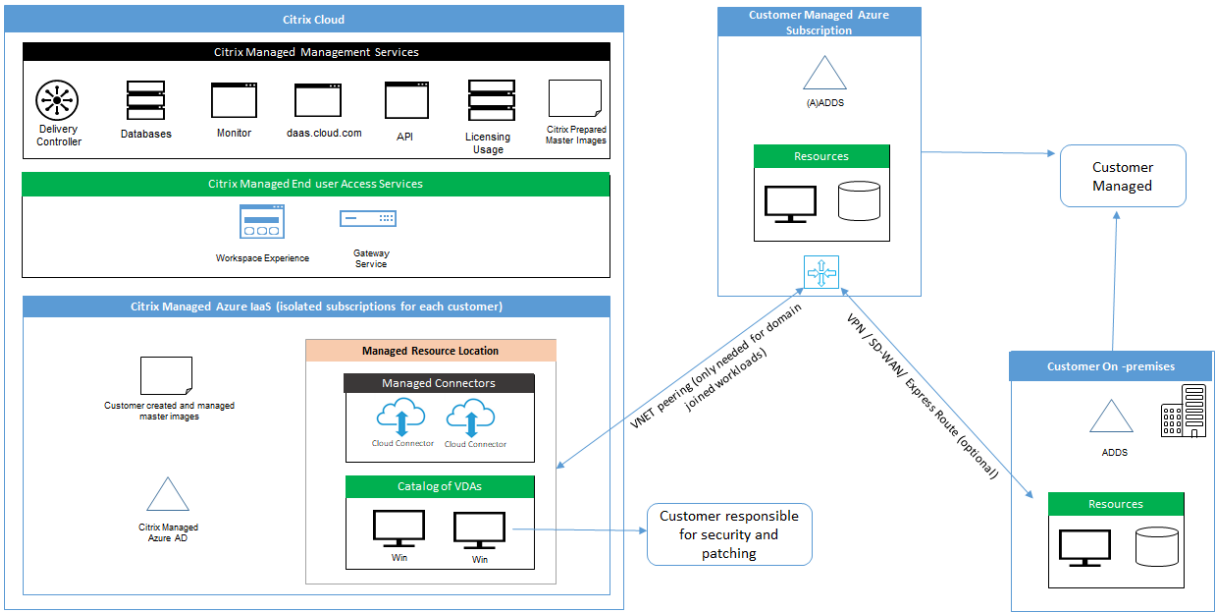
> as a configuration and administration guidance manual for Citrix Cloud or any of its components or services.

Technical security overview for Citrix Managed Azure

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

The following diagram shows the components in a Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment that uses Citrix Managed Azure. This example uses a VNet peering connection.



With Citrix Managed Azure, the customer's Virtual Delivery Agents (VDAs) that deliver desktops and apps, plus Citrix Cloud Connectors, are deployed into an Azure subscription and tenant that Citrix manages.

Citrix cloud-based compliance

As of January 2021, the use of Citrix Managed Azure Capacity with various Citrix DaaS editions and Workspace Premium Plus has not been evaluated for Citrix SOC 2 (Type 1 or 2), ISO 27001, HIPAA, or

other cloud compliance requirements. Visit the Citrix Trust Center for more information regarding Citrix Cloud Certifications, and check back frequently for updates.

Citrix responsibility

Citrix Cloud Connectors for non-domain-joined catalogs

When using a Citrix Managed Azure subscription, Citrix DaaS deploys at least two Cloud Connectors in each resource location. Some catalogs may share a resource location if they are in the same region as other catalogs for the same customer.

Citrix is responsible for the following security operations on non-domain-joined catalog Cloud Connectors:

- Applying operating system updates and security patches
- Installing and maintaining antivirus software
- Applying Cloud Connector software updates

Customers do not have access to the Cloud Connectors. Therefore, Citrix is wholly responsible for the performance of the non-domain-joined catalog Cloud Connectors.

Azure subscription and Azure Active Directory

Citrix is responsible for the security of the Azure subscription and Azure Active Directory (AAD) that are created for the customer. Citrix ensures tenant isolation, so each customer has their own Azure subscription and AAD, and cross-talk between different tenants is prevented. Citrix also restricts access to the AAD to Citrix DaaS and Citrix operations personnel only. Access by Citrix to each customer's Azure subscription is audited.

Customers employing non-domain-joined catalogs can use the Citrix-managed AAD as a means of authentication for Citrix Workspace. For these customers, Citrix creates limited privilege user accounts in the Citrix-managed AAD. However, neither customers'users nor administrators can execute any actions on the Citrix-managed AAD. If these customers elect to use their own AAD instead, they are wholly responsible for its security.

Virtual networks and infrastructure

Within the customer's Citrix Managed Azure subscription, Citrix creates virtual networks for isolating resource locations. Within those networks, Citrix creates virtual machines for the VDAs, Cloud Connectors, and image builder machines, in addition to storage accounts, Key Vaults, and other Azure

resources. Citrix, in partnership with Microsoft, is responsible for the security of the virtual networks, including virtual network firewalls.

Citrix ensures the default Azure firewall policy (network security groups) is configured to limit access to network interfaces in VNet peering and SD-WAN connections. Generally, this controls incoming traffic to VDAs and Cloud Connectors. For details, see:

- Firewall policy for Azure VNet peering connections
- Firewall policy for SD-WAN connections

Customers cannot change this default firewall policy, but may deploy additional firewall rules on Citrix-created VDA machines; for example, to partially restrict outgoing traffic. Customers that install virtual private network clients, or other software capable of bypassing firewall rules, on Citrix-created VDA machines are responsible for any security risks that might result.

When using the image builder in Citrix DaaS to create and customize a new machine image, ports 3389-3390 are opened temporarily in the Citrix-managed VNet, so that the customer can RDP to the machine containing the new machine image, to customize it.

Citrix responsibility when using Azure VNet peering connections

For VDAs in Citrix DaaS to contact on-premises domain controllers, file shares, or other intranet resources, Citrix DaaS provides a VNet peering workflow as a connectivity option. The customer's Citrix-managed virtual network is peered with a customer-managed Azure virtual network. The customer-managed virtual network may enable connectivity with the customer's on-premises resources using the cloud-to-on-premises connectivity solution of the customer's choice, such as Azure ExpressRoute or IPsec tunnels.

Citrix responsibility for VNet peering is limited to supporting the workflow and related Azure resource configuration for establishing peering relationship between Citrix and customer-managed VNets.

Firewall policy for Azure VNet peering connections Citrix opens or closes the following ports for inbound and outbound traffic that uses a VNet peering connection.

Citrix-managed VNet with non-domain-joined machines

- Inbound rules
  - Allow ports 80, 443, 1494, and 2598 inbound from VDAs to Cloud Connectors, and from Cloud Connectors to VDAs.
  - Allow ports 49152-65535 inbound to the VDAs from an IP range used by the Monitor shadowing feature. See Communications Ports Used by Citrix Technologies.

  - Deny all other inbound. This includes intra-VNet traffic from VDA to VDA, and VDA to Cloud Connector.

- Outbound rules
  - Allow all traffic outbound.

Citrix-managed VNet with domain-joined machines

- Inbound rules:
  - Allow ports 80, 443, 1494, and 2598 inbound from the VDAs to Cloud Connectors, and from Cloud Connectors to VDAs.
  - Allow ports 49152-65535 inbound to the VDAs from an IP range used by the Monitor shadowing feature. See Communications Ports Used by Citrix Technologies.
  - Deny all other inbound. This includes intra-VNet traffic from VDA to VDA, and VDA to Cloud Connector.
- Outbound rules
  - Allow all traffic outbound.

Customer-managed VNet with domain-joined machines

- It is up to the customer to configure their VNet correctly. This includes opening the following ports for domain joining.
- Inbound rules:
  - Allow inbound on 443, 1494, 2598 from their client IPs for internal launches.
  - Allow inbound on 53, 88, 123, 135-139, 389, 445, 636 from Citrix VNet (IP range specified by customer).
  - Allow inbound on ports opened with a proxy configuration.
  - Other rules created by customer.
- Outbound rules:
  - Allow outbound on 443, 1494, 2598 to the Citrix VNet (IP range specified by customer) for internal launches.
  - Other rules created by customer.

Citrix responsibility when using SD-WAN connectivity

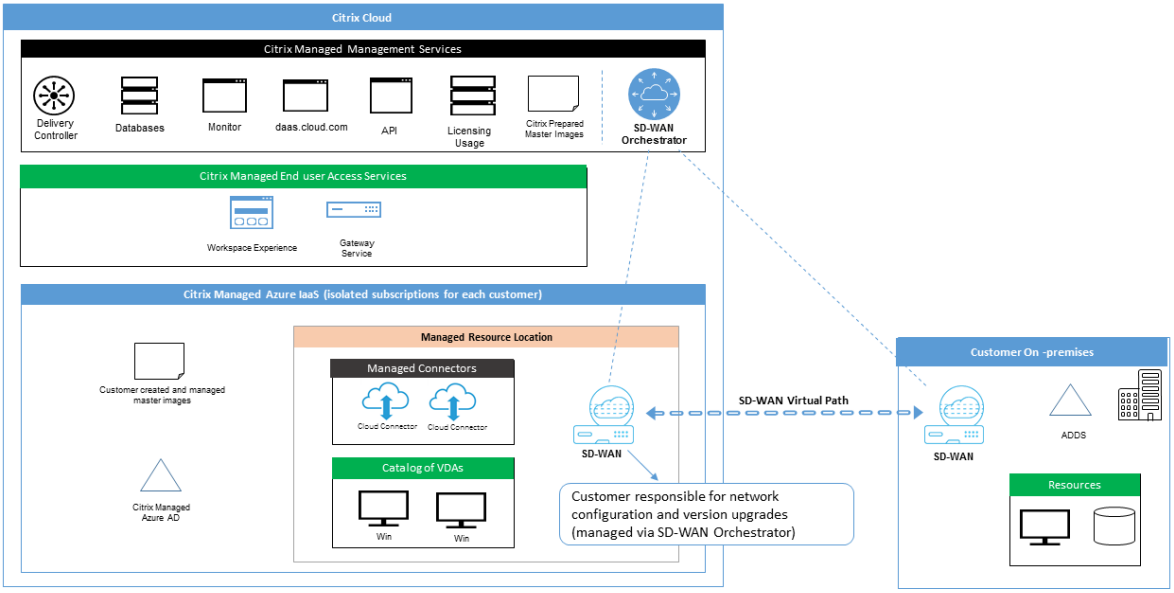
Citrix supports a fully automated way of deploying virtual Citrix SD-WAN instances to enable connectivity between Citrix DaaS and on-premises resources. Citrix SD-WAN connectivity has several advantages compared to VNet peering, including:

High reliability and security of VDA-to-datacenter and VDA-to-branch (ICA) connections.

- Best end-user experience for office workers, with advanced QoS capabilities and VoIP optimizations.
- Built-in ability to inspect, prioritize, and report on Citrix HDX network traffic and other application usage.

Citrix requires customers who want to take advantage of SD-WAN connectivity for Citrix DaaS to use SD-WAN Orchestrator for managing their Citrix SD-WAN networks.

The following diagram shows the added components in a Citrix DaaS deployment using a Citrix Managed Azure subscription and SD-WAN connectivity.



The Citrix SD-WAN deployment for Citrix DaaS is similar to the standard Azure deployment configuration for Citrix SD-WAN. For more information, see Deploy Citrix SD-WAN Standard Edition Instance on Azure. In a high availability configuration, an active/standby pair of SD-WAN instances with Azure load balancers is deployed as a gateway between the subnet containing VDAs and Cloud Connectors, and the Internet. In a non-HA configuration, only a single SD-WAN instance is deployed as a gateway. Network interfaces of the virtual SD-WAN appliances are assigned addresses from a separate small address range split into two subnets.

When configuring SD-WAN connectivity, Citrix makes a few changes to the networking configuration of managed desktops described above. In particular, all outgoing traffic from the VNet, including traffic to Internet destinations, is routed through the cloud SD-WAN instance. The SD-WAN instance is also configured to be the DNS server for the Citrix-managed VNet.

Management access to the virtual SD-WAN instances requires an admin login and password. Each

instance of SD-WAN is assigned a unique, random secure password that can be used by SD-WAN administrators for remote login and troubleshooting through the SD-WAN Orchestrator UI, the virtual appliance management UI and CLI.

Just like other tenant-specific resources, virtual SD-WAN instances deployed in a specific customer VNet are fully isolated from all other VNets.

When the customer enables Citrix SD-WAN connectivity, Citrix automates the initial deployment of virtual SD-WAN instances used with Citrix DaaS, maintains underlying Azure resources (virtual machines, load balancers, and so on), provides secure and efficient out-of-the-box defaults for the initial configuration of virtual SD-WAN instances, and enables ongoing maintenance and troubleshooting through SD-WAN Orchestrator. Citrix also takes reasonable measures to perform automatic validation of SD-WAN network configuration, check for known security risks, and display corresponding alerts through SD-WAN Orchestrator.

Firewall policy for SD-WAN connections Citrix uses Azure firewall policies (network security groups) and public IP address assignment to limit access to network interfaces of virtual SD-WAN appliances:

- Only WAN and management interfaces are assigned public IP addresses and allow outbound connectivity to the Internet.
- LAN interfaces, acting as gateways for the Citrix-managed VNet, are only allowed to exchange network traffic with virtual machines on the same VNet.
- WAN interfaces limit inbound traffic to UDP port 4980 (used by Citrix SD-WAN for virtual path connectivity), and deny outbound traffic to the VNet.
- Management ports allow inbound traffic to ports 443 (HTTPS) and 22 (SSH).
- HA interfaces are only allowed to exchange control traffic with each other.

Access to infrastructure

Citrix may access the customer's Citrix-managed infrastructure (Cloud Connectors) to perform certain administrative tasks such as collecting logs (including Windows Event Viewer) and restarting services without notifying the customer. Citrix is responsible for executing these tasks safely and securely, and with minimal impact to the customer. Citrix is also responsible for ensuring any log files are retrieved, transported, and handled safely and securely. Customer VDAs cannot be accessed this way.

Backups for non-domain-joined catalogs

Citrix is not responsible for performing backups of non-domain-joined catalogs.

Backups for machine images

Citrix is responsible for backing up any machine images uploaded to Citrix DaaS, including images created with the image builder. Citrix uses locally redundant storage for these images.

Bastions for non-domain-joined catalogs

Citrix operations personnel have the ability to create a bastion, if necessary, to access the customer's Citrix-managed Azure subscription for diagnosing and repairing customer issues, potentially before the customer is aware of a problem. Citrix does not require the customer's consent to create a bastion. When Citrix creates the bastion, Citrix creates a strong randomly generated password for the bastion and restricts RDP access to Citrix NAT IP addresses. When the bastion is no longer needed, Citrix disposes of it and the password is no longer valid. The bastion (and its accompanying RDP access rules) are disposed of when the operation completes. Citrix can access only the customer's non-domain-joined Cloud Connectors with the bastion. Citrix does not have the password to log in to non-domain-joined VDAs or domain-joined Cloud Connectors and VDAs.

Firewall policy when using troubleshooting tools

When a customer requests creation of a bastion machine for troubleshooting, the following security group modifications are made to the Citrix-managed VNet:

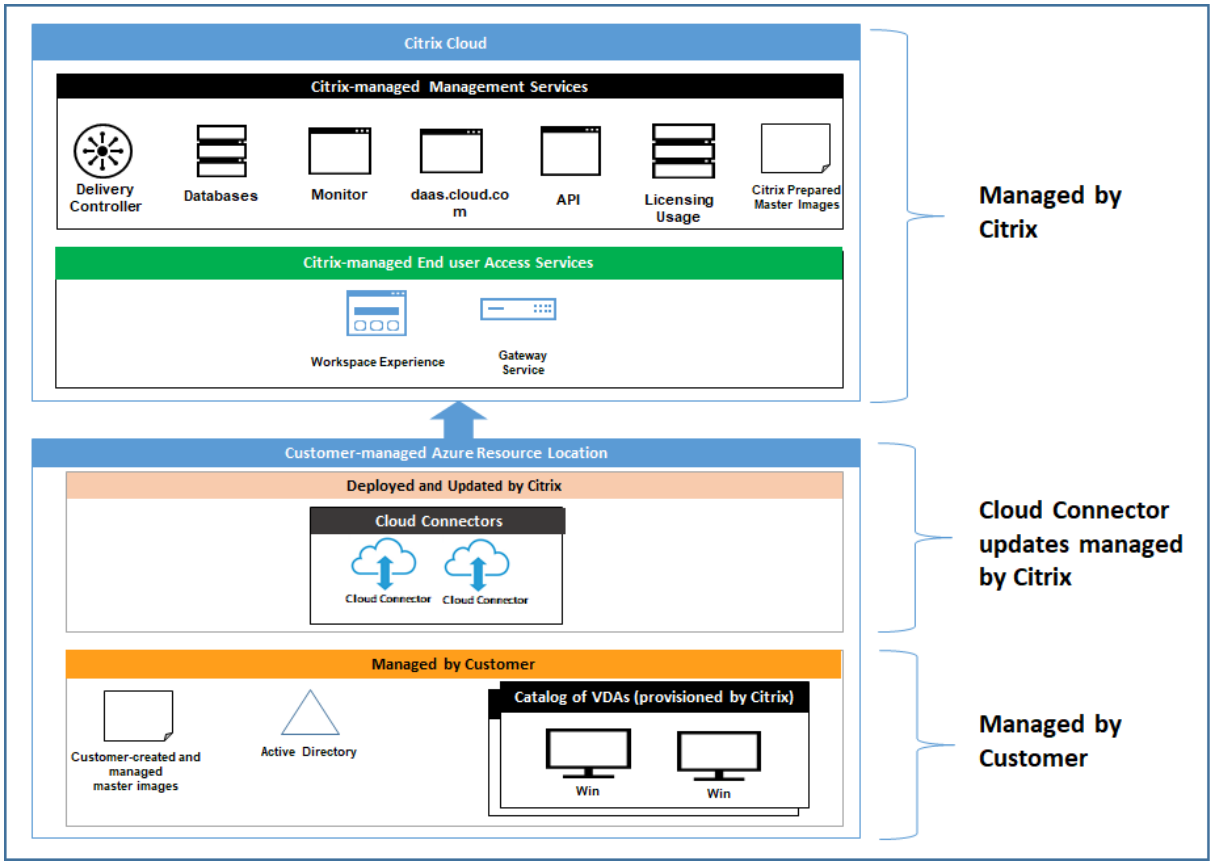
- Temporarily allow 3389 inbound from the customer-specified IP range to the bastion.
- Temporarily allow 3389 inbound from the bastion IP address to any address in the VNet (VDAs and Cloud Connectors).
- Continue to block RDP access between the Cloud Connectors, VDAs, and other VDAs.

When a customer enables RDP access for troubleshooting, the following security group modifications are made to the Citrix-managed VNet:

- Temporarily allow 3389 inbound from the customer-specified IP range to any address in the VNet (VDAs and Cloud Connectors).
- Continue to block RDP access between the Cloud Connectors, VDAs, and other VDAs.

Customer-managed subscriptions

For customer-managed subscriptions, Citrix adheres to the above responsibilities during deployment of the Azure resources. After deployment, everything above falls to the customer's responsibility, because the customer is the owner of the Azure subscription.



Customer responsibility

VDAs and machine images

The customer is responsible for all aspects of the software installed on VDA machines, including:

- Operating system updates and security patches
- Antivirus and antimalware
- VDA software updates and security patches
- Additional software firewall rules (especially outbound traffic)
- Follow Citrix security considerations and best practices

Citrix provides a prepared image that is intended as a starting point. Customers can use this image for proof-of-concept or demonstration purposes or as a base for building their own machine image. Citrix does not guarantee the security of this prepared image. Citrix will make an attempt to keep the operating system and VDA software on the prepared image up to date, and will enable Windows Defender on these images.

Customer responsibility when using VNet peering

The customer must open all ports specified in Customer-managed VNet with domain-joined machines.

When VNet peering is configured, the customer is responsible for the security of their own virtual network and its connectivity to their on-premises resources. The customer is also responsible for security of the incoming traffic from the Citrix-managed peered virtual network. Citrix does not take any action to block traffic from the Citrix-managed virtual network to the customer's on-premises resources.

Customers have the following options for restricting incoming traffic:

- Give the Citrix-managed virtual network an IP block which is not in use elsewhere in the customer's on-premises network or the customer-managed connected virtual network. This is required for VNet peering.
- Add Azure network security groups and firewalls in the customer's virtual network and on-premises network to block or restrict traffic from the Citrix-managed IP block.
- Deploy measures such as intrusion prevention systems, software firewalls, and behavioral analytics engines in the customer's virtual network and on-premises network, targeting the Citrix-managed IP block.

Customer responsibility when using SD-WAN connectivity

When SD-WAN connectivity is configured, customers have full flexibility to configure virtual SD-WAN instances used with Citrix DaaS according to their networking requirements, with the exception of a few elements required to ensure correct operation of SD-WAN in the Citrix-managed VNet. Customer responsibilities include:

- Design and configuration of routing and firewall rules, including rules for DNS and Internet traffic breakout.
- Maintenance of the SD-WAN network configuration.
- Monitoring of the operational status of the network.
- Timely deployment of Citrix SD-WAN software updates or security fixes. Since all instances of Citrix SD-WAN on a customer network must run the same version of SD-WAN software, deployments of updated software versions to Citrix DaaS SD-WAN instances need to be managed by customers according to their network maintenance schedules and constraints.

Incorrect configuration of SD-WAN routing and firewall rules, or mismanagement of SD-WAN management passwords, may result in security risks to both virtual resources in Citrix DaaS, and on-premises resources reachable through Citrix SD-WAN virtual paths. Another possible security risk stems from not updating Citrix SD-WAN software to the latest available patch release. While SD-WAN Orchestrator and other Citrix Cloud services provide the means to address such risks, customers are ultimately responsible for ensuring that virtual SD-WAN instances are configured appropriately.

Proxy

The customer may choose whether to use a proxy for outbound traffic from the VDA. If a proxy is used, the customer is responsible for:

- Configuring the proxy settings on the VDA machine image or, if the VDA is joined to a domain, using Active Directory Group Policy.
- Maintenance and security of the proxy.

Proxies are not allowed for use with Citrix Cloud Connectors or other Citrix-managed infrastructure.

Catalog resiliency

Citrix provides three types of catalogs with differing levels of resiliency:

- **Static:** Each user is assigned to a single VDA. This catalog type provides no high availability. If a user's VDA goes down, they will have to be placed on a new one to recover. Azure provides a 99.5% SLA for single-instance VMs. The customer can still back up the user profile, but any customizations made to the VDA (such as installing programs or configuring Windows) will be lost.
- **Random:** Each user is assigned randomly to a server VDA at launch time. This catalog type provides high availability via redundancy. If a VDA goes down, no information is lost because the user's profile resides elsewhere.
- **Windows 10 multisession:** This catalog type operates in the same manner as the random type but uses Windows 10 workstation VDAs instead of server VDAs.

Backups for domain-joined catalogs

If the customer uses domain-joined catalogs with a VNet peering, the customer is responsible for backing up their user profiles. Citrix recommends that customers configure on-premises file shares and set policies on their Active Directory or VDAs to pull user profiles from these file shares. The customer is responsible for the backup and availability of these file shares.

Disaster recovery

In the event of Azure data loss, Citrix will recover as many resources in the Citrix-managed Azure subscription as possible. Citrix will attempt to recover the Cloud Connectors and VDAs. If Citrix is unsuccessful recovering these items, customers are responsible for creating a new catalog. Citrix assumes that machine images are backed up and that customers have backed up their user profiles, allowing the catalog to be rebuilt.

In the event of the loss of an entire Azure region, the customer is responsible for rebuilding their customer-managed virtual network in a new region and creating a new VNet peering or a new SD-WAN instance within Citrix DaaS.

Citrix and customer shared responsibilities

Citrix Cloud Connector for domain-joined catalogs

Citrix DaaS deploys at least two Cloud Connectors in each resource location. Some catalogs may share a resource location if they are in the same region, VNet peering, and domain as other catalogs for the same customer. Citrix configures the customer's domain-joined Cloud Connectors for the following default security settings on the image:

- Operating system updates and security patches
- Antivirus software
- Cloud Connector software updates

Customers do not normally have access to the Cloud Connectors. However, they may acquire access by using catalog troubleshooting steps and logging in with domain credentials. The customer is responsible for any changes they make when logging in through the bastion.

Customers also have control over the domain-joined Cloud Connectors through Active Directory Group Policy. The customer is responsible for ensuring that the group policies that apply to the Cloud Connector are safe and sensible. For example, if the customer chooses to disable operating system updates using Group Policy, the customer is responsible for performing operating system updates on the Cloud Connectors. The customer can also choose to use Group Policy to enforce stricter security than the Cloud Connector defaults, such as by installing a different antivirus software. In general, Citrix recommends that customers put Cloud Connectors into their own Active Directory organizational unit with no policies, as this will ensure that the defaults Citrix uses can be applied without issue.

Troubleshooting

In the event the customer experiences problems with the catalog in Citrix DaaS, there are two options for troubleshooting: using bastions and enabling RDP access. Both options introduce security risk to the customer. The customer must understand and consent to undertaking this risk prior to using these options.

Citrix is responsible for opening and closing the necessary ports to carry out troubleshooting operations, and restricting which machines can be accessed during these operations.

With either bastions or RDP access, the active user performing the operation is responsible for the security of the machines that are being accessed. If the customer accesses the VDA or Cloud Connector through RDP and accidentally contracts a virus, the customer is responsible. If Citrix Support personnel access these machines, it is the responsibility of those personnel to perform operations safely. Responsibility for any vulnerabilities exposed by any person accessing the bastion or other machines in the deployment (for example, customer responsibility to add IP ranges to allow list, Citrix responsibility to implement IP ranges correctly) is covered elsewhere in this document.

In both scenarios, Citrix is responsible for correctly creating firewall exceptions to allow RDP traffic. Citrix is also responsible for revoking these exceptions after the customer disposes of the bastion or ends RDP access through Citrix DaaS.

Bastions Citrix may create bastions in the customer's Citrix-managed virtual network within the customer's Citrix-managed subscription to diagnose and repair issues, either proactively (without customer notification) or in response to a customer-raised issue. The bastion is a machine that the customer can access through RDP and then use to access the VDAs and (for domain-joined catalogs) Cloud Connectors through RDP to gather logs, restart services, or perform other administrative tasks. By default, creating a bastion opens an external firewall rule to allow RDP traffic from a customer-specified range of IP addresses to the bastion machine. It also opens an internal firewall rule to allow access to the Cloud Connectors and VDAs through RDP. Opening these rules poses a large security risk.

The customer is responsible for providing a strong password used for the local Windows account. The customer is also responsible for providing an external IP address range that allows RDP access to the bastion. If the customer elects not to provide an IP range (allowing anyone to attempt RDP access), the customer is responsible for any access attempted by malicious IP addresses.

The customer is also responsible for deleting the bastion after troubleshooting is complete. The bastion host exposes additional attack surface, so Citrix automatically shuts down the machine eight (8) hours after it is powered on. However, Citrix never automatically deletes a bastion. If the customer chooses to use the bastion for an extended period of time, they are responsible for patching and updating it. Citrix recommends that a bastion be used only for several days before deleting it. If the customer wants an up-to-date bastion, they can delete their current one and then create a new bastion, which will provision a fresh machine with the latest security patches.

RDP access For domain-joined catalogs, if the customer's VNet peering is functional, the customer can enable RDP access from their peered VNet to their Citrix-managed VNet. If the customer uses this option, the customer is responsible for accessing the VDAs and Cloud Connectors over the VNet peering. Source IP address ranges can be specified so RDP access can be restricted further, even within the customer's internal network. The customer will need to use domain credentials to log in to these machines. If the customer is working with Citrix Support to resolve an issue, the customer may need

to share these credentials with support personnel. After the issue is resolved, the customer is responsible for disabling RDP access. Keeping RDP access open from the customer's peered or on-premises network poses a security risk.

Domain credentials

If the customer elects to use a domain-joined catalog, the customer is responsible for providing to Citrix DaaS a domain account (username and password) with permissions to join machines to the domain. When supplying domain credentials, the customer is responsible for adhering to the following security principles:

- **Auditable:** The account should be created specifically for Citrix DaaS usage so that it is easy to audit what the account is used for.
- **Scoped:** The account requires only permissions to join machines to a domain. It should not be a full domain administrator.
- **Secure:** A strong password should be placed on the account.

Citrix is responsible for the secure storage of this domain account in an Azure Key Vault in the customer's Citrix-managed Azure subscription. The account is retrieved only if an operation requires the domain account password.

More information

For related information, see:

- Secure Deployment Guide for the Citrix Cloud Platform: Security information for the Citrix Cloud platform.
- Technical security overview: Security information for the Citrix DaaS
- Third party notifications

Virtual channel allow list

April 25, 2024

The virtual channel allow list is a feature that allows you to control which non-Citrix virtual channels are allowed in your environment. By default, the virtual channel allow list feature is enabled. As a result, only Citrix virtual channels are allowed to open in Citrix Virtual Apps and Desktops sessions. If there is a need to use custom virtual channels, whether homegrown or from a third party, these need to be explicitly added to the allow list.

Configuration

The virtual channel allow list is enabled by default. You can configure this feature using the following settings in the Citrix policy:

- **Virtual channel allow list**: to enable or disable the feature and to add virtual channels to the list.
- **Virtual channel allow list log throttling**: sets the throttling period for the virtual channel allow list event logging.
- **Virtual channel allow list logging**: sets the logging level for the virtual channel allow list.

Adding virtual channels to the allow list

To add a virtual channel to the allow list, you need the following information:

1. The virtual channel name as defined in the code, which can be up to seven characters long. For example, `CTXCVC1`.
2. The paths to the processes that open the virtual channel on the VDA machine. For example, `C:\Program Files\Application\run.exe`.

Once you have the required information, you must add the virtual channel to the allow list using the Virtual channel allow list policy setting. To add a virtual channel to the list, enter the virtual channel name followed by a comma, and then the path to the process that accesses the virtual channel. If there are multiple processes, you can add these processes by separating each process with commas.

For single processes

Using the previous examples, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

For multiple processes

If there are multiple processes, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```


Using wildcards

The use of wildcards (*) is supported. You can use wildcards when the names of directories or executables change based on the version of the application, or if the third-party component is installed in the users' profiles.

You can use wildcards in the following scenarios:

- To replace the full directory name.
  For example: `C:\Program Files\Application\*\run1.exe`
- To replace part of the directory name.
  For example: `C:\Program Files\Application\v*\run1.exe`
- To replace the executable's name.
  For example: `C:\Program Files\Application\v1.2\*.exe`
- To replace part of the executable's name.
  For example: `C:\Program Files\Application\v1.2\run*.exe`

The following restrictions apply:

- The wildcard can only be used to replace a single directory. For example, if the executable is located in `C:\Program Files\Application\v1.2\run1.exe`
  - Allowed: `C:\Program Files\Application\*\run1.exe`
  - Not allowed: `C:\Program Files\*\run1.exe`
- Entries must contain the file name extension.
  - Allowed: `C:\Program Files\Application\v1.2\*.exe`
  - Not allowed: `C:\Program Files\Application\v1.2\*`
- All paths must be local.

> **Note:**
>
> - Network paths are not allowed.
> - Wildcard support is available from Citrix Virtual Apps and Desktops 2206.
> - Wildcard support is available in Citrix Virtual Apps and Desktops 2203 LTSR from CU2.

Using system environment variables

You can use system environment variables to simplify the definition of the trusted processes in your allow list. You can use any of the out-of-box variables, such as `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%`, and `%systemroot%`.

You can also use custom environment variables as long as they are defined at the system level.

The following examples depict out-of-box environment variables:

- %programfiles%\Application\v1.2\run.exe
- %programfiles%\Application*\run.exe
- %programfiles(x86)%\Application\v1.*\run.exe

The following example depicts a custom system environment variable:

- Custom variable name: app
- Custom variable value: %programfiles%\Application\
- Allow list entry: CTXCVC1,%app%\run.exe

> **Note:**
>
> User environment variables are not supported.
>
> Environment variable support is available from Citrix Virtual Apps and Desktops version 2209.

Obtain virtual channel names and processes

The easiest way to obtain the name of the virtual channel and the process that opens it on the VDA machine is to get the information from the developer or a third-party vendor that provided the virtual channel.

Alternatively, you can obtain information by applying the feature's logs and following these steps:

1. Once the client and server components of the custom virtual channel are in place, launch a virtual application or virtual desktop.
2. In the VDA machine's System event log, look for the custom virtual channel's name and the process that tried to open it. For more information on available events, see Event logs.
3. Log out from the session.
4. Add an entry in the virtual channel allow list policy settings for the identified virtual channel and process.
5. Restart the machine.
6. Once the VDA is registered, run the virtual application or virtual desktop to validate that the custom virtual channels open successfully.

Considerations for Citrix virtual channels

All built-in Citrix virtual channels are trusted and allowed to open without further configuration. However, the following two features require explicit entries in the allow list because of external dependencies:

- Multimedia Redirection
- HDX RealTime Optimization Pack for Skype for Business

Multimedia Redirection

If you use a media player other than Windows Media Player as your system media player, you need to add it to the allow list as a trusted process. The following information is required for the allow list entry:

- Virtual channel name: `CTXMM`
- Process: Path to the media player used in your VDA machine. For example, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Allow list entry: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

The following information is required for the allow list entry:

- Virtual channel name: `CTXRMEP`
- Process: Path to the Skype for Business executable in your VDA machine, which can vary based on the version of Skype for Business or if you used a custom installation path. For example, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Allow list entry: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Delivery methods

May 11, 2022

A single delivery method likely cannot meet all of your requirements.

You can consider several application delivery methods. Choosing the appropriate method helps improve scalability, management, and user experience.

- **Installed app:** The application is part of the base desktop image. The install process involves dll, exe, and other files copied to the image drive in addition to registry modifications. For details, see Create machine catalogs.
- **Streamed app (Microsoft App-V):** The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings are placed in a container on the virtual desktop, isolated from the base operating system and each other. This action helps address compatibility issues. For details, see App-V.

- **Layered app (Citrix App Layering):** Each layer contains a single application, agent, or operating system. By integrating one OS layer, one platform layer (for example, VDA) and many application layers, an administrator can easily create new, deployable images. Layering simplifies ongoing maintenance, as an OS, agent and application exists in a single layer. When you update the layer, all deployed images containing that layer are updated. See Citrix App Layering.
- **Hosted Windows app:** An application installed on a multi-user Citrix Virtual Apps host and deployed as an application and not a desktop. A user accesses the hosted Windows app seamlessly from the VDI desktop or endpoint device, hiding the fact that the app is running remotely. For details, see Create delivery groups.
- **Local app:** An application deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it runs on the endpoint. For details, see Local App Access and URL redirection.

For desktops, you can consider Citrix Virtual Apps published desktops or VDI desktops.

Citrix Virtual Apps published apps and desktops

Use multi-session OS machines to deliver Citrix Virtual Apps published apps and published desktops.

Use case:

- You want inexpensive server-based delivery to minimize the cost of delivering applications to many users, while providing a secure, high-definition user experience.
- Your users perform well-defined tasks and do not require personalization or offline access to applications. Users can include task workers such as call center operators and retail workers, or users that share workstations.
- Application types: any application.

Benefits and considerations:

- Manageable and scalable solution within your data center.
- Most cost effective application delivery solution.
- Hosted applications are managed centrally and users cannot modify the application, providing a user experience that is consistent, safe, and reliable.
- Users must be online to access their applications.

User experience:

- User requests one or more applications from StoreFront, their Start menu, or a URL you provide to them.
- Applications are delivered virtually and display seamlessly in high definition on user devices.

- Depending on profile settings, user changes are saved when the user's application session ends. Otherwise, the changes are deleted.

Process, host, and deliver applications:

- Application processing takes place on hosting machines, rather than on the user devices. The hosting machine can be a physical or a virtual machine.
- Applications and desktops reside on a multi-session OS machine.
- Machines become available through machine catalogs.
- Machines from machine catalogs are organized into delivery groups that deliver the same set of applications to groups of users.
- Multi-session OS machines support delivery groups that host either desktops or applications, or both.

Session management and assignment:

- Multi-session OS machines run multiple sessions from a single machine to deliver multiple applications and desktops to multiple, simultaneously connected users. Each user requires a single session from which they can run all their hosted applications.

  For example, a user logs on and requests an application. One session on that machine becomes unavailable to other users. A second user logs on and requests an application which that machine hosts. A second session on the same machine is now unavailable. If both users request more applications, no additional sessions are required because a user can run multiple applications using the same session. If two more users log on and request desktops, and two sessions are available on that machine, that one machine now uses four sessions to host four different users.

- Within the delivery group to which a user is assigned, a machine on the least loaded server is selected. A machine with session availability is randomly assigned to deliver applications to a user when that user logs on.

VM hosted apps

Use single-session OS machines to deliver VM hosted applications

Use case:

- You want a client-based application delivery solution that is secure, provides centralized management, and supports many users per host server. You want to provide those users with applications that display seamlessly in high-definition.
- Your users are internal, external contractors, third-party collaborators, and other provisional team members. Your users do not require offline access to hosted applications.

- Application types: Applications that might not work well with other applications or might interact with the operation system, such as Microsoft .NET framework. These types of applications are ideal for hosting on virtual machines.

Benefits and considerations:

- Applications and desktops on the image are securely managed, hosted, and run on machines within your data center, providing a more cost effective application delivery solution.
- Upon logon, users can be randomly assigned to a machine within a delivery group that is configured to host the same application. You can also statically assign a single machine to deliver an application to a single user each time that user logs on. Statically assigned machines allow users to install and manage their own applications on the virtual machine.
- Running multiple sessions is not supported on single-session OS machines. Therefore, each user consumes a single machine within a delivery group when they log on, and users must be online to access their applications.
- This method can increase the amount of server resources for processing applications and increase the amount of storage for users' personal vDisks.

User experience:

- The same seamless application experience as hosting shared applications on multi-session OS machines.

Process, host, and deliver applications:

- The same as multi-session OS machines except they are virtual single-session OS machines.

Session management and assignment:

- Single-session OS machines run a single desktop session from a single machine. When accessing applications only, one user can use multiple applications (and is not limited to a single application). The operating system sees each application as a new session.
- Within a delivery group, logged-on users can access either a statically assigned machine (each time the user logs on to the same machine), or a randomly assigned machine that is selected based on session availability.

VDI desktops

Use single-session OS machines to deliver Citrix Virtual Desktops VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system.

VDI desktops require more resources than Citrix Virtual Apps published desktops, but do not require that applications installed on them support server-based operating systems. Also, depending on the

type of VDI desktop you choose, these desktops can be assigned to individual users. This allows users a high level of personalization.

When you create a machine catalog for VDI desktops, you create one of these types of desktops:

- **Random non-persistent desktop, also known as pooled VDI desktop:** Each time a user logs on to one of these desktops, that user connects to a desktop selected from a pool of desktops. That pool is based on a single image. All changes to the desktop are lost when the machine restarts.
- **Static non-persistent desktop:** During the first logon, a user is assigned a desktop from a pool of desktops. (Each machine in the pool is based on a single image.) After the first use, each time a user logs on to use one of these desktops, that user connects to the same desktop that was assigned on first use. All changes to the desktop are lost when the machine restarts.
- **Static persistent desktop:** Unlike other types of VDI desktops, users can fully personalize these desktops. During the first logon, a user is assigned a desktop from a pool of desktops. Subsequent logons from that user connect to the same desktop that was assigned on first use. Changes to the desktop are retained when the machine restarts.

Remote PC Access

Remote PC Access is a feature of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Remote PC Access eliminates the need to introduce and provide other tools to accommodate teleworking. For example, virtual desktops or applications and their associated infrastructure.

Remote PC Access uses the same Citrix DaaS components that deliver virtual desktops and applications. As a result, the requirements and process of deploying and configuring Remote PC Access are the same as those required for deploying Citrix DaaS for the delivery of virtual resources. This uniformity provides a consistent and unified administrative experience. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

For more information, Remote PC Access.

Get started: Plan and build a deployment

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

If you're not familiar with the components, terminology, and objects used with Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), see Citrix DaaS.

For a customer journey perspective, go to the Citrix Success Center. The Success Center provides guidance for the five key stages of your Citrix journey: plan, build, roll out, manage, and optimize.

- The Success Center information is an essential partner to this product documentation.
- Success Center articles and guides offer a broad solution-based perspective. They also contain links to service-specific details in this product documentation.

If you're migrating from a Citrix Virtual Apps and Desktops deployment, see Migrate to cloud.

> **Important:**
>
> To ensure that you get important information about Citrix Cloud and the Citrix services you subscribe to, make sure you can receive all email notifications.
>
> In the upper right corner of the Citrix Cloud console, expand the menu to the right of the customer name and OrgID fields. Select **Account Settings**. On the **My Profile** tab, select all entries in the **Email Notifications** section.

How to use this article

To set up your Citrix DaaS deployment, complete the tasks summarized below. Links are provided to each task's details.

Review the entire process before starting the deployment, so you know what to expect. This article also links to other helpful information sources.

> **Note:**
>
> If you plan to use the Quick Deploy interface to provision Microsoft Azure machines, follow the setup guidance in Get started with Quick Deploy.

Plan and prepare

Use the Success Center Plan guidance to help establish goals, define use cases and business objectives, identify potential risks, and create a project plan.

In the Citrix Tech Zone documentation, see a step-by-step proof of concept guide for this service.

Sign up

Sign up for a Citrix account and request a Citrix DaaS demo.

Set up a resource location

A resource location contains resources required to deliver applications and desktops to users. Creating resource locations enables DaaS to use those resources. To learn more about resource locations, see Connect to Citrix Cloud.

Before creating machines, you must connect a resource location to DaaS:

- Domain-joined machines require that you have Cloud Connectors installed in the resource location. In this case, you can:
  - Create on-premises Active Directory joined catalogs
  - Create Azure Active Directory joined catalogs
  - Create hybrid Azure Active Directory joined catalogs

  For high availability, we recommend that you install two Cloud Connectors in each resource location. See Cloud Connector installation.

  More information:

  - What are resource locations and Cloud Connectors?
  - Video about installing Cloud Connectors:

- Non-domain-joined machines don't require Cloud Connectors but require that you have Rendezvous V2 enabled. The Rendezvous protocol allows VDAs to bypass the Cloud Connectors to connect directly and securely with DaaS. See Rendezvous V2. In this case, you can:
  - Create non-domain-joined catalogs

If you're using the Quick Deploy interface to provision Azure VMs, Citrix creates the resource location and Cloud Connectors for you.

Create a connection to the resource location

After you add a resource location and Cloud Connectors, create a connection to the resource location using the Full Configuration interface of Citrix DaaS.

This step isn't necessary in either of the following cases:

- You're building a simple proof of concept deployment
- You're using the Quick Deploy interface to provision Azure VMs.

More information:

- What are hosts?
- What are host connections?

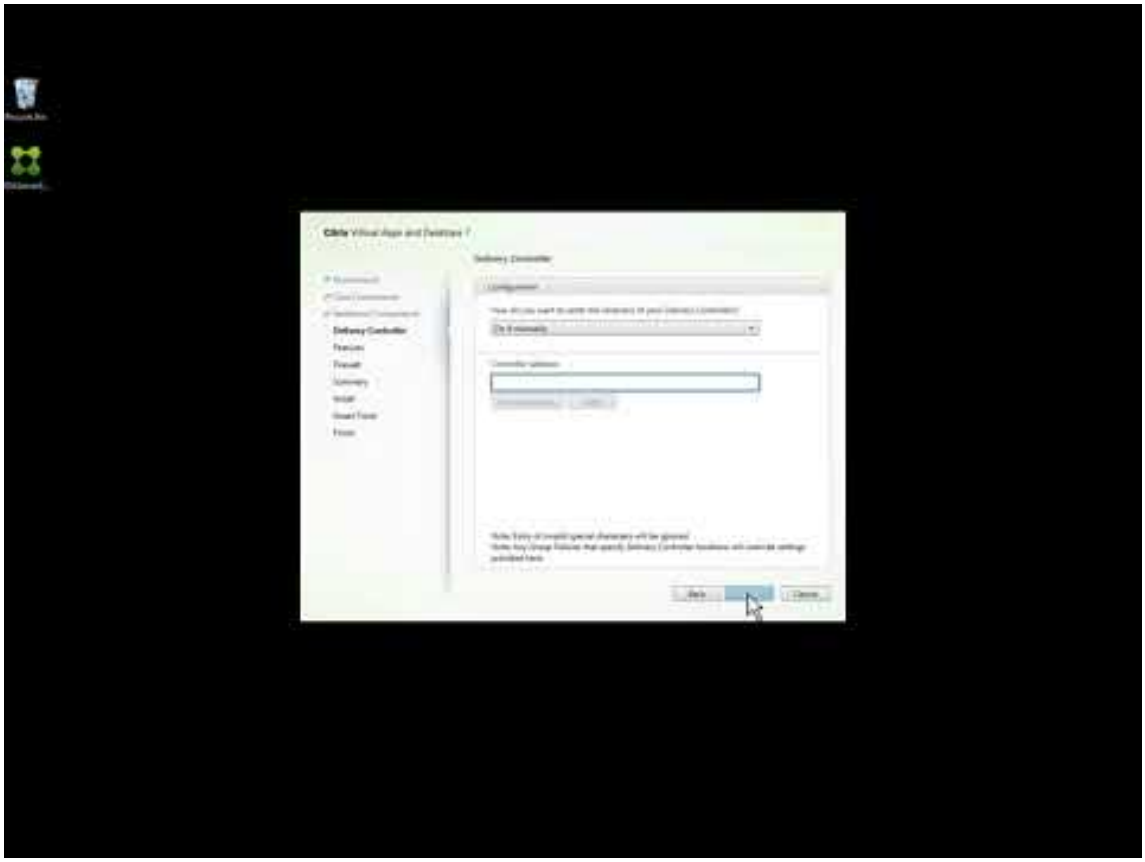
Install VDAs

Each machine that delivers applications and desktops to users must have a Citrix Virtual Delivery Agent (VDA) installed on it.

- For a simple proof of concept deployment, download and install a VDA on one machine.
- If you're using an image to provision VMs, install a VDA on the image.
- For a Remote PC Access deployment, install the core version of the VDA for single-session OS on each physical office PC.

How-to and more information:

- What are VDAs?
- Installation preparation and instruction
- Command-line VDA installation
- Video about downloading and installing a VDA:

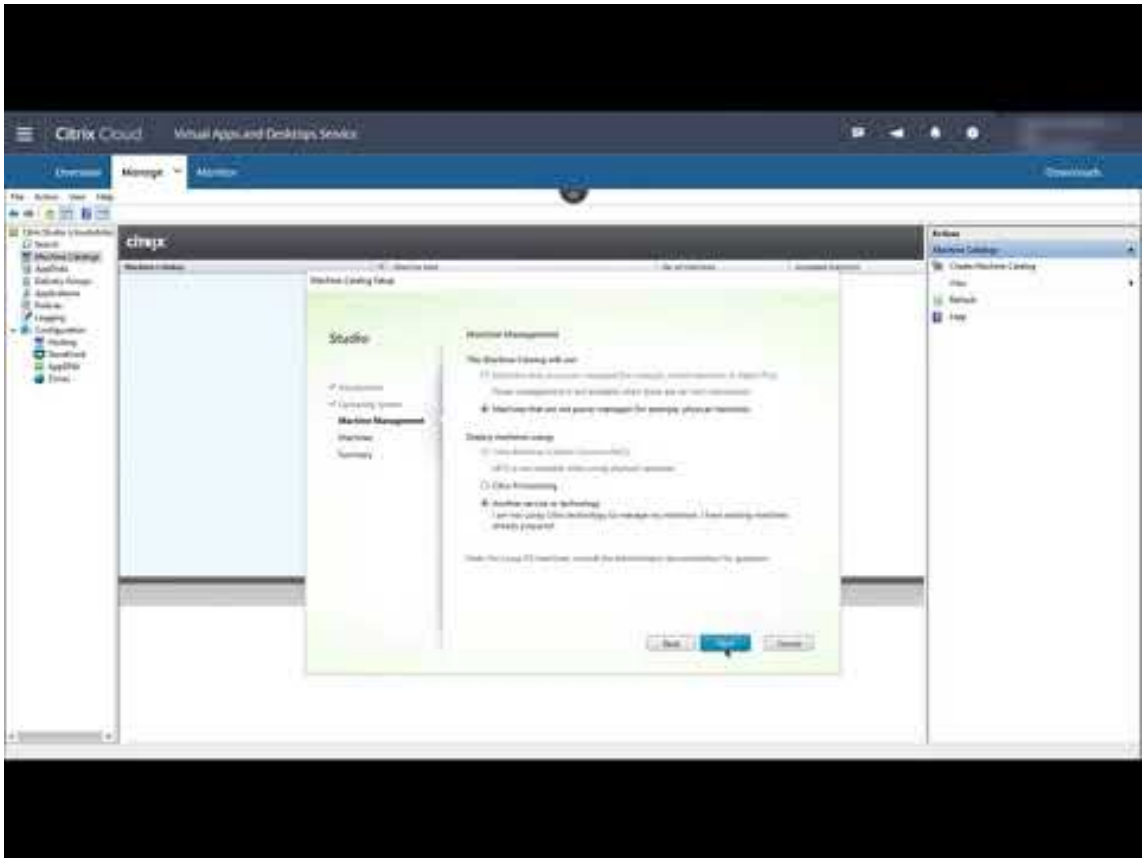


Create a catalog

After you create a connection to your resource location (if needed), you create a catalog. If you're using the Full Configuration interface, the workflow guides you automatically to this step.

How-to and more information:

- What are catalogs?
- Create a catalog
- Use the Quick Deploy interface to deploy a catalog containing Azure VMs.
- Video about creating a catalog using the full configuration management interface:



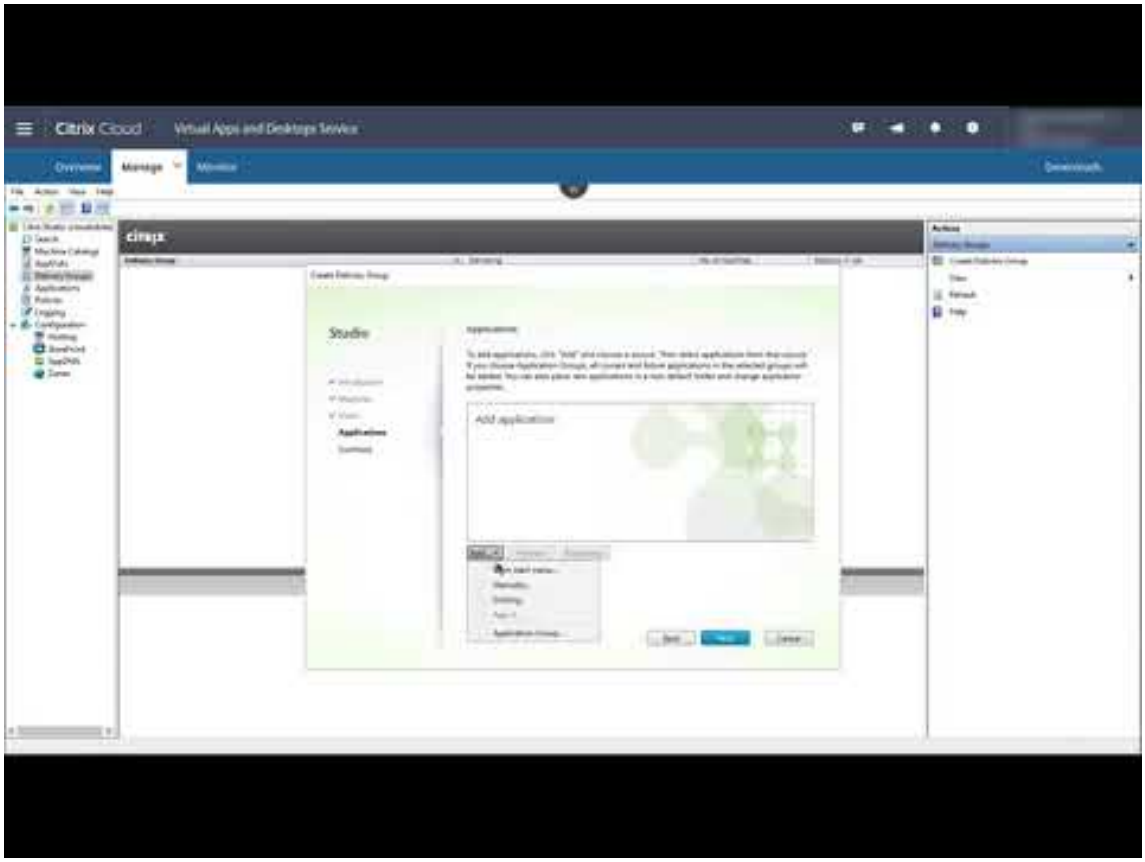
Create a delivery group

After you create your first catalog, the **Manage** workflow guides you to create a delivery group.

This step isn't necessary if you're using the Quick Deploy interface to provision Azure VMs.

How-to and more information:

- What are delivery groups?
- Create a delivery group
- Video about how to create a delivery group:



Deploy other components and technologies

After you complete the tasks above that set up the Citrix DaaS deployment, follow the guidance in the Build area of the Citrix Success Center. You'll find information about provisioning and configuring other components and technologies in the Citrix solution, such as:

- Citrix policies
- StoreFront
- App Layering
- Workspace Environment Management (WEM) Service
- Citrix Gateway service
- Zones
- Federated Authentication Service (FAS)

Complete other tasks that apply to your configuration. For example, if you plan to deliver Windows Server workloads, configure a Microsoft RDS License Server.

Launch applications and desktops

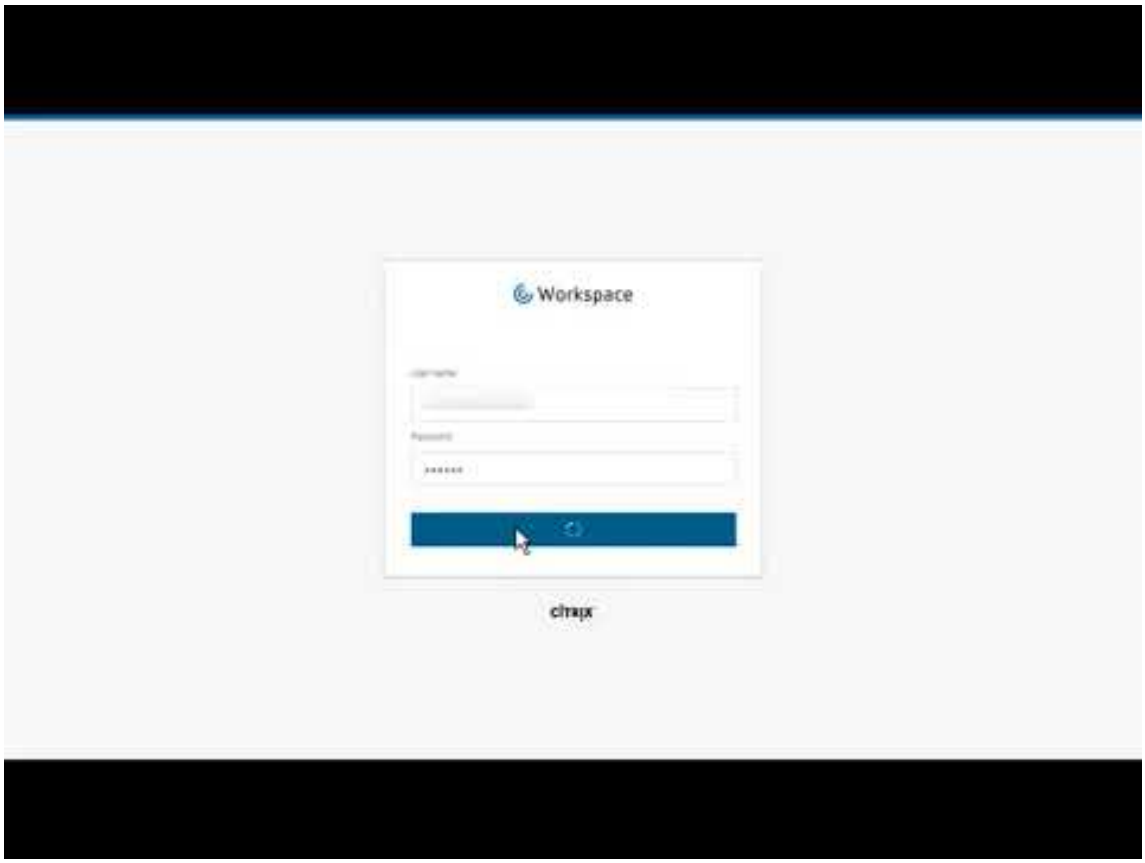
After you configure your deployment, publishing occurs automatically. Applications and desktops that you configured are available to users in their Citrix Workspace. A user simply navigates to their Workspace URL and selects an application or desktop, which launches immediately.

Send the Workspace URL to your users. You can find the workspace URL in two locations:

- From the Citrix Cloud console, select **Workspace Configuration** from the menu in the upper left corner. The **Access** tab contains the Workspace URL.
- From the Citrix DaaS **Overview** page, the workspace URL appears near the bottom of the page.

More information:

- Video about users launching applications and desktops from their Workspace:



More information

The Citrix Cloud Learning series provides education courses that are organized by your path:

- If you're new to Citrix DaaS, see New to Citrix DaaS Learning Path.

- If you're migrating from a Citrix Virtual Apps and Desktops deployment, see Migrating Citrix DaaS to Citrix Cloud Learning Path.

Sign up for Citrix DaaS

May 17, 2022

Introduction

You can subscribe to Citrix DaaS through Citrix or through the Azure Marketplace.

If you plan to use Citrix Managed Azure, you can also order the Citrix Azure Consumption Fund through Citrix or through the Azure Marketplace.

- When you order through Citrix, you can order Citrix DaaS and the Citrix Azure Consumption Fund at the same time.
- When you order through Azure Marketplace, you first order Citrix DaaS. Then, you can place another order for the Citrix Azure Consumption Fund.

If you order only Citrix DaaS now, you can order the Citrix Azure Consumption Fund later, either through Azure Marketplace or your Citrix account representative.

Demos and trials

You can evaluate Citrix DaaS by request through Citrix. From a trial, you can convert to a paid service subscription.

During a trial, you can optionally use a Citrix Managed Azure subscription for catalogs, images, and network connections. If you have Citrix-managed resources at the time you convert to a paid subscription, you must either purchase consumption or delete those Citrix-managed resources. If you do not purchase consumption, those resources are deleted automatically, which might affect users.

If you currently subscribe to a Citrix DaaS service

Generally, a Citrix Cloud account allows you to subscribe to only one of Citrix DaaS's services (or one edition) at a time per Citrix OrgID. For example, you can subscribe to Citrix DaaS Premium edition OR Citrix DaaS for Azure, but not both.

If you currently subscribe to a Citrix DaaS, and want to subscribe to this service, you have two choices:

- Subscribe to this service using a different Citrix Cloud account (OrgID).
- Decommission Citrix DaaS you already have, and then order this service. For decommission instruction, see CTX239027.

Order through Citrix

You can order this service (and the Citrix Azure Consumption Fund) through Citrix Cloud or through your Citrix account representative.

Through Citrix Cloud:

- Follow the guidance in Sign up for Citrix Cloud to get a Citrix Cloud account and Organization ID.
- You can request a Citrix DaaS demo. In the Citrix DaaS tile, click **Request Demo**. Provide the requested information.

  A Citrix representative will contact you to discuss your requirements, environment, and plans. Depending on our representative's assessment, you will be authorized to participate in an administrator demo or a proof of concept trial. For more information, see Citrix Cloud Service Trials.

When you are authorized for a trial, the text on Citrix DaaS tile in the Citrix Cloud console changes to **Manage**.

Order through Azure Marketplace

You can order the following Citrix offerings through Azure Marketplace:

- Citrix DaaS for Azure
- Citrix DaaS Advanced edition
- Citrix DaaS Premium edition
- Workspace Premium Plus

If you plan to host your Citrix Virtual Apps and Desktops workloads on Microsoft Azure, and want to use a Citrix Managed Azure subscription, order the Citrix Azure Consumption Fund after ordering Citrix DaaS or Workspace Premium Plus.

With the Citrix Azure Consumption Fund, you're charged each month for your consumption, which can vary depending on the hosting resources you choose and the hours of use. You can review your consumption use through Citrix Cloud.

From the Azure Marketplace:

- You cannot combine Citrix DaaS and consumption fund in one order.

- The order process for the Citrix Azure Consumption Fund is essentially the same as ordering Citrix DaaS, but you must have previously ordered Citrix DaaS.

Requirements for ordering through Azure Marketplace

- The OrgID of your Citrix Cloud account.
  - If you have a Citrix Cloud account, but don't know the OrgID, look in the upper right corner of the Citrix Cloud console. Or, look at the email you received when you created the account.
  - If you don't have a Citrix Cloud account, follow the guidance in Sign up for Citrix Cloud.
- An Azure account and at least one Azure subscription in that account.

Procedure for ordering through Azure Marketplace

Follow this procedure to order a Citrix DaaS or Workspace Premium Plus through Azure Marketplace. (If you want to use Citrix Managed Azure, place another order for the Citrix Azure Consumption Fund, after you order Citrix DaaS.)

1. Sign in to the Azure Marketplace using your Azure account credentials.
2. Search for and then navigate to the Citrix offering you want to order.
3. Select **Get it now**.
4. On the **One more thing** message, fill in the required information, enable the consent check box, and then select **Continue**.
5. Review the tabs containing information about the product, plans, pricing, and usage. When you're ready, select a plan (if more than one is available), and then select **Set up + subscribe**.
6. On the **Basics** tab:
   - **Subscription:** Indicates the plan that you selected.
   - **Resource group:** Select or create a resource group.
   - **Name:** Enter a name for your subscription order so you can easily identify it later.
   - The **Plan** information shows the price for the selected plan, based on the billing term. To change the plan term, select **Change plan**. Select the term you want and select **Change plan**.
7. On the **Review + subscribe** tab, review the contact information, and update it, if needed. Review the basic subscription information. Select **Subscribe**.
8. On the **Subscription in progress** page, select **Configure account now**. (If the button is disabled, wait a moment.) You're taken to a Citrix activation page.

9. On the activation page:
    - Use the **Sign in** link to sign in to Citrix Cloud. A successful sign-in automatically populates the **Organization ID** field.
    - **Quantity:** Enter the number of users. (An initial order must be at least 25.) An estimated price is displayed.
    - Agree to the terms and conditions, and then select **Activate Order**.

After ordering through Azure Marketplace

Citrix sends you an email when your service is provisioned. Provisioning can take a while. If you don't receive the email by the following day, contact Citrix Support. When you receive the email from Citrix, you can begin using Citrix DaaS.

Fulfillment of a Citrix Azure Consumption Fund order does not take much time. When Citrix is notified of the order, a banner appears in the Citrix DaaS console, indicating that a Citrix Managed Azure subscription will be prepared for you.

Do not delete Citrix DaaS resource in Azure. Deleting that resource cancels your subscription.

Order through Google Cloud Marketplace

You can order the following Citrix offerings through Google Cloud Marketplace:

- Citrix DaaS Standard for Google Cloud
- Citrix DaaS Premium for Google Cloud

You need the following to order through Google Cloud Marketplace:

- The OrgID of your Citrix Cloud account.
    - If you have a Citrix Cloud account, but don't know the OrgID, look in the upper right corner of the Citrix Cloud console. Or, look at the email you received when you created the account.
    - If you don't have a Citrix Cloud account, follow the guidance in Sign up for Citrix Cloud.
- A Google Cloud account and at least one Google Cloud subscription in that account.

To place your order:

1. Sign in to Google Cloud Marketplace
2. Follow the instructions on the Citrix DaaS for Google Cloud page to make your purchase.

Citrix sends you an email when your service is provisioned. Provisioning can take a while. If you don't receive the email by the following day, contact Citrix Support. When you receive the email from Citrix, you can begin using Citrix DaaS.

Do not delete Citrix DaaS resource in Google Cloud. Deleting that resource cancels your subscription.

What's next

After your order is fulfilled, continue with the next steps in Plan and build a deployment.

For example:

- If you haven't already set up your hypervisor or cloud service, or Active Directory, see Set up a resource location.
- If your host environment and Active Directory are already set up, see Create a connection.

Citrix HDX Plus for Windows 365

October 13, 2022

Citrix HDX Plus for Windows 365 allows you to integrate Citrix Cloud with Windows 365 to use Citrix HDX technologies for an enhanced and more secure Windows 365 Cloud PC experience in addition to other Citrix Cloud services for enhanced manageability.

For more information, see Citrix HDX Plus for Windows 365

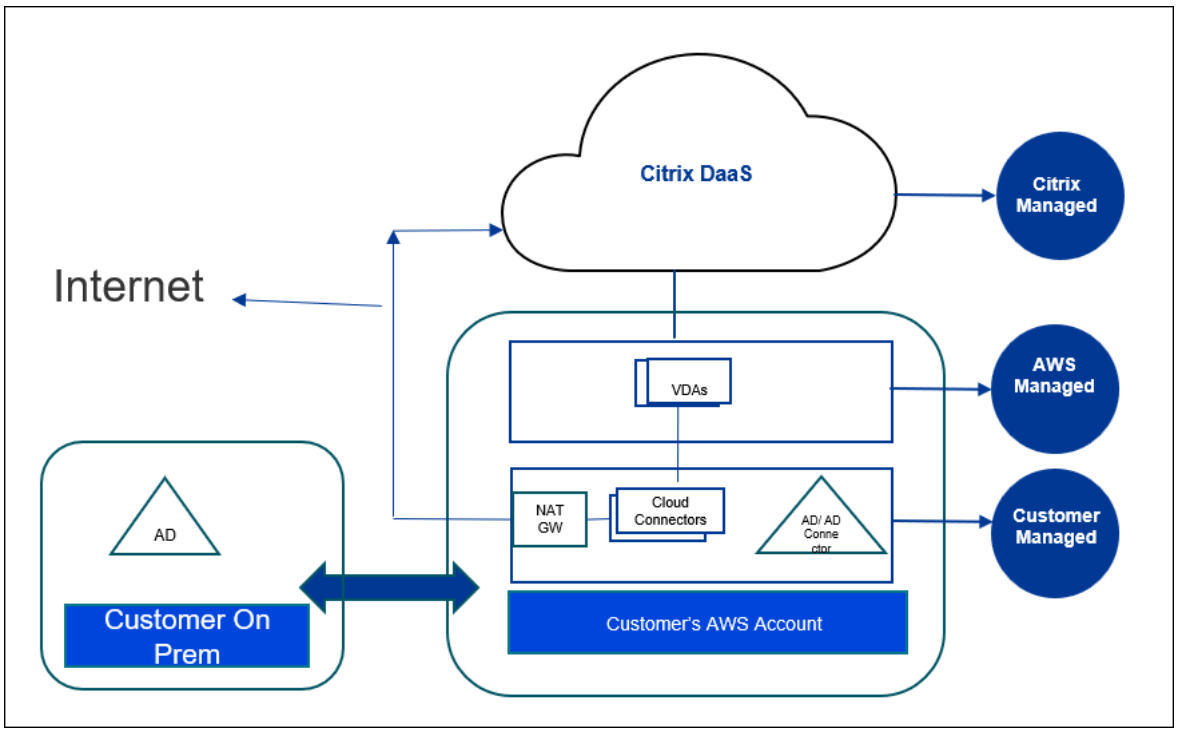
Citrix DaaS for Amazon WorkSpaces Core (Preview)

June 12, 2024

Introduction

This article describes how to prepare and create a deployment with Citrix for Amazon WorkSpaces Core. Amazon WorkSpaces Core resides in Amazon Web Services (AWS).

The following is the representation of the AWS implementation and its management with Citrix DaaS:



About this preview

- For support during this preview, contact AWS Support or Citrix Support.
- To manage the Citrix environment during this preview, use only the **Manage** console in the Citrix DaaS. No Citrix or AWS APIs are supported during this preview. (Citrix welcomes your feedback about APIs that you want to use in the future.)

Prepare and create a deployment

The deployment checklist in the **Quick Deploy** interface contains links to procedures 1-5.

1. Before you start, complete the prerequisites in Citrix Cloud and AWS.
2. Create a resource location in Citrix Cloud. (This procedure is also included as a prerequisite.)
3. Connect your AWS account. This procedure enables permissions so that the Citrix DaaS can connect to AWS.
4. Create a directory connection. This procedure configures a connection that allows access to your organization's Active Directory.
5. Import an image. This procedure enables you to create a desktop experience for your users.
6. Create a deployment. This procedure specifies the machines to be deployed and the users who can access them through Citrix Workspace.

Before you start

Make sure you've completed the following tasks before you begin preparing and creating your deployment.

There is one exception: Creating a resource location in Citrix Cloud is listed as a prerequisite. It is also the first procedure in the deployment checklist. So, if you create the resource location as part of the prerequisites, skip that procedure in the checklist sequence. Similarly, complete that procedure in the checklist if you didn't do it earlier.

Prerequisites to complete in Citrix Cloud

- Create a Citrix Cloud account and subscribe to the Citrix DaaS. Your Citrix representative can help with this. Your representative also enables this preview feature for you.
- Create a Citrix Cloud resource location. (This procedure is also linked in the Quick Deploy interface.)

Prerequisites to complete in AWS

- Create an AWS user account. The account must have:
  - Role permissions for the Citrix API client.
  - Permissions for programmatic access. For more information, see AWS account programmatic access permissions.
  - Create the workspaces_DefaultRole role. For more information, see Create the workspaces_DefaultRole Role.
- In your Active Directory:
  - Use the AD Connector option to store and manage information. For more details, see AD Connector.
  - Create an OU where VMs are created. That OU must have a Citrix policy for communication with the Cloud Connectors and Citrix Cloud. See the Reference section for details.
  - Set up a group policy for the Citrix Cloud Connector configuration:
    1. Download the latest Group Policy Management Console provided by Citrix (CitrixGroupPolicyManagement_64.msi) from the Citrix download site.
    2. Install the MSI (that machine must have the Visual Studio 2015 runtime installed). Then create a Citrix policy that contains the Controllers policy setting. That setting specifies the Cloud Connector addresses.
- Create or use an existing NAT gateway. For more information, see NAT gateway.

- Create or use one or more existing security groups that allow the Citrix Cloud Connectors to communicate with the deployed VMs. For more information, see Control traffic to your AWS resources using security groups
- Open an AWS Support ticket to enable BYOL on your account. To get started, contact your AWS account manager or sales representative, or contact the AWS Support Center. Your contact will verify and enable BYOL. For more information, see Enable BYOL for your account for BYOL using the Amazon WorkSpaces console.

  > **Note:**
  >
  > Windows 10 N and Windows 11 N versions are not supported for BYOL currently.

  - Using the Citrix DaaS for Amazon WorkSpaces Core feature will automatically enable the Bring Your Own Protocol (BYOP) feature in AWS WorkSpaces Core.
  - Have sufficient Windows 10 licenses for the desktops that will be created. For more information, see Bring Your Own Windows desktop licenses.

General preparation

Review each procedure before you start. Benefit: This will help the processes to be completed easily.

Create a resource location

You create a resource location in Citrix Cloud.

- A resource location contains two or more Cloud Connectors that communicate with Citrix Cloud. The servers on which you install the Cloud Connectors must be in an EC2 VPC, domain-joined, and have Internet connectivity. The Cloud Connectors must be in the same VPC as the directory you plan to use.
- For more information on Cloud Connectors, see Citrix Cloud Connector and how to provision them.
- The resource location can also contain your Active Directory servers. For more information, see Connect Active Directory to Citrix Cloud.

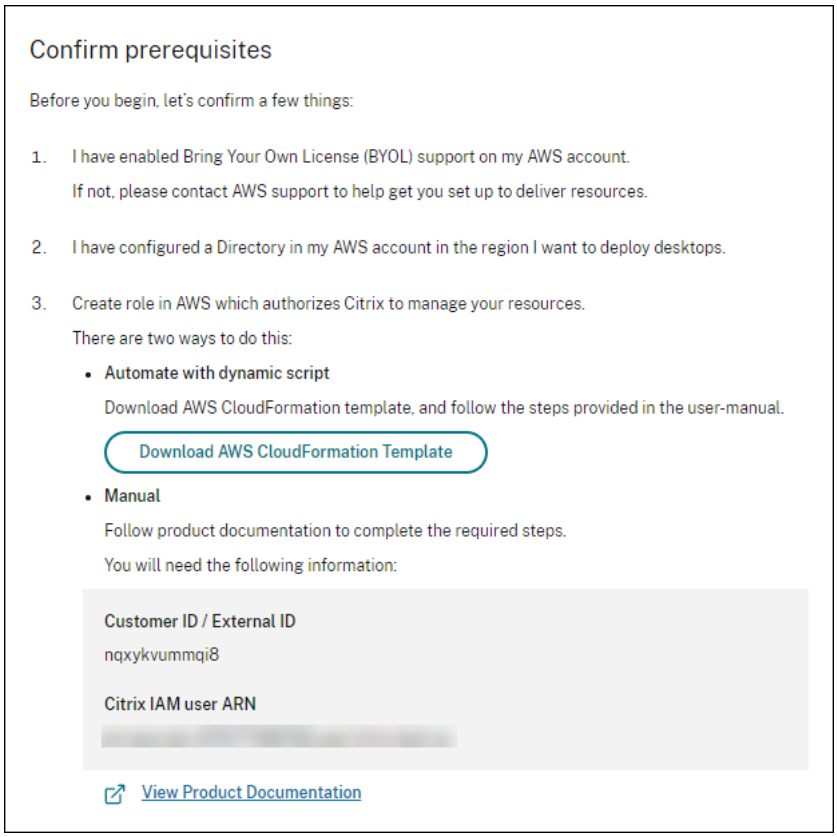
Connect your AWS account

This procedure enables permissions for the Citrix DaaS to connect to AWS.

To create AssumeRole for AWS WorkSpaces Core, follow these steps:

1. In Citrix DaaS, under **Manage > Quick Deploy > Accounts**, click **Connect account**.

2. In the **Connect AWS account** page, under **Confirm prerequisites**, click **Download AWS CloudFormation Template**. After the template is downloaded, click **Next**.



1. To upload the template, see Create AssumeRole for AWS Workspace Core integration.
2. In the **Authenticate account** page, add the **Amazon Resource Name** (ARN) generated in the **Role ID** field, provide a name in the **Name** field, and click **Next**. The **Pick region** page opens.

   Role ID corresponds to the ARN of the role that will authorize Citrix to manage the resources. The Role ID can be found in the AWS management console by navigating to **IAM > Roles**.

   If you are using the `CloudFormation` script, then navigate to CloudFormation and click the corresponding stack that was used to create the role. Navigate to the **Resources** tab and click the resource with LogicalID `CitrixAssumeRole`.

   > **Note:**
   >
   > You cannot connect two accounts on the same region for the same AWS account.

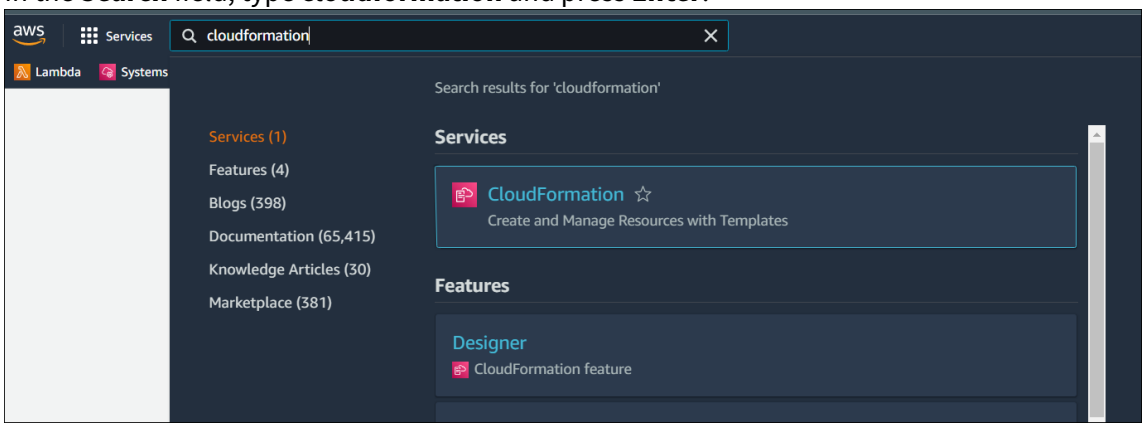
3. In the **Pick region** page, select the region you want to deploy your desktops and click **Next**.
4. In the **Configure BYOL support** page, to configure the BYOL support, a management network interface that is connected to a secure Amazon network is required. Select an IP address range to search for use as that interface. Then select Display available CIDR blocks. If CIDR blocks are

available in the selected search range, select an available CIDR block. A message confirms when you successfully select a search address range and available CIDR block. Click **Next**.

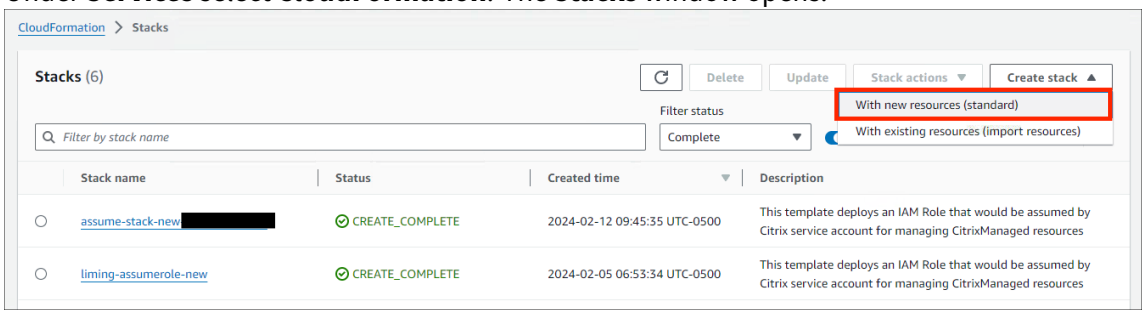
5. In the **Summary** page, review the information you have specified. You can return to the earlier pages. When you're done, click **Finish**.
   The connection process might take several hours to complete.

Create AssumeRole for AWS Workspace Core integration

1. In your browser window, open the **Amazon Web Services** website and sign in.
2. In the **Search** field, type **cloudformation** and press **Enter**.



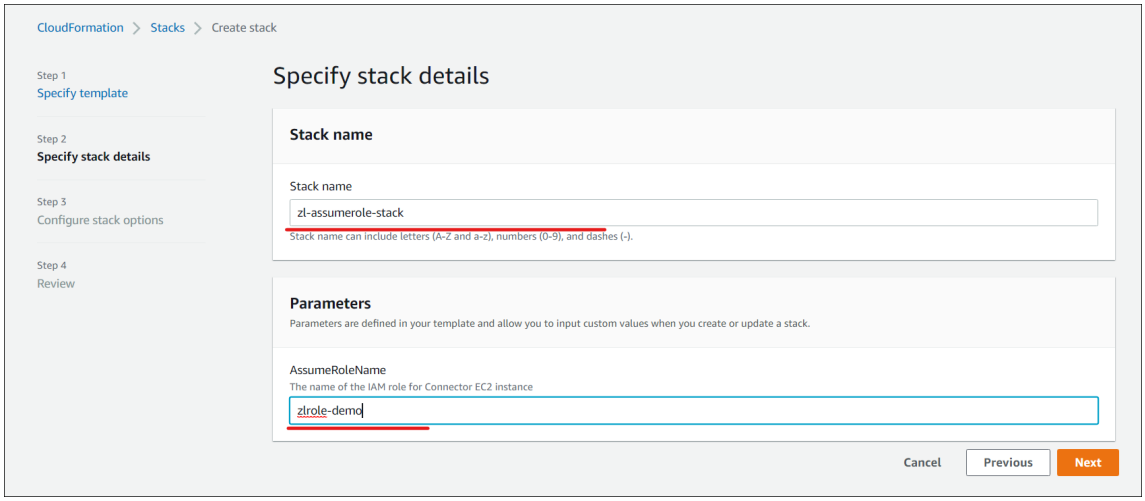
3. Under **Services** select **CloudFormation**. The **Stacks** window opens.



4. Click **Create stack > With new resources (standard)** at the top right corner. The **Create stack** window opens.

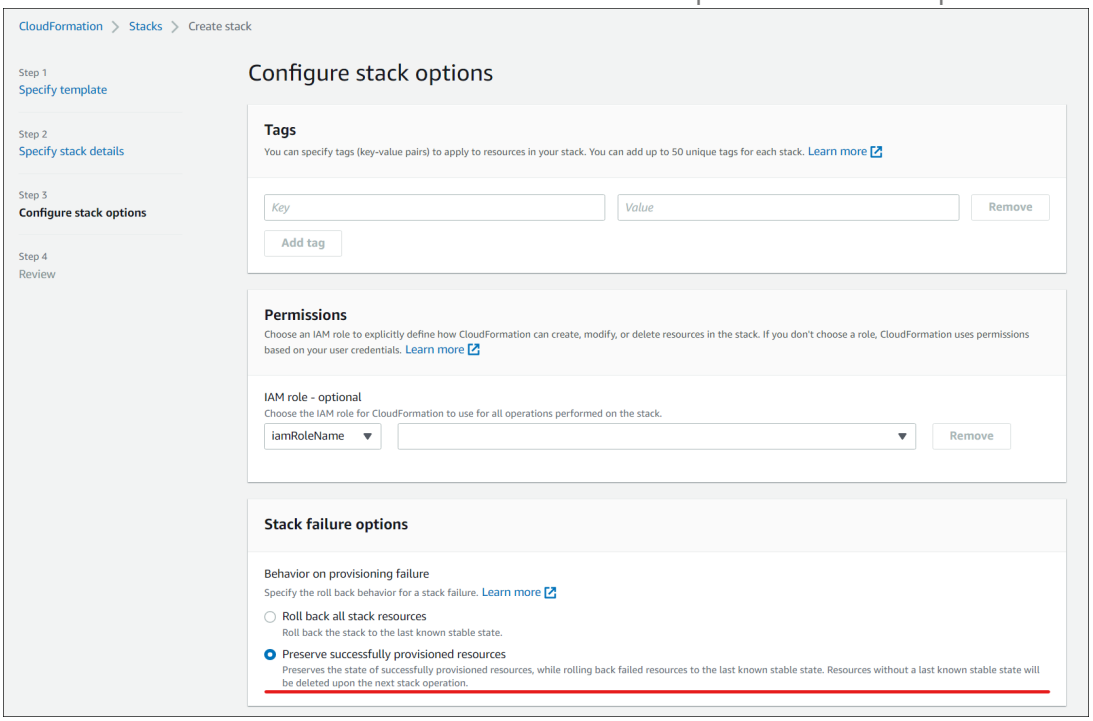
   a) Under **Prerequisite –Prepare template**, select **Template is ready**.
   b) Under **Specify template**, click **Upload a template file > Choose file** and click **Next**. The **Specify stack details** pane opens.

5. In the **Specify stack details** pane, provide a **Stack name** and **AssumeRoleName** and click **Next**. The **Configure stack options** pane opens.

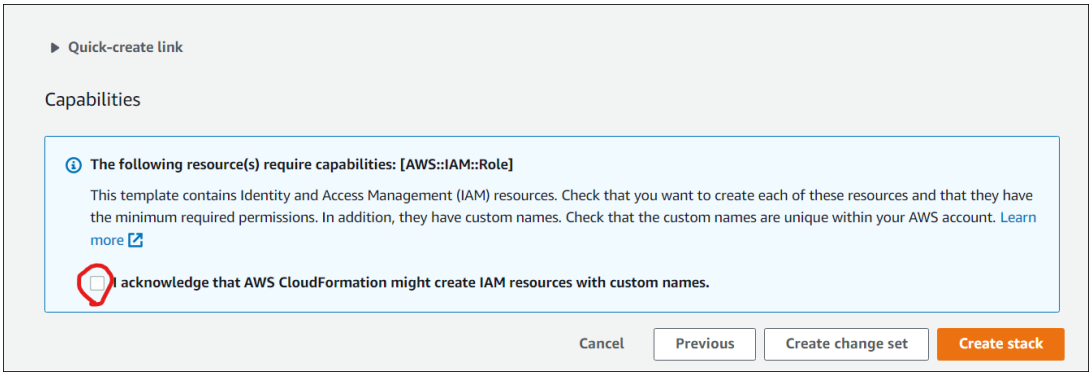


Note:

- In the **Configure stack options** pane, select the **Preserve successfully provisioned resources** option. This option preserves the state of successfully provisioned resources. Resources without a last known stable state are deleted upon the next stack operation.

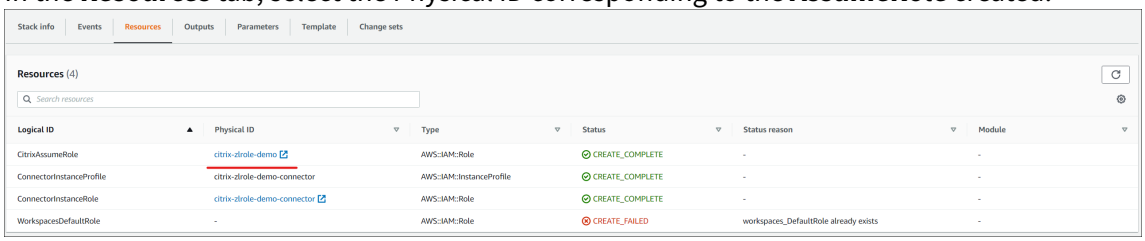


- In the **Capabilities** pop-up window, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** check box and click **Create stack**.

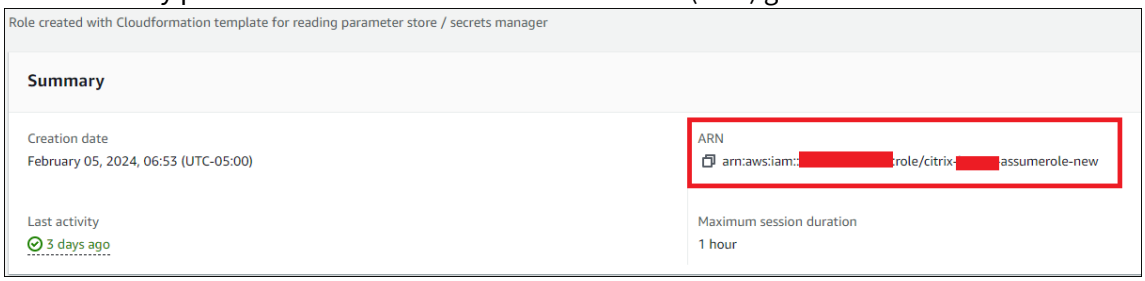


Stack creation might fail at the end because **workspace_DefaultRole** has already been created. This does not affect the **AssumeRole** creation.

1. The **Events** tab shows the status of the Stack created.
2. In the **Resources** tab, select the Physical ID corresponding to the **AssumeRole** created.



3. The Summary pane shows the **Amazon Resource Name** (ARN) generated.



4. Resume the procedure from step 4 in Connect your AWS account

Create a directory connection

> **Note:**
>
> Deregister your AWS Directory at the beginning of this step. After you create a Directory Connection with Citrix DaaS, the selected directory gets registered to create Amazon WorkSpaces with Citrix DaaS.

This procedure creates a connection that allows access to your organization's Active Directory.

Prerequisites:

- A resource location containing two Cloud Connectors.
- A security group.

- An OU in your Active Directory.

For prerequisite details, see Before you start.

You can start this procedure from one of two places:

- A link on the Get Started checklist.
- From the DaaS **Manage** console, select **Quick Deploy** in the left pane, **Directory Connections** under the **Amazon WorkSpaces Core** section. Then select **Create Directory Connection**.

Follow the **Create directory connection** sequence:

1. **Connect directory:** Select the account from the drop down. Select either **Dedicated** or **Shared** for the tenancy.
2. **Resource location:** Select the account and directory. (The selected account must have at least one directory.)
    - Select two subnets in which the desktop machines will be deployed. The subnets must be in appropriate availability zones.
    - Specify a friendly name for this connection.
    - When you're done, click **Next**.
3. **Virtual machine settings:** The settings you select apply to all VMs that use this directory connection.
    - The OU selected must match the OU targeted by the Citrix Group Policy.
    - Select a security group.
    - Indicate whether you want to give administrator privileges to each user assigned to VMs.

Import an image

This procedure enables you to create a desktop experience for your users.

Prerequisites to import the image:

- Must be an EC2 image.
- Must have a Citrix Virtual Delivery Agent (VDA) installed.
- Must be prepared for BYOL. A BYOL script is available at: BYOLChecker.zip.

To import the image, follow the steps:

1. **Prerequisites:** After the prerequisites steps, click **Next**. (If you haven't prepared the image for BYOL, you can download the script from this page.) For more information, see Requirements.
2. **Choose image**
    - Provide a friendly name for the image.

- Select an account.
- Select an AMI. If the selected AMI is a desktop image, then it is a dedicated image and if the selected AMI is a server OS, then it is a shared image.
- Click **Next**. The **Summary** page opens.

3. In the **Summary** page review the information you provided. After verifying, select **Import Image**.

> **Note:**
>
> Importing an image might take several hours.

Integrate Microsoft Office 2019 Image when importing an image

To integrate Microsoft Office 2019 image while importing an image:

1. In **Web Studio > Quick Deploy**, click **Images**.
2. In **My Images**, click **Import Image**.
3. In **Import Image > Prerequisites**, click **Next: Choose Image**.
4. In **Import Image > Choose image:**

   - Select an account from the **Account** dropdown.
   - Select an AMI from the **AMI** dropdown.
   - Enter the name of the image in the **Name** field.
   - Select the **Include Microsoft Office 2019 Professional Plus** in the image.
   - Enter a description in the **Description** field.

5. In **Import Image > Choose image**, click **Next: Summary**.
6. In **Choose Image > Summary**, ensure that **Selected** appears for **Microsoft Office 2019**.
7. In **My Images**, click **Import Image**.
   The status of the recently deployed image displays **importing** until the import operation completes.
8. In **My Images**, select the recently deployed image and click **View Detail**.
9. In the **Detail** panel, the **Microsoft Office 2019** field displays **Included**.

> **Note:**
>
> Only the following versions of the OS are compatible:
>
> - Windows 10 Version 21H2 (December 2021 Update)
> - Windows 10 Version 22H2 (November 2022 Update)
> - Windows 10 Enterprise LTSC 2019 (1809) (1809)

> - Windows 10 Enterprise LTSC 2021 (21H2) (21H2)
> - Windows 11 Version 22H2 (October 2022 release)

Create a deployment

A deployment is a group of desktops that users can access from their Citrix Workspace. This procedure specifies the characteristics of the virtual machines to be deployed as desktops, and which AD users can use them.

Prerequisites

Complete all the steps listed in Prepare and create a deployment.

1. In **Web Studio > Quick Deploy**, click **Deployments** in the **Amazon Web Services** column. Click **Create deployment**.
2. **Image and performance:** Select a **Directory connection** from the drop down. If the selected directory connection has a dedicated tenancy, then the **Image** drop down lists the images with dedicated tenancy and if the selected directory connection has shared tenancy then the **Image** drop down lists the images with default tenancy. Click **Next: Users**.
3. **Users:** Search and select the users who will be allowed to access the desktops.
   If you want to customize volume sizes for a user, select **Edit user and root volume sizes**, and then specify the sizes. Click **Next: Summary**.
4. **Summary:** Review the information you provided and click **Create deployment**.

Integrate Microsoft 365 Windows apps

To integrate Microsoft 365 Apps, see Microsoft 365 Apps for enterprise now available on Amazon WorkSpaces services and Microsoft 365 Bring Your Own License (BYOL).

Manage machines in a deployment

In addition to the machine management features described in Manage machine catalogs, for some actions, you can select machines to manage from a deployment.

To manage machines in a deployment:

1. In **Web Studio > Quick Deploy**, select **Deployments**.
2. In the **Deployments** pane, select the deployment containing machines you want to manage.
3. Click **View details**.
4. In the **Deployment details** pane, select the machine you want to manage.
5. From the actions displayed, select the action you want to perform on the machine:

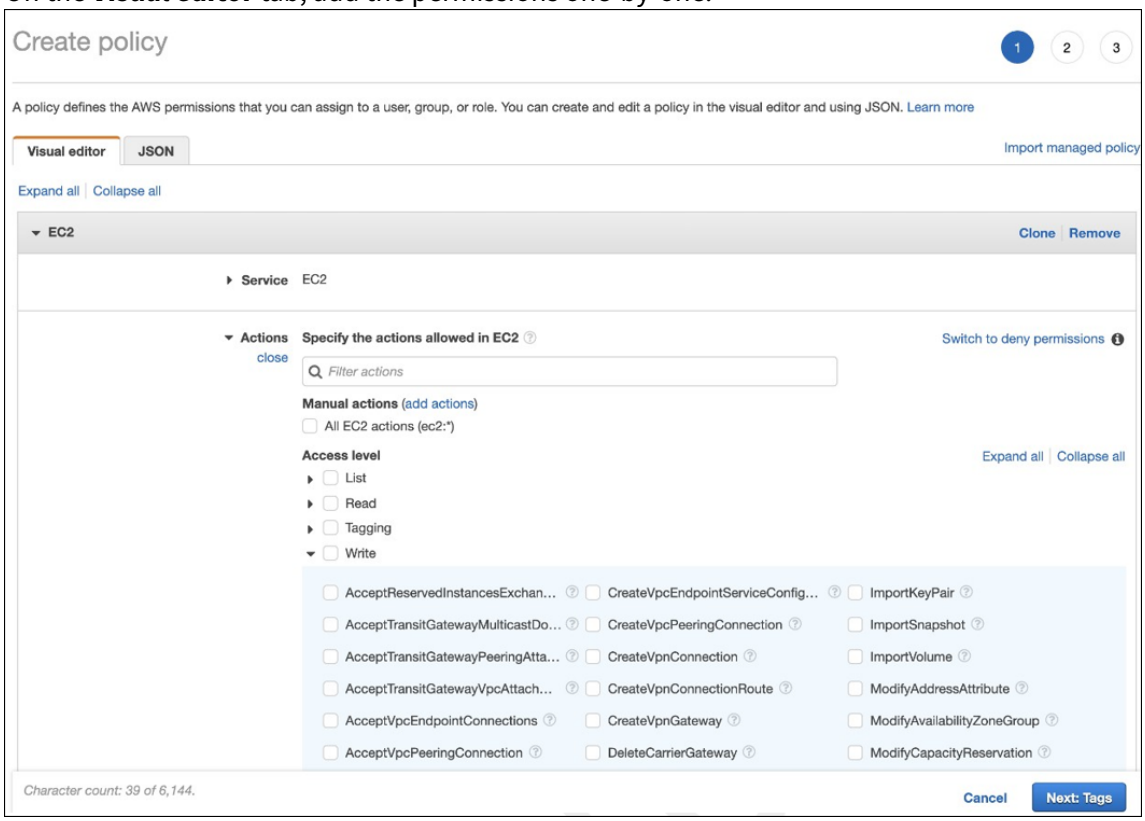
- Click **Edit volume size** to change the volume size of the machine.
- Click **Delete** to delete the machine from the deployment and AWS. If a machine is in a delivery group, it can be deleted only if it is maintenance mode.
- Click **Turn maintenance mode on/off** to turn maintenance mode on (if it is off) or off (if it is on) for the machine.

Reference

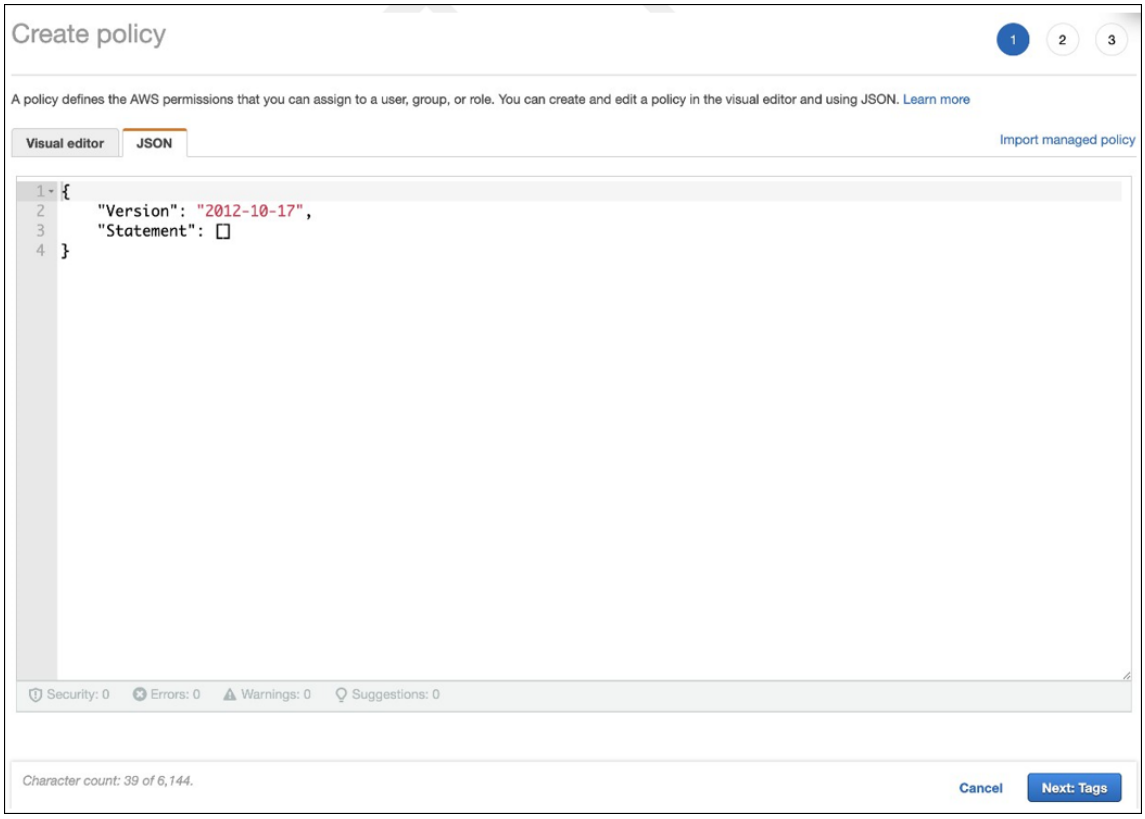
AWS account programmatic access permissions

The AWS user account must have certain programmatic access permissions to make API calls to the AWS resource layer. Programmatic access creates an access key ID and a secret access key.
You can create a policy containing these permissions in the IAM console. As shown in the following graphics, you can use the visual editor (adding the permissions one by one) or the JSON (adding the snippet below).
For more information, see Creating an IAM user in your AWS account.

- On the **Visual editor** tab, add the permissions one-by-one.



- On the **JSON** tab, add the snippet shown after the following graphic.



Required permissions

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                    "workdocs:DeregisterDirectory",
                    "workdocs:RegisterDirectory",
                    "workdocs:AddUserToGroup",
                    "ec2:ImportInstance",
                    "ec2:DescribeImages",
                    "ec2:DescribeImageAttribute"
                    "ec2:CreateKeyPair",
                    "ec2:DescribeKeyPairs",
                    "ec2:ModifyImageAttribute",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeSubnets",
                    "ec2:RunInstances",
                    "ec2:DescribeSecurityGroups",
                    "ec2:CreateTags",
                    "ec2:DescribeRouteTables",
                    "ec2:DescribeInternetGateways",
```



```
                    "ec2:CreateSecurityGroup",
                    "ec2:DescribeInstanceTypes",
                    "servicequotas:ListServices",
                    "servicequotas:GetRequestedServiceQuotaChange",
                    "servicequotas:ListTagsForResource",
                    "servicequotas:GetServiceQuota",
                    "servicequotas:
                       GetAssociationForServiceQuotaTemplate",
                    "servicequotas:ListAWSDefaultServiceQuotas",
                    "servicequotas:ListServiceQuotas",
                    "servicequotas:GetAWSDefaultServiceQuota",
                    "servicequotas:
                       GetServiceQuotaIncreaseRequestFromTemplate",
                    "servicequotas:
                       ListServiceQuotaIncreaseRequestsInTemplate",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistory",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
                    "iam:SimulatePrincipalPolicy"

                ],
                "Resource": "*"
            }

        ]
 }

<!--NeedCopy-->
```

Citrix DaaS for Google Cloud

November 2, 2022

Citrix DaaS for Google Cloud enables you to deploy Google Cloud desktops and apps using the Full Configuration management interface of Citrix DaaS. Citrix DaaS for Google Cloud is available in Standard and Premium editions.

For information about supported features, see the Citrix Virtual Apps and Desktops feature matrix.

You can order Citrix DaaS for Google Cloud from the Google Cloud Marketplace.

After you order Citrix DaaS, sign in to Citrix Cloud. In the upper left menu, select **My Services > DaaS**.

Follow the setup guidance in this product documentation. Using the Full Configuration interface, you can create connections, catalogs, and delivery groups, just as you would when using that interface with other product editions. (These editions currently don't have a Quick Deploy management interface.)

Some displays in the Full Configuration interface might differ from displays in the documentation. For example, when creating a connection in a Citrix Virtual Apps and Desktops edition for Google Cloud, the available connection types include the supported hypervisors and Google Cloud. Other cloud services are not available.

Similarly, use the information in the product documentation that applies to supported hypervisors and Google Cloud.

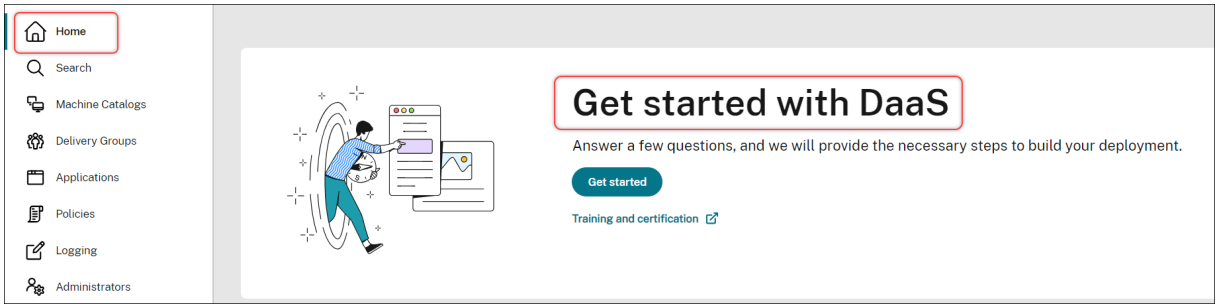
For step-by-step instructions on deploying and configuring Citrix DaaS on Google Cloud, see this Citrix Tech Zone article: Citrix virtualization on Google Cloud. This article covers defining the deployment architecture, preparing the Google Cloud project, configuring network services, and deploying Active Directory.

Use DaaS get-started guide (preview)

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

DaaS get-started guide streamlines and simplifies the DaaS deployment process for both new and experienced administrators. Using the guide, you can quickly set up your DaaS deployments by answering a series of questions.



This article walks you through the processes of setting up five typical DaaS deployment scenarios.

Benefits

Benefits of using this guide include:

- **Easy to get started**. This guide connects essential deployment steps through a questionnaire-led, step-by-step workflow. If you're a new administrator, you can quickly set up your deployment while learning concepts and terminology through contextual help.
- **Simplify complex configurations**. This guide provides pre-configured settings wherever necessary and provides access to the Full Configuration UI for advanced configurations. If you're an experienced administrator, you can use the guide as a starting point for complex configurations.

Supported deployment scenarios

This guide provides quick deployments for these scenarios:

What to deliver?	Machines already exist?	Machine type	Remark
Virtual apps and desktops	No	Virtual machines (Provisioned by DaaS)	Power managed
Virtual apps and desktops	Yes	Virtual machines or blade PCs	Power managed
Virtual apps and desktops	Yes	Physical or virtual machines	Not power managed
Office PCs	Yes	Physical machines	Power managed
Office PCs	Yes	Physical machines	Not power managed

See the following sections for detailed instructions:

- Deliver apps and desktops from scratch (power managed)
- Deliver apps and desktops using existing machines (power managed)
- Deliver apps and desktops using existing machines (not power-managed)
- Deliver office PCs (power managed)
- Deliver office PCs (not power-managed)

Terminology

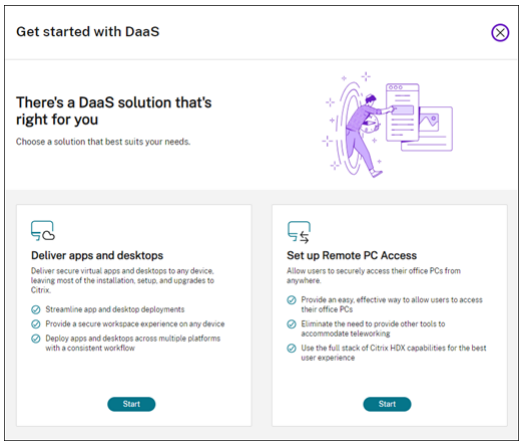
The following are DaaS-specific terms:

- **Resource location.** Contains the resources required to deliver apps and desktops to users.

- **Host connection.** Connects DaaS to a host (hypervisor or cloud service) in a resource location. Creating host connections is required when you want to create and manage machines on hosts or to power manage existing machines.
- **Master image.** Serves as a template for replicating virtual machines on your host. It includes the operating system, applications, Virtual Delivery Agent (VDA), and other software.
- **Machine catalog.** Collection of identical machines. They can be virtual or physical depending on your needs. You can create a machine catalog to create identically configured machines on a host or import machines into DaaS for management.
- **Delivery group.** Contains machines from machine catalogs. Also, it specifies which users can use those machines and which applications and desktops are available to those users.
- **Machine Profile.** Specifies the properties of virtual machines. VMs in a catalog can inherit properties from a machine profile.

Access the guide

1. Go to the **DaaS > Home** page.
2. Locate **Get started with DaaS**.
3. Click **Get Started** to initiate your deployment process.



> **Note:**
>
> You can exit the process at any time by clicking **Close** and the guide saves your settings automatically. To continue your configuration, click **Continue**. To start fresh, click **Start over**.

Deliver apps and desktops from scratch (power managed)

This section guides you through the deployment process of creating VMs and delivering apps and desktops using them.

Prerequisites

Before you start, you need:

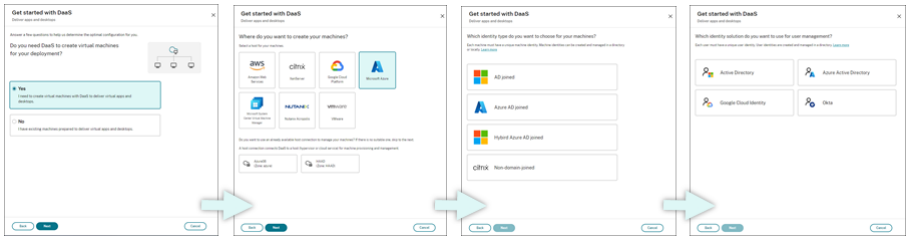
- Connectivity from Citrix Cloud to the target identity provider

  For more information, see the corresponding section in Identity providers.
- Role: Full Administrator or Cloud Administrator
- Required permissions on the target hypervisor or cloud service.

  For more information, see the corresponding sections in the Create and manage connections.
- Administrator credentials for VM account creation

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings. See the following table for details.

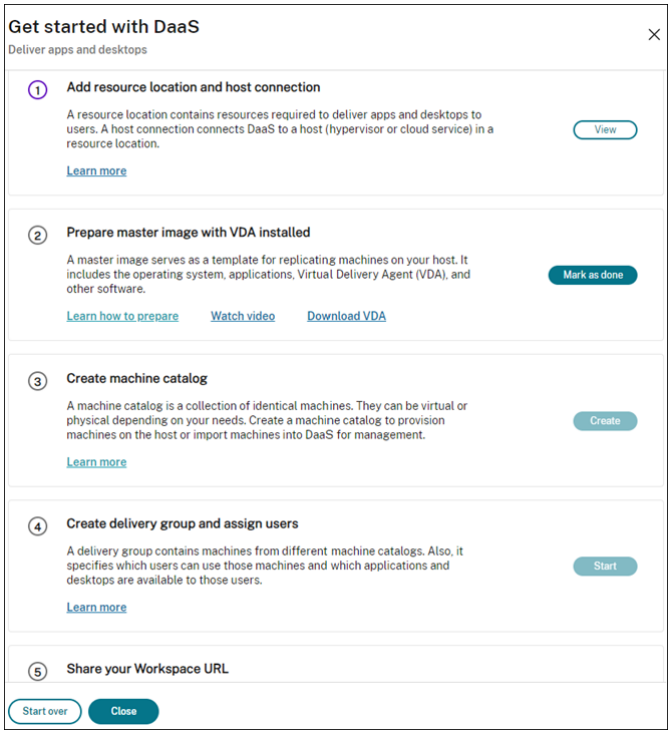


#	Setting	Description
1	Specify whether VM creation is needed	Select **Yes**.
2	Select the host type	Select a host type for your deployment. Options: AWS, XenServer (formerly Citrix Hypervisor), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis, and VMware
3	Select the machine identity type	Select an identity type for machine management.

#	Setting	Description
4	Select the user identity type	Options: AD joined, Azure AD joined, Hybrid Azure AD joined, and Non-domain-joined Select an identity type for user management. Options: Active Directory, Azure Active Directory, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear as follows.



Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location and host connections Set up your resource location by installing Cloud Connectors and configure connections to hypervisors or cloud services in the location.

1. Name the resource location.

2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.
4. Add and configure host connections for the resource location. Detailed settings of a connection include:

    - Connection details, such as the connection address, user name, and password.
    - Storage resources
    - Network resources

    > **Note:**
    >
    > DaaS creates and manages VMs on hosts through those connections. You must specify connections when you create machine catalogs.

Step 2: Prepare master images for your machines Prepare master images on VMs in your resource location. For more information, see Prepare a master image on the hypervisor or cloud service.

Step 3: Create machine catalogs Create a machine catalog to create a group of identically configured machines on a host. Detailed steps are as follows:

1. Name the catalog.
2. Select the machine type.

    Options: Multi-session, Single-session static (personal desktops), and Single-session random (pooled desktops).
3. Select a host connection.

    Options originate from all host connections that you've configured for your resource locations in Step 1.
4. Select a master image.
5. Select a machine profile.

    > **Note:**
    >
    > Machine profile support is currently available for Azure, GCP, and AWS cloud services, and the use of machine profile is optional for GCP.

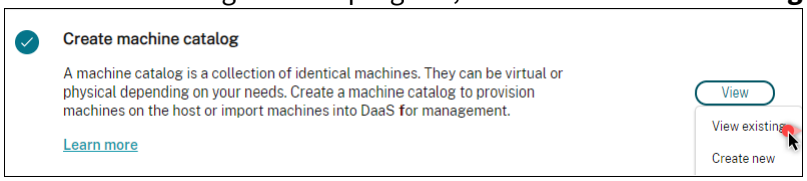
6. Set how many machines you want to create.
7. Set the machine identities.

    By default, the machine identity type that you selected in the preparation phase is shown. Provide the required identity settings for the VMs, such as domain, OU, and naming scheme.

8. Enter the administrator credentials required for machine creation.
9. Click **Create**.

> **Tip:**
>
> The **Create** button is available only after you provide all required settings.

To view the catalog creation progress, select **View > View existing**.



Step 4: Create delivery groups and assign users

> **Tip:**
>
> Before creating delivery groups, view the existing catalogs to ensure that at least one catalog has been created successfully. Otherwise, you're prevented from creating delivery groups.

Creating a delivery group includes the following subtasks:

- Add VMs to the group
- Assign users to the group
- Specify which apps and desktops you want to make available to assigned users

1. Name the group.
2. Add machines to the group by selecting a machine catalog and specifying how many VMs are available for the group.
3. Specify available applications and desktops for this group:
    - To add applications from a running machine in the selected catalog, click **Add new > From start menu**.
    - To add applications deployed on network shares, click **Add new > Manually**, and then provide the required settings, such as path, working directory, and more.
    - (Visible only with multi-session OS machines) For desktop delivery, keep **Enable desktop delivery** selected.
4. Add users who can access apps and desktops in this group.

Step 5: Share the Workspace URL with your users Go to Workspace **Configuration > Access**, and then share the Workspace URL with your users

Deliver apps and desktops using existing machines (power managed)

This section guides you through the deployment process of delivering apps and desktops using existing machines (power managed).

Prerequisites

Before you start, you need:

- Connectivity from Citrix Cloud to the target identity provider

  For more information, see the corresponding section in Identity providers.

- Role: Full Administrator or Cloud Administrator

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	Setting	Description
1	Specify whether VM creation is needed	Select **No**.
2	Select whether power management is required	Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
3	Select the host platform	Select the host platform where your existing machines reside. Options: AWS, Citrix, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis, and VMware
4	Select the user identity type	Select an identity type for user management. Options: Active Directory, Azure Active Directory, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location and host connections Set up your resource location by installing Cloud Connectors and configure connections to hypervisors or cloud services in your location.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.
4. Add and configure host connections for the resource location. Examples of connection settings include the connection address, user name, and password.

> **Note:**
>
> DaaS power manages machines in resource locations through connections. You need to specify a connection when importing your machines to a catalog.

Step 2: Create machine catalogs Create a machine catalog and import your machines to it.

1. Name the catalog
2. Select the machine type.

   Options: Multi-session, Single-session static (personal desktops), and Single-session random (pooled desktops).
3. Select a resource location.
4. Import machines to the catalog.
   Machines are organized by host connection. Choose a host connection to import associated machines.
5. Click **Create**.

Step 3: Create delivery groups and assign users To create a delivery group, you must:

- Add VMs to the group
- Assign users to the group
- Specify which apps and desktops you want to make available to assigned users

1. Name the group.
2. Select a machine catalog as needed, and then specify how many machines are available for the delivery group.

3. Specify available applications and desktops for this group:
   - To add applications from a running machine in the selected catalog, click **Add new > From start menu**.
   - To add applications deployed on network shares, click **Add new > Manually**, and then provide the required settings, such as path, working directory, and more.
   - (Visible only with multi-session OS machines) For desktop delivery, keep **Enable desktop delivery** selected.
4. Add users to the group.

Step 4: Share the Workspace URL with your users Go to **Workspace Configuration > Access**, and then share the Workspace URL with your users.

Deliver apps and desktops using existing machines (not power-managed)

This section guides you through the deployment process of delivering apps and desktops using existing machines (not power-managed).

Prerequisites

Before you start, you need:

- Connectivity from Citrix Cloud to the target identity provider

  For more information, see the corresponding section in Identity providers
- Role: Full Administrator or Cloud Administrator

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	Setting	Description
1	Specify whether VM creation is needed	Select **No**.
2	Select whether power management is required	Select **Machines that are not power managed (for example, physical machines)**.

#	Setting	Description
3	Select the user identity type	Select an identity type for user management. Options: Active Directory, Azure Active Directory, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location Set up your resource location by installing Cloud Connectors.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.

> **Note:**
>
> Creating host connections is required only when you want to power manage machines.

Step 2: Create a machine catalog Create a machine catalog and import your machines to it.

1. Name the catalog
2. Select the machine type.

   Options: Multi-session, Single-session static (personal desktops), and Single-session random (pooled desktops).
3. Select a resource location.
4. Import machines to the catalog.

   To ease machine search, use partial computer names and directory selection.
5. Click **Create**.

Step 3: Create delivery groups and assign users To create a delivery group, you must:

- Add VMs to the group
- Assign users to the group

- Specify which apps and desktops you want to make available to assigned users

1. Name the group.
2. Select a machine catalog as needed, and then specify how many machines are available for the delivery group.
3. Specify available applications and desktops for this group:
    - To add applications from a running machine in the selected catalog, click **Add new > From start menu**.
    - To add applications deployed on network shares, click **Add new > Manually**, and then provide the required settings, such as path, working directory, and more.
    - (Visible only with multi-session OS machines) For desktop delivery, keep **Enable desktop delivery** selected.
4. Add users to the group.

Step 4: Share the Workspace URL with your users Go to **Workspace Configuration > Access**, and then share the Workspace URL with your users.

Deliver office PCs (power managed)

This section guides you through the deployment process of delivering office PCs (power managed).

Prerequisites

Before you begin, you need:

- Machine names of the PCs.
- Citrix Virtual Delivery Agent (VDA) is installed on each PC. (This step can be done after catalog creation.)

  For more information, see Download VDA.

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	Step	Description
1	Select the machine allocation type.	Select how the machines are assigned. Options: Static auto-assigned, Static preassigned, and Random pool unassigned
2	Determine whether to allow users to power on machines	Select **I want remote users to power on machines by themselves**.
3	Select the user identity type	Select an identity type for user management. Options: Active Directory, Azure Active Directory, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location and host connections Set up your resource location by installing Cloud Connectors and add a connection of the **Remote PC Wake on LAN** type.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.
4. Click **Add new** to add a connection:
    a) Select a resource location (zone).
    b) Select **Remote PC Wake on LAN** for **Connection type**.
    c) Enter a name for the connection.

> **Note:**
>
> DaaS power manages machines through the configured connections. You must configure connections of the **Remote PC Wake on LAN** type when creating Remote PC Access catalogs for power-managed machines.

Step 2: Create a Remote PC Access catalog Create a machine catalog and import your office PCs to it.

1. Name the catalog
2. Select a resource location.
3. Select a machine allocation type. By default, the type that you selected in the preparation phase is shown.
4. Select the **Wake on LAN connection**. Options are the connections of the **Remote PC Wake on LAN** type that you configured for the selected location.
5. Import your machines.
6. Click **Create**.

Step 3: Create delivery groups and assign users Create a delivery group to group machines that you want to deliver and specify who can access them.

1. Name the group.
2. Select a machine catalog as needed. Only the **Remote PC Access** catalogs appear.
3. Assign users to the group.

Step 4: Share the Workspace URL with your users Go to **Workspace Configuration > Access**, and then share the Workspace URL with your users.

Deliver office PCs (not power-managed)

This section guides you through the deployment process of delivering office PCs (not power-managed).

Prerequisites

Before you begin, you need:

- Machine names of the PCs.
- Citrix Virtual Delivery Agent (VDA) is installed on each PC. (This step can be done after catalog creation.)

  For more information, see Download VDA.

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	Setting	Description
1	Select the machine allocation type.	Select how the machines are assigned. Options: Static auto-assigned, static preassigned, and random pool unassigned
2	Determine whether to allow users to power on machines	Keep **I want remote users to power on machines by themselves** cleared.
3	Select the user identity type	Select an identity type for user management. Options: Active Directory, Azure Active Directory, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location Set up your resource location by installing Cloud Connectors.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.

> **Note:**
>
> Creating host connections is required only when you want to power manage machines.

Step 2: Create a Remote PC Access catalog Create a catalog and import your office PCs to it.

1. Name the catalog
2. Select a resource location.
3. Select an allocation type. By default, the type that you selected in the preparation phase is shown.

4. Import your machines.
5. Click **Create**.

Step 3: Create delivery groups and assign users Create a delivery group for machines that you want to deliver and specify who can access them.

1. Name the group.
2. Select a machine catalog as needed. Only the **Remote PC Access** catalogs appear.
3. Assign users for the group.

Step 4: Share the Workspace URL with your users Go to **Workspace Configuration > Access**, and then share the Workspace URL with your users.

Machine identities

September 9, 2023

Each machine must have a unique machine identity, also known as computer account. Machine identities can be created and managed in the machines locally or in a directory, such as on-premises Active Directory (AD) or Azure AD. Citrix supports hosting virtual applications and desktops on machines that are Active Directory joined, Azure Active Directory joined, Hybrid Azure Active Directory joined, or non-domain joined.

Machine identity types

The following machine identity types are supported.

Machine identity type	Description
AD joined	Identities are created and managed in on-premises Active Directory. Provisioned machines are joined to on-premises Active Directory using the assigned machine identities.
Azure AD joined	Identities are created and managed in Azure AD. Provisioned machines are joined to Azure AD using the assigned machine identities. Importing VMs to Citrix DaaS is not supported.

Machine identity type	Description
Hybrid Azure AD joined	Identities are created in on-premises Active Directory and are synced with Azure AD through Azure AD Connect. Provisioned machines are joined to on-premises Active Directory and Azure AD. The machines are then Hybrid Azure AD joined. For importing a Hybrid Azure AD joined VM, the VM is treated as an Active Directory joined VM by Citrix DaaS.
Non-domain-joined	Identities are created and managed in the machines locally. Importing VMs to Citrix DaaS is not supported.

Supported Configurations

The following are details of the supported configurations for each scenario.

Supported infrastructure

Machine identity	Citrix DaaS	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
AD joined	Yes	Yes	Yes	Yes	Yes
Azure AD joined	Yes	Yes	No	Yes	No
Hybrid Azure AD joined	Yes	Yes	Yes	Yes	Yes
Non-domain-joined	Yes	Yes	Yes	Yes	Yes

> **Note**
>
> Neither Local Host Cache nor Service Continuity are available for Non-domain joined session hosts when using Storefront.

Supported workspace authentication identity providers

Machine identity	Azure Active Directory	Active Directory	Active Directory and Token	Okta	SAML	Citrix Gateway	Adaptive Authentication
AD joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Azure AD joined	Yes	No	No	No	No	No	No
Hybrid Azure AD joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-domain-joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Active Directory joined

June 16, 2023

Identities are created and managed in on-premises Active Directory. Provisioned machines are joined to on-premises Active Directory using the assigned machine identities. For more information on supported functional levels for the forest and domain, see Active Directory functional levels.

For information on how to create Active Directory (AD) joined catalogs using Citrix DaaS, see Create machine catalogs.

Azure Active Directory joined

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

This article describes the requirements to create Azure Active Directory (AAD) joined catalogs using Citrix DaaS in addition to the requirements outlined in the Citrix DaaS system requirements section.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- VDA version: 2203 or later
- Provisioning type: Machine Creation Services (MCS), Persistent and Non-persistent using Machine Profile workflow
- Assignment type: Dedicated and pooled
- Hosting platform: Azure only
- Rendezvous V2 must be enabled

Limitations

- Service continuity is not supported.
- Single sign-on to virtual desktops not supported. Users must manually enter credentials when signing in to their desktops.
- Logging in with Windows Hello in the virtual desktop is not supported. Only username and password are supported at this time. If users try to log in with any Windows Hello method, they receive an error stating that they are not the brokered user, and the session is disconnected. Associated methods include PIN, FIDO2 key, MFA, and so on.
- Support only Microsoft Azure Resource Manager cloud environments.
- The first time a virtual desktop session is launched, the Windows sign-in screen may show the logon prompt for the last logged on user without the option to switch to another user. The user must wait until the logon times out and the desktop's lock screen appears, and then click the lock screen to reveal the logon screen once again. At this point, the user is able to select **Other Users** and enter their credentials. This is the behavior with every new session when the machines are non-persistent.

Considerations

Image configuration

- Consider optimizing your Windows image using the Citrix Optimizer tool.

Azure AD joined

- Consider disabling Windows Hello so users are not prompted to set it up when they log into their virtual desktop. If you are using VDA 2209 or later, this is done automatically. For earlier versions, you can do this in one of two ways:

  - Group policy or local policy
    * Navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business**.
    * Set **Use Windows Hello for Business** to:
      · **Disabled**, or
      · **Enabled** and select **Do not start Windows Hello provisioning after sign-in**.
  - Microsoft Intune
    * Create a device profile that disables Windows Hello for Business. Refer to Microsoft documentation for details.
    * Currently, Microsoft supports Intune enrollment of persistent machines only, meaning you cannot manage non-persistent machines with Intune.

- Users must be granted explicit access in Azure to log into the machines using their AAD credentials. This can be facilitated by adding the role assignment at the resource group level:

  1. Sign into the Azure portal.
  2. Select **Resource Groups**.
  3. Click the resource group where the virtual desktop workloads reside.
  4. Select **Access control (IAM)**.
  5. Click **Add role assignment**.
  6. Search for **Virtual Machine User Login**, select it on the list, and click **Next**.
  7. Select **User, group, or service principal**.
  8. Click **Select members** and select the users and groups you want to provide access to the virtual desktops.
  9. Click **Select**.
  10. Click **Review + assign**.
  11. Click **Review + assign** once again.

> **Note:**
>
> If you choose to let MCS create the resource group for the virtual desktops, you add this role assignment after the machine catalog is created.

- Master VMs can be Azure AD joined or non-domain-joined. This functionality requires VDA version 2212 or later.

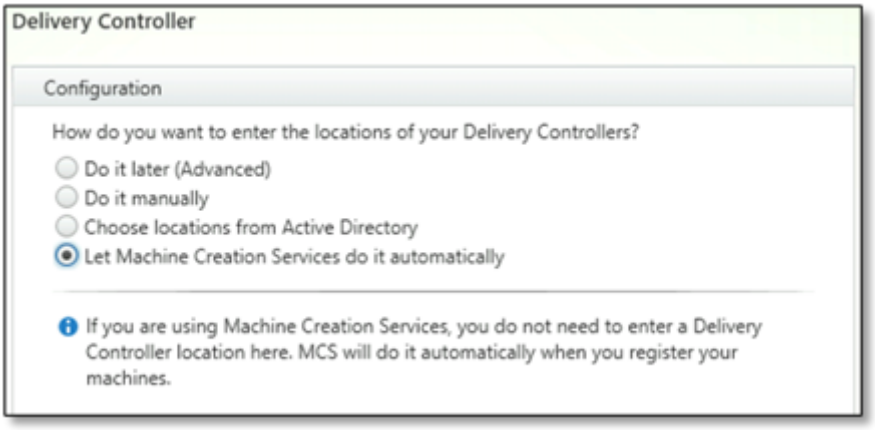
VDA installation and configuration

Follow the steps for installing the VDA:

1. Make sure to select the following options in the installation wizard:

- In the Environment page, select **Create a master MCS image**.

- In the Delivery Controller page, select **Let Machine Creation Services do it automatically**.



2. After the VDA is installed, add the following registry value:

   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Value type: DWORD
   - Value name: GctRegistration
   - Value data: 1

3. For Windows 11 22H2 based master VM, create a scheduled task in the master VM that executes the following command at system startup using SYSTEM account. This task of scheduling a task in the master VM is only required for VDA version 2212 or earlier.

```
reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
    /d Citrix /f
<!--NeedCopy-->
```


4. If you join the master VM to Azure AD, and then manually remove the join by `dsregcmd` utility, make sure that the value of `AADLoginForWindowsExtensionJoined` under HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension is zero.

Where to go next

Once the resource location and hosting connection are available, proceed to create the machine catalog. For more information on creating Azure Active Directory joined machine catalogs, see Create Azure Active Directory joined catalogs.

Microsoft Intune

February 27, 2024

This article describes the requirements to create Microsoft Intune enabled catalogs using Citrix DaaS in addition to the requirements outlined in the Citrix DaaS system requirements section.

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. For more information, see Microsoft Intune. The devices must meet the minimum system requirements. For more information, see the Microsoft documentation Supported operating systems and browsers in Intune.

Microsoft Intune works by using the functionality of Azure AD.

> **Important:**
>
> Before enabling this feature, verify that your Azure environment meets the licensing requirements to use Microsoft Intune. For more information, see the Microsoft documentation: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses. Do not enable the feature if you do not have the appropriate Intune license.

Requirements

- Control plane: Citrix DaaS
- VDA type: Single-session OS VDA
- VDA version: 2203 or later
- Provisioning type: Machine Creation Services (MCS) Persistent using the Machine Profile workflow only
- Assignment type: Dedicated

Limitations

- Support only single-session Azure AD joined persistent VMs.
- Support only single-session Hybrid Azure AD joined persistent VMs using user credential or device credential with co-management capability. For more information, see Enroll a Windows device automatically using Group Policy.
- Do not skip image preparation while creating or updating machine catalogs.

Considerations

- Create a device profile that disables Windows Hello for Business.
- Use VDA version 2212 or later if Microsoft Intune must manage a master VM.

Where to go next

For information on creating Microsoft Intune enabled catalogs, see Create Microsoft Intune enabled catalogs.

Hybrid Azure Active Directory joined

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

This article describes the requirements to create Hybrid Azure Active Directory (HAAD) joined catalogs using Citrix DaaS in addition to the requirements outlined in the Citrix DaaS system requirements section.

Hybrid Azure AD joined machines use on-premises AD as the authentication provider. You can assign them to domain users or groups in on-premises AD. To enable Azure AD seamless SSO experience, you need to have the domain users synced to Azure AD.

> **Note:**
>
> Hybrid Azure AD joined VMs are supported in both federated and managed identity infrastructures.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- VDA version: 2212 or later
- Provisioning type: Machine Creation Services (MCS), Persistent and Non-persistent
- Assignment type: Dedicated and pooled
- Hosting platform: Any hypervisor or cloud service

Limitations

- If Citrix Federated Authentication Service (FAS) is used, single sign-on is directed to on-premises AD rather than Azure AD. In this case, it is recommended to configure Azure AD certificate-based authentication so that the primary refresh token (PRT) is generated upon user logon, which facilitates single sign-on to Azure AD resources within the session. Otherwise, the PRT will not be present and SSO to Azure AD resources will not work. For information on achieving Azure AD single sign-on (SSO) to hybrid joined VDAs using Citrix Federated Authentication Service (FAS), see Hybrid-joined VDAs.
- Do not skip image preparation while creating or updating machine catalogs. If you want to skip image preparation, make sure the master VMs are not Azure AD or Hybrid Azure AD joined.

Considerations

- Creating hybrid Azure Active Directory joined machines requires the `Write userCertificate` permission in the target domain. Make sure that you enter credentials of an administrator with that permission during catalog creation.
- The hybrid Azure AD joining process is managed by Citrix. You need to disable `autoWorkplaceJoin` controlled by Windows in the master VMs as follows. The task of manually disabling `autoWorkplaceJoin` is only required for VDA version 2212 or earlier.

  1. Run `gpedit.msc`.
  2. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Device Registration**.
  3. Set **Register domain joined computers as devices** to **Disabled**.

- Select the Organizational Unit (OU) that is configured to be synced with Azure AD when you create the machine identities.
- For Windows 11 22H2 based master VM, create a scheduled task in the master VM that executes the following commands at system startup using SYSTEM account. This task of scheduling a task in the master VM is only required for VDA version 2212 or earlier.


```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
    Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
        "Provider", $null)
    if ($provider -eq 'Citrix')
    {

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
            Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
            autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }

   }


  Start-Sleep 1
 }

<!--NeedCopy-->
```

Where to go next

For more information on creating Hybrid Azure Active Directory joined catalogs, see Create Hybrid Azure Active Directory joined catalogs.

Non-domain-joined

October 19, 2023

This article describes the requirements to create non-domain-joined catalogs using Citrix DaaS in addition to the requirements outlined in the Citrix DaaS system requirements section.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- VDA version: 2203 or later
- Provisioning type: Machine Creation Services (MCS), Persistent and Non-persistent
- Assignment type: Dedicated and pooled
- Hosting platform: All platforms supported by MCS
- Rendezvous V2 must be enabled
- Cloud Connectors: Only required if you plan to provision machines on on-premises hypervisors or if you want to use Active Directory as the identity provider in Workspace.

Limitations

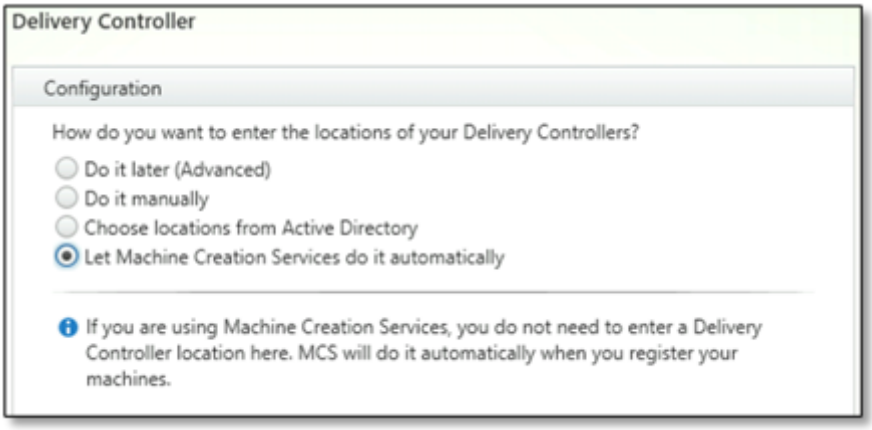
- Service continuity is not supported.
- Whenever we use a multi session non domain joined VDA, the local user's profile data is not retained and is deleted on logoff.

VDA installation and configuration

Follow the steps for installing the VDA:

1. Make sure to select the following options in the installation wizard:
    - In the Environment page, select **Create a master MCS image**.

- In the Delivery Controller page, select **Let Machine Creation Services do it automatically**.



2. After the VDA is installed, add the following registry value:

   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Value type: DWORD
   - Value name: GctRegistration
   - Value data: 1

Where to go next

Once the resource location and hosting connection are available, proceed to create the machine catalog. For more information on creating non-domain-joined machine catalogs, see Create non-domain-joined catalogs.

Set up resource locations

May 28, 2024

Resource locations contain the resources required to deliver applications and desktops to users. You manage the resources from Citrix Cloud. Typically, resources include:

- Hypervisors or cloud services, known as *hosts* that include:
  - Active Directory domain controllers.
  - Virtual Delivery Agents (VDAs): VDAs are installed on a machine that delivers the applications and desktops to the users.
  - Citrix Gateway (optional): To enable secure external access to the applications and desktops offered to users, add a Citrix Gateway VPX appliance to the resource location. Then, set up Citrix Gateway.
  - Citrix StoreFront servers.
  - To communicate with Citrix Cloud, every resource location must contain a Citrix Cloud Connector. A minimum of two Cloud Connectors per resource location is recommended.

A zone is equivalent to a resource location. When you create a resource location and install a Cloud Connector, a zone is automatically created for you. For more information, see Zones.

To learn more about resource types, see Connect to Citrix Cloud.

Host requirements

The hypervisor or cloud service, where you provision VMs, need unique permissions or setup.

- If the hypervisor or cloud service requires virtual networks, follow the guidance in its documentation.
- Create the appropriate Virtual Private Cloud (VPC) (for AWS or GCP) or Virtual Network (VNET) (for Azure) for the machines that you'll add to your resource location.
- Create the appropriate rules to secure inbound and outbound traffic between machines in the virtual network. For example, when using AWS, ensure that the VPC's security group has the appropriate rules configured so that machines in the VPC are accessible to only the IP addresses you specify.

The following host types are supported:

- Amazon Web Services (AWS) virtualization environments
- XenServer virtualization environments
- Google Cloud Platform virtualization environments

- HPE Moonshot virtualization environments
- Microsoft Azure Resource Manager virtualization environments
- Microsoft System Center Virtual Machine Manager virtualization environments
- Nutanix virtualization environments
- Nutanix cloud and partner solutions
- VMware virtualization environments
- VMware cloud and partner solutions

Active Directory

Provision a Windows server, install Active Directory Domain Services (AD DS), and promote it to a Domain Controller. For guidance, see the Microsoft documentation on Active Directory Domain Services Overview.

The important considerations are:

- You must have at least one Domain Controller running Active Directory Domain Services.
- Do not install any Citrix components on a Domain Controller.

For more information, see:

- Active Directory functional levels
- Identity and access management in Citrix Cloud.
- Connect Active Directory to Citrix Cloud
- Deployment scenarios for using Connector Appliance with Active Directory

Cloud Connectors

The Cloud Connector is a group of services from Citrix Cloud that allow communication between the VDAs, StoreFront, and the cloud-based Delivery Controller. You can install Cloud Connectors interactively or from the command line.

For more information on Cloud Connectors, see:

- Citrix Cloud Connector
- Technical details
- Proxy and firewall configuration
- Installation
- Connector updates

Size and scale considerations

- When evaluating Citrix DaaS for sizing and scalability, consider all components.

- Research and test the configuration of the Cloud Connectors and StoreFront for your specific requirements.
- Undersizing the machines can impact system performance negatively.

The article Size and scale considerations for Cloud Connectors includes:

- Size and scale testing information
- Tested maximum capacities
- Best practice recommendations for Cloud Connector machine configuration

Add a resource type

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **Resource Locations**.
3. Select **+ Resource Locations** to add a resource location.
4. Enter a name for the resource location, and then click **Save**. For information about naming considerations, see Name restrictions.
5. Under the new resource location, select **+ Cloud Connectors**.
6. Download and install the Cloud Connector software on at least two servers in the domain where you have your Citrix DaaS resources.

   - During the installation, select the resource location you created in the previous steps.
   - After installation, Citrix Cloud adds the servers to the resource location, and registers the domains in which you installed the Cloud Connectors.

7. Verify that the registered domains are active:

   - From the Citrix Cloud menu, select **Identity Access Management**.
   - Select **Domains**. A list of domains where Cloud Connectors have been deployed displays.
   - Locate the domains that you are using with Citrix DaaS. Active domains display with a green bar on the left side of the domain entry.

   If your domain does not have the visual indicator, the domain is in an **unused** state. If you specify an unused domain during machine catalog setup, catalog creation fails. To ensure machine catalog setup occurs without errors, follow the steps in Activate an unused domain.

   For more information, see CTX473009: DaaS Catalog Creation Wizard: "Internal Server Error" when creating adding new machine accounts.

Activate an unused domain

1. From the **Domain** tab, in **Identity and Access Management**, select **Show Unused Domains**. After you select this option, the label changes to **Hide Unused Domains**.
2. Locate the unused domain in the list. Unused domains display a gray bar on the left side of the domain entry, and a single-option ellipsis menu on the right side.
3. Select the ellipsis menu, and then select **Use domain**. The gray bar becomes green, and the ellipsis menu change to **Disable**.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For setting up resource location for specific host types:
  - AWS virtualization environments
  - Google Cloud virtualization environments
  - HPE Moonshot virtualization environments
  - Microsoft Azure Resource Manager virtualization environments
  - Microsoft System Center Virtual Machine Manager virtualization environments
  - Nutanix virtualization environments
  - Nutanix cloud and partner solutions
  - VMware virtualization environments
  - VMware cloud and partner solutions
  - XenServer virtualization environments
- For a full deployment, Create and manage connections and resources to a resource location.
- Review all the steps in the installation and configuration process

AWS virtualization environments

March 20, 2024

This article describes how to set up your AWS account as a resource location you can use with Citrix DaaS.

The resource location includes a basic set of components, ideal for a proof-of-concept, or other deployment that does not require resources spread over multiple availability zones.

When you complete the tasks in this article, your resource location includes the following components:

- A virtual private cloud (VPC) with public and private subnets inside a single availability zone.
- An instance that runs as both an Active Directory Domain Controller and DNS server, located in the private subnet of the VPC.
- Two domain-joined instances on which the Citrix Cloud Connector is installed, located in the private subnet of the VPC.
- An instance that acts as a bastion host, located in the public subnet of your VPC. This instance is used to initiate RDP connections to the instances in the private subnet for administration purposes. After you finish setting up your resource location, you can shut down this instance so it is no longer readily accessible. When you must manage other instances in the private subnet, such as VDA instances, you can restart the bastion host instance.

After you complete the tasks, you can install VDAs, provision machines, create machine catalogs, and create Delivery Groups.

Task overview

Set up a virtual private cloud (VPC) with public and private subnets. When you complete this task, AWS deploys NAT gateways with an Elastic IP address in the public subnet. This enables instances in the private subnet to access the Internet. Instances in the public subnet are accessible to inbound public traffic while instances in the private subnet are not.

Configure security groups. Security groups act as virtual firewalls that control traffic for the instances in your VPC. You add rules to your security groups that allow instances in your public subnet to communicate with instances in your private subnet. You also associate these security groups with each instance in your VPC.

Create a DHCP options set. An Amazon VPC, DHCP, and DNS services are provided by default, which affects how you configure DNS on your Active Directory Domain Controller. Amazon's DHCP cannot be disabled and Amazon's DNS can be used only for public DNS resolution, not Active Directory name resolution. To specify the domain and name servers handed to instances through DHCP, create a DHCP options set. The set assigns the Active Directory domain suffix and specifies the DNS server for all instances in your VPC. To ensure Host (A) and Reverse Lookup (PTR) records are automatically registered when instances join the domain, you configure the network adapter properties for each instance you add to the private subnet.

Add a bastion host, Domain Controller, and Cloud Connectors to the VPC. Through the bastion host, you can log on to instances in the private subnet to set up the domain, join instances to the domain, and install the Cloud Connector.

Task 1: Set up the VPC

1. From the AWS management console, select **VPC**.
2. From the VPC Dashboard, select **Create VPC**.
3. Select **VPC and more**.
4. Under NAT gateways ($), select **In 1 AZ** or **1 per AZ**.
5. Under DNS options, leave **Enable DNS hostnames** selected.
6. Select **Create VPC**. AWS creates the public and private subnets, Internet gateway, route tables, and default security group.

> **Note:**
>
> Changing the name of an AWS Virtual Private Cloud (VPC) in the AWS console breaks the existing hosting unit in the Citrix Cloud. When the hosting unit is broken, you cannot create catalogs or add machines to existing catalogs. From Known Issue: PMCS-7701

Task 2: Configure security groups

This task creates and configures the following security groups for your VPC:

- A public security group to associate with the instances in your Public subnet.
- A private security group to associate with the instances in your Private subnet.

To create the security groups:

1. In the VPC Dashboard, select **Security Groups**.
2. Create a security group for the public security group. Select **Create Security Group** and enter a name tag and description for the group. In VPC, select the VPC you created earlier. Select **Yes, Create**.

Configure the Public security group

1. From the security group list, select the Public security group.
2. Select the **Inbound Rules** tab and select Edit to create the following rules:

Type	Source
ALL Traffic	Select the Private security group.
ALL Traffic	Select the Public security group.
ICMP	0.0.0.0/0

Type	Source
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Session Reliability)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. When finished, select **Save**.
4. Select the **Outbound Rules** tab and select **Edit** to create the following rules.

Type	Destination
ALL Traffic	Select the Private security group.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. When finished, select **Save**.

Configure the private security group

1. From the security group list, select the Private security group.
2. If you have not yet setup traffic from the public security group, you must set TCP ports. Select the **Inbound Rules** tab and select **Edit** to create the following rules:

Type	Source
ALL Traffic	Select the Private security group.
ALL Traffic	Select the Public security group.
ICMP	Select the Public security group.
TCP 53 (DNS)	Select the Public security group.
UDP 53 (DNS)	Select the Public security group.
80 (HTTP)	Select the Public security group.

Type	Source
TCP 135	Select the Public security group.
TCP 389	Select the Public security group.
UDP 389	Select the Public security group.
443 (HTTPS)	Select the Public security group.
TCP 1494 (ICA/HDX)	Select the Public security group.
TCP 2598 (Session Reliability)	Select the Public security group.
3389 (RDP)	Select the Public security group.
TCP 49152–65535	Select the Public security group.

3. When finished, select **Save.**
4. Select the **Outbound Rules** tab and select **Edit** to create the following rules.

Type	Destination
ALL Traffic	Select the Private security group.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. When finished, select **Save**.

Task 3: Launch instances

Do the following steps to create four EC2 instances and decrypt the default Administrator password that Amazon generates:

1. From the AWS management console, select **EC2**.
2. From the EC2 Dashboard, select **Launch Instance**.
3. Select a Windows Server machine image and instance type.
4. On the **Configure Instance Details** page, enter a name for the instance and select the VPC that you had set up earlier.
5. In **Subnet**, make the following selections for each instance:

- Bastion host: Select the Public subnet
- Domain controller and Connectors: Select the Private subnet

6. In **Auto-assign Public IP address**, make the following selections for each instance:

   - Bastion host: Select **Enable**
   - Domain controller and Connectors: Select **Use default setting** or **Disable**

7. In **Network Interfaces**, enter a primary IP address within the IP range of your private subnet for the Domain Controller and Cloud Connector instances.
8. If necessary, on the **Add Storage** page, modify the disk size.
9. On the **Tag Instance** page, enter a friendly name for each instance.
10. On the **Configure Security Groups** page, select **Select an existing security group** and then make the following selections for each instance:

    - Bastion host: Select the Public security group.
    - Domain controller and Cloud Connectors: Select the Private security group.

11. Review your selections and then select **Launch**.
12. Create a new key pair or select an existing one. If you create a new key pair, then download your private key (`.pem`) file and keep it in a safe place. You must supply your private key when you acquire the default Administrator password for the instance.
13. Select **Launch Instances**. Select **View Instances** to display a list of your instances. Wait until the newly launched instance has passed all status checks before accessing it.
14. Acquire the default Administrator password for each instance.

    a) From the instance list, select the instance and then select **Connect**.
    b) Go to the **RDP client** tab, select **Get Password**, and upload your private key (`.pem`) file when prompted.
    c) Select **Decrypt Password** to get the human readable password. AWS displays the default password.

15. Repeat all the steps from step 2 until you have created four instances:

    - One bastion host instance in your public subnet
    - Three instances in your private subnet to be used as:
      - One as a Domain Controller
      - Two as Cloud Connectors

Task 4: Create a DHCP options set

1. From the VPC Dashboard, select **DHCP Options Sets**.
2. Enter the following information:
   - Name tag: Enter a friendly name for the set.
   - Domain name: Enter the fully qualified domain name that you use when you configure the Domain Controller instance.
   - Domain name servers: Enter the private IP address you assigned to the Domain Controller instance and the string **AmazonProvidedDNS**, separated by commas.
   - NTP servers: Leave this field blank.
   - NetBIOS name servers: Enter the private IP address of the Domain Controller instance.
   - NetBIOS node type: Enter **2**.
3. Select **Yes, Create.**
4. Associate the new set with your VPC:
   a) From the VPC Dashboard, select **Your VPCs** and then select the VPC you set up earlier.
   b) Select **Actions > Edit DHCP Options Set**.
   c) When prompted, select the new set you created, and then select **Save**.

Task 5: Configure the instances

1. Using an RDP client, connect to the public IP address of the bastion host instance. When prompted, enter the credentials for the Administrator account.
2. From the bastion host instance, launch **Remote Desktop Connection** and connect to the private IP address of the instance you want to configure. When prompted, enter the Administrator credentials for the instance.
3. For all instances in the private subnet, configure the DNS settings:
   a) Select **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**. Double-click the network connection displayed.
   b) Select **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties**.
   c) Select **Advanced > DNS**. Ensure that the following settings are enabled, and then select **OK**:
      - **Register this connection's addresses in DNS**
      - **Use this connection's DNS suffix in DNS registration**
4. Configure the Domain Controller:

a) Using Server Manager, add the Active Directory Domain Services role with all default features.
b) Promote the instance to a Domain Controller. During promotion, enable DNS and use the domain name you specified when you created the DHCP options set. Restart the instance when prompted.

5. Configure the first Cloud Connector:

a) Join the instance to the domain and restart when prompted. From the bastion host instance, reconnect to the instance using RDP.
b) Sign in to Citrix Cloud. Select **Resource Locations** from the upper left menu.
c) Download the Cloud Connector.
d) When prompted, run the `cwcconnector.exe` file and supply your Citrix Cloud credentials. Follow the wizard.
e) Once complete, select **Refresh** to display the **Resource Locations** page. When the Cloud Connector is registered, the instance appears on the page.

6. Repeat the steps to configure the Cloud Connector to configure the second Cloud Connector.
7. Attach an IAM Policy to the Cloud Connectors to support AWS hosting connections with role-based authorization. You must have the same IAM Policy attached to all the Cloud Connectors in a resource location. For information about AWS permissions, see Required AWS permissions.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to AWS.
- Review all the steps in the installation and configuration process

More information

- Create and manage connections and resources
- Create machine catalogs

Google Cloud virtualization environments

April 15, 2024

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) lets you provision and manage machines on Google Cloud.

Prerequisites

Before you start provisioning the VMs to Google Cloud Platform (GCP), you must make sure the following prerequisites are met.

1. The Citrix subscription must include support for Hybrid Multi-Cloud workloads. For more information, see Compare Citrix subscription features.
2. The admin account must have sufficient permissions to create host connections, machine catalogs, and delivery groups. For more information, see Configure Delegated Administration.
3. Identify a Google Cloud project, in which all compute resources associated with the machine catalog are stored. It can be an existing project or a new one. For more information, see Google Cloud projects.
4. Enable the Google Cloud APIs required for the integration with Citrix DaaS. For more information, see Enable Google Cloud APIs.
5. Create the service accounts in Google Cloud and grant the appropriate permissions. For more information, see Configure and update service accounts.
6. Download the key file for the Citrix Cloud Service Account. For more information, see Citrix Cloud Service Account key.
7. The virtual machines must have access to the Google APIs without a public IP address. For more information, see Enable Private Google Access.

Google Cloud projects

There are basically two types of Google Cloud projects:

- Provisioning project: In this case, the current admin account owns the provisioned machines in the project. This project is also referred to as a local project.
- Shared VPC project: Project in which machines created in the provisioning project use the VPC from the Shared VPC project. The admin account used for provisioning projects has limited permissions in this project, specifically, only permissions to use the VPC.

Service endpoint URLs

You must have access to the following URLs:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`

- https://compute.googleapis.com
- https://storage.googleapis.com
- https://cloudbuild.googleapis.com

Enable Google Cloud APIs

To use the Google Cloud functionality through the Citrix DaaS Full Configuration interface, enable these APIs in your Google Cloud project:

- Compute Engine API
- Cloud Resource Manager API
- Identity and Access Management (IAM) API
- Cloud Build API

From the Google Cloud console, complete these steps:

1. In the upper left menu, select **APIs and Services > Enabled APIs & services**.
2. On the **Enabled APIs & services** screen, ensure that the Compute Engine API is enabled. If not, follow these steps:
    a) Navigate to **APIs and Services > Library**.
    b) In the search box, type *Compute Engine*.
    c) From the search results, select **Compute Engine API**.
    d) On the **Compute Engine API** page, select **Enable**.
3. Enable Cloud Resource Manager API.
    a) Navigate to **APIs and Services > Library**.
    b) In the search box, type *Cloud Resource Manager*.
    c) From the search results, select **Cloud Resource Manager API**.
    d) On the **Cloud Resource Manager API** page, select **Enable**. The status of the API appears.
4. Similarly, enable **Identity and Access Management (IAM) API** and **Cloud Build API**, and **Cloud Key Management Service (KMS) API**.

You can also use Google Cloud Shell to enable the APIs. To do this:

1. Open the Google Console and load the Cloud Shell.
2. Run the following four commands in the Cloud Shell:
    - gcloud services enable compute.googleapis.com
    - gcloud services enable cloudresourcemanager.googleapis.com
    - gcloud services enable iam.googleapis.com

- gcloud services enable cloudbuild.googleapis.com
- gcloud services enable cloudkms.googleapis.com

3. Click **Authorize** when the Cloud Shell prompts.

Configure and update service accounts

> **Note:**
>
> GCP is introducing changes to Cloud Build Service's default behavior and use of service accounts after April 29, 2024. For more information, see Cloud Build Service Account Change. Your existing Google projects with Cloud Build API enabled before April 29, 2024 are not affected by this change. However, if you want to have existing Cloud Build Service behavior after April 29, you can create or apply the organization policy to disable the constraint enforcement before you enable the Cloud Build API. As a result, the following content is divided into two: Before April 29, 2024 and After April 29, 2024. If you set the new organization policy, follow the section Before April 29, 2024.

Before April 29, 2024

Citrix Cloud uses three separate service accounts within the Google Cloud project:

- *Citrix Cloud Service Account*: This service account enables Citrix Cloud to access the Google project, provision, and manage machines. This service account authenticates to Google Cloud using a key generated by Google Cloud.

  You must create this service account manually as outlined here. For more information, see Create a Citrix Cloud Service Account.

  You can identify this service account with an email address. For example, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cloud Build Service Account*: This service account is provisioned automatically after you enable all the APIs mentioned in Enable Google Cloud APIs. To view all automatically created service accounts, navigate to **IAM & Admin > IAM** in the **Google Cloud** console and select the **Include Google-provided role grants** checkbox.

  You can identify this service account by an email address that begins with the **Project ID** and the word **cloudbuild**. For example, `<project-id>@cloudbuild.gserviceaccount.com`

  Verify if the service account has been granted the following roles. If you must add roles, follow the steps outlined in Add roles to the Cloud Build Service Account.

  - Cloud Build Service Account
  - Compute Instance Admin

  - Service Account User

- *Cloud Compute Service Account*: This service account is added by Google Cloud to instances created in Google Cloud once the Compute API is activated. This account has the IAM basic editor role to do the operations. However, if you delete the default permission to have more granular control, you must add a **Storage Admin** role that requires the following permissions:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

You can identify this service account by an email address that begins with the **Project ID** and the word **compute**. For example, `<project-id>-compute@developer.gserviceaccount.com`.

Create a Citrix Cloud Service Account To create a Citrix Cloud Service Account, follow these steps:

1. In the Google Cloud console, navigate to **IAM & Admin > Service accounts**.
2. On the **Service accounts** page, select **CREATE SERVICE ACCOUNT**.
3. On the **Create service account** page, enter the required information, and then select **CREATE AND CONTINUE**.
4. On the **Grant this service account access to project** page, click the **Select a role** drop-down menu and select the required roles. Click **+ADD ANOTHER ROLE** if you want to add more roles.

   Each account (personal or service) has various roles defining the management of the project. Grant the following roles to this service account:

   - Compute Admin
   - Storage Admin
   - Cloud Build Editor
   - Service Account User
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   The Cloud KMS Crypto Operator requires the following permissions:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **Note:**
>
> Enable all the APIs to get the complete list of roles available while creating a new service account.

5. Click **CONTINUE**
6. On the **Grant users access to this service account** page, add users or groups to grant them access to perform actions in this service account.
7. Click **DONE**.
8. Navigate to the IAM main console.
9. Identify the service account created.
10. Validate the roles are assigned successfully.

Considerations:

When creating the service account, consider the following:

- The steps **Grant this service account access to project** and **Grant users access to this service account** are optional. If you choose to skip these optional configuration steps, the newly created service account does not display in the **IAM & Admin > IAM** page.
- To display roles associated with a service account, add the roles without skipping the optional steps. This process ensures that roles appear for the configured service account.

Citrix Cloud Service Account key The Citrix Cloud Service Account key is required for creating a connection in Citrix DaaS. The key is contained in a credential file (.json). The file is automatically downloaded and saved to the **Downloads** folder after you create the key. When you create the key, be sure to set the key type to JSON. Otherwise, the Citrix Full Configuration interface cannot parse it.

To create a Service Account Key, navigate to **IAM & Admin > Service accounts** and click the email address of the Citrix Cloud Service Account. Switch to the **Keys** tab and select **Add Key > Create new key**. Make sure to select **JSON** as the key type.

> **Tip:**
>
> Create keys using the **Service accounts** page in the Google Cloud console. We recommend that you change keys regularly for security purposes. You can provide new keys to the Citrix Virtual Apps and Desktops application by editing an existing Google Cloud connection.

Add roles to the Citrix Cloud Service Account To add roles to the Citrix Cloud Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.

2. On the **IAM > PERMISSIONS** page, locate the service account you created, identifiable with an email address.

   For example, <my-service-account>@<project-id>.iam.gserviceaccount.com

3. Select the pencil icon to edit the access to the principal of the service account.
4. On the **Edit access to "project-id"** page for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your service account one by one and then select **SAVE**.

Add roles to the Cloud Build Service Account To add roles to the Cloud Build Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.
2. On the **IAM** page, locate the Cloud Build service account, identifiable with an email address that begins with the **Project ID** and the word **cloudbuild**.

   For example, <project-id>@cloudbuild.gserviceaccount.com

3. Select the pencil icon to edit the Cloud Build account roles.
4. On the **Edit access to "project-id"page** for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your Cloud Build service account one by one and then select **SAVE**.

   > **Note:**
   >
   > Enable all the APIs to get the complete list of roles.

After April 29, 2024

Citrix Cloud uses two separate service accounts within the Google Cloud project:

- *Citrix Cloud Service Account*: This service account enables Citrix Cloud to access the Google project, provision, and manage machines. This service account authenticates to Google Cloud using a key generated by Google Cloud.

  You must create this service account manually.

  You can identify this service account with an email address. For example, <my-service-account>@<project-id>.iam.gserviceaccount.com.

- *Cloud Compute Service Account*: This service account is provisioned automatically after you enable all the APIs mentioned in Enable Google Cloud APIs. To view all automatically created service accounts, navigate to **IAM & Admin > IAM** in the **Google Cloud** console and select the **Include Google-provided role grants** checkbox. This account has the IAM basic editor role to do

the operations. However, if you delete the default permission to have more granular control, you must add **Storage Admin** role that requires the following permissions:

- resourcemanager.projects.get
- storage.objects.create
- storage.objects.get
- storage.objects.list

You can identify this service account by an email address that begins with the **Project ID** and the word **compute**. For example, `<project-id>-compute@developer.gserviceaccount.com`.

Verify if the service account has been granted the following roles.

- Cloud Build Service Account
- Compute Instance Admin
- Service Account User

Create a Citrix Cloud Service Account To create a Citrix Cloud Service Account, follow these steps:

1. In the Google Cloud console, navigate to **IAM & Admin > Service accounts**.
2. On the **Service accounts** page, select **CREATE SERVICE ACCOUNT**.
3. On the **Create service account** page, enter the required information, and then select **CREATE AND CONTINUE**.
4. On the **Grant this service account access to project** page, click the **Select a role** drop-down menu and select the required roles. Click **+ADD ANOTHER ROLE** if you want to add more roles.

   Each account (personal or service) has various roles defining the management of the project. Grant the following roles to this service account:

   - Compute Admin
   - Storage Admin
   - Cloud Build Editor
   - Service Account User
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   The Cloud KMS Crypto Operator requires the following permissions:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get

- cloudkms.keyRings.list

> **Note:**
>
> Enable all the APIs to get the complete list of roles available while creating a new service account.

5. Click **CONTINUE**
6. On the **Grant users access to this service account** page, add users or groups to grant them access to perform actions in this service account.
7. Click **DONE**.
8. Navigate to the IAM main console.
9. Identify the service account created.
10. Validate the roles are assigned successfully.

Considerations:

When creating the service account, consider the following:

- The steps **Grant this service account access to project** and **Grant users access to this service account** are optional. If you choose to skip these optional configuration steps, the newly created service account does not display in the **IAM & Admin > IAM** page.
- To display roles associated with a service account, add the roles without skipping the optional steps. This process ensures that roles appear for the configured service account.

Citrix Cloud Service Account key The Citrix Cloud Service Account key is required for creating a connection in Citrix DaaS. The key is contained in a credential file (.json). The file is automatically downloaded and saved to the **Downloads** folder after you create the key. When you create the key, be sure to set the key type to JSON. Otherwise, the Citrix Full Configuration interface cannot parse it.

To create a Service Account Key, navigate to **IAM & Admin > Service accounts** and click the email address of the Citrix Cloud Service Account. Switch to the **Keys** tab and select **Add Key > Create new key**. Make sure to select **JSON** as the key type.

> **Tip:**
>
> Create keys using the **Service accounts** page in the Google Cloud console. We recommend that you change keys regularly for security purposes. You can provide new keys to the Citrix Virtual Apps and Desktops application by editing an existing Google Cloud connection.

Add roles to the Citrix Cloud Service Account To add roles to the Citrix Cloud Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.
2. On the **IAM > PERMISSIONS** page, locate the service account you created, identifiable with an email address.

   For example, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Select the pencil icon to edit the access to the principal of the service account.
4. On the **Edit access to "project-id"** page for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your service account one by one and then select **SAVE**.

Add roles to the Cloud Compute Service Account To add roles to the Cloud Compute Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.
2. On the **IAM** page, locate the Cloud Compute Service Account, identifiable with an email address that begins with the **Project ID** and the word **compute**.

   For example, `<project-id>-compute@developer.gserviceaccount.com`
3. Select the pencil icon to edit the Cloud Build account roles.
4. On the **Edit access to "project-id"page** for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your Cloud Build service account one by one and then select **SAVE**.

   > **Note:**
   >
   > Enable all the APIs to get the complete list of roles.

Storage permissions and bucket management

Citrix DaaS improves the process of reporting cloud build failures for the Google Cloud service. This service runs builds on the Google Cloud. Citrix DaaS creates a storage bucket named `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` where the Google Cloud services captures build log information. An option is set on this bucket that deletes the contents after a period of 30 days. This process requires that the service account used for the connection has Google Cloud permissions set to `storage.buckets.update`. If the service account does not have this permission, Citrix DaaS ignores errors and proceeds with the catalog creation process. Without this permission, the size of the build logs increases and requires manual cleanup.

Enable private Google access

When a VM lacks an external IP address assigned to its network interface, packets are only sent to other internal IP addresses destinations. When you enable private access, the VM connects to the set of external IP addresses used by the Google API and associated services.

> **Note:**
>
> Whether private Google access is enabled, all VMs that are with and without public IP addresses, must be able to access Google Public APIs, especially if third-party networking appliances have been installed in the environment.

To ensure that a VM in your subnet can access the Google APIs without a public IP address for MCS provisioning:

1. In Google Cloud, access the **VPC network configuration**.
2. Identify the subnets used or the Citrix environment in the **Subnets in current project** tab.
3. Click the name of the subnets and enable **Private Google Access**.

For more information, see Configuring Private Google Access.

> **Important:**
>
> If your network is configured to prevent VM access to the internet, ensure that your organization assumes the risks associated with enabling Private Google access for the subnet to which the VM is connected.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Google cloud environments.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

HPE Moonshot virtualization environments

May 28, 2024

Citrix DaaS manages your HPE Moonshot workloads through a Citrix-managed HPE Moonshot plug-in present in the DaaS control plane. With this plug-in, you can create connections to your HPE Moonshot chassis, create catalogs, and power manage machines in the catalog.

Key steps

1. Set up your HPE environments.
2. Create a connection to the HPE Moonshot chassis.

   > **Note:**
   >
   > After you enable the feature toggle, the Citrix-managed HPE Moonshot plug-in is automatically installed. You can, therefore, continue to use the existing machine catalog using the Citrix-managed Moonshot plug-in instead of the HPE-managed HPE Moonshot plug-in.

3. Create a machine catalog.

   > **Note:**
   >
   > Before creating a catalog, ensure to have one or more HPE Moonshot cartridge nodes and install VDAs on those nodes. You can consider the HPE Moonshot chassis as the hypervisor and the cartridge nodes as VMs.

4. Create a delivery group.
5. Migrate the rest of unmanaged HPE Moonshot nodes to the managed catalog or delivery group.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine that will deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to HPE Moonshot.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Microsoft Azure Resource Manager virtualization environments

April 10, 2024

When using the Microsoft Azure Resource Manager to provision virtual machines in your Citrix DaaS deployment, get familiar with the following:

- What is Microsoft Entra ID?
- Integrating Microsoft Entra ID with applications getting started guide
- Application and service principal objects in Microsoft Entra ID

To set up your Microsoft Azure Resource Manager, see Set up resource location.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Microsoft Azure.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs
- CTX219211: Set up a Microsoft Entra ID account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Microsoft System Center Virtual Machine Manager virtualization environments

December 11, 2023

Follow this guidance if you use Hyper-V with the Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

See System requirements for a list of supported VMM versions.

You can use Machine Creation Services or Citrix Provisioning (formerly Provisioning Services) to provision:

- Generation 1 Desktop or Server OS VMs
- Generation 2 Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10, and Windows 11 VMs (with or without secure boot)

Install and configure a hypervisor

Install the Microsoft Hyper-V role and VMM on your servers.

Verify the following account information:

In **Manage > Full Configuration**, the account you specify when creating a connection must be a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account has only the delegated administrator role in VMM, the storage data is not listed in the **Full Configuration** interface during the connection creation process.

Your user account must also be a member of the administrators local security group on each Hyper-V server to support VM lifecycle management (such as VM creation, update, and deletion).

In large deployments where a single SCVMM manages multiple clusters in different data centers, you can limit the host groups scope of the admins.

To limit the host groups scope, use the delegated admin role in the Microsoft System Center Virtual Machine Manager (VMM) console.

1. On **Create User Roles Wizard**, select **Fabric Administrator** (delegated administrator) as a user role.
2. In **Members**, add the user account in the Active Directory that you want to use as delegated admin.
3. In **Scope**, select the host groups you want the delegated admin to have access to.
4. Create a new **Run As Account** using delegated admin user credentials. Use these credentials to create a hypervisor connection later. Do not use the main administrator role accounts.

Install the VMM console

Install a System Center Virtual Machine Manager console on each server having a Citrix Cloud Connector.

The console version must match the management server version. Although an earlier console can connect to the management server, provisioning VDAs fails if the versions differ.

Azure Stack HCI provisioning through SCVMM

Azure Stack HCI is a hyper-converged infrastructure (HCI) cluster solution that hosts virtualized Windows and Linux workloads and their storage in a hybrid, on-premises environment.

Azure hybrid services enhance the cluster with capabilities such as cloud-based monitoring, site recovery, and VM backups. You can also have a central view of all your Azure Stack HCI deployments in the Azure portal.

Integrate Azure Stack HCI with SCVMM

To integrate Azure Stack HCI with SCVMM, you need to first create an Azure Stack HCI cluster, and then integrate that cluster with SCVMM.

1. To create the Azure Stack HCI cluster and register it with Azure, see the Microsoft document Connect Azure Stack HCI to Azure.
2. To integrate Azure Stack HCI cluster with SCVMM, do the following:

   a) Log in to the machine that is prepared to host the SCVMM server and install SCVMM 2019 UR3 or later.

   > **Note:**
   >
   > Install SCVMM 2019 UR3 or later Administrator Console in the Cloud Connector VMs.

   b) In the **Settings** page of the VMM console, create a run as account.

   c) Run the following PowerShell commands with administrative permissions in the SCVMM server to add the Azure Stack HCI cluster as a host:

   ```
   $runAsAccountName = 'Admin'
   $runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
   $hostGroupName = 'All Hosts'
   $hostGroup = Get-SCVMHostGroup -Name $hostGroupName
   $hostCluster = 'FQDN of Azure Stack HCI cluster'
   Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
       VMHostGroup
   $hostGroup -Credential $runAsAccount -RemoteConnectEnabled
       $true
   <!--NeedCopy-->
   ```

   d) You can now see the Azure Stack HCI cluster along with the nodes in the VMM console.

   e) Create the SCVMM hosting connection in the **Full Configuration** interface.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Microsoft System Center Virtual Machine Manager.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Nutanix virtualization environments

February 5, 2024

Follow this guidance when using Nutanix Acropolis to provide virtual machines in your Citrix DaaS deployment. The setup process includes the task of installing and registering the Nutanix plug-in in your Citrix DaaS environment.

For more information on the Nutanix Acropolis MCS plug-in Installation guide, see Nutanix Support Portal.

> **Important:**
>
> Install the Nutanix plug-in on all Cloud Connectors where Citrix DaaS must create a host connection to the resource location that has a Nutanix hypervisor.

Install and register the Nutanix plug-in

Complete the procedure to install and register the Nutanix plug-in on all your Cloud Connectors. Use the **Manage > Full Configuration** functions in Citrix Cloud to create a connection to Nutanix.

For information about installing the Nutanix plug-in, see the Nutanix Documentation site.

For more information on how to set up your Nutanix virtualization environments, see Add a resource type or activate an unused domain in Citrix Cloud.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing a connections, see Connection to Nutanix.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources

- Create machine catalogs

Nutanix cloud and partner solutions

December 11, 2023

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) supports the following Nutanix cloud and partner solution:

- Nutanix Cloud Clusters on AWS

Nutanix Cloud Clusters on AWS

Citrix DaaS supports Nutanix Cloud Clusters on AWS. Nutanix clusters simplify how applications are run on private or multiple public clouds. For more information on Nutanix Cloud Clusters on AWS, see Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Tip:**
>
> This support provides the same functionality as a Nutanix on-premises cluster. Only a single cluster is supported, the *Prism Element*. For more information, see here.

Requirements

You need the following accounts to use Nutanix Clusters on AWS:

- A Nutanix account
- An AWS account with the following permissions:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Create a Nutanix Cluster

To create a Nutanix Cluster:

1. Log in to your Nutanix account.
2. Locate the **Nutanix cluster** option, and click **Launch**. The **Nutanix Console** opens. For more information, see Get Started with Nutanix Cluster on AWS.

3. Choose to create a **new VPC**.

The cluster creation process might fail with the following errors:

- Cluster failed to create within a given time. Deleting cluster.
- Host Nutanix Cluster - Node `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Host Nutanix Cluster - Node `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

If the cluster fails to create, then:

- Try to recreate one in a different region.
- Make sure to delete the Nutanix CloudFormation Stack (CFS) before retrying.

In addition to other resources, the Nutanix CFS creates:

- 1 VPC named *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 subnets 10.0.128.0/24 and 10.0.129.0/24
- 1 Internet gateway
- 1 NAT gateway

Once the cluster is created, retrieve the address of the **Nutanix Prism**:

1. Go to the **Nutanix Console**.
2. In the upper right on the console, hover over the link **Launch Prism Element** and copy the URL.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Nutanix cloud and partner solutions.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

VMware virtualization environments

December 11, 2023

Follow this guidance if you use VMware to provide virtual machines.

Install vCenter Server and the appropriate management tools. (No support is provided for vSphere vCenter Linked Mode operation.)

> **Note:**
>
> No support is provided for vSphere vCenter Linked Mode operation.

If you plan to use Machine Creation Services (MCS), do not disable the Datastore Browser feature in vCenter Server as described in Disabling the vCenter Server Datastore Browser. If you disable this feature, MCS does not work correctly.

To set up your VMware virtualization environments, see Add a resource type or activate an unused domain in Citrix Cloud.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to VMware.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

VMware cloud and partner solutions

December 11, 2023

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) supports the following VMware cloud and partner solutions:

- Azure VMware Solution (AVS)

- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Use Citrix DaaS to migrate VMware based on-premises Citrix workloads to the respective VMware partner solutions.

Azure VMware Solution (AVS) integration

Citrix DaaS supports AVS. AVS provides cloud infrastructure containing vSphere clusters created by Azure infrastructure. Leverage DaaS to use AVS for provisioning your VDA workload in the same way that you would using vSphere in on-premises environments.

Set up the AVS cluster

To enable Citrix DaaS to use AVS, do the following steps in Azure:

- Request a host quota
- Register the `Microsoft.AVS` resource provider
- Verify networking planning checklist
- Network Checklist
- Create an AVS private cloud
- Access the AVS private cloud
- Configure networking for your VMware private cloud in Azure
- Configure DHCP for AVS
- Add a network segment in AVS
- Verify the AVS environment

Request host quota for Azure Enterprise Agreement customers In the Azure portal's **Help + Support** page select **New support request**, and include the following information:

- Issue type: Technical
- Subscription: Select your subscription
- Service:**All services > Azure VMware Solution**
- Resource: General question
- Summary: Need capacity
- Problem type: Capacity Management Issues
- Problem subtype: Customer Request for Additional Host Quota/Capacity

In the **Description** of the support ticket, include the following information in the **Details** tab:

- POC or Production

- Region Name
- Number of hosts
- Any other details

> **Note:**
>
> AVS requires a minimum of three hosts, and recommends that you use redundancy of N+1 hosts.

After specifying details for the support ticket, select **Review + Create** to submit the request to Azure.

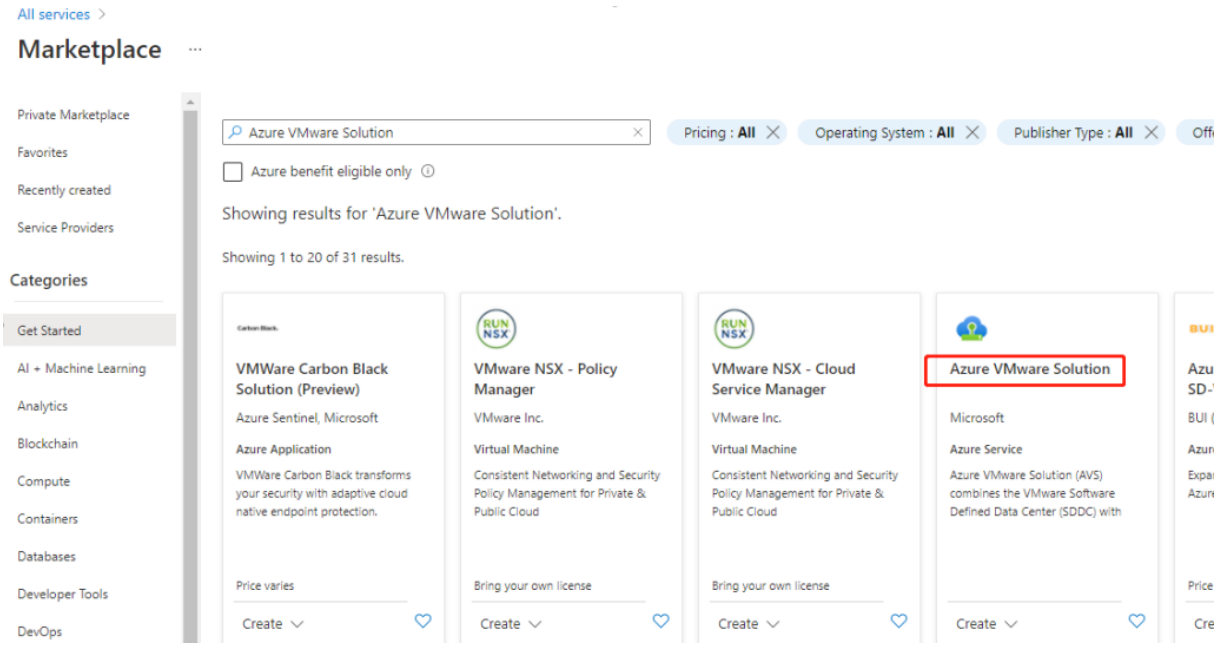
Register the Microsoft.AVS resource provider After requesting the host quota, register the resource provider:

1. Sign in to the Azure portal.
2. On the Azure portal menu, select **All services**.
3. In the **All services** menu, enter the subscription, and select **Subscriptions**.
4. Select the subscription from the subscription list.
5. Select **Resource providers** and enter **Microsoft.AVS** in the search bar.
6. If the resource provider is not registered, select **Register**.

Networking considerations AVS offers networking services requiring specific network address ranges and firewall ports. See Networking planning checklist for Azure VMware Solution for more information.

Create an AVS private cloud After considering network requirements for your environment, create an ASV private cloud:

1. Sign in to the Azure portal.
2. Select **Create a new resource**.
3. In the **Search the Marketplace** text box type, *Azure VMware Solution*, and select **Azure VMware Solution** from the list.



In the **Azure VMware Solution** window:

1. Select **Create**.
2. Go to the **Basics** tab.
3. Enter the values for the fields, using the information in the table below:

Field	Value
Subscription	Select the subscription that you plan to use for the deployment. All resources in an Azure subscription are billed together.
Resource group	Select the resource group for your private cloud. An Azure resource group is a logical container into which Azure resources are deployed and managed. Alternatively, you can create a new resource group for your private cloud.
Location	Select a location, such as east us. This is the region you defined during the planning phase.
Resource name	Provide the name of your Azure VMware Solution private cloud.
Size of host	Select the size as per your need.

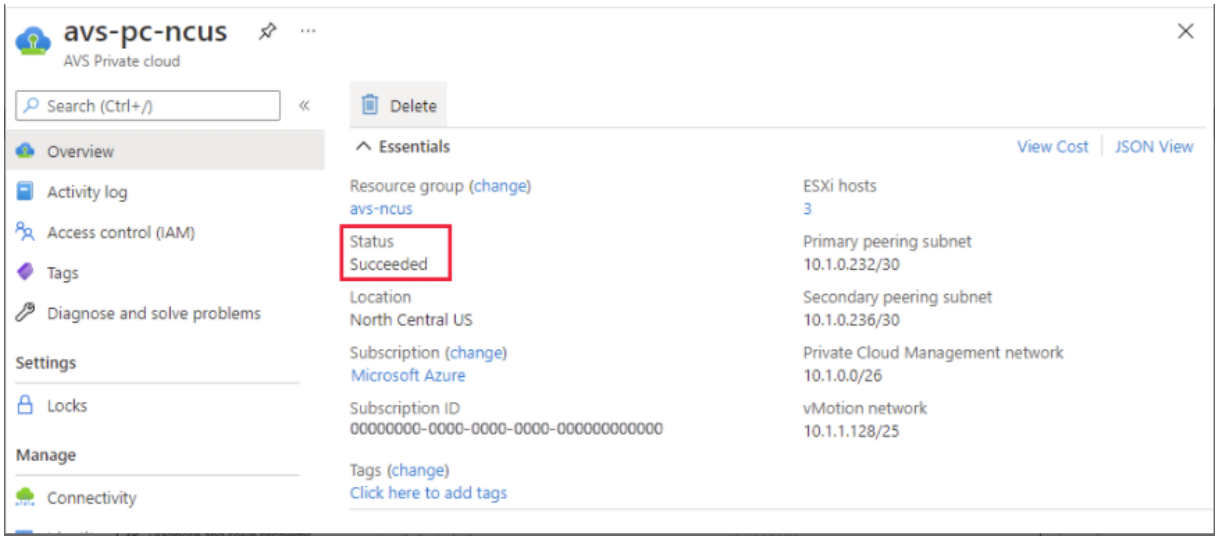
Field	Value
Number of hosts	Shows the number of hosts allocated for the private cloud cluster. The default value is 3, which can be raised or lowered after deployment.
Address block for private cloud	Provide an IP address block for the private cloud. The CIDR represents the private cloud management network and will be used for the cluster management services, such as vCenter Server and NSX-T Manager. Use /22 address space, for example, 10.175.0.0/22. The address should be unique and not overlap with other Azure Virtual Networks and with on-premises networks.

In the **Create a private cloud** screen:

1. In the **Location** field, select the region that has the AVS. The resource group region is the same as the AVS region.
2. In the **Size of host** field, select a size as per your need.
3. Specify an IP address in the **Address Block for private cloud** field. For example, 10.15.0.0/22.
4. Select **Review + Create**.
5. After reviewing the information, click **Create**.

> **Tip:**
>
> Creating a private cloud can take 3–4 hours. Adding a single host to the cluster can take 30–45 minutes.

Verify that the deployment was successful. Navigate to the resource group that you created and select your private cloud. Once the **Status** is **Succeeded** the deployment is complete.



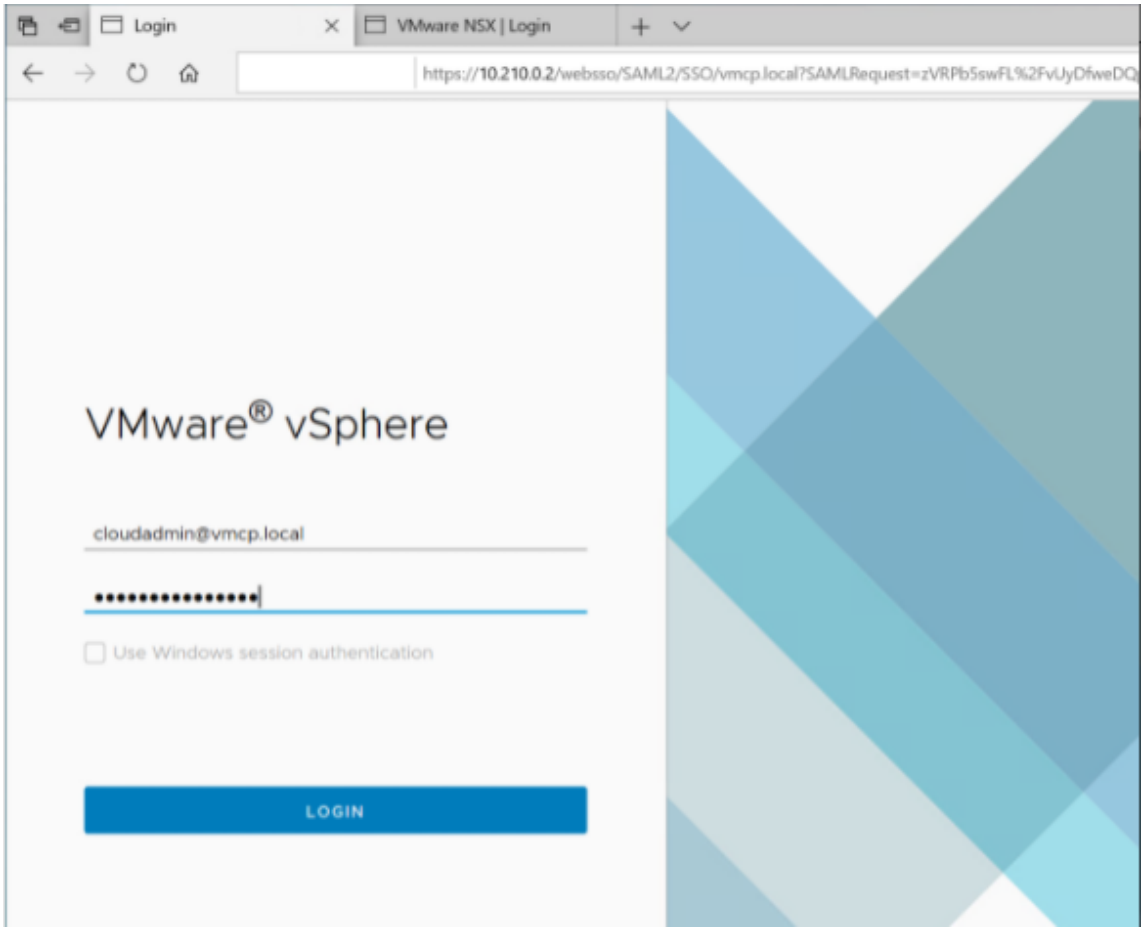
Access the AVS private cloud Once you have created a private cloud, create a Windows VM and connect to the local vCenter of your private cloud.

Create a new Windows virtual machine

1. In the resource group, select **+ Add** then search and select **Microsoft Windows 10/11 or Windows Server 2016/2019**.
2. Enter the required information, then select **Review + Create**.
3. Once validation passes, select **Create** to start the virtual machine creation process.

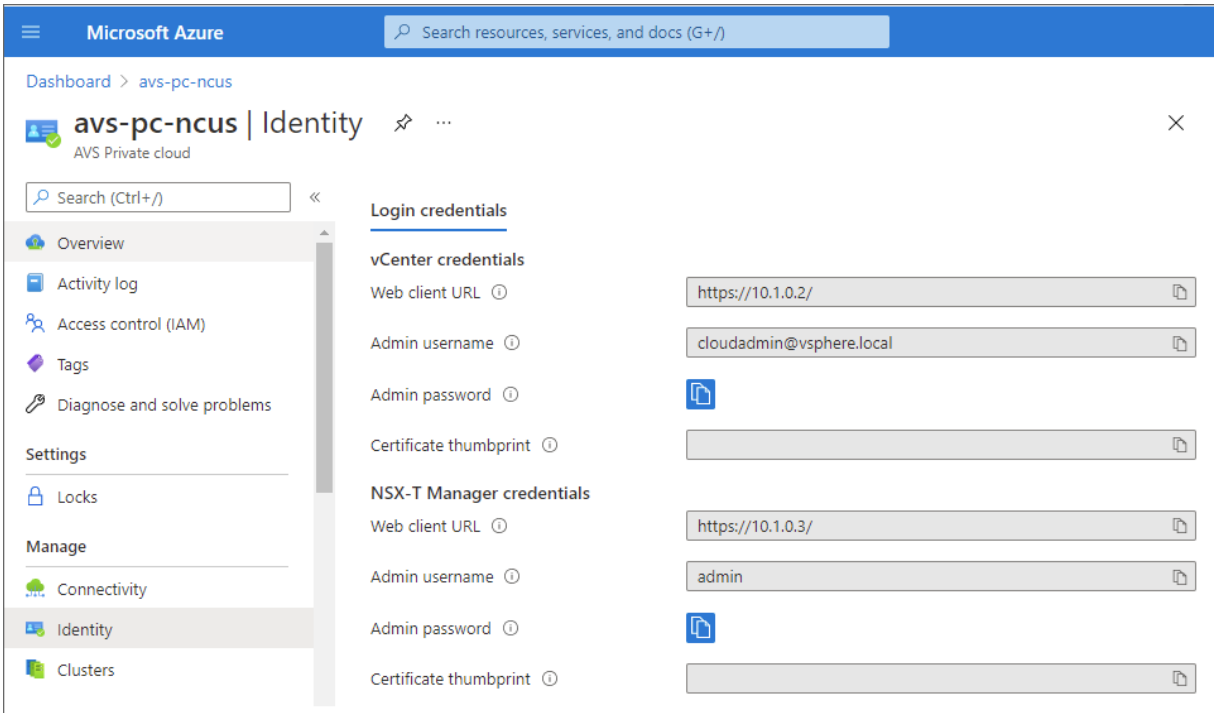
Connect to the local vCenter of your private cloud

1. Sign in to **vSphere Client with VMware vCenter SSO** as a cloud administrator.



2. In the Azure portal, select your private cloud, and then **Manage> Identity**.

The URLs and user credentials for private cloud vCenter and NSX-T Manager appear:



Display private cloud vCenter and NSX Manager URLs and credentials.

After confirming URLs and user credentials:

1. Navigate to the VM that you created in the preceding step and connect to the virtual machine.
2. In the Windows VM, open a browser and navigate to the vCenter and NSX-T Manager URLs in two browser tabs. In the vCenter tab, enter the *cloudadmin@vmcp.local* user credentials from the previous step.

Configure networking for your VMware private cloud in Azure After accessing an ASV private cloud, configure networking by creating a virtual network and gateway.

Create a virtual network

1. Sign in to the Azure portal.
2. Navigate to the previously created resource group.
3. Select **+ Add** to define a new resource.
4. In the **Search the Marketplace** text box, type *virtual network*. Find the virtual network resource and select it.
5. On the **Virtual Network** page, select **Create** to set up the virtual network for your private cloud.
6. On the **Create Virtual Network** page, enter the details for your virtual network.
7. On the **Basics** tab, enter a name for the virtual network, select the appropriate region, and click **Next : IP Addresses.**
8. On the **IP Addresses** tab, under IPv4 address space, enter the previously created address.

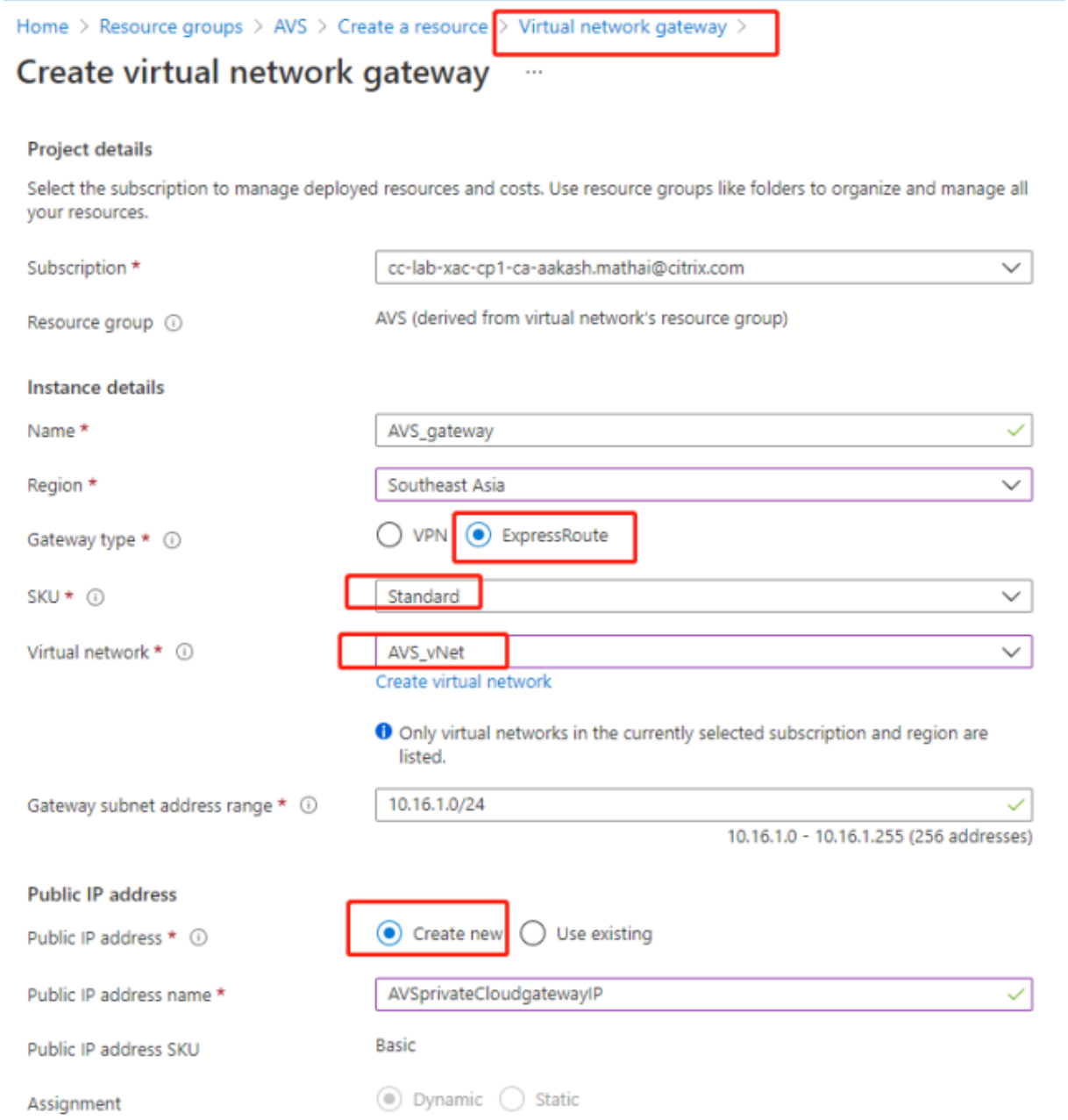
> **Important:**
>
> Use an address that does not overlap with the address space you used when you created your private cloud.

After entering the address space:

1. Select **+ Add subnet**.
2. On the **Add subnet** page, give the subnet a name and appropriate address range.
3. Click **Add.**
4. Select **Review + create**.
5. Verify the information and click **Create**. Once the deployment is complete, the virtual network appears in the resource group.

Create a virtual network gateway After creating a virtual network, create a virtual network gateway.

1. In your resource group, select **+ Add** to add a new resource.
2. In the **Search the Marketplace** text box, type *virtual network gateway*. Find the virtual network resource and select it.
3. On the **Virtual Network gateway** page, click **Create**.
4. On the **Basics** tab in the **Create virtual network gateway** page, provide values for the fields.
5. Click **Review + create**.



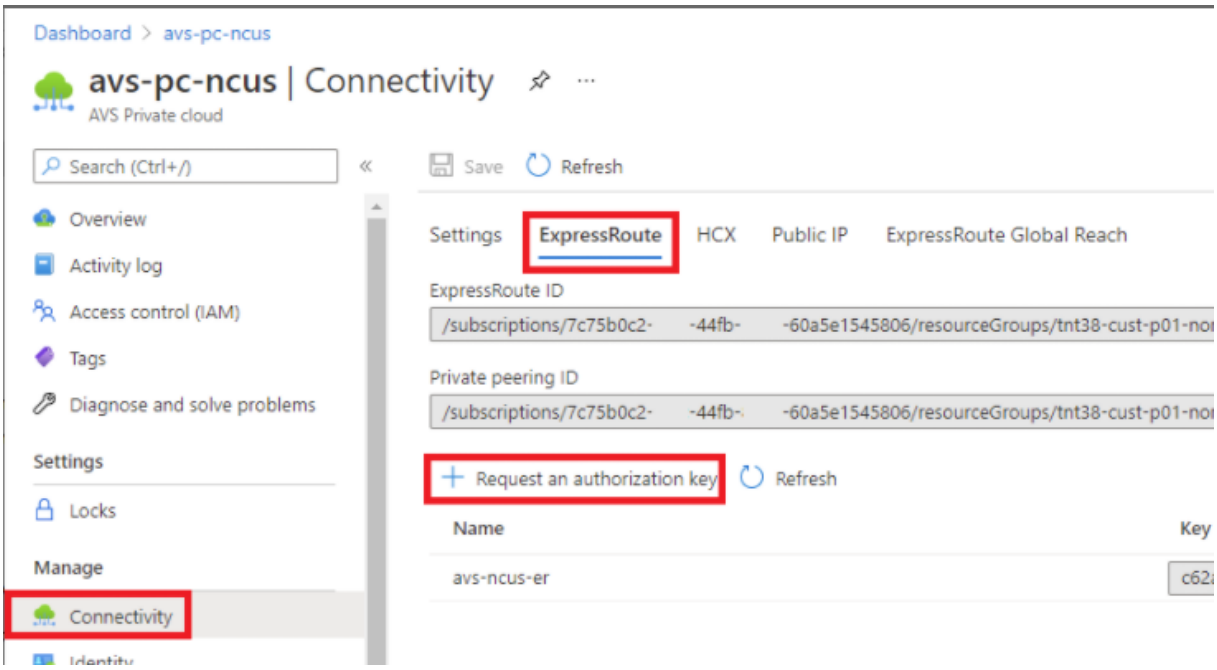
After reviewing the virtual network gateway configuration, click **Create** to deploy your virtual network gateway.

Once the deployment completes, connect your **ExpressRoute** connection to the virtual network gateway containing your Azure AVS private cloud.

Connect ExpressRoute to the virtual network gateway After deploying a virtual network gateway, add a connection between it and your Azure AVS private cloud:

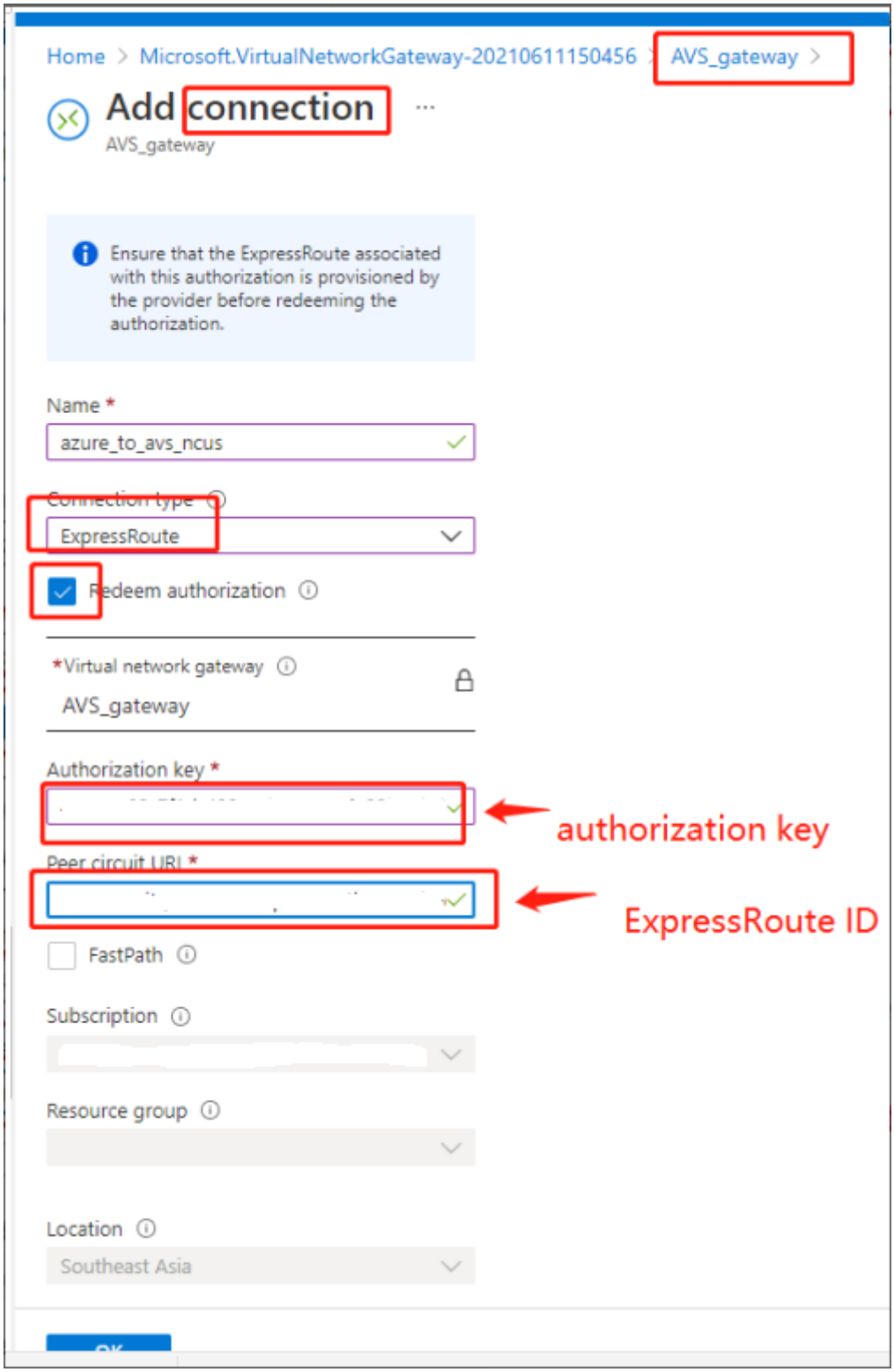
1. Request an ExpressRoute authorization key.

2. In the Azure portal, navigate to the **Azure VMware Solution private cloud**. Select **Manage> Connectivity > ExpressRoute** and then select **+ Request an authorization key.**

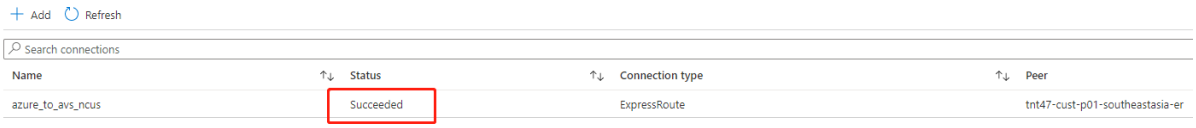


After requesting an authorization key:

1. Enter a name for the key and click **Create**. It may take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.
2. Copy the **authorization key** and **ExpressRoute ID**. You'll need them to complete the peering process. The authorization key disappears after some time, so copy it when it appears.
3. Navigate to the **virtual network gateway** you plan to use and select **Connections> + Add**.
4. On the **Add connection** page, provide values for the fields, and select **OK.**



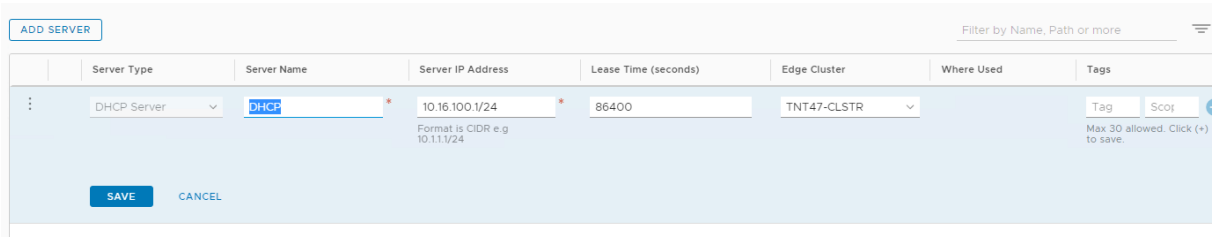
The connection is established between your ExpressRoute circuit and your virtual network:



Configure DHCP for Azure VMware Solution After connecting ExpressRoute to the virtual gateway, configure DHCP.

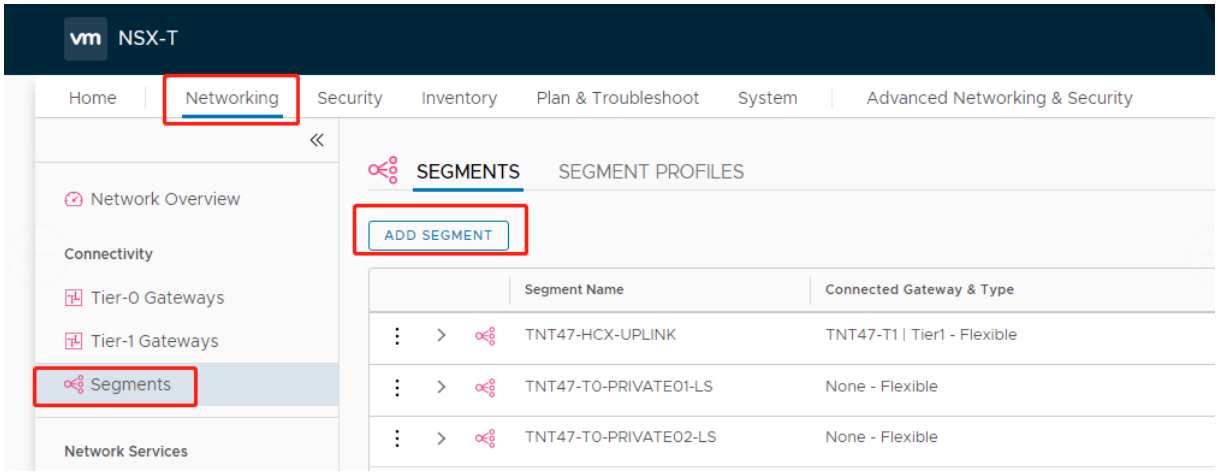
Use NSX-T to host your DHCP server In NSX-T Manager:

1. Select **Networking> DHCP**, and then select **Add Server**.
2. Select **DHCP** for the **Server Type**, provide the server name and IP address.
3. Click **Save**.
4. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
5. Select **No IP Allocation Set** to add a subnet.
6. Select **DHCP Local Server** for the **Type**.
7. For the **DHCP Server**, select **Default DHCP**, and then click **Save**.
8. Click **Save** again and then select **Close Editing**.



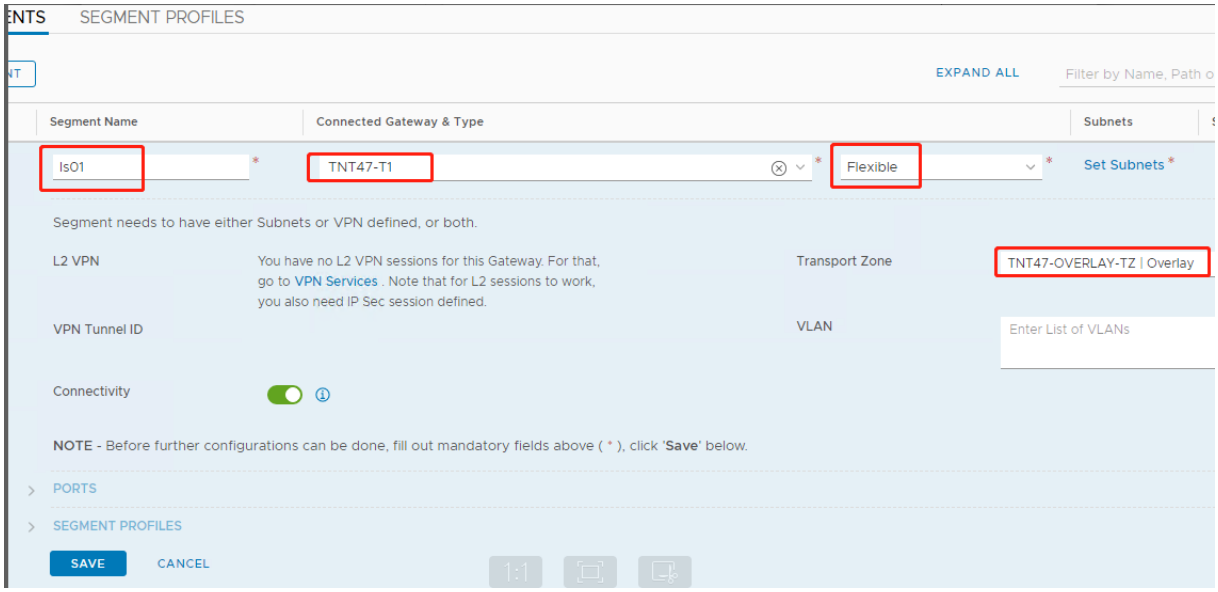
Add a network segment in the Azure VMware Solution After setting up DHCP, add a network segment.

To add a network segment, in NSX-T Manager, select **Networking> Segments**, and then click **Add Segment**.



In the **Segments profile** screen:

1. Enter a **name** for the segment.
2. Select the **Tier-1 Gateway (TNTxx-T1)** as the **Connected Gateway** and leave the **Type** as **Flexible**.
3. Select the pre-configured overlay **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Click **Set Subnets**.



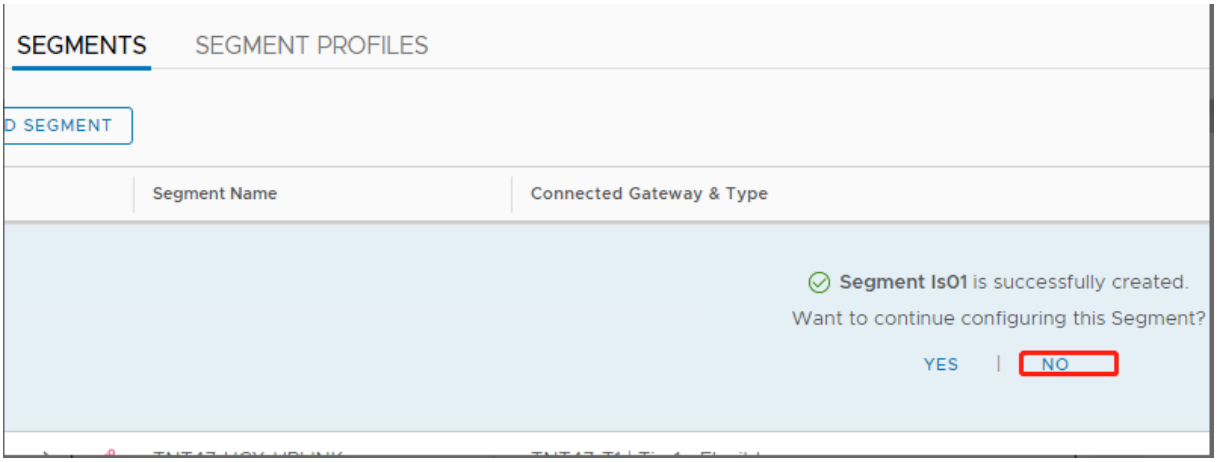
In the **Subnets** section:

1. Enter the gateway IP address.
2. Select **Add**.

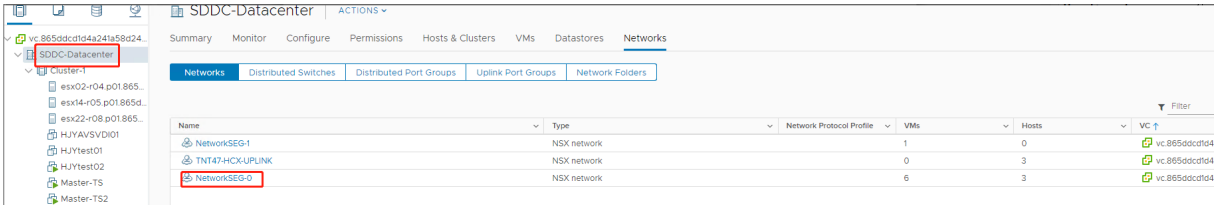
> **Important:**
>
> This segment IP address must belong to the Azure gateway IP address, 10.15.0.0/22.

DHCP range must belong to segment IP address:

Select **No** to decline the option to continue configuring the segment:



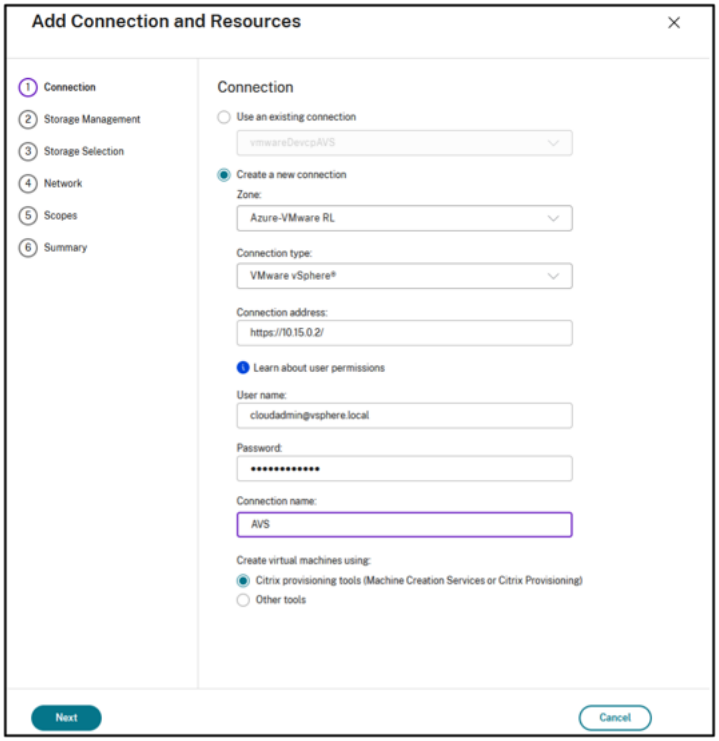
In vCenter, select **Networking > SDDC-Datacenter**:



Verify the AVS environment Set up resource location for the AVS private cloud and install a pair of cloud connectors.

Create the AVS connection in Citrix Studio

1. Create a machine in vCenter and install a pair of Cloud Connectors in the machine. See Configure the instances.
2. From **Manage > Full Configuration**, select Hosting in the left pane.
3. Select the hosting node, and click **Add Connection and Resources**.
4. On the **Connection** screen, select **Create a new Connection**, and the following details:



a) Select **Connection type** as **VMware vSphere**.
b) In the **Connection address**, enter the vCenter private IP address.
c) Enter the vCenter credentials.
d) Enter a connection name.
e) Choose the tool to create virtual machines.

5. On the **Network** screen, select the subnet created in the NSX-T server.
6. Complete the wizard.

Google Cloud VMware Engine

Citrix DaaS lets you migrate VMware-based on-premises Citrix workloads to Google Cloud VMware Engine.

Configure Google Cloud VMware Engine

The following procedure describes how to acquire and set up cluster on Google Cloud VMware Engine.

Access the VMware Engine portal

1. In the **Google Cloud Console**, click the navigation menu.

2. In the **Compute** section, click **VMware Engine** to open VMware Engine in a new browser tab.

Requirements to create first private cloud You must have access to Google Cloud VMware Engine, available VMware Engine node quota, and an appropriate IAM role. Set up the following requirements before you continue to create your private cloud:

1. Request API access and node quota. For more information, see Requesting API access and quota.
2. Note the address ranges you want to use for VMware management appliances and the HCX deployment network. For more information, see Networking requirements.

   > **Note:**
   >
   > The HCX deployment is only applicable to IP Plan version 1.0.

3. Get the VMware Engine Service Admin IAM role.

Create your first private cloud

1. Access the VMware Engine portal.
2. On the VMware Engine Home page, click **Create a private cloud**. The hosting location and hardware node types are listed.
3. Select the number of nodes for the private cloud. At least three nodes are required.
4. Enter a Classless Inter-Domain Routing (CIDR) range for the VMware management network.
5. Enter a CIDR range for the HCX deployment network.

   > **Important:**
   >
   > - The CIDR range must not overlap with any of your on-premises or cloud subnets. The CIDR range must be /27 or higher.
   > - The HCX deployment is only applicable to IP Plan version 1.0.

6. Select **Review and create**.
7. Review the settings. To change any settings, click **Back**.
8. Click **Create** to begin creating the private cloud.

As VMware Engine creates your new private cloud, it deploys several VMware components and sets up initial Autoscale policies for clusters in the private cloud. Private cloud creation can take 30 minutes to 2 hours. After the provisioning is complete, you receive an email.

Set up Google Cloud VMware Engine VPN Gateway To establish an initial connectivity to Google Cloud VMware Engine, you can use a VPN gateway. This is an OpenVPN-based client VPN using which you can connect to your VMware Software Defined Data Center (SDDC) vCenter and do any initial configuration required.

Before deploying a VPN gateway, configure the **Edge Services** range for the region where your SDDC is deployed. To do this:

1. Log on to the **Google Cloud VMware Engine** portal, and go to **Network > Regional Settings**. Click **Add Region**.
2. Choose the region where your SDDC is deployed and enable **Internet Access** and **Public IP Service**.
3. Supply the Edge Services range noted during planning and click **Submit**. Enabling these services take 10–15 minutes.

   Once complete, the Edge Services show as **Enabled** on the Regional Settings page. Enabling these settings allow Public IPs to be allocated to your SDDC, which is a requirement for deploying a VPN gateway.

Deploy a VPN gateway

1. In the **Google Cloud VMware Engine** portal, go to **Network > VPN Gateways**. Click **Create New VPN Gateway**.
2. Supply the name for the VPN gateway and the client subnet reserved during planning. The location of the VPN must be the same as the private cloud region. Click **Next**.
3. Select users to grant VPN access. Click **Next**.
4. Specify the networks that must be accessible over VPN. Click **Next**.
5. A summary screen is displayed. Verify the selections, and click **Submit** to create the VPN Gateway. The VPN Gateways page is displayed with the status of the new VPN gateway as **Creating**.
6. After the status changes to **Operational**, click the new VPN gateway.
7. Click **Download my VPN configuration** to download a ZIP file containing pre-configured OpenVPN profiles for the VPN gateway. Profiles for connecting through UDP/1194 and TCP/443 are available. Choose your preference and import it into Open VPN, and then connect.
8. Go to **Resources** and select your SDDC.

Connect the VPN

1. Establish a point-to-site connection between your on-premises network and the private cloud through the VPN Gateway setup. See Set up Google Cloud VMware Engine VPN Gateway.
2. Upload the VPN configuration downloaded in Set up Google Cloud VMware Engine VPN Gateway.

3. Import to your VPN client, for example, OpenVPN Connect.

For more information, see Connecting using VPN.

Create first subnet

Access NSX-T Manager from the VMware Engine portal The process of creating a subnet happens in NSX-T, which you access through VMware Engine. Do the following to access NSX-T Manager.

1. Log on to the **Google Cloud VMware Engine** portal.
2. From the main navigation, go to **Resources**.
3. Click the **Private cloud name** corresponding to the private cloud where you want to create the subnet.
4. On the details page of your private cloud, click the **vSphere Management Network** tab.
5. Click the **FQDN** corresponding to the NSX-T Manager.
6. When prompted, enter your sign-in credentials. If you have set up vIDM and connected it to an identity source, such as Active Directory, use your identity source credentials instead.

> **Reminder:**
>
> You can retrieve generated credentials from the private cloud details page.

Set up DHCP service for the subnet Before you can create a subnet, set up a DHCP service:

In NSX-T Manager:

1. Go to **Networking > DHCP**. The networking dashboard shows that the DHCP service creates one Tier-0 and one Tier-1 gateway.
2. To begin provisioning a DHCP server, click **Add Server**.
3. Select **DHCP** for the **Server Type**, provide the server name and IP address.
4. Click **Save** to create the DHCP service.

Do the following to attach this DHCP service to the relevant Tier-1 gateway. A default Tier-1 gateway is already provisioned by the DHCP service:

1. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
2. In the **IP Address Management** field, select **No IP Allocation Set**.
3. Select **DHCP Local Server** for the **Type**.
4. Select the DHCP server that you created for the **DHCP Server**.
5. Click **Save**.
6. Click **Close Editing**.

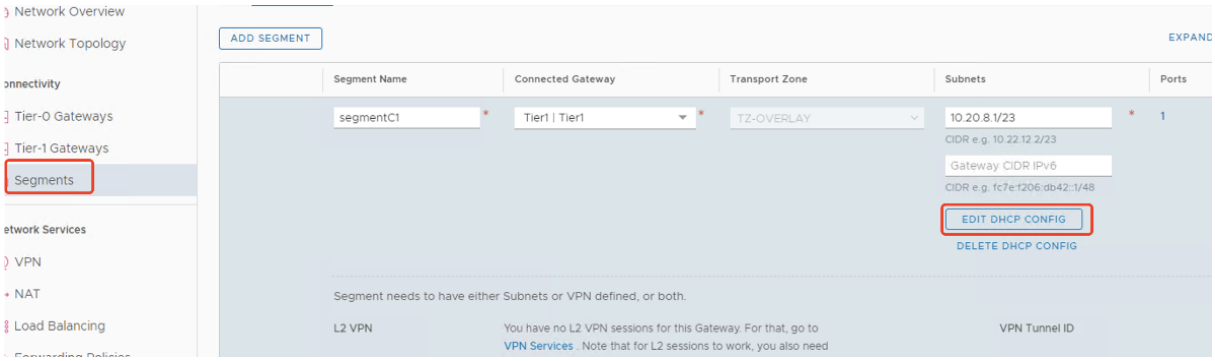
You can now create a network segment in NSX-T. For more information about DHCP in NSX-T, see the VMware documentation for DHCP.

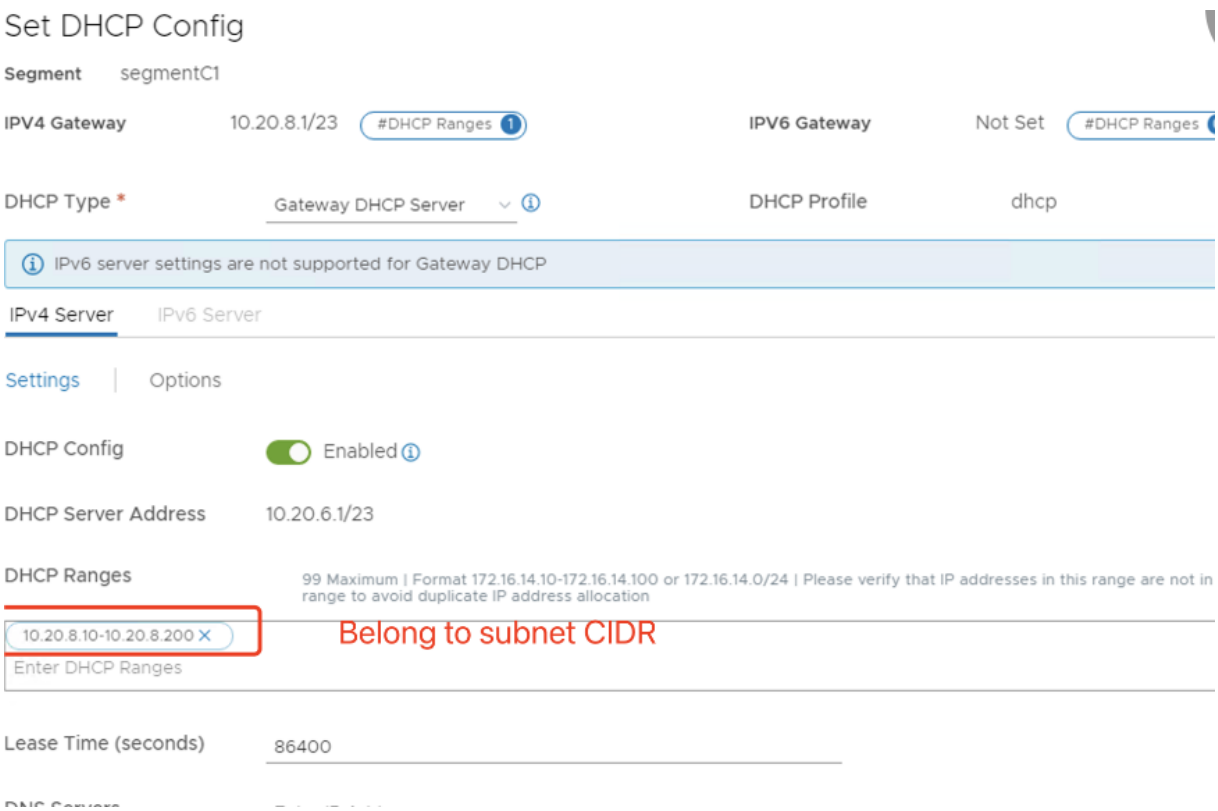
Create a network segment in NSX-T For workload VMs, you create subnets as NSX-T network segments for your private cloud:

1. In NSX-T Manager, go to **Networking > Segments**.
2. Click **Add Segment**.
3. Enter a name for the segment.
4. Select the **Tier-1** as the **Connected Gateway** and leave the Type as **Flexible**.
5. Click **Set Subnets**.
6. Click **Add Subnets**.
7. Enter the subnet range in the **Gateway IP/Prefix Length**. Specify the subnet range with **.1** as the last octet. For example, **10.12.2.1/24**.
8. Specify the DHCP Ranges and click **ADD**.
9. In **Transport Zone**, select **TZ-OVERLAY** from the drop-down list.
10. Click **Save**. You can now select this network segment in vCenter when creating a VM.

In a given region, you can set up at most 100 unique routes from VMware Engine to your VPC network using private services access. This includes, for example, private cloud management IP address ranges, NSX-T workload network segments, and HCX network IP address ranges. This limit includes all private clouds in the region.

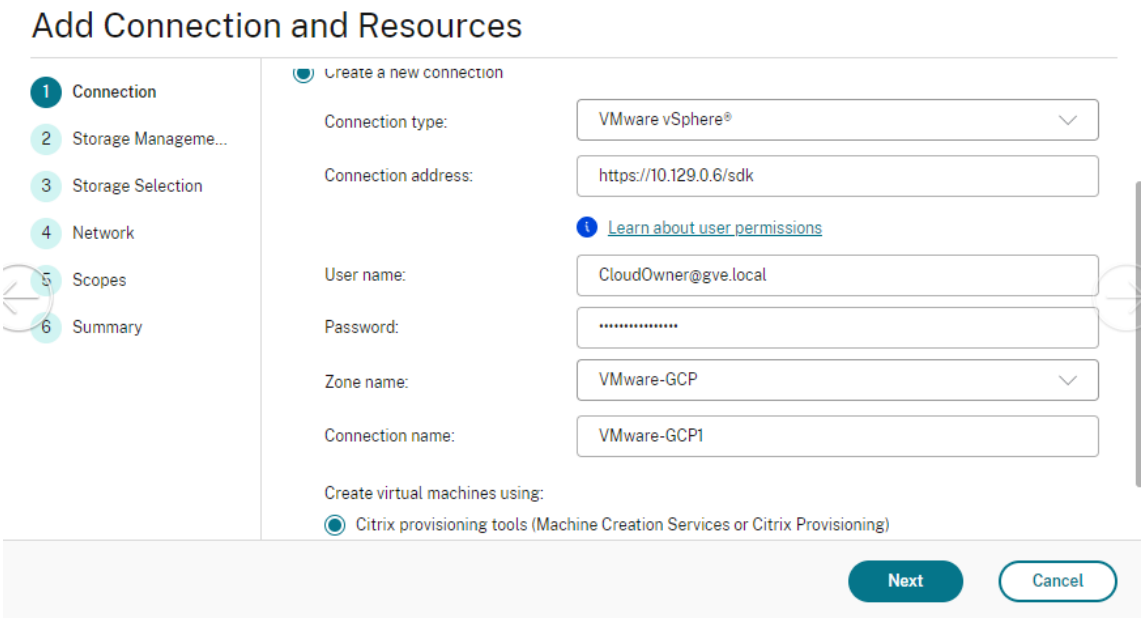
> **Note:**
>
> There is a Google Cloud configuration issue because of which you need to configure DHCP range setting several times. Therefore, make sure to configure the DHCP range setting after Google Cloud configuration. Click **EDIT DHCP CONFIG** to configure the DHCP ranges.





Create the Google Cloud VMware connection in Citrix Studio

1. Create a machine in vCenter and install a pair of Cloud Connectors in the machine. See Configure the instances.
2. Launch the Citrix Studio.
3. Select the hosting node, and click **Add Connection and Resources**.
4. On the **Connection** screen, select **Create a new Connection**, and the following details:



a) Select **Connection type** as **VMware vSphere**.
b) In the **Connection address**, enter the vCenter private IP address.
c) Enter the vCenter credentials.
d) Enter a connection name.
e) Choose the tool to create virtual machines.

5. On the **Network** screen, select the subnet created in the NSX-T server.
6. Complete the wizard.

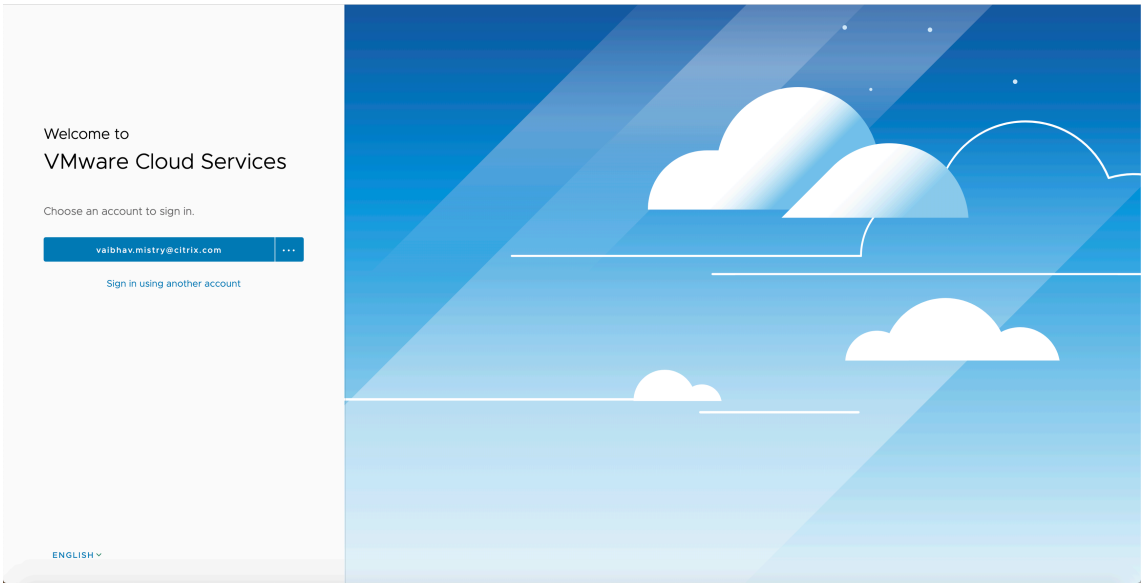
VMware cloud on Amazon Web Services (AWS)

VMware cloud on Amazon Web Services (AWS) enables you to migrate VMware based on-premises Citrix workloads to AWS Cloud and your core Citrix Virtual Apps and Desktops environment to Citrix DaaS.

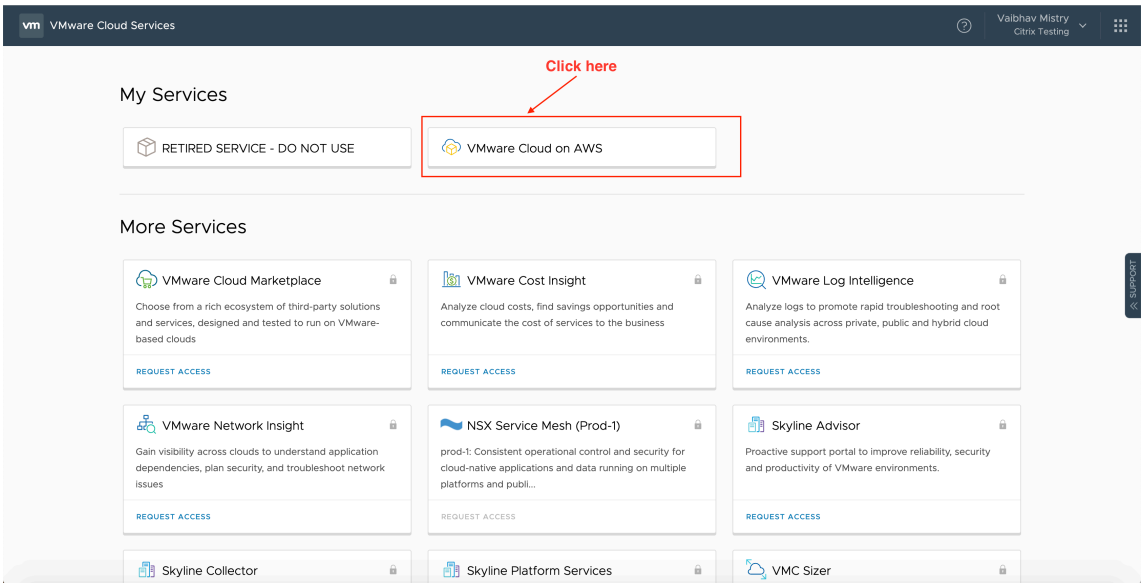
This article describes the procedure to set up a VMware cloud on AWS.

Access the VMware cloud environment

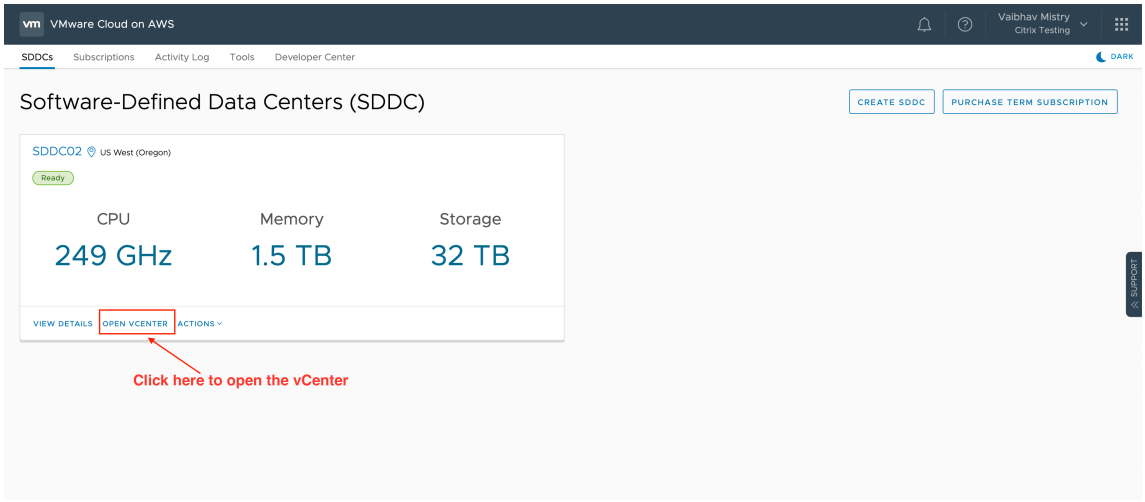
1. Log in to VMware cloud services using the URL https://console.cloud.vmware.com/.

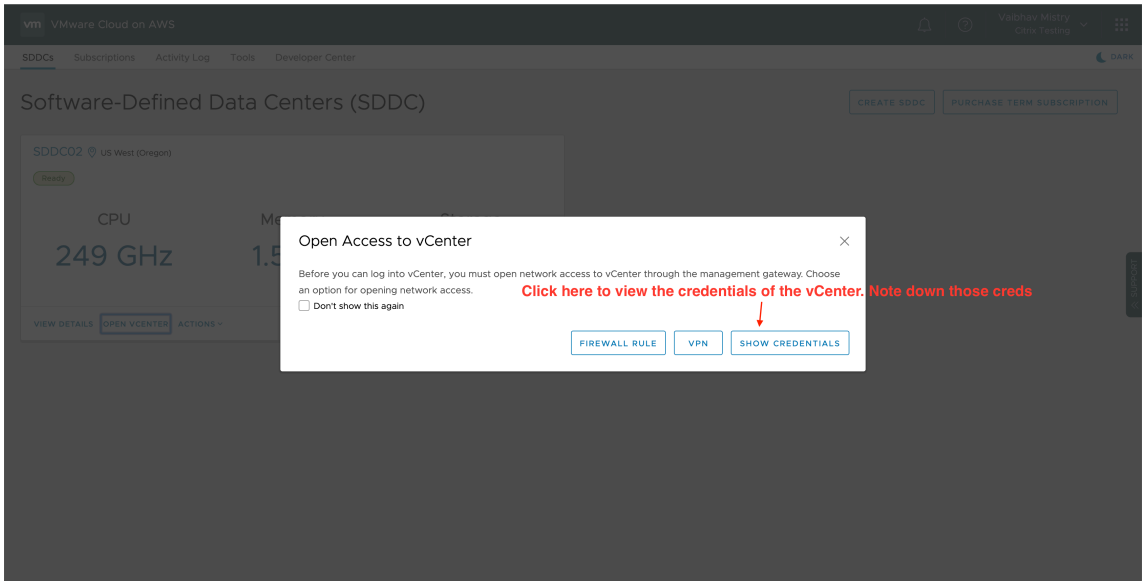


2. Click **VMware Cloud on AWS**. The page Software-Defined Data Centers (SDDC) appears.

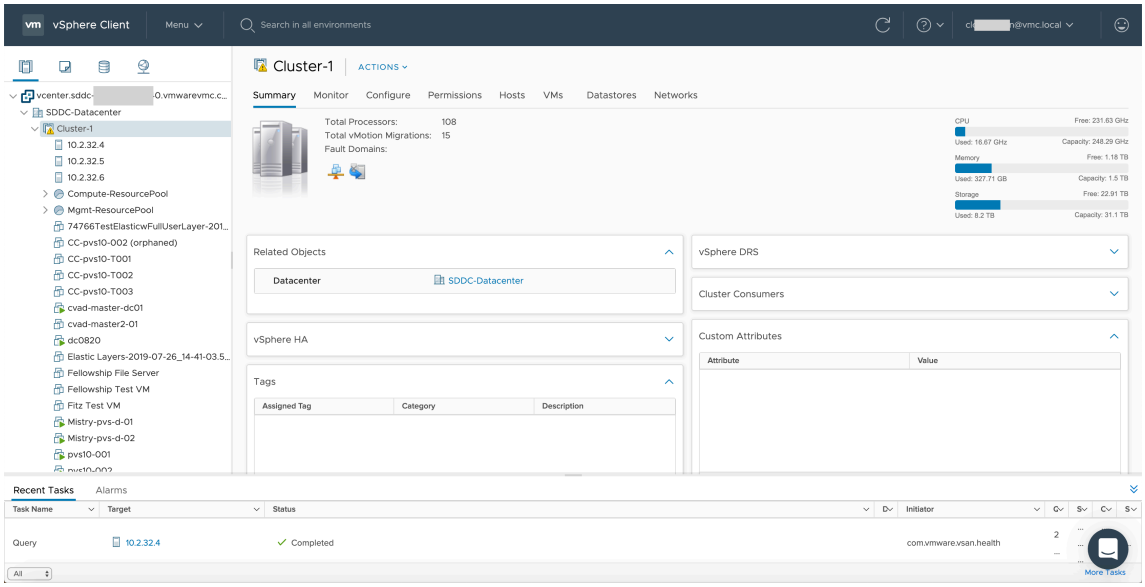


3. Click **OPEN VCENTER**, and then click **SHOW CREDENTIALS**. Note the credentials for later use.





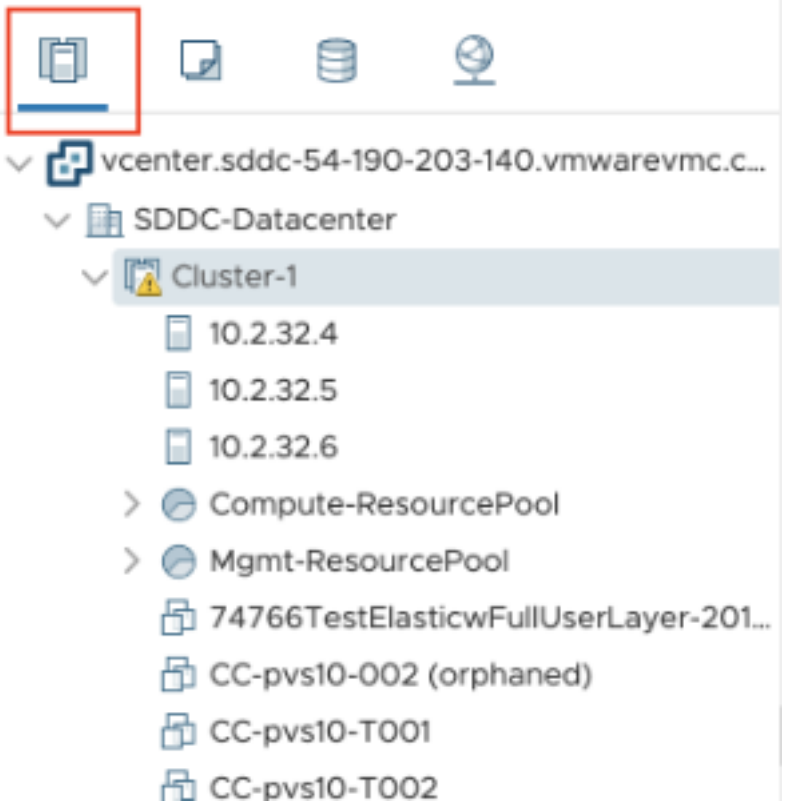
4. Open a Web browser and enter the URL for the vSphere Web Client.
5. Enter the credentials as noted and click **Login**. The vSphere client webpage is similar to the on-premises environment.



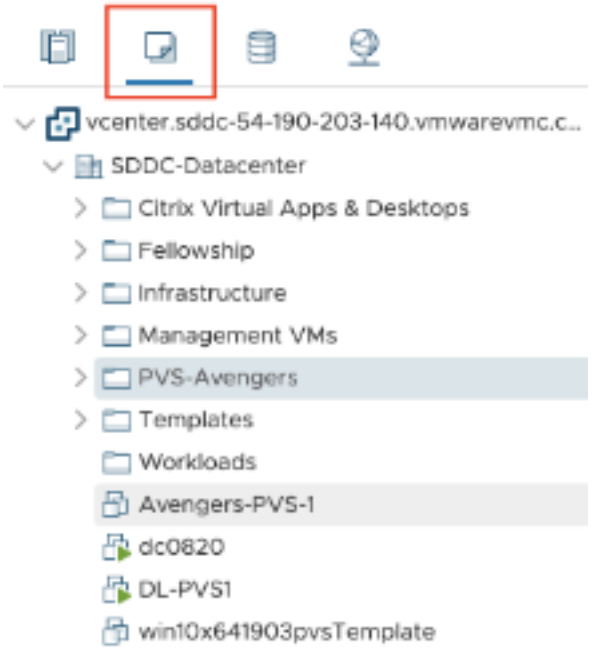
About VMware cloud environment

There are four views on the vSphere client webpage.

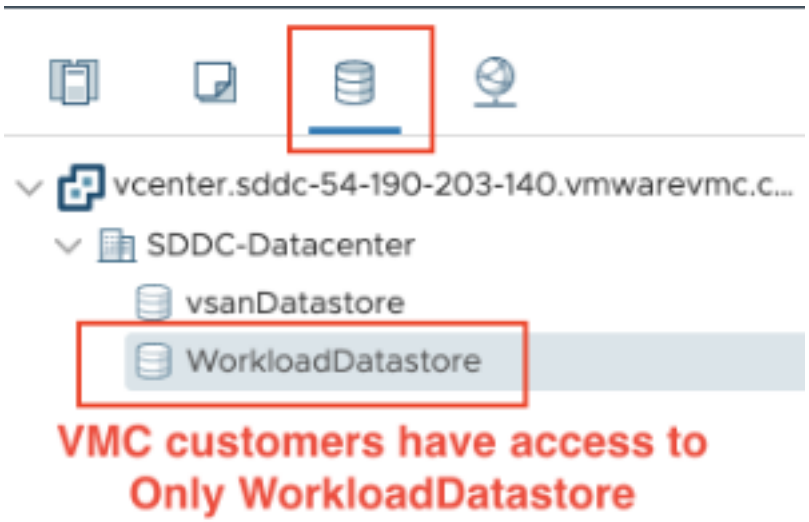
- Host and Cluster view: You cannot create a new Cluster, but the cloud admin can create multiple resource pools.



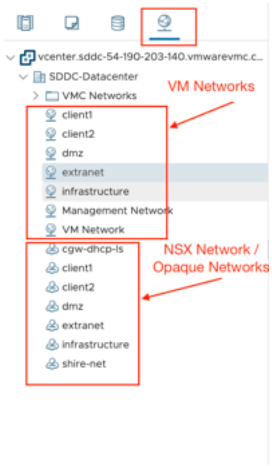
- VM and Template view: Cloud admin can create many folders.



- Storage View: Select **WorkloadDatastore** storage when you add hosting unit in the Citrix Studio because you have access to only Workload Datastore.



- Network View: The icons are different for VMware cloud networks and opaque networks.



After you set up the cluster, refer to VMware virtualization environments for adding connections and resources.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.

- For creating and managing a connection, see Connection to VMware cloud and partner solutions.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

XenServer virtualization environments

December 11, 2023

XenServer simplifies your operational management while ensuring a high definition user experience for intensive workloads.

To set up your XenServer, see Add a resource type.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to XenServer.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Size and scale considerations for Cloud Connectors

December 18, 2023

When evaluating Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) for sizing and scalability, consider all the components. Research and test the configuration of Citrix Cloud Connectors and

StoreFront for your specific requirements. Providing insufficient resources for sizing and scalability negatively affects the performance of your deployment.

> **Note:**
>
> - These recommendations apply to Citrix DaaS Standard for Azure in addition to Citrix DaaS.
> - The tests and recommendations given in this article are guidelines to help you start your testing. We recommend that you perform the testing in your environment to validate the correct connector sizing.

This article provides details of the tested maximum capacities and best practice recommendations for Cloud Connector machine configuration. Tests were performed on deployments configured with StoreFront and Local Host Cache (LHC).

The information provided applies to deployments in which each resource location contains either VDI workloads or RDS workloads. For resource locations that contain mixed workloads of VDI and RDS together, contact Citrix Consulting Services.

The Cloud Connector links your workloads to Citrix DaaS in the following ways:

- Provides a proxy for communication between your VDAs and Citrix DaaS
- Provides a proxy for communication between Citrix DaaS and your Active Directory (AD) and hypervisors
- In deployments that include StoreFront servers, the Cloud Connector serves as a temporary session broker during cloud outages, providing users with continued access to resources

It is important to have your Cloud Connectors properly sized and configured to meet your specific needs.

Each set of Cloud Connectors is assigned to a resource location (also known as a zone). A resource location is a logical separation that specifies which resources communicate with that set of Cloud Connectors. At least one resource location is required per domain to communicate with the Active Directory (AD).

Each machine catalog and hosting connection is assigned to a resource location.

For deployments with more than one resource location, assign machine catalogs and VDAs to the resource locations to optimize the ability of LHC to broker connections during outages. For more information on creating and managing resource locations, see Connect to Citrix Cloud. For optimum performance, configure your Cloud Connectors on low-latency connections to VDAs, AD servers, and hypervisors.

Recommended processors and storage

For performance similar to that seen in these tests, use modern processors that support SHA extensions. SHA extensions reduce the cryptographic load on the CPU. Recommended processors include:

- Advanced Micro Devices (AMD) Zen and newer processors
- Intel Ice Lake and newer processors

The recommended processors run efficiently. You can use older processors, however, it might lead to a higher CPU load. We recommend increasing your vCPU count to offset this behavior.

The tests described in this article were performed with AMD EPYC and Intel Cascade Lake processors.

Cloud Connectors have a heavy cryptographic load while communicating with the cloud. Cloud Connectors using processors with SHA extensions experience lower load on their CPU which is expressed by lower CPU usage by the Windows Local Security Authority Subsystem Service (LSASS).

Citrix recommends using modern storage with adequate I/O operations per second (IOPS), especially for deployments that use LHC. Solid state drives (SSDs) are suggested but premium cloud storage tiers are not needed. Higher IOPS are needed for LHC scenarios where the Cloud Connector runs a small copy of the database. This database is updated with site configuration changes regularly and provides brokering capabilities to the resource location in times of Citrix Cloud outages.

Recommended compute configuration for Local Host Cache

Local Host Cache (LHC) provides high availability by enabling connection brokering operations in a deployment to continue when a Cloud Connector cannot communicate with Citrix Cloud.

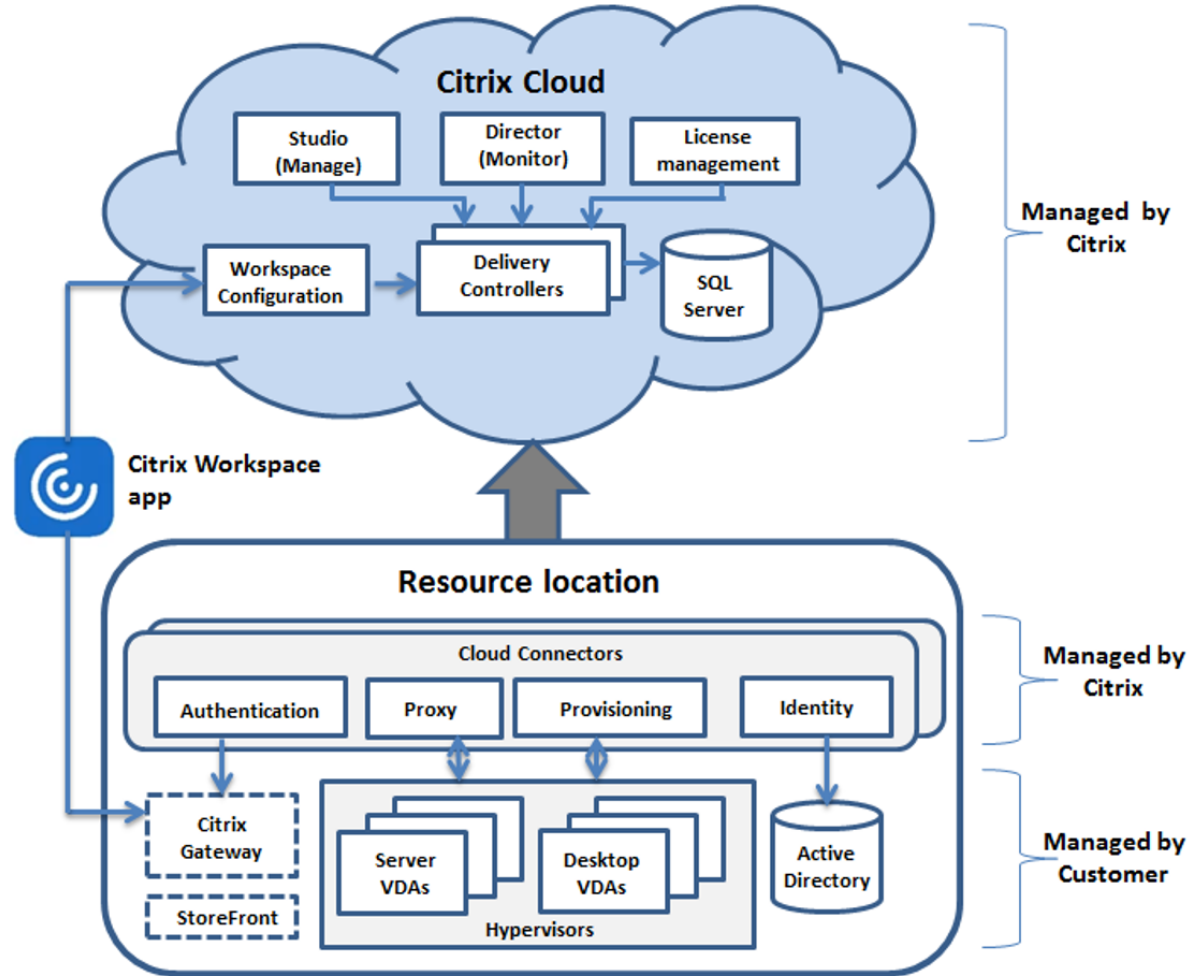
Cloud Connectors run Microsoft SQL Express Server LocalDB, which is automatically installed when you install the Cloud Connector. The CPU configuration of the Cloud Connector, especially the number of cores available to SQL Express Server LocalDB, directly affects LHC performance. The number of CPU cores available to SQL Server Express Server LocalDB affects LHC performance even more than memory allocation does. This CPU overhead is observed only when in LHC mode when Citrix DaaS is not reachable, and the LHC broker is active. For any deployment using LHC, Citrix recommends four cores per socket, with a minimum of four CPU cores per Cloud Connector. For information on configuring compute resources for SQL Express Server LocalDB, see Compute capacity limits by edition of SQL Server.

If compute resources available to the SQL Express Server LocalDB are misconfigured, configuration synchronization times might be increased and performance during outages might be reduced. In some virtualized environments, compute capacity might depend on the number of logical processors and not CPU cores.

Summary of test findings

All results in this summary are based on the findings from a test environment as configured in the detailed sections of this article. The results shown here are for a single resource location. Different system configurations might yield different results.

This illustration gives a graphical overview of the tested configuration.



This table provides a quick guide to sizing your resource location. 10k is the maximum for a single resource location. See Limits for information on the resource location limits.

> **Note:**
>
> Exceeding the limit may cause connectivity as well as performance issues during an outage. Therefore, you must not exceed the recommended limit as this can lead to unregistered VDAs.

Results are based on Citrix internal testing. The configurations described were tested with varying workloads, including high-rate session launch tests and registration storms.

	Medium	Large	Maximum
VDAs	1000 VDI or 250 RDS	5000 VDI or 500 RDS	10,000 VDI or 1000 RDS
Hosting connections	20	40	40
CPUs for Connectors	4 vCPU	4 vCPU	8 vCPU
Memory for Connectors	6 GB	8 GB	10 GB

Test methodology

Tests were conducted to add load and to measure the performance of the environment components. The components were monitored by collecting performance data and procedure timing, such as logon time and registration time. Sometimes, proprietary Citrix simulation tools are used to simulate VDAs and sessions. These tools are designed to exercise Citrix components the same way that traditional VDAs and sessions do, without the same resource requirements to host real sessions and VDAs. Tests were conducted in both cloud brokering and LHC mode for scenarios with Citrix StoreFront.

Recommendations for Cloud Connector sizing in this article are based on data gathered from these tests.

The following tests were run:

- **Session logon/launch storm:** a test that simulates high-volume logon periods.
- **VDA registration storm:** a test that simulates high-volume VDA registration periods. For example, following an upgrade cycle or transitioning between cloud brokering and Local Host Cache mode.
- **VDA power action storm:** a test that simulates high-volume of VDA power actions.

Test scenarios and conditions

These tests were performed with LHC configured. For more information about using LHC, see the Local Host Cache article. LHC requires an on-premises StoreFront server. For detailed information about StoreFront, see the StoreFront product documentation.

Recommendations for StoreFront configurations:

- If you have multiple resource locations with a single StoreFront server or server group, enable the advanced health check option for the StoreFront store. See StoreFront requirement in the Local Host Cache article.
- For higher session launch rates, use a StoreFront server group. See Configure server groups in the StoreFront product documentation.

Test conditions:

- CPU and memory requirements are for the base OS and Citrix services only. Third-party apps and services might require additional resources.
- VDAs are any virtual or physical machines running Citrix Virtual Delivery Agent.
- Tests are performed using Windows VDAs only.
- All VDAs tested were power-managed using Citrix DaaS.
- Workloads of 1000 to 10,000 VDI and 250–1000 RDS servers with 1000-20000 sessions were tested.
- RDS sessions were tested up to 20,000 per resource location.
- Tests were performed using one Cloud Connector in both normal operations as well as during outage. Citrix recommends using at least two Cloud Connectors for high availability. When in outage mode, only one of the connectors is used for VDA registrations and brokering.
- Tests were performed with the Cloud Connector configured with Intel Cascade Lake processors.
- Sessions were launched via a single Citrix StoreFront server.
- LHC outage sessions launch tests conducted after machines had re-registered.

RDS session counts are a recommendation and not a limit. Test your own RDS session limit in your environment.

> **Note:**
>
> Session count and launch rate are more important for RDS than the VDA count.

Medium workloads

These workloads were tested with 4 vCPUs and 6 GB memory.

Test workloads	Site condition	VDA registration time	Registration CPU and memory usage	Launch test length	Session launch CPU and memory usage	Launch rate
1000 VDI	Online	5 minutes	CPU maximum = 36%, CPU average = 33%, memory maximum = 5.3 GB	2 minutes	CPU maximum = 29%, CPU average = 27%, memory maximum = 3.7 GB	500 per minute

Test workloads	Site condition	VDA registration time	Registration CPU and memory usage	Launch test length	Session launch CPU and memory usage	Launch rate
1000 VDI	Outage	4 minutes	CPU maximum = 11%, CPU average = 10%, memory maximum = 4.5 GB	2 minutes	CPU maximum = 42%, CPU average = 28%, memory maximum = 4.0 GB	500 per minute
250 RDS, 5000 sessions	Online	3 minutes	CPU maximum = 14%, CPU average = 4%, memory maximum = 3.5 GB	9 minutes	CPU maximum = 46%, CPU average = 21%, memory maximum = 3.7 GB	555 per minute
250 RDS, 5000 sessions	Outage	3 minutes	CPU maximum = 15%, CPU average = 5%, memory maximum = 3.7	9 minutes	CPU maximum = 51%, CPU average = 32%, memory maximum = 4.2 GB	555 per minute

Large workloads

These workloads were tested with 4 vCPUs and 8 GB memory.

Test workloads	Site condition	VDA registration time	Registration CPU and memory usage	Launch test length	Session launch CPU and memory usage	Launch rate
5000 VDI	Online	3–4 minutes	CPU maximum = 45%, CPU average = 25%, memory maximum = 7.0 GB	5 minutes	CPU maximum = 75%, CPU average = 55%, memory maximum = 7.0 GB	1000 per minute
5000 VDI	Outage	4–6 minutes	CPU maximum = 15%, CPU average = 5%, memory maximum = 7.5 GB	5 minutes	CPU maximum = 45%, CPU average = 40%, memory maximum = 7.5 GB	1000 per minute
500 RDS, 10,000 sessions	Online	3 minutes	CPU maximum = 45%, CPU average = 25%, memory maximum = 7.0 GB	10 minutes	CPU maximum = 75%, CPU average = 55%, memory maximum = 7.0 GB	1000 per minute
500 RDS, 10,000 sessions	Outage	3 minutes	CPU maximum = 15%, CPU average = 5%, memory maximum = 7.5	10 minutes	CPU maximum = 45%, CPU average = 40%, memory maximum = 7.5 GB	1000 per minute

Maximum workloads

These workloads were tested with 8 vCPUs and 10 GB memory.

Test workloads	Site condition	VDA registration time	Registration CPU and memory usage	Launch test length	Session launch CPU and memory usage	Launch rate
10,000 VDI	Online	3–4 minutes	CPU maximum = 85%, CPU average = 10%, memory maximum = 8.5 GB	7 minutes	CPU maximum = 66%, CPU average = 28%, memory maximum = 7.0 GB	1400 per minute
10,000 VDI	Outage	4–5 minutes	CPU maximum = 90%, CPU average = 17%, memory maximum = 8.2 GB	5 minutes	CPU maximum = 90%, CPU average = 45%, memory maximum = 8.5 GB	2000 per minute
1000 RDS, 20,000 sessions	Online	1–2 minutes	CPU maximum = 60%, CPU average = 20%, memory maximum = 8.6 GB	17 minutes	CPU maximum = 66%, CPU average = 25%, memory maximum = 6.8 GB	1200 per minute

Test workloads	Site condition	VDA registration time	Registration CPU and memory usage	Launch test length	Session launch CPU and memory usage	Launch rate
1000 RDS, 20,000 sessions	Outage	3–4 minutes	CPU maximum = 22%, CPU average = 10%, memory maximum = 8.5	21 minutes	CPU maximum = 90%, CPU average = 50%, memory maximum = 7.5 GB	1000 per minute

> **Note:**
>
> The workloads shown here are the maximum recommended workloads for one resource location. To support larger workloads, add more resource locations.

Configuration synchronization resource usages

The configuration synchronization process keeps the Cloud Connectors up to date with Citrix DaaS. Updates are automatically sent to the Cloud Connectors to make sure that the Cloud Connectors are ready to take over brokering if an outage occurs. The configuration synchronization updates the LHC database, SQL Express Server LocalDB. The process imports the data to a temporary database then switches to that database once imported. This ensures that there is always an LHC database ready to take over.

CPU, memory, and disk usage are temporarily increased while data is imported to the temporary database.

Test results:

- **Data import time:** 7–10 minutes
- **CPU usage:**
  - maximum = 25%
  - average = 15%
- **Memory usage:**
  - maximum = 9 GB

  - increase of approximately 2 GB to 3 GB

- **Disk usage:**
  - 4 MB/s disk read spike
  - 18 MB/s disk write spike
  - 70 MB/s disk write spike during downloading and writing of xml config files
  - 4 MB/s disk read spike at the completion of import

- **LHC database size:**
  - 400–500 MB database file
  - 200–300 MB log database

Test conditions:

- Tested on an 8 vCPU AMD EPYC
- The imported site configuration database was for an environment with site-wide total of 80,000 VDAs and 300,000 users (three shifts of 100,000 users)
- Data import time was tested on a resource location with 10,000 VDI

Additional resource usage considerations:

- During import the full site configuration data is downloaded. This download might cause a memory spike, depending on the site size.
- The tested site used approximately 800 MB for the database and database log files combined. During a configuration synchronization, these files are duplicated with a maximum combined size of approximately 1600 MB. Ensure that your Cloud Connector has enough disk space for the duplicated files. The configuration synchronization process fails if the disk is full.

Install VDAs

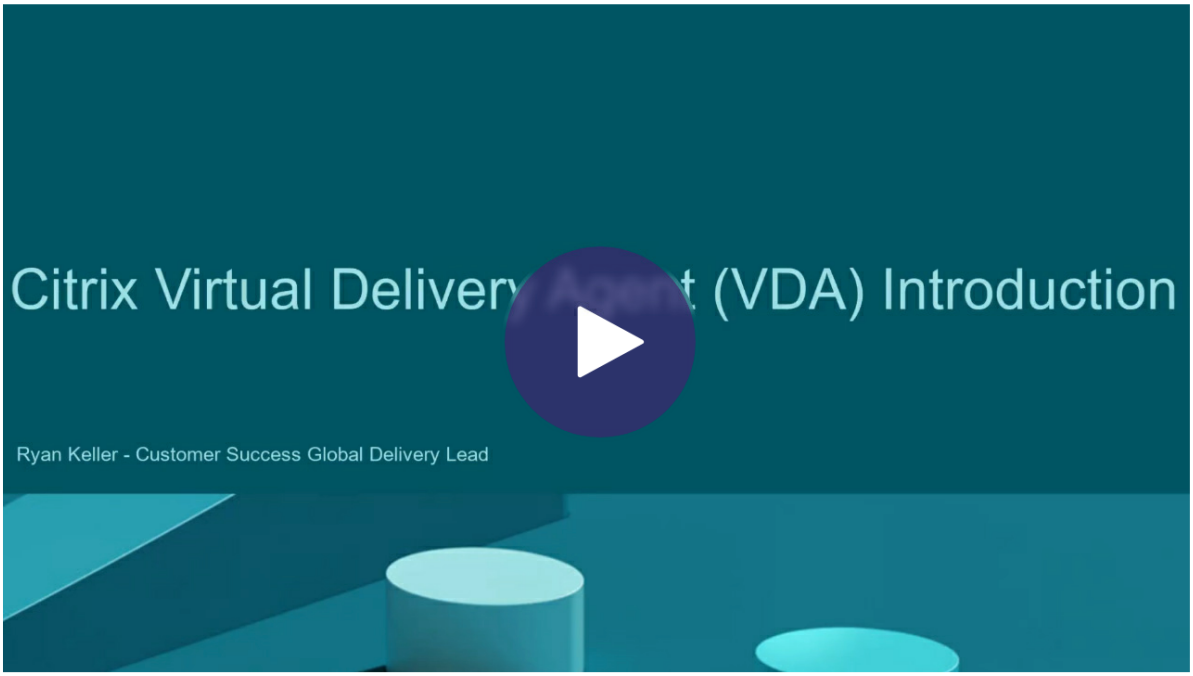
April 24, 2024

Introduction

This article begins with a description of Windows VDAs and the available VDA installers. The remainder of the article describes the steps in the VDA installation wizard. Command-line equivalents are provided. For details, see Install VDAs using the command line.

For information about Linux VDAs, see Linux Virtual Delivery Agent.

View an introduction to VDAs.



Installation considerations

The Citrix DaaS article describes what VDAs are and what they do. Here's more information.

- **Analytics collection:** Analytics are collected automatically when you install or upgrade components. By default, that data is uploaded to Citrix automatically when the installation completes. Also, when you install components, you are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP), which uploads anonymous data. Also, during an installation or upgrade, you're offered the opportunity to enroll in Call Home.

  If a VDA installation fails, an MSI analyzer parses the failing MSI log, displaying the exact error code. The analyzer suggests a CTX article, if it is a known issue. The analyzer also collects anonymized data about the failure error code. This data is included with other data collected by CEIP. If you end enrollment in CEIP, the collected MSI analyzer data is no longer sent to Citrix.

  For information about these programs, see Citrix Insight Services.

- **Citrix Workspace app:** Citrix Workspace app for Windows is not installed by default when you install a VDA. You can download and install or upgrade Citrix Workspace app for Windows and other Citrix Workspace apps from the Citrix website. Alternatively, you can make those Citrix Workspace apps available from the Workspace or a StoreFront server.

- **Print Spooler Service:** The Microsoft Print Spooler Service must be enabled. You cannot successfully install a VDA if that service is disabled.

- **Microsoft Media Foundation:** Most supported Windows editions come with Media Foundation already installed. If the machine on which you're installing a VDA does not have Microsoft Media Foundation (such as N editions), several multimedia features are not installed and do not work.

  - Flash Redirection
  - Windows Media Redirection
  - HTML5 Video Redirection
  - HDX RealTime Webcam Redirection

  You can acknowledge the limitation, or end the VDA installation and restart it later, after installing Media Foundation. In the graphical interface, this choice is presented in a message. In the command line, you can use the `/no_mediafoundation_ack` option to acknowledge the limitation.

- **Local user group:** When you install the VDA, a new local user group called Direct Access Users is created automatically. For a single-session OS VDA, this group applies only to RDP connections. For a multi-session OS VDA, this group applies to ICA and RDP connections.

- **Cloud Connector address requirement:** The VDA must have at least one valid Cloud Connector address (in the same resource location) with which to communicate. Otherwise, sessions cannot be established. You specify Cloud Connector addresses when you install the VDA. For information about other ways to specify Cloud Connector addresses where VDAs can register, see VDA registration.

- **Operating system considerations:**

  - Review the System requirements for supported platforms, operating systems, and versions.
  - Ensure that each operating system maintains the latest updates.
  - Ensure that VDAs have synchronized system clocks. The Kerberos infrastructure that secures communication between the machines requires synchronization.
  - Optimization guidance for Windows 10 machines is available in CTX216252.
  - If you try to install (or upgrade to) a Windows VDA on an OS that is not supported for that VDA version, a message describes your options. For example, if you try to install the latest VDA on an older Windows machine, a message guides you to CTX139030. For more information, see Earlier operating systems.

- **Installed MSIs:** Several MSIs are installed automatically when you install a VDA. You can prevent the installation of some MSIs on the **Additional Components** page of the graphical interface or with the `/exclude` option in the CLI. For others, the only way to prevent their installation is with the `/exclude` CLI option.

- **Domain-joined:** Ensure that the machine is domain-joined before installing the VDA software.

VDA supportability tools

Each VDA installer includes a supportability MSI that contains Citrix tools for checking the VDA's performance, such as its overall health and the quality of connections. Enable or disable installation of this MSI on the **Additional Components** page of the VDA installer's graphical interface. From the command line, disable installation with the `/exclude "Citrix Supportability Tools"` option.

By default, the supportability MSI is installed in `C:\Program Files (x86)\Citrix\Supportability Tools\`. You can change this location on the **Components** page of the VDA installer's graphical interface, or with the `/installdir` command-line option. Keep in mind that changing the location changes it for all installed VDA components, not just the supportability tools.

Current tools in the supportability MSI:

- Citrix Health Assistant: For details, see CTX207624.
- VDA Cleanup Utility: For details, see CTX209255.

If you do not install the tools when you install the VDA, the CTX article contains a link to the current download package.

Restarts during VDA installation

A restart is required at the end of the VDA installation. That restart occurs automatically by default.

To minimize the number of other restarts needed during VDA installation:

- Ensure that a supported Microsoft .NET Framework version is installed before beginning the VDA installation.
- For Windows multi-session OS machines, install and enable the RDS role services before installing the VDA.

If you do not install those prerequisites before installing the VDA:

- If you are using the graphical interface or the command line interface without the `/noreboot` option, the machine restarts automatically after installing the prerequisite.
- If you are using the command line interface with the `/noreboot` option, you must initiate the restart.

After each restart, the VDA installation continues. If you're installing from the command line, you can prevent the automatic resumption with the `/noresume` option.

When upgrading a VDA to version 7.17 or a later supported version, a restart occurs during the upgrade. This restart cannot be avoided.

Restore on install or upgrade failure

> **Note:**
>
> This feature is available only for single-session VDAs.

If a single-session VDA installation or upgrade fails, and the "restore on failure"feature is enabled, the machine is returned to a restore point that was set before the installation or upgrade began.

When a single-session VDA installation or upgrade starts with this feature enabled, the installer creates a system restore point before beginning the actual install or upgrade. If the VDA installation or upgrade fails, the machine is returned to the restore point state. The `%temp%/Citrix` folder contains deployment logs and other information about the restore.

By default, this feature is disabled.

If you plan to enable this feature, make sure that system restore is not disabled through a GPO setting (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

To enable this feature when installing or upgrading a single-session VDA:

- When using a VDA installer's graphical interface (such as using **Autostart** or the `XenDesktopVDASetup.exe` command without any restore or quiet options), select the **Enable automatic restore if update fails** check box on the **Summary** page.

  If the install/upgrade completes successfully, the restore point is not used, but is retained.

- Run a VDA installer with either the `/enablerestore` or `/enablerestorecleanup` option.

  - If you use the `/enablerestorecleanup` option, and the install/upgrade completes successfully, the restore point is removed automatically.
  - If you use the `/enablerestore` option, and the install/upgrade completes successfully, the restore point is not used, but is retained.

VDA installers

VDA installers can be downloaded directly from the Citrix Cloud console.

By default, files in the self-extracting installers are extracted to the `Temp` folder. The files extracted to the `Temp` folder are automatically deleted after the installation completes. Alternatively, you can use the `/extract` command with an absolute path.

Three standalone VDA installers are available for download.

VDAServerSetup.exe Installs a multi-session OS VDA.

VDAWorkstationSetup.exe Installs a single-session OS VDA.

VDAWorkstationCoreSetup.exe Installs a single-session OS VDA that is optimized for Remote PC Access deployments or core VDI installations. Remote PC Access uses physical machines. Core VDI installations are VMs that are not being used as an image. This installer deploys only the core services necessary for VDA connections. Therefore, it supports only a subset of the options that are valid with the VDAWorkstationSetup installer.

This installer for the current release does not install or contain the components used for:

- App-V.
- Profile Management. Excluding Citrix Profile Management from the installation affects Monitor displays.
- Machine Identity Service.
- Citrix Workspace app for Windows.
- Citrix Supportability Tools.
- Citrix Files for Windows.
- Citrix Files for Outlook.
- MCSIO write cache for storage optimization.

This installer does not install or contain a Citrix Workspace app for Windows.

This installer automatically installs the Browser Content Redirection MSI. Automatic installation applies to VDA release 2003 and later supported releases.

Using `VDAWorkstationCoreSetup.exe` is equivalent to using the `VDAWorkstationSetup.exe` installer to install a single-session OS VDA and either:

- In the graphical interface: Selecting the **Remote PC Access** option on the **Environment** page.
- In the command-line interface: Specifying the `/remotepc` option.
- In the command line interface: Specifying `/components vda` and `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"`.

If you install a VDA with the `VDAWorkstationCoreSetup.exe` installer and later upgrade that VDA using the`VDAWorkstationSetup.exe` installer, you can optionally install the omitted components and features.

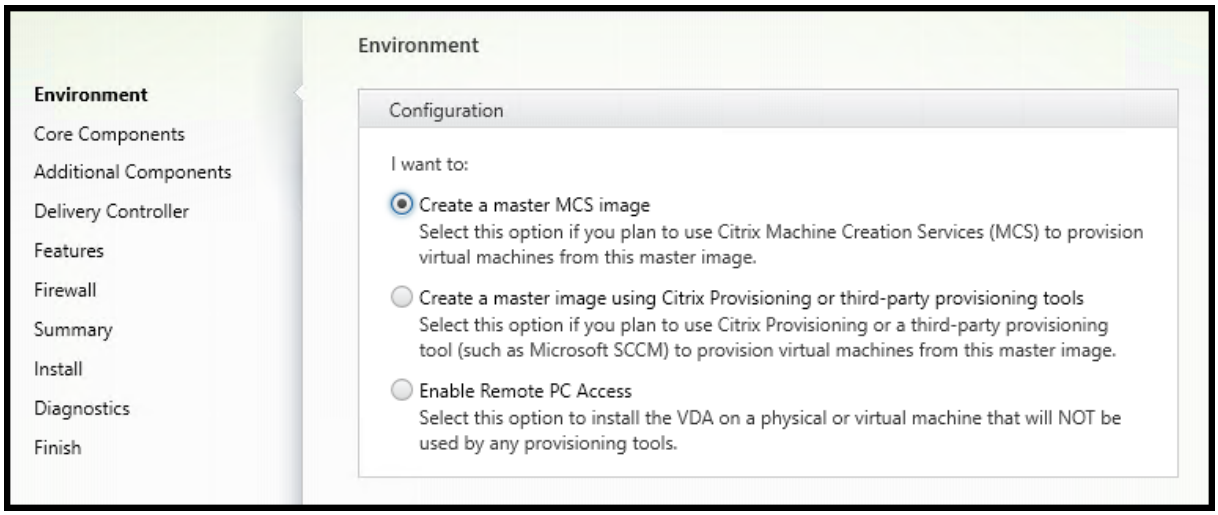
Step 1. Download the product software and launch the wizard

1. On the machine where you're installing the VDA, sign in to Citrix Cloud.
2. In the upper left menu, select the Citrix DaaS in the **My Services** list.

3. On the right side, click **Downloads** and select **Download VDA**. You are redirected to the VDA download page. Find the VDA installer you want and then select **Download File**.
4. After the download completes, right-click the file and select **Run as administrator**. The installation wizard launches.

As an alternative to steps 1-3, you can download the VDA directly from the Citrix download page.

Step 2. Specify how the VDA will be used



On the **Environment** page, specify how you plan to use the VDA, indicating whether you'll use this machine as an image to provision machines. The option you choose affects which Citrix provisioning tools are installed automatically (if any), and the default values on the **Additional Components** page of the VDA installer.

Choose one of the following:

- **Create a master MCS image:** Select this option to install a VDA on a VM image, if you plan to use Machine Creation Services to provision VMs. This option installs the Machine Identity Service. This is the default option.

  Command-line option: `/mastermcsimage` or `/masterimage`

- **Create a master image using Citrix Provisioning or third-party provisioning tools:** Select this option to install a VDA on a VM image, if you plan to use Citrix Provisioning or third-party provisioning tools (such as Microsoft System Center Configuration Manager). Use this option for previously provisioned VMs that were booted from a Citrix Provisioning read/write disk.

  Command-line option: `/masterpvsimage`

- (Appears only on multi-session OS machines) **Enable brokered connections to a server:** Select this option to install a VDA on a physical or virtual machine that will not be used as an image.

Command-line option: `/remotepc`

- (Appears only on multi-session OS machines) **Enable Remote PC Access:** Select this option to install a VDA on a physical machine for use with Remote PC Access.

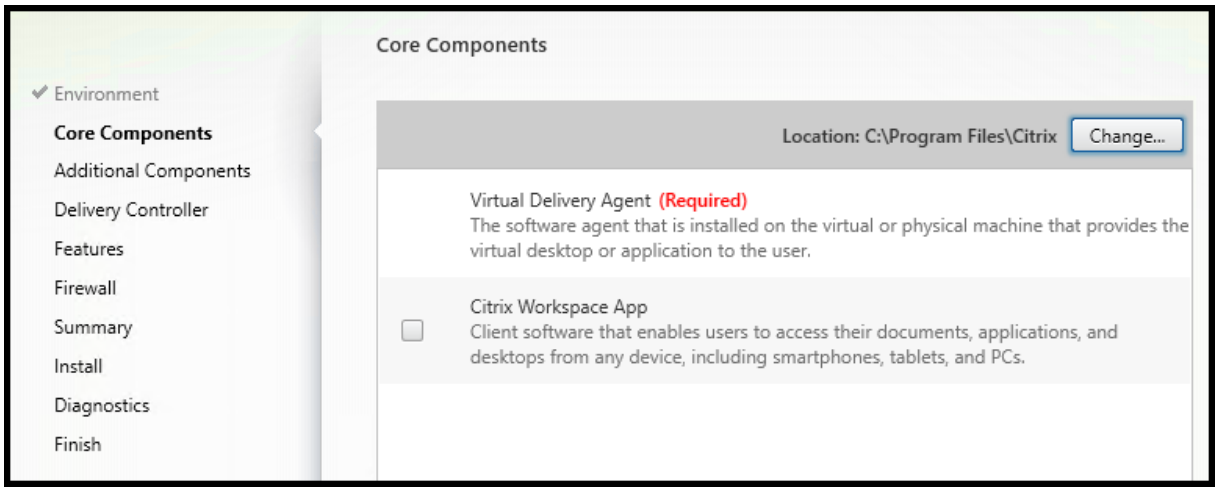
  Command-line option: `/remotepc`

Select **Next**.

This page does not appear:

- When upgrading a VDA.
- When using the `VDAWorkstationCoreSetup.exe` installer.

Step 3. Select the components to install and the installation location



On the **Core components** page:

- **Location:** By default, components are installed in `C:\Program Files\Citrix`. This default is fine for most deployments. If you specify a different location, that location must have execute permissions for the network service.

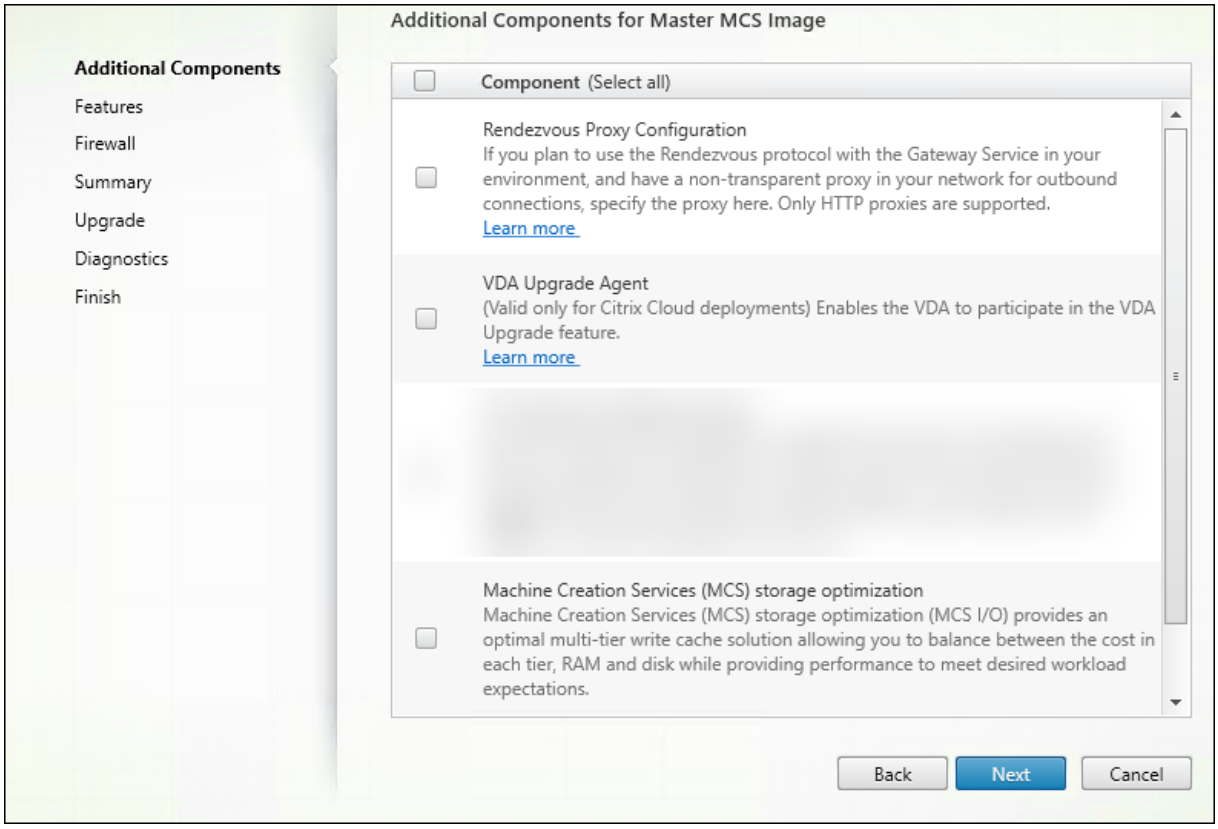
  Command-line option: `/installdir`

- **Components:** By default, Citrix Workspace app for Windows is not installed with the VDA. If you are using the `VDAWorkstationCoreSetup.exe` installer, Citrix Workspace app for Windows is never installed, so this check box is not displayed.

  Command-line option: `/components vda,plugin` to install the VDA and the Citrix Workspace app for Windows

Select **Next**.

Step 4. Install additional components



The **Additional Components** page contains check boxes to enable or disable installation of other features and technologies with the VDA. In a command-line installation, you can use the `/exclude` or `/includeadditional` option to omit or include one or more available components.

The following table indicates the default setting of items on this page. The default setting depends on the option you selected on the **Environment** page.

Additional Components page	Environment page: "Master image with MCS"or "Master image with Citrix Provisioning …"selected	Environment page: "Enable brokered connections to server"(for multi-session OS) or "Remote PC Access"(for single-session OS) selected
Citrix Personalization for App-V	Not selected	Not selected
User Personalization Layer	Not selected	Not shown because it's not valid for this use case
Citrix Supportability tools	Selected	Not selected
Citrix Profile Management	Selected	Not selected

Additional Components page	Environment page: “Master image with MCS”or “Master image with Citrix Provisioning …”selected	Environment page: “Enable brokered connections to server”(for multi-session OS) or “Remote PC Access”(for single-session OS) selected
Citrix Profile Management WMI Plug-in	Selected	Not selected
Citrix VDA Upgrade Agent	Not selected	Not selected
Citrix Backup and Restore	Not selected	Not selected
Citrix Files for Windows	Not selected	Not selected
Citrix Files for Outlook	Not selected	Not selected
Machine Creation Services (MCS) storage optimization	Not selected	Not selected
Rendezvous protocol configuration	Not selected	Not selected

This page does not appear when:

- Using the `VDAWorkstationCoreSetup.exe` installer. Also, the command-line options for the additional components are not valid with that installer.
- Upgrading a VDA and all the additional components are already installed. If some of the additional components are already installed, the page lists only the components that are not installed.

The components list can include:

- **Citrix Personalization for App-V:** Install this component if you use applications from Microsoft App-V packages. For details, see App-V.

  Command-line option: `/includeadditional "Citrix Personalization for App-V – VDA"` to enable component installation, `/exclude "Citrix Personalization for App-V – VDA"` to prevent component installation

- **Citrix User Personalization Layer:** Installs the MSI for the user personalization layer. For details, see User personalization layer.

  This component appears only when installing a VDA on a single-session Windows 10 machine.

  Command-line option: `/includeadditional "User Personalization Layer"` to enable component installation, `/exclude "User Personalization Layer"` to prevent component installation

- **Citrix Supportability Tools:** Installs the MSI that contains Citrix supportability tools.

  Command-line option: `/includeadditional "Citrix Supportability Tools"` to enable component installation, `/exclude "Citrix Supportability Tools"` to prevent component installation

- **Citrix Profile Management:** This component manages user personalization settings in user profiles. For details, see Profile Management.

  Excluding Citrix Profile Management from the installation affects the monitoring and troubleshooting of VDAs in Citrix Cloud.

  - On the **User details** and **EndPoint** pages of the **Monitor** tab, the **Personalization** panel and the **Logon Duration** panel fail.
  - On the **Dashboard** and **Trends** pages, the **Average Logon Duration** panel display data only for machines that have Profile Management installed.

  Even if you are using a third-party user profile management solution, Citrix recommends that you install and run the Citrix Profile Management Service. Enabling the Citrix Profile Management Service is not required.

  Command-line option: `/includeadditional "Citrix Profile Management"` to enable component installation, `/exclude "Citrix Profile Management"` to prevent component installation

- **Citrix Profile Management WMI Plug-in:** This plug-in provides Profile Management runtime information in WMI (Windows Management Instrumentation) objects (for example, profile provider, profile type, size, and disk usage). WMI objects provide session information to Director.

  Command-line option: `/includeadditional "Citrix Profile Management WMI Plugin"` to enable component installation, `/exclude "Citrix Profile Management WMI Plugin"` to prevent component installation

- **VDA Upgrade Agent:** (Applicable only to Citrix DaaS deployments.) Enables the VDA to participate in the VDA Upgrade feature. You can use that feature to upgrade a catalog's VDAs from the management console, immediately or at a scheduled time. If this agent is not installed, you can upgrade a VDA by running the VDA installer on the machine.

  Command-line options: `/includeadditional "Citrix VDA Upgrade Agent"` to enable component installation, `/exclude "Citrix VDA Upgrade Agent"` to prevent component installation

- **Citrix Files for Windows:** This component enables users to connect to their Citrix Files account. They can then interact with Citrix Files through a mapped drive in the Windows file system, without requiring a full sync of their content.

Command-line options: `/includeadditional "Citrix Files for Windows"` to enable component installation, `/exclude "Citrix Files for Windows"` to prevent component installation

- **Citrix Files for Outlook:** This component allows you to bypass file size restrictions and add security to your attachments or emails by sending them through Citrix Files. You can provide a secure file upload request directly in your email. For more information, see Citrix Files for Outlook.

  Command-line options: `/includeadditional "Citrix Files for Outlook"` to enable component installation, `/exclude "Citrix Files for Outlook"` to prevent component installation

- **Machine Creation Services (MCS) storage optimization:** Installs the Citrix MCS IO driver. For more information, see Storage shared by hypervisors and Configure cache for temporary data.

  Command-line options: `/includeadditional "Citrix MCS IODriver"` to enable component installation, `/exclude "Citrix MCS IODriver"` to prevent component installation

- **Proxy Configuration:** Install this component if you plan to use the Rendezvous protocol with the Citrix Gateway Service in your environment, and you have a non-transparent proxy in your network for outbound connections. Only HTTP proxies are supported.

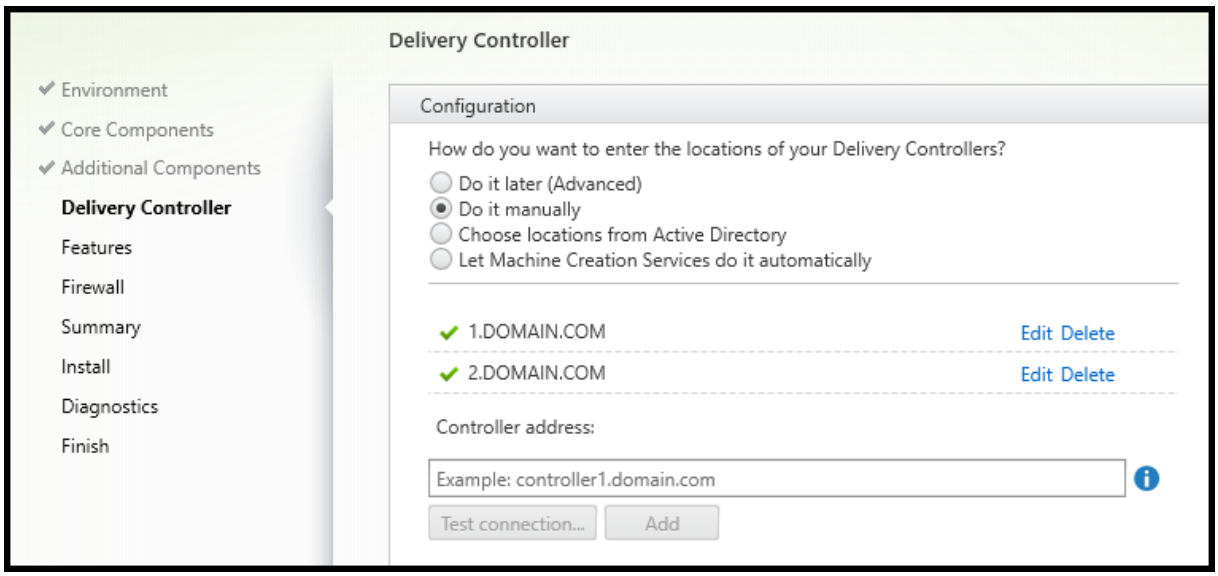
  If you install this coponent, specify the address of the proxy or PAC file path on the **Rendezvous Proxy Configuration** page. For feature details, see Rendezvous protocol.

  Command-line option: `/includeadditional "Citrix Rendezvous V2"` to enable component installation, `/exclude "Citrix Rendezvous V2"` to prevent component installation

- **Citrix Backup and Restore:** If a VDA installation or upgrade fails, then this component can return the machine to a backup that was done before the installation or upgrade.

  Command-line option: `/includeadditional "Citrix Backup and Restore"` to enable component installation, `/exclude "Citrix Backup and Restore"` to prevent component installation.

Step 5. Cloud Connector addresses



On the **Delivery Controller** page, select **Do it manually.** Enter the DNS name of an installed Cloud Connector and then select **Add**. If you've installed additional Cloud Connectors in the resource location, add their DNS names.

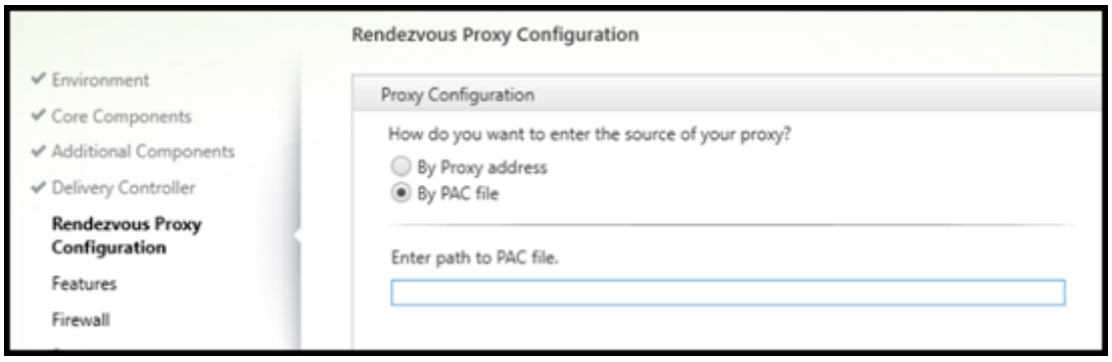
Select **Next**.

Considerations:

- The address can contain only alphanumeric characters.
- Successful VDA registration requires that the firewall ports used to communicate with the Cloud Connector are open. That action is enabled by default on the **Firewall** page of the wizard.

Command-line option: `/controllers`

Step 6. Proxy Configuration



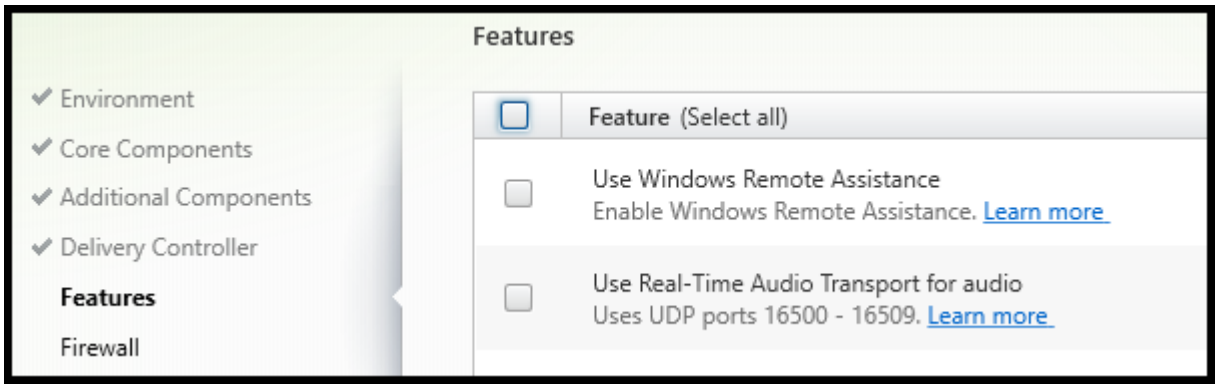
The **Rendezvous Proxy Configuration** page appears only if you enabled the **Rendezvous Proxy Configuration** check box on the **Additional Components** page.

1. Select whether you will specify the proxy source by proxy address or PAC file path.
2. Specify the proxy address or PAC file path.
   - Proxy address format: `http://<url-or-ip>:<port>`
   - PAC file format: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

The firewall for the proxy port must be open for the connection test to succeed. If a connection cannot be made to the proxy, you can choose whether to continue with the VDA installation.

Command-line option: `/proxyconfig`

Step 7. Enable or disable features



On the **Features** page, use the check boxes to enable or disable features you want to use.

- **Use Windows Remote Assistance:** When this feature is enabled, Windows Remote Assistance is used with the user shadowing feature of the Director component in Citrix Cloud. Windows Remote Assistance opens the dynamic ports in the firewall. (Default = disabled)

  Command-line option: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio:** Enable this feature if voice-over-IP is widely used in your network. The feature reduces latency and improves audio resilience over lossy networks. It allows audio data to be transmitted using RTP over UDP transport. (Default = disabled)

  Command-line option: `/enable_real_time_transport`

- **Use screen sharing:** When enabled, ports used by screen sharing are opened in the Windows firewall. (Default = disabled)

  Command-line option: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud:** This setting helps Citrix to correctly identify resource locations for on-premises and service (Citrix Cloud) VDA deployments for telemetry purposes. This feature has no impact on customer side utilization. Enable this setting if your deployment uses Citrix DaaS. (Default = disabled)

Command-line option: `/xendesktopcloud`

Select **Next**.

If this page contains a feature named **MCS I/O**, do not use it. The MCS IO feature is configured on the **Additional Components** page.

Step 8. Firewall ports

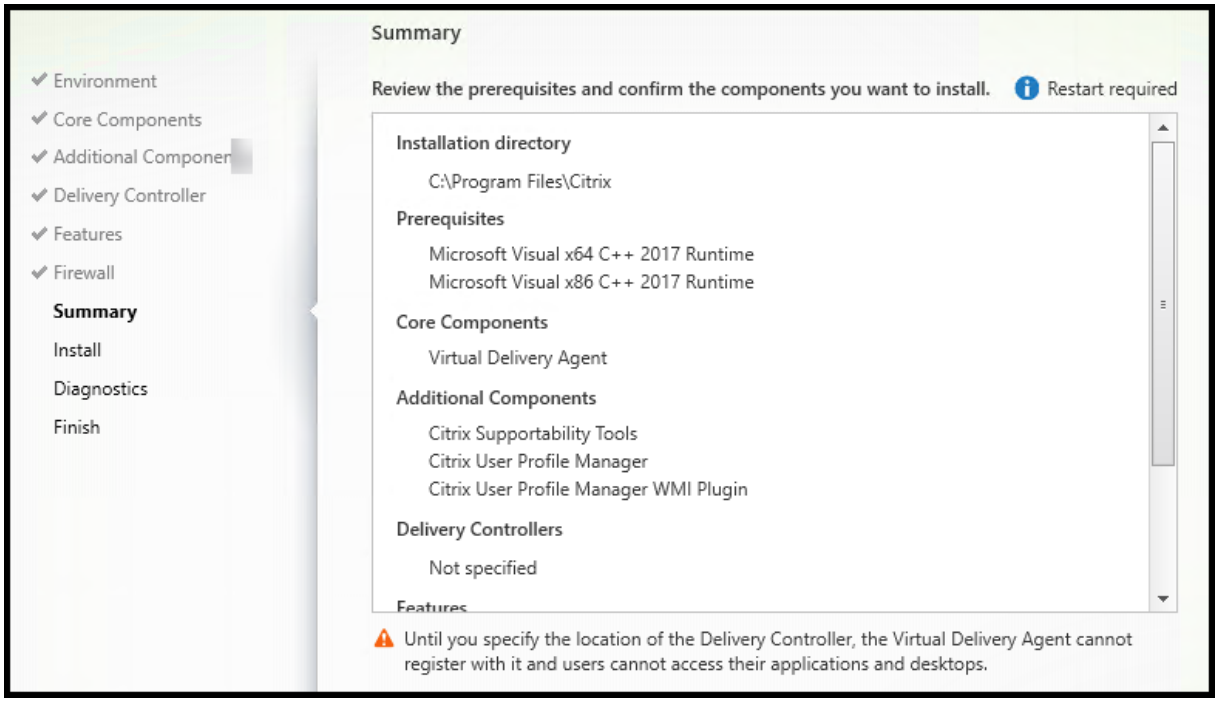
The **Firewall** page indicates which ports the VDA and Cloud Connectors use to communicate with each other. By default, these ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. This default setting is fine for most deployments.

For port information, see Network ports.

Select **Next**.

Command-line option: `/enable_hdx_ports`

Step 9. Review prerequisites and confirm installation

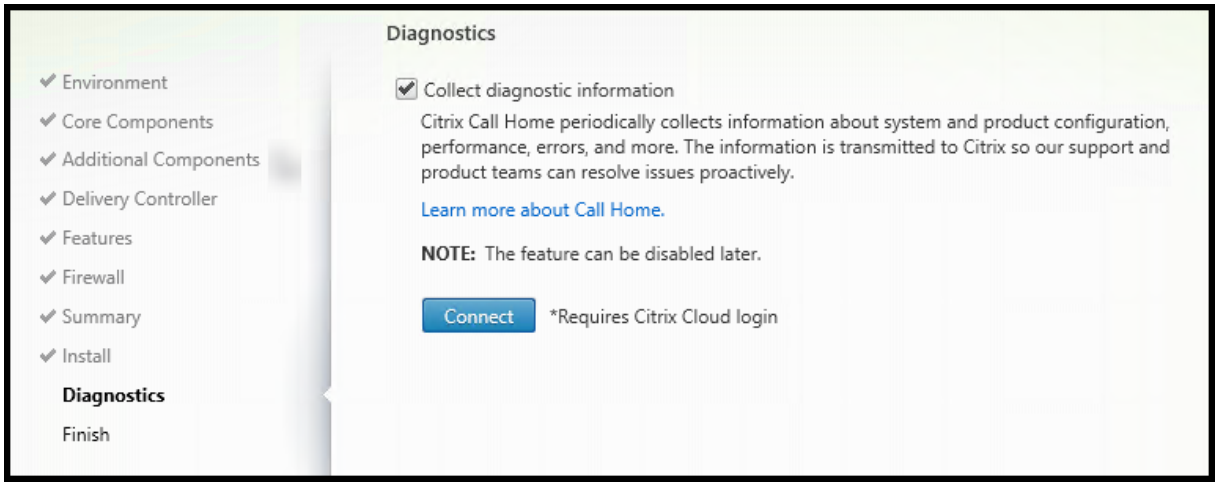


The **Summary** page lists what will be installed. You can return to earlier wizard pages and change selections, if needed.

(Single-session VDAs only) Select the **Enable automatic restore if update fails** check box to enable the restore on failure feature. For details, see Restore on install or upgrade failure.

When you're ready, select **Install**.

Step 10. Diagnose

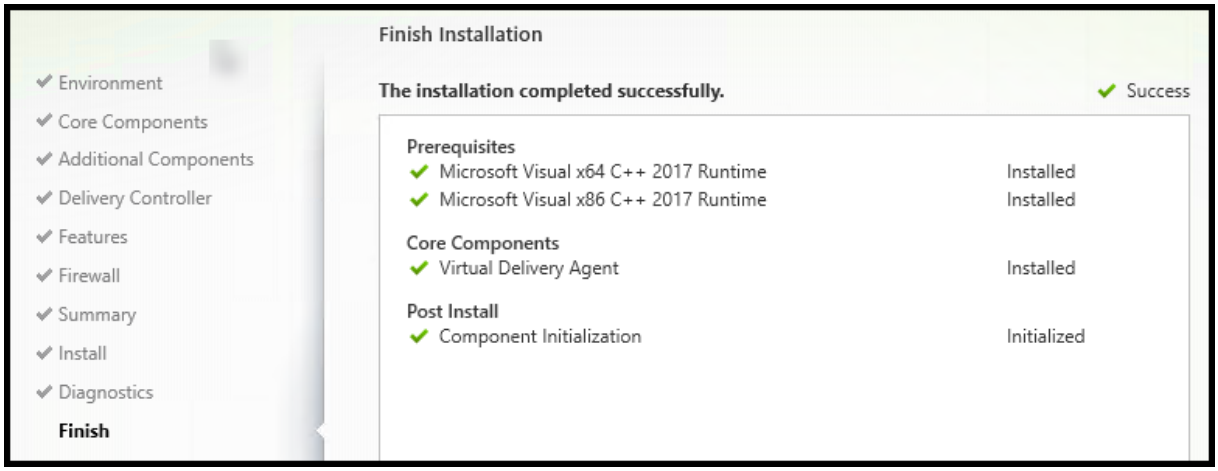


On the **Diagnostics** page, choose whether to participate in Citrix Call Home. If you choose to participate (the default), select **Connect**. When prompted, enter your Citrix account credentials.

After your credentials are validated (or if you choose not to participate), select **Next**.

For more information, see Call Home.

Step 11. Complete this installation



The **Finish** page contains green check marks for all prerequisites and components that installed and initialized successfully.

Select **Finish**. By default, the machine restarts automatically. Although you can disable this automatic restart, the VDA cannot be used until the machine restarts.

If you are installing a VDA on individual machines (rather than an image), repeat the steps above to install a VDA on other machines, as needed.

Troubleshoot

In the **Manage > Full Configuration** display for a delivery group, the **Installed VDA version** entry in the details pane might not be the version installed on the machines. The machine's Windows Programs and Features display shows the actual VDA version.

Citrix Optimizer

Citrix Optimizer is a tool for Windows OS that helps Citrix administrators optimize VDAs by removing and optimizing various components.

After installing a VDA and completing the final restart, download and install Citrix Optimizer. See CTX224676. The CTX article contains the download package, plus instructions about installing and using Citrix Optimizer.

Customize a VDA

Later, to customize (change information for) an installed VDA:

1. From the Windows feature for removing or changing programs, select **Citrix Virtual Delivery Agent** or **Citrix Remote PC Access/VDI Core Services VDA**. Then right-click and select **Change**.
2. Select **Customize Virtual Delivery Agent Settings**.

When the installer launches, change any available settings.

Customize the port for communicating with Cloud Connectors

You can customize the port that VDAs use to communicate with Cloud Connectors based on your specific security requirements. This feature is useful if your security team doesn't allow the default port (port 80) to be open or if the default port is already in use.

To customize the port, complete the following steps:

1. Add the Controller port number on Citrix Cloud Connectors.
2. Add the VDA port number on VDAs.

Add the Controller port number on Citrix Cloud Connectors

Go to the Citrix Cloud Connector and run the following two PowerShell commands:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

Example:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

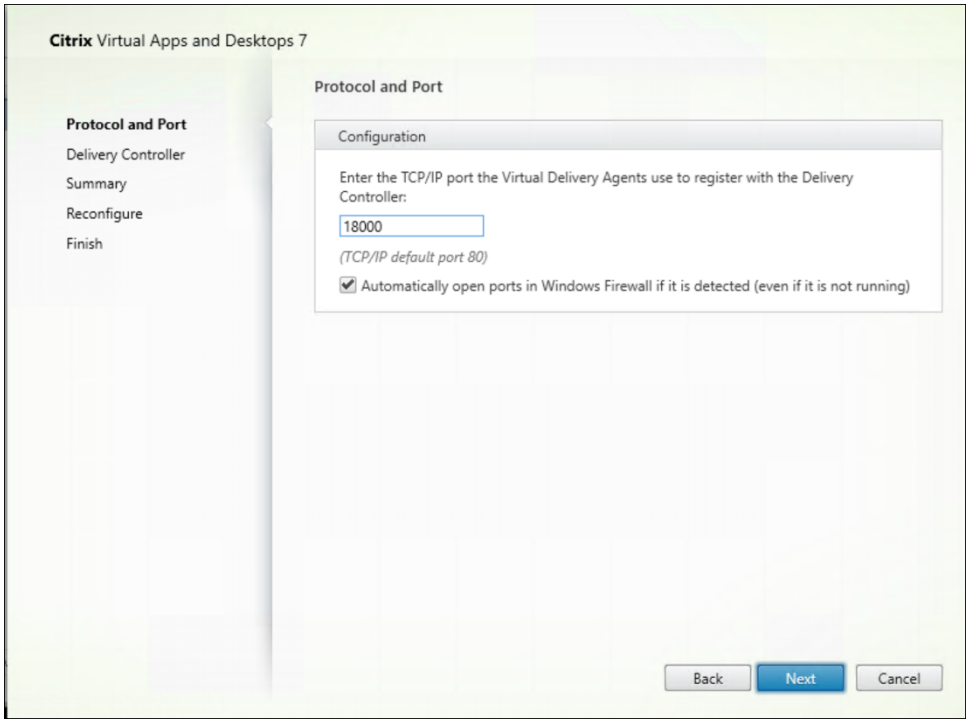
When customizing the port, consider the following:

- You must use the same port number in both commands.
- You must run both commands *on all Cloud Connectors*.
- To successfully communicate with Cloud Connectors, ensure that all VDAs use the same port number.
- The port you configure persists across connector updates.

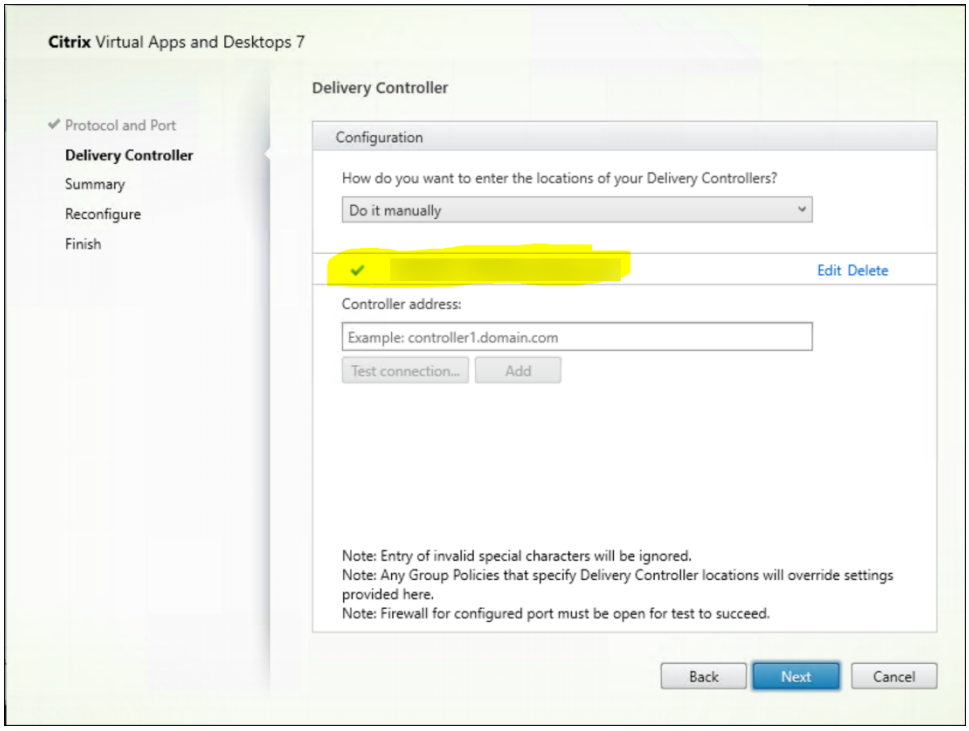
Add the VDA port number on VDAs

Install the VDA with default settings and configure as follows. If the VDA is already installed, continue with the steps below.

1. On the VDA, open **XenDesktopVdaSetup.exe**, which is located at `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe`.
2. On the **Protocol and Port** page, add the custom port number.



3. On the **Delivery Controller** page, enter the FQDN of the Controller.



4. Click **Next** to proceed through the wizard to complete the configuration.

The port numbers are then reconfigured successfully.

> **Note:**
>
> You might see the following error message when you test a Controller connection: No running instance of a Controller found on < the Controller address you entered >. If the address is correct, you can dismiss the message.

Troubleshooting

To check whether the custom ports are configured correctly, go to the Cloud Connector and perform the following troubleshooting steps:

1. Verify that the following two registry keys exist.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Name: CustomVDAPortNumber
   Type: REG_DWORD
   Data: 18000

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Name: CustomVDAPortNumberHA
   Type: REG_DWORD
   Data: 18000

2. Run the following command to create a .txt file.

   - `netsh http show urlacl > <filepath>.txt`

   Example:

   - `netsh http show urlacl > c:\reservations.txt`

3. Open the .txt file and check the following four URLs to verify that the correct port is used.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Verify that the following two firewall rules are created and required ports are open.

   - Citrix XaXdProxy
   - Citrix Broker Service (TCP-In)

Other information

- After you install a VDA, you can check the health and availability of the site and its components with a Cloud Health check.

Where to go next

Create machine catalogs.

To review the entire configuration process, see Plan and build a deployment.

Install VDAs using the command line

March 1, 2023

Introduction

This article applies to installing, upgrading, and customizing Virtual Delivery Agents (VDAs) on machines with Windows operating systems.

This article describes how to issue VDA installation commands. Before beginning an installation, review Install VDAs to learn about installation considerations, installers, and what you specify during installation.

Install a VDA from the command line

To install a VDA (and see command execution progress and return values), you must have elevated administrative permissions or use **Run as administrator**.

1. On the machine where you're installing the VDA, sign to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. On the upper right side, click **Downloads** and select **Download VDA**. You're redirected to the VDA download page. Find the VDA installer that you want and click **Download File**.
4. After the download completes, run its name. Use the options described in this article.
    - For the multi-session OS Virtual Delivery Agent, run `VDAServerSetup.exe`
    - For the single-session OS Virtual Delivery Agent, run `VDAWorkstationSetup.exe`
    - For the single-session OS Core Services Virtual Delivery Agent, run `VDAWorkstationCoreSetup.exe`

To extract the files before installing them, use `/extract` with the absolute path, for example `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. (The directory must exist. Otherwise, the extract fails.) Then in a separate command, run the appropriate command, using the valid options listed in this article.

- For `VDAServerSetup_XXXX.exe`, run `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- For `VDAWorkstationCoreSetup_XXXX.exe`, run `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- For `VDAWorkstationSetup_XXXX.exe`, run `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Command-line options to install a VDA

The following options are valid with one or more of the commands: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, and `VDAWorkstationCoreSetup.exe`.

- **/components** *component*[,*component*]

  Comma-separated list of components to install or remove. Valid values are:

  - **VDA:** Virtual Delivery Agent
  - **PLUGINS:** Citrix Workspace app for Windows

To install the VDA and Citrix Workspace app, specify `/components vda,plugins`.

If the `plugins` option is left out, only the VDA is installed (not the Citrix Workspace app).

This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer cannot install Citrix Workspace app.

- **/controllers** "*controller* [*controller*]…"

  Space-separated FQDNs of Citrix Cloud Connectors with which the VDA can communicate, enclosed in straight quotation marks. Do not specify both the `/site_guid` and `/controllers` options.

- **/disableexperiencemetrics**

  Prevents the automatic upload of analytics collected during installation, upgrade, or removal to Citrix.

- **/enable_hdx_ports**

  Opens ports in the Windows firewall required by the VDA and enabled features (except Windows Remote Assistance), if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually. For port information, see Network ports.

  To open the UDP ports that HDX adaptive transport, specify the `/enable_hdx_udp_ports` option, in addition to the `/enable_hdx_ports` option.

- **/enable_hdx_udp_ports**

  Opens UDP ports in the Windows firewall that HDX adaptive transport requires, if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually. For port information, see Network ports.

  To open the ports that the VDA uses, specify the `/enable_hdx_ports` option, in addition to the `/enable_hdx_udp_ports` option.

- **/enable_real_time_transport**

  Enables or disables use of UDP for audio packets (RealTime Audio Transport for audio). Enabling this feature can improve audio performance. Include the `/enable_hdx_ports` option if you want the UDP ports opened automatically when the Windows Firewall Service is detected.

- **/enable_remote_assistance**

  Enables the shadowing feature in Windows Remote Assistance for use with the **Monitor** functions. If you specify this option, Windows Remote Assistance opens the dynamic ports in the firewall.

- **/enablerestore** or **/enablerestorecleanup**

  (Valid only for single-session VDAs) Enables automatic return to the restore point, if the VDA install or upgrade fails.

  If the install/upgrade completes successfully:

  - `/enablerestorecleanup` instructs the installer to remove the restore point.
  - `/enablerestore` instructs the installer to keep the restore point, even though it was not used.

  For details, see Restore on install or upgrade failure.

- **/enable_ss_ports**

  Opens ports in the Windows Firewall that are required for screen sharing, if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.

- **/exclude** "*component*"[,"*component*"]

  Prevents installation of one or more comma-separated optional components, each enclosed in straight quotation marks. For example, installing or upgrading a VDA on an MCS-managed image needs the Machine Identity Service component. Valid values are:

  - Machine Identity Service
  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2

  Excluding Citrix Profile Management from the installation (`/exclude "Citrix Profile Management"`) affects monitoring and troubleshooting of VDAs from the **Monitor** tab. On the **User details** and **EndPoint** pages, the Personalization panel and the Logon Duration panel fail. On the **Dashboard** and **Trends** pages, the Average Logon Duration panel display data only for machines that have Profile Management installed.

  Even if you are using a third-party Profile Management solution, Citrix recommends that you install and run the Citrix Profile Management Service. Enabling the Citrix Profile Management Service is not required.

  If you plan to use MCS to provision VMs, do not exclude the Machine Identity Service.

  If you specify both `/exclude` and `/includeadditional` with the same component name, the component isn't installed.

This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer automatically excludes many of these items.

- **/h** or **/help**

  Displays command help.

- **/includeadditional** "*component*"[,"*component*"] ...

  Includes installation of one or more comma-separated optional components, each enclosed in straight quotation marks. The component names are case-sensitive.

  This option can be helpful when you are creating a Remote PC Access deployment, and want to install components that are not included by default. Valid values are:

  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2
  - User personalization layer
  - Citrix Web Socket VDA Registration Tool

  If you specify both `/exclude` and `/includeadditional` with the same component name, that component isn't installed.

- **/installdir** *directory*

  Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.

- **/install_mcsio_driver**

  Do not use. Instead, use `/includeadditional "Citrix MCS IODriver"` or `/exclude "Citrix MCS IODriver"`

- **/logpath** *path*

  Log file location. The specified folder must exist. The installer does not create it. Default = "%TEMP%\Citrix\XenDesktop Installer"

  This option isn't available in the graphical interface.

- **/masterimage**

  Valid only when installing a VDA on a VM. Sets up the VDA as an image. This option is equivalent to `/mastermcsimage`.

  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer.

- **/mastermcsimage**

  Specifies that this machine will be used as an image with Machine Creation Services. This option is equivalent to `/masterimage`.

- **/masterpvsimage**

  Specifies that this machine will be used as an image with either Citrix Provisioning or a third-party provisioning tool (such as Microsoft System Center Configuration Manager).

- **/no_mediafoundation_ack**

  Acknowledges that Microsoft Media Foundation is not installed, and several HDX multimedia features are not installed and do not work. If this option is omitted and Media Foundation is not installed, the VDA installation fails. Most supported Windows editions come with Media Foundation already installed, except N editions.

- **/nodesktopexperience**

  Valid only when installing a multi-session OS VDA. Prevents enabling of the Enhanced Desktop Experience feature. This feature is also controlled with the Enhanced Desktop Experience Citrix policy setting.

- **/noreboot**

  Prevents a restart after installation. The VDA cannot be used until after a restart.

- **/noresume**

  By default, when a machine restart is needed during an installation, the installer resumes automatically after the restart completes. To override the default, specify `/noresume`. This can be helpful if you must remount the media or want to capture information during an automated installation.

- **/portnumber** *port*

  Valid only when the `/reconfig` option is specified. Port number to enable for communications between the VDA and the Controller. The previously configured port is disabled, unless it is port 80.

- **/proxyconfig** "*address or PAC file path*"

  Valid only if command contains `/includeadditional "Citrix Rendezvous V2"`. The address or PAC file path of the proxy for use with the Rendezvous protocol. For feature details, see Rendezvous protocol.

  - Proxy address format: `http://<url-or-ip>:<port>`
  - PAC file format: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** or **/passive**

No user interface appears during the installation. The only evidence of the installation and configuration process is in Windows Task Manager. If this option is omitted, the graphical interface launches.

- **/reconfigure**

  Customizes previously configured VDA settings when used with the /portnumber, /controllers, or /enable_hdx_ports options. If you specify this option without also specifying the /quiet option, the graphical interface for customizing the VDA launches.

- **/remotepc**

  Valid only for Remote PC Access deployments (single-session OS) or brokered connections (multi-session OS).

  This option is not valid when using the VDAWorkstationCoreSetup.exe installer. That installer automatically excludes installation of these components.

- **/remove_appdisk_ack**

  Authorizes the VDA installer to uninstall the AppDisks VDA plug-in if it's installed.

- **/remove_pvd_ack**

  Authorizes the VDA installer to uninstall Personal vDisk if it's installed.

- **/remove**

  Removes the components specified with the /components option.

- **/removeall**

  Removes the VDA. It does not remove the Citrix Workspace app (if installed).

- **/sendexperiencemetrics**

  Automatically sends analytics collected during the installation, upgrade, or removal to Citrix. If this option is omitted (or the /disableexperiencemetrics option is specified), analytics are collected locally, but not sent automatically.

- **/servervdi**

  Installs a single-session OS VDA on a supported Windows server. Omit this option when installing a multi-session VDA on a Windows server. Before using this option, see Server VDI.

- **/site_guid** *guid*

  Globally Unique Identifier of the site Active Directory Organizational Unit (OU). This associates a virtual desktop with a site when you are using Active Directory for discovery (auto-update is the recommended and default discovery method). The site GUID is a site property displayed in **Manage > Full Configuration**. Do not specify both the /site_guid and /controllers options.

- **/tempdir** *directory*

  Directory to hold temporary files during installation. Default = c:\Windows\Temp.

  This option is not available in the graphical interface.

- **/virtualmachine**

  Valid only when installing a VDA on a VM. Overrides detection by the installer of a physical machine, where BIOS information passed to VMs makes them appear as physical machines.

  This option is not available in the graphical interface.

- **/xendesktopcloud**

  Indicates that the VDA is installed in a Citrix DaaS (Citrix Cloud) deployment.

Examples: Install a VDA

- **Install a VDA on a multi-session OS.** The following command installs a VDA on a multi-session OS.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  The VDA will be used as an image.

- **Install a multi-session OS VDA or single-session OS VDA.** The following command installs a multi-session OS VDA or a single-session OS VDA.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com",
  "ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /
  enable_real_time_transport /enable_ss_ports /noreboot
  ```

  Separate each delivery controller FQDN by a comma. Note that `XXXX` represents the VDA version.

- **Install a Core Services VDA on a single-session OS.** The following command installs a Core Services VDA on a single session OS for use in a Remote PC Access or VDA deployment.

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
  domain.com"/enable_hdx_ports /noreboot
  ```

  Citrix Workspace app and other non-core services are not installed. The address of a Cloud Connector is specified, and ports in the Windows Firewall Service are automatically opened. The administrator handles restarts.

Customize a VDA using the command line

After you install a VDA, you can customize several settings. Run `XenDesktopVDASetup.exe`, using one or more of the following options.

- `/reconfigure` (required when customizing a VDA)
- `/h` or `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Where to go next

- Create machine catalogs
- To review the entire configuration process, see Plan and build a deployment.

Create and manage connections and resources

February 15, 2024

Introduction

Configuring a connection involves selecting the connection type from the list of supported hypervisors and cloud services, and choosing the appropriate storage and network resources for that connection.

> **Note:**
>
> You must have Full Administrator privileges to perform tasks related to connection and resource management.

Where to find information about connection types

System requirements provide a list of supported hypervisors and cloud service versions, along with links to articles for each specific host.

Host storage

A storage product is supported if it is manageable through a supported hypervisor. Citrix Support assists only those storage product vendors in troubleshooting and resolving issues, and documenting these issues and solutions in the Knowledge Center as necessary.

When provisioning machines, data is classified by type:

- Operating system (OS): includes images
- Temporary data: include all non-persistent data written to MCS-provisioned machines, Windows page files, and any data that is synchronized with ShareFile. This data is discarded each time a machine restarts. If the base image includes user profile data, this data remain persistent. If a centralized user profile solution is in use, the user profile data is synchronized with the external profile store. The locally cached user profile data is discarded upon each machine restart.

Allocating distinct storage resources for different types of data can minimize system load and enhance IOPS (Input/Output Operations Per Second) performance on each storage device. This strategic allocation makes optimal use of the host's available resources. Also, it allows for the selection of the most suitable storage medium based on the specific needs of each data type, such as greater persistence or resilience for certain kinds of data.

- Shared and local storage options: Storage resources can either be centralized that is, separate from any host and used by all hosts, or localized to a specific hypervisor. Centralized options include Windows cluster shared volumes, which might or might not have additional attached storage, or appliances from storage vendors. Centralized storage solutions might offer advanced features for optimizations, for example, hypervisor-specific storage control paths, and direct plug-in access.
- Local storage benefits and trade-offs: Storing temporary data locally avoids going to the network to access shared storage, thereby reduces IOPS load on the shared resources. While centralized storage can be more expensive, using local storage can be a cost-effective alternative. However, these benefits can be weighed against the availability of sufficient storage on the hypervisor servers.

Storage shared by hypervisors

The storage shared by hypervisors method stores data that needs longer-term persistence centrally, providing centralized backup, and management. That storage holds the OS disks.

When you select this method, you can choose whether to use local storage (on servers in the same hypervisor pool) for temporary machine data. This data does not require persistence or as much resilience as the data in the shared storage. This is called the *temporary data cache*. The local disk

helps reduce traffic to the main OS storage. This disk is cleared after every machine restart. The disk is accessed through a write-through memory cache. Keep in mind that if you use local storage for temporary data, the provisioned VDA is tied to a specific hypervisor host. If that host fails, the VM cannot start.

Exception: If you use Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks to be created on local storage.

If you store temporary data locally, you can then enable and configure non-default values for each VM's cache disk and memory size when you create a machine catalog that uses that connection. However, the default values are as per the connection type, and are sufficient for most cases.

The hypervisor can also provide optimization technologies through in-memory read-caching of the disk images locally. For example, XenServer offers IntelliCache. This can also reduce network traffic to the central storage.

Storage local to the hypervisor

The storage local to the hypervisor method stores data locally on the hypervisor. With this method, images and other OS data are transferred to all the hypervisors used in the site, both for initial machine creation and future image updates. This results in significant traffic on the management network. Image transfers are also time-consuming, and the images become available to each host at a different time.

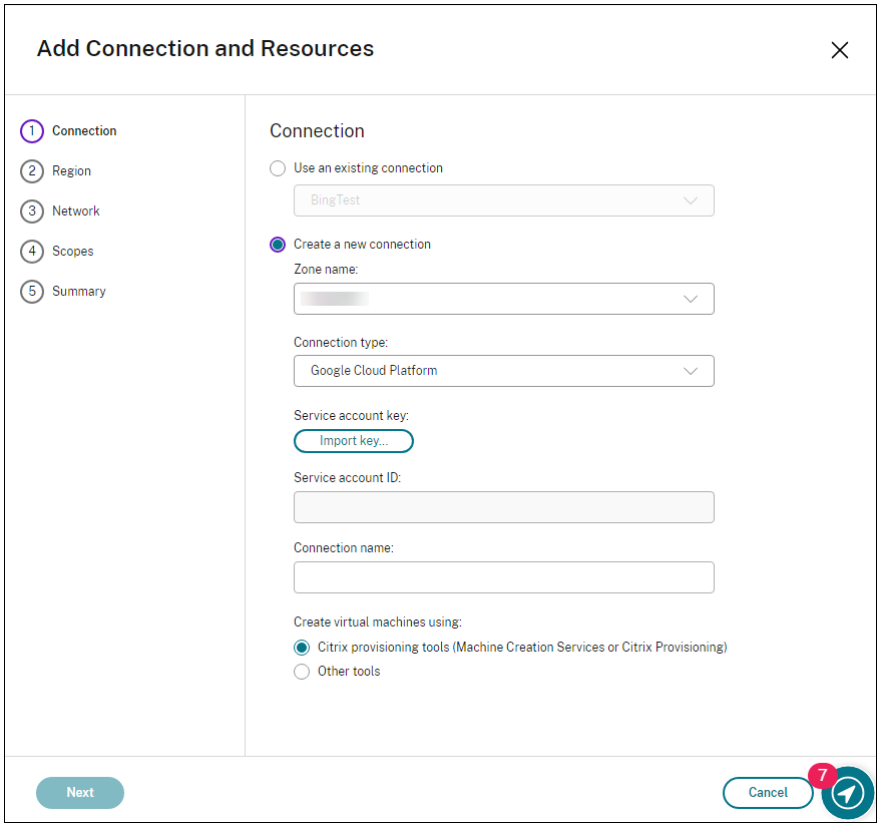
Create a connection and resources

> **Important:**
>
> The host resources (storage and network) in your resource location must be available before you create a connection.

1. Sign in to Citrix Cloud.
2. Navigate to the upper left menu and select **My Services > DaaS**.
3. From **Manage > Full Configuration**, select **Hosting** in the left pane.
4. Click **Add Connections and Resources** in the action bar.
5. The wizard guides you through the configuration process described in the following steps. Specific page content depends on the selected connection type. After completing the steps on each page, select **Next** until you reach the **Summary** page.

> **Note:**
>
> The content of each page within the wizard varies based on the type of connection that you've selected.

Step 1. Connection



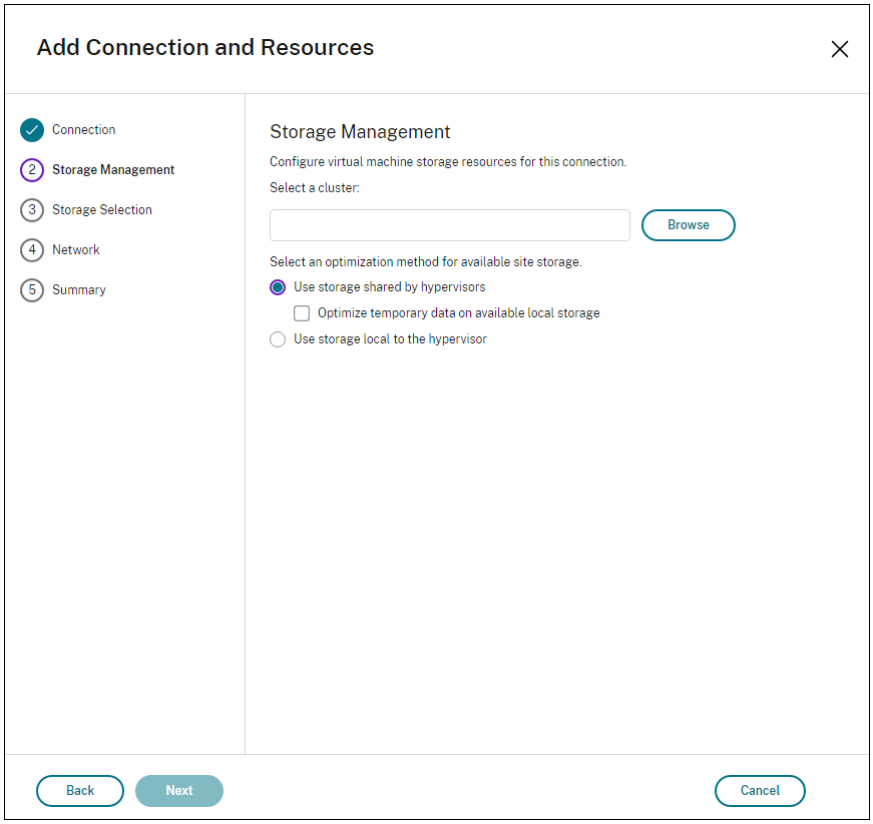
On the **Connection** page:

- To create a new connection, select **Create a new Connection**. To create a connection based on the same host configuration as an existing connection, select **Use an existing Connection**, and then choose the relevant connection.
- Select a zone in the **Zone name** field. The options are all resource locations you configured.
- Select a hypervisor or cloud service in the **Connection type** field. The options include all Citrix-supported hypervisors and cloud services:
  - For a resource location without accessible Cloud Connectors, only hypervisors and cloud services that support connectorless deployments are available.
  - For a resource location with accessible Cloud Connectors, only hypervisors and cloud services that have their plug-ins properly installed on those connectors are available.

  Alternatively, you can use the PowerShell command `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false or true to get the list of available hypervisors and Cloud services.
- Enter a connection name. This name appears in the **Hosting** display.
- Choose a tool to create virtual machines.

> **Note:**
>
> Information on the **Connection** page differs depending on the host or connection type that you're using. For example, when using Azure Resource Manager, you can use an existing service principal or create a new one. For details, see Connection to Microsoft Azure.

Step 2. Storage management



For information about storage management types and methods, see Host storage.

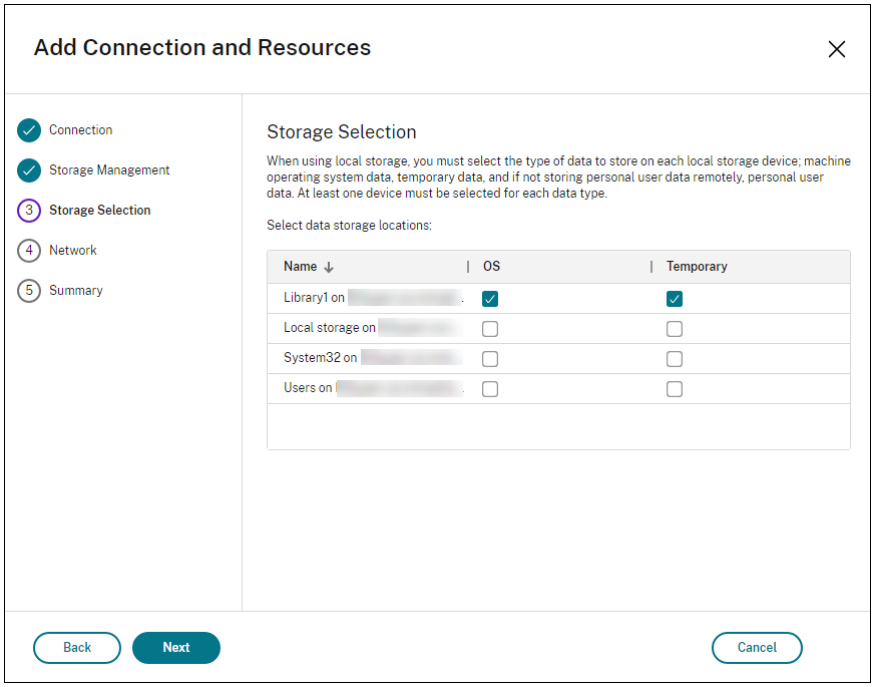
If you are configuring a connection to a Hyper-V or VMware host, browse to and then select a cluster name. Other connection types do not request a cluster name.

Select a storage management method: storage shared by hypervisors or storage local to the hypervisor.

For more information, see Storage shared by hypervisors and Storage local to the hypervisor.

If you use shared storage on a XenServer pool, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Use IntelliCache for XenServer connections.

Step 3. Storage selection



For more information about storage selection, see Host storage.

Select at least one host storage device for each available data type. The storage management method that you selected on the previous page affects which data types are available for selection on this page. You must select at least one storage device for each supported data type before you can proceed to the next page in the wizard.

You can get more configuration options on **Storage Selection** page if you chose **Use storage shared by hypervisors** and select **Optimize temporary data on available local storage** on **Storage Management** page. For example, you can select which local storage devices (in the same hypervisor pool) to use for temporary data.

The number of currently selected storage devices is shown (in the graphic, "1 storage device selected"). When you hover over that entry, the selected device names appear (unless no devices are configured).

1. Select **Select** to change the storage devices to use.
2. In the **Select Storage** dialog box, select or clear the storage device checkboxes, and then select **OK**.

Step 4. Region

> **Note:**
>
> The **Region** page appears only for some host types.

The region selection indicates where VMs will be deployed. Ideally, choose a region close to where users will access their applications.

Step 5. Network

Enter a name for the resources. This name appears in the Manage console to identify the storage and network combination associated with the connection.

Select one or more networks that the VMs will use.

Some connection types (such as Azure Resource Manager) also list subnets that VMs will use. Select one or more subnets.

Step 6. Summary

Review your selections. If you want to make changes, return to the previous wizard pages. When you complete your review, select **Finish**.

> **Note:**
>
> - If you store temporary data locally, you can configure non-default values for temporary data storage when you create the catalog containing machines that use this connection.
> - A scope is not shown for Full access administrators. For more information, see Administrators, roles, and scopes.

Edit connection settings

You cannot use this procedure to:

- Rename a connection or create a new connection.
- Change the GPU settings for a connection. Catalogs accessing this resource must use an appropriate GPU-specific image. Therefore, if you want to change the GCP settings, create a new connection instead of editing an existing connection.

Edit a connection

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.

2. Select the connection and then select **Edit Connection** in the action bar.
3. Use the **Connection Properties** page to change the connection address and credentials. Change the address only if the current host machine has a new address. Entering an address to a different machine breaks the connection's machine catalogs.

    - Select **Edit settings…**, and then enter the new information.
    - To specify the high-availability servers for a XenServer connection, select **Edit servers…** and select the servers. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails.

        > **Note:**
        >
        > If you are using HTTPS and want to configure high-availability servers, do not install a wildcard certificate for all servers in a pool. An individual certificate for each server is required. For more information, see Create a connection to XenServer.

4. Use the **Advanced** page to edit the settings to specify a maximum number of simultaneous actions (or concurrent machines) per hosting connection. These settings can help when power management settings allow too many or too few machines to start at the same time. Each connection type has specific default values that are appropriate for most cases. Usually, they do not need to be changed.

    - The **Simultaneous actions (all types)** and **Simultaneous Personal vDisk inventory updates** settings specify two values: a maximum absolute number that can occur simultaneously on this connection, and a maximum percentage of all machines that use this connection. You must specify both absolute and percentage values. The actual limit applied is the lower of the values.

        For example, in a deployment with 34 machines, if **Simultaneous actions (all types)** is set to an absolute value of 10 and a percentage value of 10, the actual limit applied is 3 (that is, 10 percent of 34 rounded to the nearest whole number, which is less than the absolute value of 10 machines).
    - The **Maximum new actions per minute** is an absolute number. There is no percentage value.
    - Enter information in **Connection options** only under the guidance of a Citrix Support representative.

5. Use the **Scopes** page to select one or more scopes for this host.

    > **Note:**

> A scope is not shown for Full access administrators. By definition, those administrators can access all customer-managed Citrix Cloud and subscribed services objects.

For more information, see Administrators, roles, and scopes.

6. Use the **Shared Tenants** page to add tenants and subscriptions that share the Azure Compute Gallery with the subscription of this connection.
   a) Enter the **Application secret** for the application associated with this connection. With this information, you can authenticate to Azure. We recommend that you change keys regularly to ensure security.
   b) Add shared tenants and subscriptions. You can add up to eight shared tenants. For each tenant, you can add up to eight subscriptions.
7. Click **Save** and **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Turn maintenance mode on or off for a connection

Turning on maintenance mode for a connection prevents any new power action from affecting any machine stored on the connection. Users cannot connect to a machine when it is in maintenance mode. If users are already connected, maintenance mode takes effect when they log off.

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection. To turn maintenance mode on, select **Turn On Maintenance Mode** in the action bar. To turn maintenance mode off, select **Turn Off Maintenance Mode**.

You can also turn the maintenance mode on or off for individual machines. You can turn maintenance mode on or off for machines in machine catalogs or delivery groups.

Delete a connection

> **Caution:**
>
> Deleting a connection can result in the deletion of large numbers of machines and loss of data. Ensure that user data on affected machines is backed up or no longer required.

Before deleting a connection, ensure that:

- All users are logged off from the machines stored on the connection.
- No disconnected user sessions are running.
- Maintenance mode is turned on for pooled and dedicated machines.
- All machines in machine catalogs used by the connection are powered off.

A machine catalog becomes unusable when you delete a connection that the catalog references. If this connection is referenced by a catalog, you can delete the catalog. Before you delete a catalog, make sure it is not used by other connections.

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection and then select **Delete Connection** in the action bar.
3. If this connection has machines stored on it, you are asked whether to delete the machines. If they are to be deleted, specify what to do with the associated Active Directory computer accounts.

Rename a connection

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection and then select **Rename Connection**.

Test a connection

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection and then select **Test Connection**.

View machine details on a connection

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection and then select **View Machines** in the action bar.

The upper pane lists the machines accessed through the connection. Select a machine to view its details in the lower pane. Session details are also provided for open sessions.

Use the search feature to find machines quickly. Either select a saved search from the list at the top of the window, or create a new search. You can either search by typing all or part of the machine name, or you can build an expression to use for an advanced search. To build an expression, select **Unfold**, and then select from the lists of properties and operators.

Manage machines on a connection

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select a connection and then select **View Machines** in the action bar.
3. Select one of the following in the action bar. Some actions might not be available, depending on the machine state and the connection host type.

- **Start:** Starts the machine if it is powered off or suspended.
- **Suspend:** Pauses the machine without shutting it down, and refreshes the list of machines.
- **Shut down:** Requests the operating system to shut down.
- **Force shut down:** Forcibly powers off the machine, and refreshes the list of machines.
- **Restart:** Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the desktop remains in its current state.
- **Enable maintenance mode:** Temporarily stops connections to a machine. Users cannot connect to a machine in this state. If users are connected, maintenance mode takes effect when they log off. (You can also turn maintenance mode on or off for all machines accessed through a connection, as described earlier.)
- **Remove from Delivery Group:** Removing a machine from a Delivery Group does not delete it from the machine catalog that the Delivery Group uses. You can remove a machine only when no user is connected to it. Turn on maintenance mode to temporarily prevent users from connecting while you are removing the machine.
- **Delete:** When you delete a machine, users no longer have access to it, and the machine is deleted from the machine catalog. Before deleting a machine, ensure that all user data is backed up or no longer required. You can delete a machine only when no user is connected to it. Turn on maintenance mode to temporarily stop users from connecting while you are deleting the machine.

For actions that involve machine shutdown, if the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during shutdown, there is a risk that the machine will be powered off before the updates are complete.

Edit storage

You can display the status of servers that are used to store the operating system, temporary, and personal (PvD) data for VMs that use a connection. You can also specify which servers to use for storage of each data type.

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection and then select **Edit Storage** in the action bar.
3. In the left pane, select the data type: operating system or temporary.
4. Select or clear the checkboxes for one or more storage devices for the selected data type.
5. Select **OK**.

Each storage device in the list includes its name and storage status. Valid storage status values are:

- **In use**: The storage is being used for creating machines.
- **Superseded**: The storage is being used only for existing machines. No new machines are added to this storage.

- **Not in use**: The storage is not being used for creating machines.

If you clear the checkbox for a device that is currently **In use**, its status changes to **Superseded**. Existing machines will continue to use that storage device (and can write data to it). So, that location can become full even after it stops being used for creating machines.

Detect Orphaned Azure resources

Orphaned resources are unused resources present in the system and they can lead to unnecessary expenses.

This feature allows you to detect the orphaned Azure resources in the hosts on your cloud site.

Follow the steps on Citrix DaaS:

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select a connection, and then select **Detect Orphaned Resources** in the action bar. The **Detect Orphaned Resources** dialog box displays the orphaned resource report.
3. To view the orphaned resource report, select **View Report**.

Alternatively, you can detect orphaned Azure resources using PowerShell. For more information, see Retrieve a list of orphaned resources.

To understand the reasons behind the orphaned resources, and to learn how to proceed further, see Efficiently manage Orphaned Azure resources with Citrix.

Connection timers

You can use Citrix policy settings to configure three connection timers:

- **Maximum connection timer:** Determines the maximum duration of an uninterrupted connection between a user device and a virtual desktop. Use the **Session connection timer** and **Session connection timer interval** policy settings.
- **Connection idle timer:** Determines how long an uninterrupted user device connection to a virtual desktop is maintained if there is no input from the user. Use the **Session idle timer** and **Session idle timer interval** policy settings.
- **Disconnect timer**: Determines how long a disconnected, locked virtual desktop can remain locked before the session is logged off. Use the **Disconnected session timer** and **Disconnected session timer interval** policy settings.

When you update any of these settings, ensure they are consistent across your deployment.

See the policy settings documentation for more information.

Edit networks of resources

You can change networks for a connection. Do the following:

1. Go to **Manage > Full Configuration > Hosting**.
2. Select the target resources under the connection and then select **Edit Network** in the action bar.
3. Select one or more networks for the virtual machines to use.
4. Click **Save** to save your changes and exit.

Delete, rename, or test resources

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the target resources under the connection, and then select the appropriate entry in the action bar:
    - **Delete Resources**
    - **Rename Resources**
    - **Test Resources**

Retrieve a list of orphaned resources

You can get a list of orphaned resources that are created by MCS but are no longer tracked by MCS. This is currently applicable to Azure environments. To get the list, you can use PowerShell commands. You can filter using connections.

> **Note:**
>
> The PowerShell command is rejected if any provisioning or image update is in progress.

Limitations

- Only a built-in full admin or cloud admin role admin user can run the PowerShell command and get the list of orphaned resources.
- To avoid incorrect recognition of orphaned resources, do not power on VMs while you are filtering orphaned resources.
- Around 2,000 records are displayed as orphaned if there is possible heavy workload.

Display the list of orphaned resources

To display the list of orphaned resources

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
3. Run the following commands:

   a) Get the connection uid. The connection uid is the value of the HypervisorConnectionUid attribute.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.PluginId -like 'Azure*'  }
    "
   <!--NeedCopy-->
   ```

   b) Get the list of orphaned resources.

   ```
   get-provorphanedresource
   -HypervisorConnectionUid <connection uid>
   <!--NeedCopy-->
   ```

Display the list of orphaned resources from an subscription id

To display the list of orphaned resources from an subscription id:

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
3. Run the following commands:

   a) Find the connection uid using the subscription ID. The connection uid is the value of the HypervisorConnectionUid attribute.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.CustomProperties -match '<subscriptionId>'  }

   <!--NeedCopy-->
   ```

   b) Get the list of orphaned resources.

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
      uid>
   <!--NeedCopy-->
   ```

> **Note:**
>
> Check the resources carefully before deleting.

Where to go next

- For information on connection to specific host types, see:
  - Connection to AWS
  - Connection to Google cloud environments
  - Connection to Microsoft Azure
  - Connection to Microsoft System Center Virtual Machine Manager
  - Connection to Nutanix
  - Connection to Nutanix cloud and partner solutions
  - Connection to VMware
  - Connection to VMware cloud and partner solutions
  - Connection to XenServer

If you're in the initial deployment process, create a machine catalog.

Connection to AWS

May 6, 2024

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to AWS cloud environments.

> **Note:**
>
> Before creating a connection to AWS, you need to first finish setting up your AWS as a resource location. See AWS virtualization environments.

Create a connection

When you create a connection from the Full Configuration interface:

- You must provide the API key and secret key values. You can export the key file containing those values from AWS and then import them. You must also provide the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials.
- The credentials file for the root AWS account (retrieved from the AWS console) is not formatted the same as credentials files downloaded for standard AWS users. Therefore, Citrix DaaS cannot use the file to populate the API key and secret key fields. Ensure that you are using AWS Identity Access Management (IAM) credentials files.

> **Note:**
>
> After you create a connection, attempts to update the API key and secret key might fail. To resolve the issue, check your proxy server or firewall restrictions and ensure that the following address is contactable: `https://*.amazonaws.com`.

Limitation

If you change the name of an AWS Virtual Private Cloud (VPC) in the AWS console, then the existing hosting unit in Citrix Cloud breaks. When the hosting unit is broken, you cannot create catalogs or add machines to existing catalogs. To resolve the issue, change the name of the AWS VPC back to the original name.

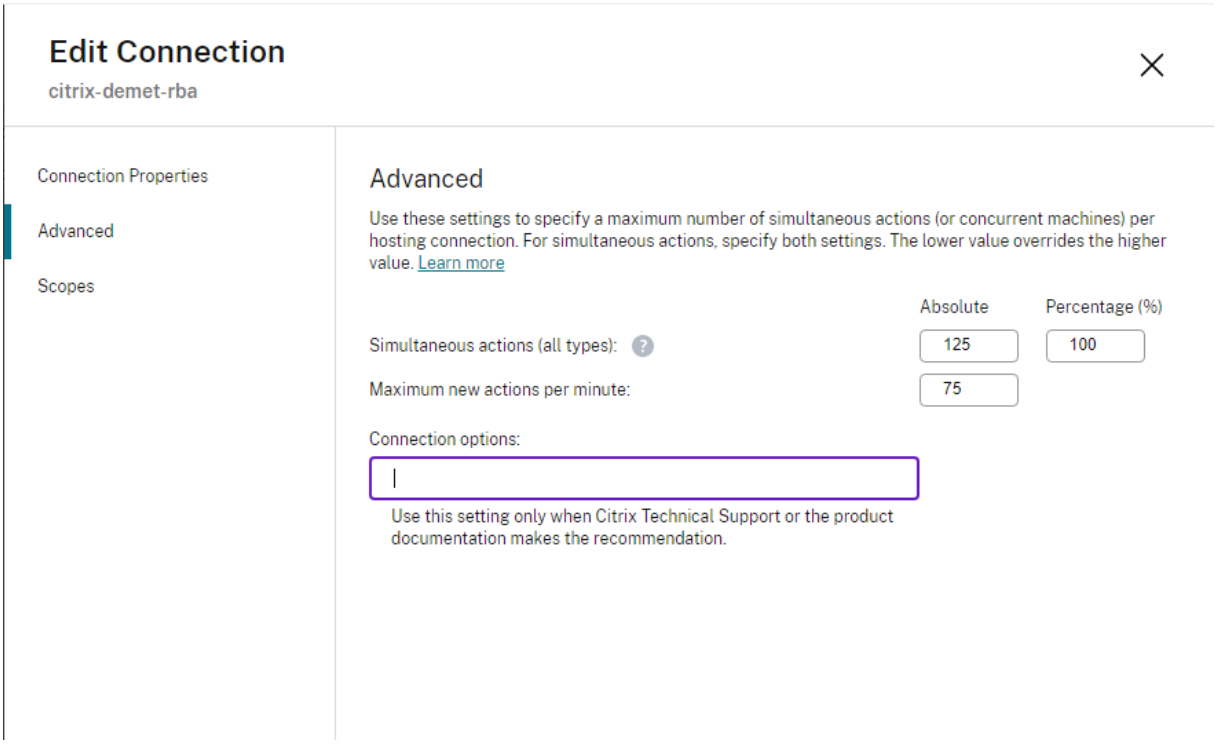
Host connection default values

When you create host connections in the Full Configuration interface of the AWS cloud environment, the following default values display:

Option	Absolute	Percentage
Simultaneous actions (all types)	125	100
Maximum new actions per minute	150	n/a
Maximum concurrent provisioning operations	100	n/a

MCS supports 100 maximum concurrent provisioning operations by default.

You can configure these values by accessing the Citrix Studio **Advanced** section on the **Edit Connection** screen:



Alternatively, you can use the Remote PowerShell SDK to set the maximum number of concurrent operations for optimal settings per your environment.

Use the PowerShell custom property, `MaximumConcurrentProvisioningOperations`, to specify the maximum number of concurrent AWS provisioning operations.

Before configuration:

- Ensure you have installed the PowerShell SDK for Cloud.
- Understand that the default value for `MaximumConcurrentProvisioningOperations` is 100.

Perform the following steps to customize the `MaximumConcurrentProvisioningOperations` value:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Enter `cd xdhyp:\Connections\`.
4. Enter `dir` to list the connections.
5. Change or Initialize the Custom Properties string:
    - If the Custom Properties string has a value, copy the Custom Properties into Notepad. Next, change the `MaximumConcurrentProvisioningOperations` property to your preferred value. You can enter a value ranging 1–1000.

For example, <Property xsi:type="IntProperty"Name="MaximumConcurrentProvis
"Value="xyz"/>.

- If the Custom Properties string is empty/null, you must initialize the string by entering the proper syntax for both the schema and the MaximumConcurrentProvisioningOperations property.

6. In the **PowerShell** window, paste the modified Custom Properties from Notepad and assign a variable to the modified Custom Properties. If you initialized the Custom Properties, add the following lines after the syntax:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
   org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'.
   ```

   This string sets the MaximumConcurrentProvisioningOperations property to 100. In the Custom Properties string, you must set the MaximumConcurrentProvisioningOperations property to a value that aligns with your needs.

7. Enter Get-XDAuthentication, which prompts you for your credentials.
8. Run $cred = Get-Credential, which might prompt you for solely a Password (or a Name and Password). You might also be prompted for the application ID and associated secret. For connections using role-based authentication, **role_based_auth** is both the Name and Password. Otherwise, enter the AWS API ID and secret.
9. Run set-item -PSPath 'XDHyp:\Connections<connection-name>'-CustomProperties $customProperties -username $cred.username -Securepassword $cred.password. You must set the <*connection-name*> to the name of the connection.
10. Enter dir to verify the updated CustomProperties string.

Configure security groups per network interface

When editing a host connection, you can now configure the maximum number of security groups allowed per elastic network interface (ENI) using a PowerShell command. For information on AWS security groups quota values, see Security groups.

To configure security groups per network interface:

1. Open a PowerShell window.
2. Run asnp citrix* to load the Citrix-specific PowerShell modules.
3. Run cd xdhyp:\Connections\.

4. Run `dir` to list the connections.
5. Run the following PowerShell command to configure security groups per network interface:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws
    -Name "Citrix_MachineManagement_Options" -Value "
    AwsMaxENISecurityGroupLimit=<number>"
<!--NeedCopy-->
```

> **Note:**
>
> If you do not set a value for `AwsMaxENISecurityGroupLimit`, then it takes the default value of 5.

Service endpoint URL

Standard zone service endpoint URL

When you use MCS, a new AWS connection is added with an API key and an API secret. With this information, along with the authenticated account, MCS queries AWS for the supported zones using the AWS DescribeRegions EC2 API call. The query is made using a generic EC2 Service Endpoint URL `https://ec2.amazonaws.com/`. Use MCS to select the zone for the connection from the list of supported zones. The preferred AWS service endpoint URL is automatically selected for the zone. However, after you create the service endpoint URL, you can no longer set or modify the URL.

Non-standard service endpoint URL

There can be situations where you might not need the automatically chosen AWS Service Endpoint URL for the connection. For such cases, you can use Citrix Cloud SDK and PowerShell to create a connection with a non-standard service endpoint URL. For example, to create a connection using the service endpoint URL `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Set up the AWS hosted Cloud Connector and ensure that it has connectivity.
2. Run the following PowerShell commands to see the list of Cloud Connectors.

```
 PS C:\> asnp citrix.*
 PS C:\> Get-XDAuthentication
 PS C:\> Get-ConfigEdgeServer
<!--NeedCopy-->
```

3. Find the ZoneUid from the newly created Cloud Connector and enter it into the following PowerShell commands. Replace the italicized items with the respective values.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidZoneUid-
Name"My New Connection"-ConnectionType "AWS"-HypervisorAddress @
```



```
("https://ec2.cn-north-1.amazonaws.com.cn")-UserName"APIkey"        -
Password"API Secret" -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
 $hyp. HypervisorConnectionUid
```

4. Refresh the **Full Configuration > Hosting** tab to verify that the EC2 connection has been created.
5. Add a resource location using the new connection.

Define IAM permissions

Use the information in this section to define IAM permissions for Citrix DaaS on AWS. Amazon's IAM service permits accounts having multiple users, which can be further organized into groups. These users can possess different permissions to control their ability to perform operations associated with the account. For more information about IAM permissions, see the IAM JSON policy reference.

To apply IAM permissions policy to a new group of users:

1. Log in to the AWS management console and select the **IAM service** from the drop-down list.
2. Select **Create a New Group of Users**.
3. Type a name for the new user group and select **Continue**.
4. On the **Permissions** page, choose **Custom Policy** then **Select**.
5. Type a name for the **Permissions policy**.
6. In the **Policy Document** section, enter the relevant permissions.

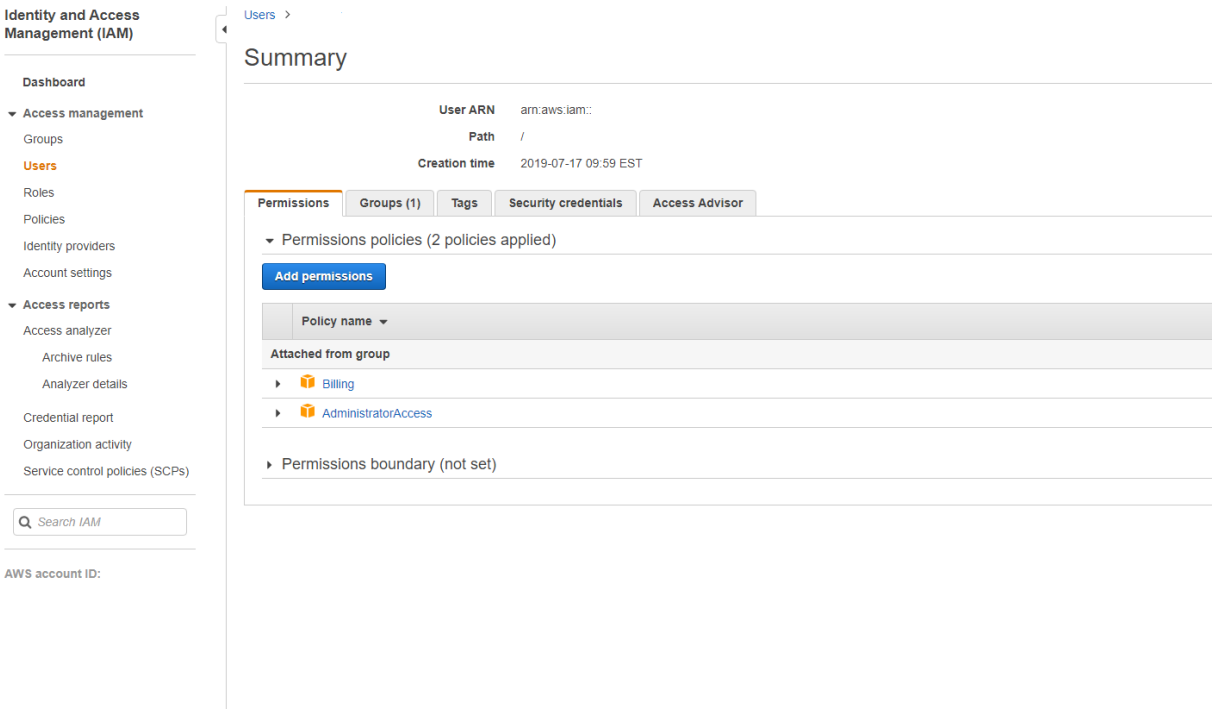
After entering the policy information, select **Continue** to complete the application of the IAM permissions policy to the group of users. Users in the group are granted permissions to do only those actions that are required for Citrix DaaS.

> **Important:**
>
> Use the policy text provided in the example below to list the actions that a Citrix DaaS uses to perform actions within an AWS account without restricting those actions to specific resources. Citrix recommends that you use the example for testing purposes. For production environments, you might choose to add further restrictions on resources.

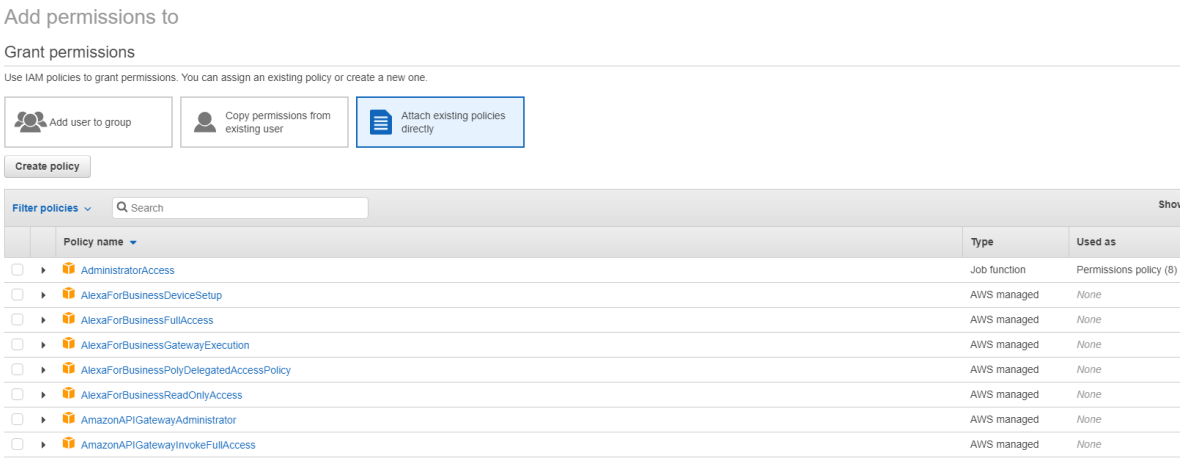
Add IAM permissions

Add the permissions in the **IAM** section of the AWS Management Console:

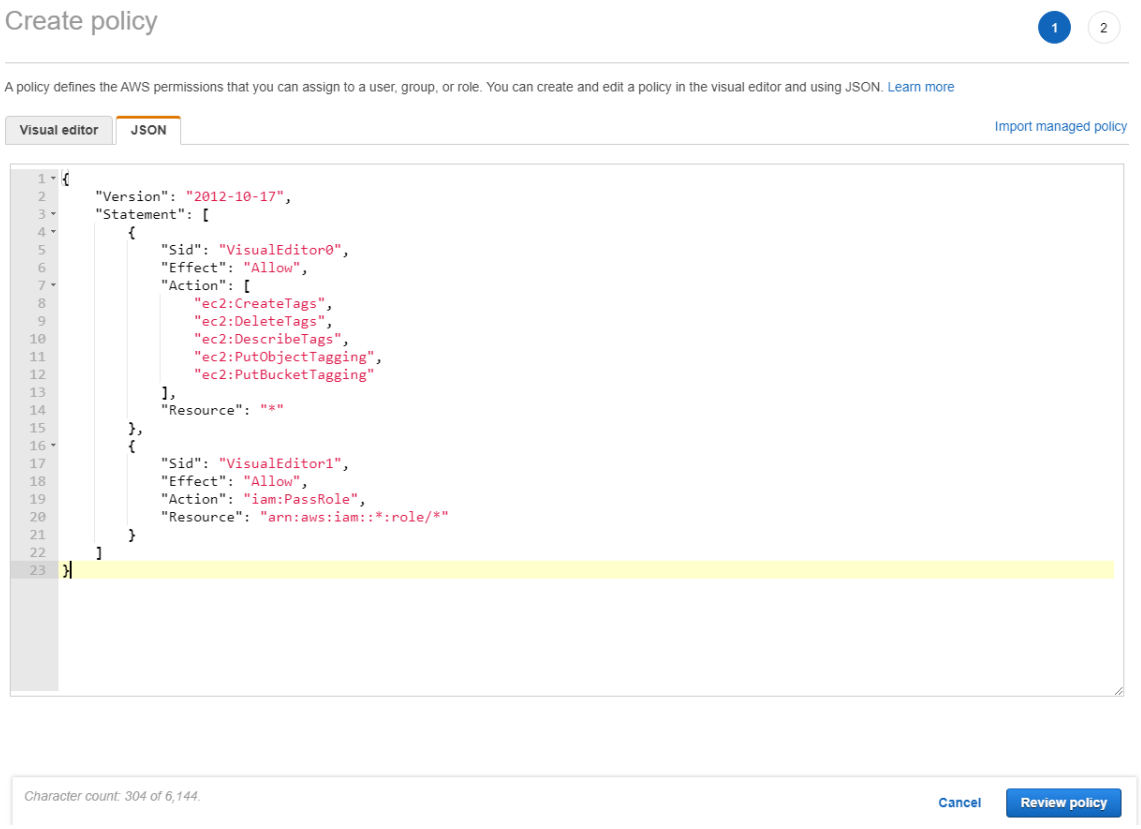
1. In the **Summary** panel, select the **Permissions** tab.
2. Select **Add permissions.**



In the **Add Permissions to** screen, grant permissions:



Use the following as an example in the **JSON** tab:



> **Tip:**
>
> The noted JSON example might not include all the permissions for your environment. See About AWS permissions for more information.

Required AWS permissions

This section contains the complete list of AWS permissions. Use the complete set of permissions as given in the section for the functionality to work correctly.

> **Note:**
>
> The *iam:PassRole* permission is needed only for **role_based_auth**.

Creating a host connection

A new host connection is added using the information obtained from AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```



```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeImages",
10                  "ec2:DescribeInstances",
11                  "ec2:DescribeInstanceTypes",
12                  "ec2:DescribeSecurityGroups",
13                  "ec2:DescribeSubnets",
14                  "ec2:DescribeVpcs"
15              ],
16              "Effect": "Allow",
17              "Resource": "*"
18          }
19
20      ]
21  }
22
23  <!--NeedCopy-->
```

Power management of VMs

Machine instances are powered on or off.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:CreateVolume",
10                 "ec2:DeleteVolume",
11                 "ec2:DescribeInstances",
12                 "ec2:DescribeVolumes",
13                 "ec2:DetachVolume",
14                 "ec2:StartInstances",
15                 "ec2:StopInstances"
16             ],
17             "Effect": "Allow",
18             "Resource": "*"
19         }
20
21     ]
22  }
23
24  <!--NeedCopy-->
```


Creating, updating, or deleting VMs

A machine catalog is created, updated, or deleted with VMs provisioned as AWS instances.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
 ,
```



```
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Note:

> - The EC2 section related to SecurityGroups is only needed if an Isolation Security Group must be created for the Preparation VM during catalog creation. Once this is done, these permissions are not required.

Direct disk upload and download Direct disk upload eliminates the volume worker requirement for machine catalog provisioning, and instead uses public APIs provided by AWS. This functionality reduces the cost associated with extra storage accounts and the complexity for maintaining volume worker operations.

> **Note:**
>
> The support for volume worker is deprecated.

The following permissions must be added to the policy:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **Important:**
>
> - You can add a new VM to existing machine catalogs without any volume worker resources such as volume worker AMI, and volume worker VM.
> - If you delete an existing catalog that used any volume worker before, all artifacts that are volume worker related are deleted.

EBS encryption of created volumes

EBS can auto-encrypt newly created volumes if the AMI is encrypted, or EBS is configured to encrypt all new volumes. However, to implement the functionality, the following permissions must be included in the IAM policy.

```
{

      "Version": "2012-10-17",
      "Statement": [
         {

```



```
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Note:

The permissions can be limited to specific keys by including a Resource and Condition block at the discretion of the user. For example, **KMS Permissions with Condition**:

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
            ],
            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true
                 }

             }

         }
```



```
30
31      ]
32   }
33
34  <!--NeedCopy-->
```

The following key policy statement is the entire default key policy for KMS keys that is required to allow the account to use IAM policies to delegate permission for all actions (kms:*) on the KMS key.

```
1  {
2
3  "Sid": "Enable IAM policies",
4  "Effect": "Allow",
5  "Principal": {
6
7  "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10 "Action": "kms:",
11 "Resource": ""
12  }
13
14 <!--NeedCopy-->
```

For more information, see the AWS Key Management Service official documentation.

IAM role-based authentication

The following permissions are added to support role-based authentication.

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": "iam:PassRole",
9              "Resource": "arn:aws:iam::*:role/*"
10          }
11
12      ]
13   }
14
15 <!--NeedCopy-->
```


Minimal IAM permissions policy

The following JSON can be used for all currently supported features. You can create host connections, create, update, or delete VMs, and do power management using this policy.
The policy can be applied to the users as explained in Defining IAM permissions sections or you can also use role-based authentication using **role_based_auth** security key and secret key.

> **Important:**
>
> To use **role_based_auth**, first configure the desired IAM role on the cloud connector ec2 instance when setting up the cloud connector. Using Citrix Studio, add the hosting connection and supply the role_based_auth for the authentication key and secret. A hosting connection with these settings then uses role-based authentication.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
```



```
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
```



```
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }

    ]
}

<!--NeedCopy-->
```

Note:

- The EC2 section related to SecurityGroups is only needed if an Isolation Security Group must be created for the Preparation VM during catalog creation. Once this is done, these permissions are not required.
- The KMS section is only required when using EBS volume encryption.
- The `iam:PassRole` permission section is needed only for **role_based_auth**.
- Specific resource-level permissions can be added instead of full access based on your requirements and environment. Refer to AWS documents Demystifying EC2 Resource-Level Permissions and Access management for AWS resources for more details.
- Use `ec2:CreateNetworkInterface` and `ec2:DeleteNetworkInterface` permissions only if you are using the volume worker method.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For AWS specific information, see Create an AWS catalog.

More information

- Create and manage connections and resources
- AWS virtualization environments

Connection to Google cloud environments

July 1, 2024

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Google cloud environments.

> **Note:**
>
> Before creating a connection to Google cloud environments, you need to first finish setting up your Google cloud account as a resource location. See Google Cloud virtualization environments.

Add a connection

In the Full Configuration interface, follow the guidance in Create and manage connections and resources. The following description guides you through setting up a hosting connection:

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select **Add Connection and Resources** in the action bar.
3. On the **Connection** page, select **Create a new Connection** and **Citrix provisioning tools**, and then select **Next**.
    - **Zone name**. Select a zone (equivalent to a resource location) where you want your host resources to reside. Zones are created automatically when you create a resource location and add a Cloud Connector to it. For more information, see Zones.
    - **Connection type**. Select **Google Cloud Platform** from the menu.

- **Service account key**. Import the key contained in your Google credential file (.json). You can either paste the key from the credential file or browse to the credential file. To paste the key:

  a) Locate your credential file
  b) Open the file with Notepad (or any text editor)
  c) Copy the content.
  d) Return to the **Connection** page, select **Add key**, paste the content, and then select **Done**.

- **Service account ID**. The field automatically populates with the information from the service account key.
- **Connection name**. Type a name for the connection.
- **Route traffic through Citrix Cloud Connectors**. To route the API requests through an available Citrix Cloud Connector, select this checkbox. You can also select **Enable Google Cloud Build to use private pools** checkbox for an additional layer of security.

  Alternatively, you can enable this feature using PowerShell. For more information, see Create a secure environment for GCP-managed traffic.

> **Note:**
>
> This option is available only when there are active Citrix Cloud Connectors in your deployment. Currently, this feature is not supported for Connector Appliances.

- **Create virtual machines using**. Select a method to create virtual machines.

4. On the **Region** page, select a project name from the menu, select a region containing the resources you want to use, and then select **Next**.
5. On the **Network** page, type a name for the resources, select a virtual network from the menu, select a subset, and then select **Next**. The resource name helps identify the region and network combination. Virtual networks with the *(Shared)* suffix appended to their name represent shared VPCs. If you configure a subnet-level IAM role for a shared VPC, only specific subnets of the shared VPC appear on the subnet list.

   > **Note:**
   >
   > - The resource name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. On the **Summary** page, confirm the information and then select **Finish** to exit the **Add Connection and Resources** window.

After you create the connection and resources, the connection and resources you created are listed. To configure the connection, select the connection and then select the applicable option in the action bar.

Similarly, you can delete, rename, or test the resources created under the connection. To do so, select the resource under the connection and then select the applicable option in the action bar.

Create a secure environment for GCP managed traffic

You can allow only private Google access to your Google Cloud projects. This implementation enhances security to handle sensitive data. To do this:

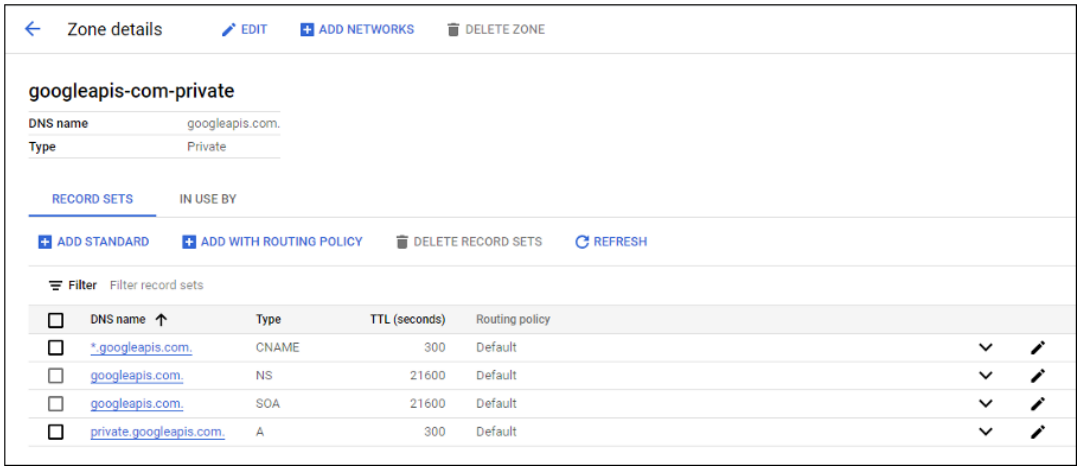
1. Install Cloud Connectors in the VPC where you want to enforce VPC service controls. See VPC Service Controls for more information.
2. Add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` in case of Citrix Cloud deployment. If you are using a private worker pool, add `UsePrivateWorkerPool` in `CustomProperties`. For information on the private worker pool, see Private pools overview.

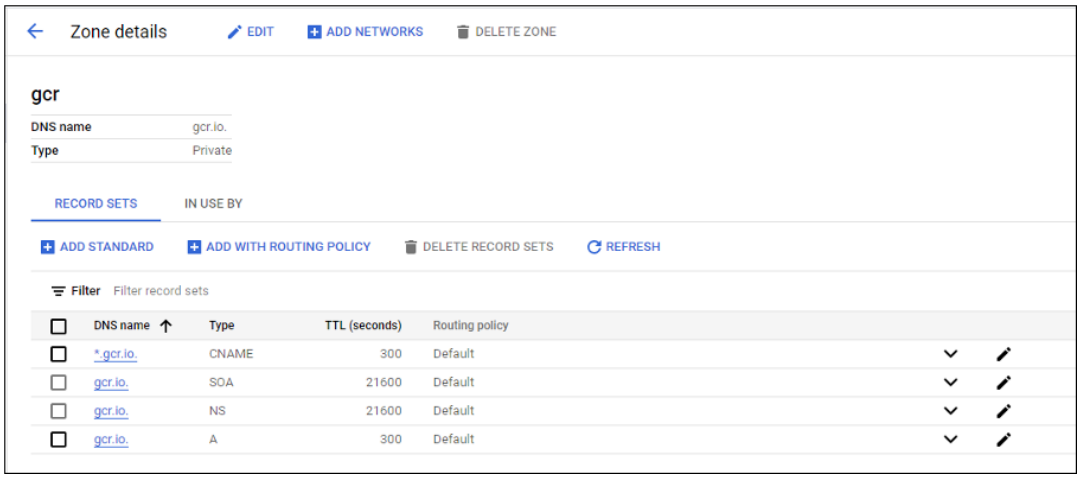
> **Note:**
>
> Currently, this feature is not supported for Connector Appliance.

Requirements to create a secure environment for GCP managed traffic

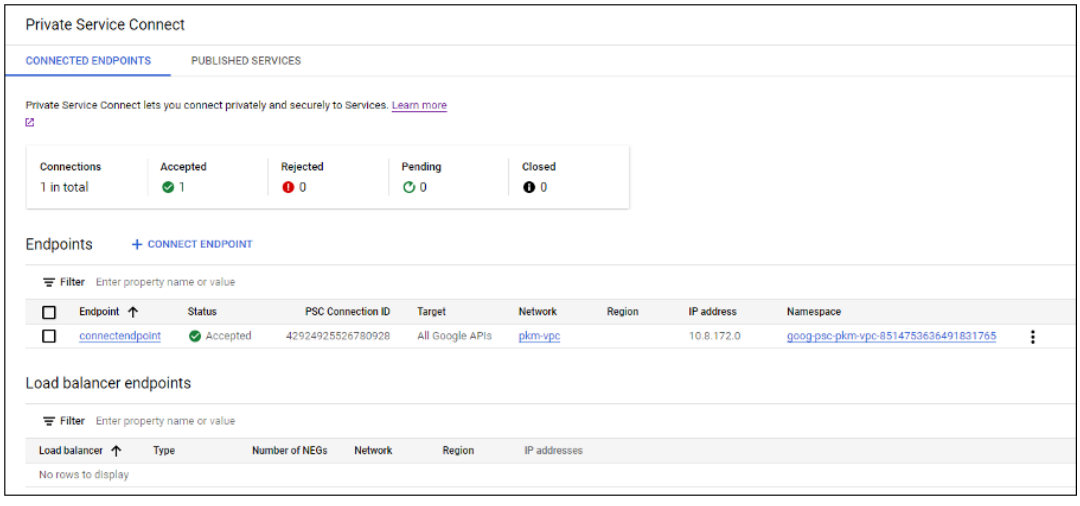
The requirements to create a secure environment for GCP managed traffic are:

- Ensure that the hosting connection is in maintenance mode when updating the custom properties.
- To use private worker pools, the following changes are required:
  - For Citrix Cloud Service Account, add the following IAM roles:
    - Cloud Build Service Account
    - Compute Instance Admin
    - Service Account User
    - Service Account Token Creator
    - Cloud Build WorkerPool Owner
  - Create the Citrix Cloud Service Account in the same project that you use for creating a hosting connection.
  - Set up DNS zones for **`private`**`.googleapis.com` and `gcr.io` as described in DNS configuration.

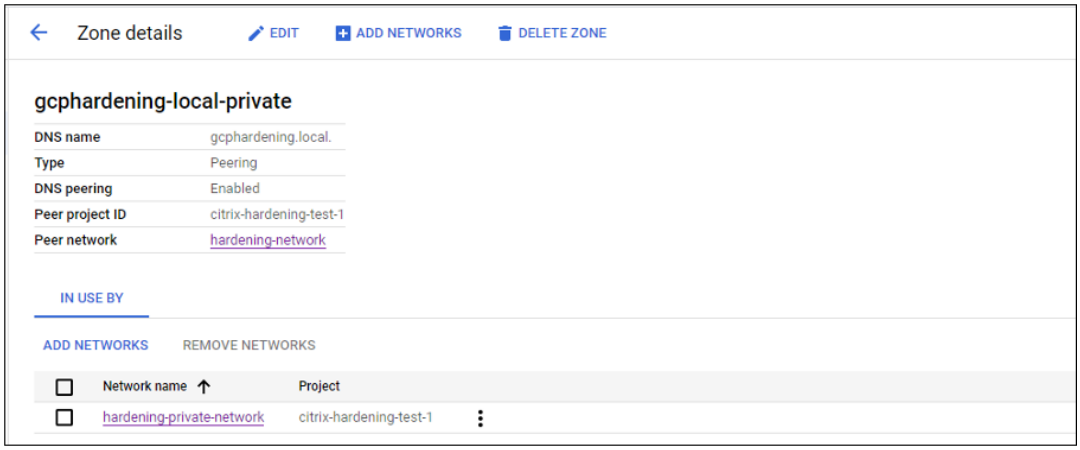




- Set up private Network Address Translation (NAT) or use private service connect. For more information, see Access Google APIs through endpoints.



- If using a peered VPC, create a Cloud DNS zone peering to the peered VPC. For more information, see Create a peering zone.



- In VPC service controls, set up Egress rules so that the APIs and VMs can talk to the internet. Ingress rules are optional. For example:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

Enable the proxy

To enable the proxy, set the custom properties as follows on the host connection:

1. Open a PowerShell window from the Delivery Controller host or use the Remote PowerShell SDK. For more information on Remote PowerShell SDK, see SDKs and APIs.
2. Run the following commands:
   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Copy the `CustomProperties` from the connection to a notepad.
4. Append the property setting as follows:
   - In case of cloud deployment (using public pools): Append property setting `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughConnector "Value="True"/>` to the `CustomProperties` to enable the proxy. For example:


```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
   -instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

Allow ingress rule for Cloud Build Service Account in VPC service perimeter. For example:

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
<!--NeedCopy-->
```

For information on VPC service perimeter, see Service perimeter details and configuration.

- In case of a private worker pool in a cloud deployment, append property setting `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughC "Value="True"/>` and `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool"Value="True"/>` to the `CustomProperties` to enable the proxy. For example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
   -instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
<Property xsi:type="StringProperty" Name="
   UsePrivateWorkerPool" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

5. In the PowerShell window, assign a variable to the modified custom properties. For example: `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Run `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"` .
7. Run `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Run `$securePassword = ConvertTo-SecureString $gcpPrivateKey -`

`AsPlainText -Force`.

9. Run the following to update an existing host connection:

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR
    CONNECTION NAME HERE>') -SecurePassword $securePassword -
    UserName $gcpServiceAccount -CustomProperties $customProperty
<!--NeedCopy-->
```

Specify CMEK global and regional key

There are two types of customer-managed encryption keys (CMEK) in GCP:

- Regional: Encryption keys that can only be used by resources in the same region.
- Global: Encryption keys that can be used by resources from multiple regions.

You can browse and use global or regional customer-managed encryption keys (CMEK) from all projects that are accessible to the service account. You can then use the key to create a CMEK enabled MCS machine catalog and update an existing CMEK enabled MCS machine catalog using `Set-ProvScheme` command. For information creating a CMEK enabled catalog using PowerShell, see Create a catalog with CMEK using custom properties.

For this feature, you need additional permissions for the following two service accounts:

- The service account of the current project with which the hosting connection is created.
- The Compute Engine Service Agent of the current project (that has the email: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com`). For more information, see Compute Engine Service Agent.

In Service accounts, you must assign the following roles in the project that has crypto keys that you want to use (for example, shared project):

- Cloud KMS Viewer
- Cloud KMS CryptoKey Encrypter/Decrypter

If you do not assign to the roles, then make sure that you have the following permissions:

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

List the encryption keys

You can list the global and regional encryption keys within the same project and all other accessible projects using the PowerShell commands. To do this:

1. Open a PowerShell window from the Delivery Controller host.
2. Run the command `asnp citrix*` to load Citrix-specific PowerShell modules.
3. Run the following command to list the encryption keys. Example:

   - To list global encryption keys within the same project:

   ```
   XDHyp:\Connections\abc-Connection\my_project.project \us-
       east1.region\encryptionKeys.folder\myglobalkeyring.
       globalkeyring\myglobalkey.cryptokey
   <!--NeedCopy-->
   ```

   - To list regional encryption keys within the same project:

   ```
   XDHyp:\Connections\abc-Connection\my_project.project\us-
       central1.region\encryptionKeys.folder\regional-ring.
       keyring\shared-key.key
   <!--NeedCopy-->
   ```

   - To list global encryption keys from another accessible project (for example: myanother-project):

   ```
   XDHyp:\Connections\abc-Connection\my_project.project\us-
       central1.region\encryptionKeys.folder\myanotherproject .
       project\extglobalkeyring.globalkeyring\externalglobalkey.
       cryptokey
   <!--NeedCopy-->
   ```

   - To list regional encryption keys from another accessible project (for example: myanother-project):

   ```
   XDHyp:\Connections\abc-Connection\my_project.project\us-
       central1.region\encryptionKeys.folder\myanotherproject .
       project\extkeyring.keyring\externalkey.cryptokey
   <!--NeedCopy-->
   ```

> **Note:**
>
> - The extension of the key ring inventory item for a global key ring is `.globalkeyring`.
> - The id of global key rings has the word `global` in it.

Required GCP permissions

This section has the complete list of GCP permissions. Use the complete set of permissions as given in the section for the functionality to work correctly.

> **Note:**
>
> GCP is introducing changes to Cloud Build Services's default behavior and use of service accounts after April 29, 2024. For more information, see Cloud Build Service Account Change. Your existing Google projects with Cloud Build API enabled before April 29, 2024 are not affected by this change. However, if you want to have existing Cloud Build Service behavior after April 29, you can create or apply the organization policy to disable the constraint enforcement before you enable the API. If you set the new organization policy, you can still follow the existing permissions in this section and the items that are marked **Before Cloud Build Service Account Change**. If not, then follow the existing permissions and items that are marked **After Cloud Build Service Account Change**.

Creating a host connection

- Minimum permissions required for Citrix Cloud Service Account in Provisioning project:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  The following Google defined roles have the permissions as listed above:

  - Compute Admin
  - Cloud Datastore User

- Additional permissions required for Shared VPC for Citrix Cloud Service Account in Shared VPC project:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  The following Google defined roles have the permissions as listed above:

  - Compute Network User

- In Service accounts, you must assign the following roles in the project that has crypto keys that you want to use (for example, shared project):
  - Cloud KMS Viewer
  - Cloud KMS CryptoKey Encrypter/Decrypter

  If you do not assign to the roles, then make sure that you have the following permissions:
  - resourcemanager.projects.get
  - cloudkms.keyRings.list
  - cloudkms.keyRings.get
  - cloudkms.cryptoKeys.get
  - cloudkms.cryptoKeys.list
  - cloudkms.cryptoKeyVersions.useToDecrypt
  - cloudkms.cryptoKeyVersions.useToEncrypt

Power management of VMs

Minimum permissions required for Citrix Cloud Service Account in Provisioning project in case of power managed only catalogs:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
<!--NeedCopy-->
```

The following Google defined roles have the permissions as listed above:

- Compute Admin
- Cloud Datastore User

Creating, updating, or deleting VMs

- Minimum permissions required for Citrix Cloud Service Account in Provisioning project:


```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
```



```
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use

<!--NeedCopy-->
```

The following Google defined roles have the permissions as listed above:

- Compute Admin
- Storage Admin
- Cloud Build Editor
- Service Account User
- Cloud Datastore User

- Additional permissions required for Shared VPC for Citrix Cloud Service Account in Shared VPC project to create a hosting unit using VPC and subnetwork from Shared VPC project:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

The following Google defined roles have the permissions as listed above:

  - Compute Network User
  - Cloud Datastore User

- (Before Cloud Build Service Account Change): Minimum permissions required for Cloud Build Service Account in Provisioning project required by Google Cloud Build service when downloading preparation instruction disk to MCS:
- (After Cloud Build Service Account Change): Minimum permissions required for Cloud Compute Service Account in Provisioning project required by Google Cloud Compute service when downloading preparation instruction disk to MCS:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```


The following Google defined roles have the permissions as listed above:

- Cloud Build Service Account (After Cloud Build Service Account Change, it is Cloud Compute Service Account)
- Compute Instance Admin
- Service Account User

- Minimum permissions required for Cloud Compute Service Account in Provisioning project required by Google Cloud Build service when downloading preparation instruction disk to MCS:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

The following Google defined roles have the permissions as listed above:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- (Before Cloud Build Service Account Change): Additional permissions required for Shared VPC for Cloud Build Service Account in Provisioning project required by Google Cloud Build service when downloading preparation instruction disk to MCS:
- (After Cloud Build Service Account Change): Additional permissions required for Shared VPC for Cloud Compute Service Account in Provisioning project required by Google Cloud Compute service when downloading preparation instruction disk to MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

The following Google defined roles have the permissions as listed above:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- Additional permissions required for Cloud Key Management Service (KMS) for Citrix Cloud Service Account in Provisioning project:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
```



```
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

The following Google defined roles have the permissions as listed above:

- Compute KMS Viewer

General permissions

Following are the permissions for Citrix Cloud Service Account in Provisioning project for all features supported in MCS. These permissions provide the best compatibility going forward:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
```



```
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
```



```
iam.serviceAccounts.actAs
compute.resourcePolicies.use
cloudkms.cryptoKeyVersions.useToDecrypt
cloudkms.cryptoKeyVersions.useToEncrypt
<!--NeedCopy-->
```

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Google Cloud Platform (GCP) specific information, see Create a Google Cloud Platform catalog.

More information

- Create and manage connections and resources
- Google Cloud virtualization environments.

Connection to HPE Moonshot

April 16, 2024

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to HPE Moonshot.

> **Note:**
>
> Before creating a connection to HPE Moonshot, you need to first finish setting up your HPE account. See HPE Moonshot virtualization environments.

Create a connection

You can create a connection to HPE Moonshot using the:

- Full Configuration interface
- PowerShell commands

Create a connection using the Full Configuration interface

1. In the **Add Connection and Resources** page, select the **HPE Moonshot** as the connection type.

2. Enter the connection address of your Moonshot iLO Chassis Manager. You can use an IP address, host name, or FQDN for the address.
3. Enter your chassis administrative credentials and a friendly connection name.

Connection setup stops when either of the situations occurs:

- DaaS receives a public CA-signed certificate with errors: An error message appears. Follow the on-screen instructions to fix the issue. Otherwise, you can't proceed with connection creation.
- DaaS receives a private CA-signed certificate. A warning page appears. Compare the received thumbprint with the server's for the certificate validity. If it's valid, select **Trust certificate** and click **OK** to proceed with connection creation. DaaS will then trust the certificate and store the thumbprint for future validation.

Create a connection using PowerShell commands

When you create a connection using PowerShell command, provide the following information:

- IP: HPE Server IP Address
- Username: HPE username
- Password: HPE password

For example:

```
1 New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
2  "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
3   -Path @("XDHyp:\Connections\$connectionName") -Persist -PluginId "
       HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
       $UserName -sslthumbprint $SslThumbprint New-
       BrokerHypervisorConnection -HypHypervisorConnectionUid
       $HypervisorConnectionID
4 <!--NeedCopy-->
```

> **Note:**
>
> The `sslthumbprint` parameter is required for only Private CA-signed certificates.

Certificate and thumbprint validation

For creating a successful connection to **HPE Moonshot**, the certificate must not have errors and the thumbprint must have a correct value. Following are the use cases related to the certificate and thumbprint validation:

- Public CA-signed certificate has errors. The connection is not created successfully. See the error details and resolve the issue.

- Public CA-signed certificate without errors. The connection is created successfully, and the `SslThumbprints` value is **Null**.
- Private CA-signed certificate without errors and a `sslthumbprint` value. The connection is created successfully with a correct `SslThumbprints` value.
- Private CA-signed Certificate with an incorrect thumbprint value. The connection is not created successfully.
- Private CA-signed Certificate without errors. The connection is created successfully. The `SSlThumbprints` is **Null** when creating the connection. The `SSlThumbprints` value is updated to a value by the site service.

Manage connections

This section details how you can manage connections:

- Fix certificate issues using Full Configuration interface
- Update thumbprint value using PowerShell command

Fix certificate issues

DaaS blocks an HPE Moonshot connection when certificate issues arise, preventing you from delivering and managing workloads on associated HPE Moonshot nodes. You'll see an error icon next to the connection in the **Host connections** list. See the following table for specific issues and solutions.

Issue	Solution
A certificate error occurs to the public CA-signed certificate	Click the connection and select the **Troubleshoot** tab. View the error details and resolve the issue.
The received certificate is private CA-signed or expired.	Edit the host connection to update the certificate thumbprint. Details steps 1. Select the connection and click **Edit Connection**. 1. On the **Connection Properties** page, click **Edit settings**. 1. Enter the password to connect to the HPE Moonshot chassis, and then click **Save**.

Issue	Solution
	1. On the **Warning** page that appears, compare the received thumbprint with the server's for certificate validity. 1. If they are the same, select **Trust certificate** and then click **OK**.

Update thumbprint value

After creating the connection, you can update the thumbprint value of a connection using the `Set-Item` PowerShell command. For example, run the following commands:

1. Get the connection details of a connection. For example:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

2. Update the thumbprint value. For example:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
<!--NeedCopy-->
```

3. Check the updated thumbprint value. For example:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

> **Note:**
>
> The update fails if you provide an incorrect thumbprint value in the `Set-Item` command.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For HPE Moonshot specific information, see Create an HPE Moonshot machine catalog.

More information

- Create and manage connections and resources
- HPE Moonshot virtualization environments

Connection to Microsoft Azure

April 17, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Azure Resource Manager cloud environments.

> **Note:**
>
> Before creating a connection to Microsoft Azure, you must finish setting up your Azure account as a resource location. See Microsoft Azure Resource Manager virtualization environments.

Create service principals and connections

Before creating connections, you must set up service principals that connections use to access Azure resources. You can create a connection in two ways:

- Create a service principal and a connection together using Full Configuration
- Create a connection using a previously created service principal

This section shows you how to complete these tasks:

- Create a service principal and connection using Full Configuration
- Create a service principal using PowerShell
- Get the application secret in Azure
- Create a connection using an existing service principal

Considerations

Before you start, be aware of these considerations:

- Citrix recommends using service principals with a *Contributor* role. However, see the Minimum permissions section to get the list of minimum permissions.
- When creating the first connection, Azure prompts you to grant it the necessary permissions. For future connections you must still authenticate, but Azure remembers your previous consent and does not display the prompt again.

- After you authenticate with Azure for the first time, a Citrix owned multi-tenant application (ID: `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`) is invited to your Azure Active Directory on behalf of the authenticated account. Citrix uses this application to create new service principals and grant proper permissions for workload provisioning and for Azure AD device management if you select **Enable Azure AD joined device management** on the **Connection Details** page.
- Accounts used for authentication must be a co-administrator of the subscription.
- The account used for authentication must be a member of the subscription's directory. There are two types of accounts to be aware of: 'Work or School'and 'personal Microsoft account.' See CTX219211 for details.
- While you can use an existing Microsoft account by adding it as a member of the subscription's directory, there can be complications if the user was previously granted guest access to one of the directory's resources. In this case, they might have a placeholder entry in the directory that does not grant them the necessary permissions, and an error is returned.

  Rectify this by removing the resources from the directory and adding them back explicitly. However, exercise this option carefully, because it has unintended effects on other resources that this account can access.
- There is a known issue where certain accounts are detected as directory guests when they are actually members. Configurations like this typically occur with older established directory accounts. Workaround: add an account to the directory, which takes the proper membership value.
- Resource groups are simply containers for resources, and they can contain resources from regions other than their own region. This can potentially be confusing if you expect resources displayed in a resource group's region to be available.
- Ensure that your network and subnet are large enough to host the number of machines you require. This requires some foresight, but Microsoft helps you specify the right values, with guidance about the address space capacity.

Create a service principal and connection using Full Configuration

> **Important:**
>
> This feature is not yet available for Azure China subscriptions.

With Full Configuration, you can create both a service principal and a connection in a single workflow. Service principals give connections access to Azure resources. When you authenticate to Azure to create a service principal, an application is registered in Azure. A secret key (called *client secret* or

application secret) is created for the registered application. The registered application (a *connection* in this case) uses the client secret to authenticate to Azure AD.

Before you start, make sure that you've met these prerequisites:

- You have a user account in your subscription's Azure Active Directory tenant.
- The Azure AD user account is also a co-administrator for the Azure subscription that you want to use for provisioning resources.
- You have global administrator, application administrator, or application developer permissions for authentication. The permissions can be revoked after you create a host connection. For more information about roles, see Azure AD built-in roles.

Use the **Add Connection and Resources** wizard to create a service principal and a connection together:

1. On the **Connection** page, select **Create a new connection**, the **Microsoft Azure** connection type, and your Azure environment.
2. Select which tools to use to create the virtual machines and then select **Next**.
3. On the **Connection Details** page, create a service principal and set the connection name as follows:

    a) To grant the connection permission to automatically clean stale Azure AD joined devices, select **Enable Azure AD joined device management**. We recommend that you select this option if you want to create Azure AD joined machines through this connection. For more information, see Enable Azure AD joined device management.

    b) Enter your Azure subscription ID and a name for the connection. After you enter the subscription ID, the **Create new** button is enabled.

    > **Note:**
    >
    > The connection name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{ } "'()'`.

    a) Select **Create new** and then enter the Azure Active Directory account user name and password.

    b) Select **Sign in**.

    c) Select **Accept** to give Citrix DaaS the listed permissions. Azure creates a service principal that allows Citrix DaaS to manage Azure resources on behalf of the specified user.

    d) After you select **Accept**, you're taken back to the **Connection Details** page.

> **Note:**
>
> After you successfully authenticate to Azure, the **Create new** and **Use existing** buttons disappear. The **Connection successful** text appears with a green check mark, indicating the successful connection to your Azure subscription.

e) To route API requests to Azure through Citrix Cloud Connectors, select the **Route traffic through Citrix Cloud Connectors** checkbox.

Alternatively, you can enable this feature using PowerShell. For more information, see Create a secure environment for Azure-managed traffic.

> **Note:**
>
> This option is available only when there are active Citrix Cloud Connectors in your deployment. Currently, this feature is not supported for Connector Appliances.

f) Select **Next**.

> **Note:**
>
> You cannot proceed to the next page until you successfully authenticate to Azure and consent to giving the required permissions.

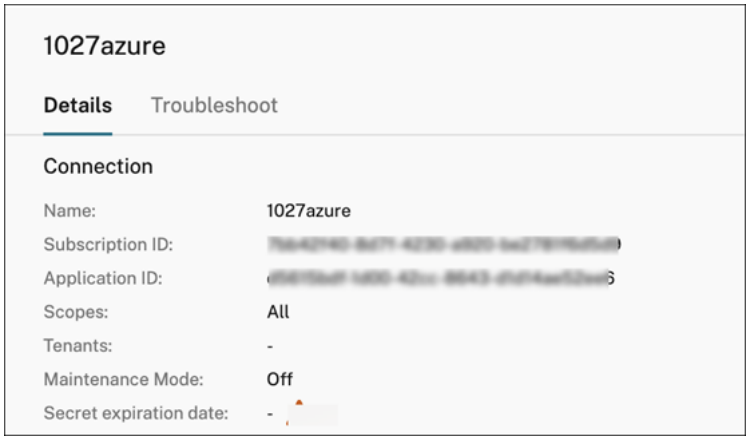
4. Configure the resources for the connection as follows:

   - On the **Region** page, select a region.
   - On the **Network** page, do the following:
     - Type a 1–64 character resource name to help identify the region and network combination. A resource name cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{ } "'()'`.
     - Select a virtual network/resource group pair. (If you have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If the region you selected on the previous page does not have any virtual networks, return to that page and select a region that has virtual networks.

5. On the **Summary** page, view a summary of settings and select **Finish** to complete your setup.

View the application ID After you create a connection, you can view the application ID that the connection uses to access Azure resources.

In the **Add Connection and Resources** list, select the connection to view the details. The **Details** tab shows the Application ID.



Create a service principal using PowerShell

To create a service principal using PowerShell, connect to your Azure Resource Manager subscription and use the PowerShell cmdlets provided in the following sections.

Make sure that you have these items ready:

- **SubscriptionId:** Azure Resource Manager `SubscriptionID` for the subscription where you want to provision VDAs.
- **ActiveDirectoryID**: Tenant ID of the application that you registered with Azure AD.
- **ApplicationName:** Name for the application to be created in Azure AD.

Detailed steps are as follows:

1. Connect to your Azure Resource Manager subscription.

   ```
   Connect-AzAccount
   ```

2. Select the Azure Resource Manager subscription where you want to create the service principal.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

3. Create the application in your AD tenant.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. Create a service principal.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. Assign a role to the service principal.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

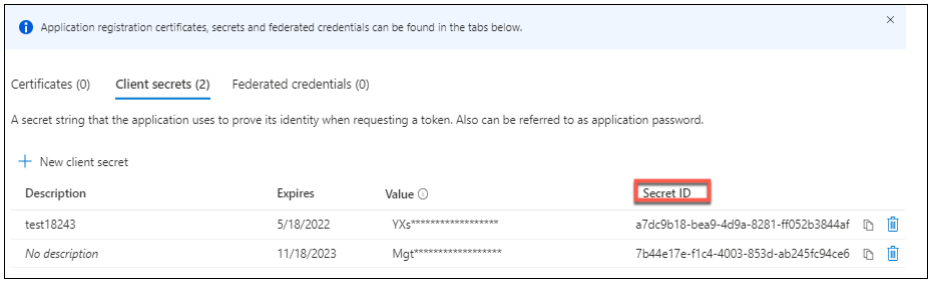

6. From the output window of the PowerShell console, note the ApplicationId. You provide that ID when creating the host connection.

Get the application secret in Azure

To create a connection using an existing service principal, you must first get the application ID and secret of the service principal in the Azure portal.

Detailed steps are as follows:

1. Get the **Application ID** from the Full Configuration interface or using PowerShell.
2. Sign in to the Azure portal.
3. In Azure, select **Azure Active Directory**.
4. From **App registrations** in Azure AD, select your application.
5. Go to **Certificates & secrets**.
6. Click **Client secrets**.



Create a connection using an existing service principal

If you already have a service principal, you can use it to create a connection using Full Configuration.

Make sure you have these items ready:

- SubscriptionId
- ActiveDirectoryID (tenant ID)
- Application ID
- Application secret

  For more information, see Get the application secret.
- Secret expiration date

Detailed steps are as follows:

In the **Add Connection and Resources** wizard:

1. On the **Connection** page, select **Create a new connection**, the **Microsoft Azure** connection type, and your Azure environment.
2. Select which tools to use to create the virtual machines and then select **Next**.
3. On the **Connection Details** page, enter your Azure subscription ID and a name for the connection.

   > **Note:**
   >
   > The connection name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{ } "'()'`.

4. Select **Use existing**. In the **Existing Service Principal Details** window, enter the following settings for the existing service principal. After you enter the details, the **Save** button is enabled. Select **Save**. You cannot progress beyond this page until you provide valid details.

   - **Subscription ID**. Enter your Azure subscription ID. To obtain your subscription ID, sign in to the Azure portal and navigate to **Subscriptions > Overview**.
   - **Active Directory ID** (tenant ID). Enter the Directory (tenant) ID of the application that you registered with Azure AD.
   - **Application ID**. Enter the Application (client) ID of the application that you registered with Azure AD.
   - **Application secret**. Enter a secret key (client secret). The registered application uses the key to authenticate to Azure AD. We recommend that you change keys regularly for security purposes. Be sure to save the key because you cannot retrieve the key later.
   - **Secret expiration date**. Enter the date after which the application secret expires. You receive an alert on the console before the secret key expires. However, if the secret key expires, you receive errors.

     > **Note:**
     >
     > For security purposes, the expiration period cannot be more than two years from now.

   - **Authentication URL**. This field is automatically populated and isn't editable.
   - **Management URL**. This field is automatically populated and isn't editable.
   - **Storage suffix**. This field is automatically populated and isn't editable.

     Access to the following endpoints is required for creating an MCS catalog in Azure. Access to these endpoints optimizes connectivity between your network and the Azure portal and its services.

- Authentication URL: https://login.microsoftonline.com/
- Management URL: https://management.azure.com/. This is a request URL for Azure Resource Manager provider APIs. The endpoint for management depends on the environment. For example, for Azure Global, it is https://management.azure.com/, and for Azure US Government, it is https://management.usgovcloudapi.net/.
- Storage suffix: https://*.core.windows.net./. This (*) is a wildcard character for storage suffix. For example, https://demo.table.core.windows.net/.

5. After selecting **Save**, you're taken back to the **Connection Details** page. Select **Next** to proceed to the next page.
6. Configure the resources for the connection as follows:
   - On the **Region** page, select a region.
   - On the **Network** page, do the following:
     - Type a 1–64 character resource name to help identify the region and network combination. A resource name cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{ } "'()'`.
     - Select a virtual network/resource group pair. (If you have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If the region you selected on the previous page does not have any virtual networks, return to that page and select a region that has virtual networks.
7. On the **Summary** page, view a summary of settings and select **Finish** to complete your setup.

Manage service principals and connections

This section details how you can manage service principals and connections:

- Configure Azure throttling settings
- Enable Azure AD joined device management
- Manage service principal of an existing hosting connection
- Enable image sharing in Azure
- Add shared tenants to a connection using Full Configuration
- Implement image sharing using PowerShell
- Create a secure environment for Azure-managed traffic
- Manage the application secret and secret expiration date

Configure Azure throttling settings

Azure Resource Manager throttles requests for subscriptions and tenants, routing traffic based on defined limits, tailored to the specific needs of the provider. See Throttling Resource Manager requests on the Microsoft site for more information. Limits exist for subscriptions and tenants, where managing many machines can become problematic. For example, a subscription containing many machines might experience performance problems related to power operations.

> **Tip:**
>
> For more information, see Improving Azure performance with Machine Creation Services.

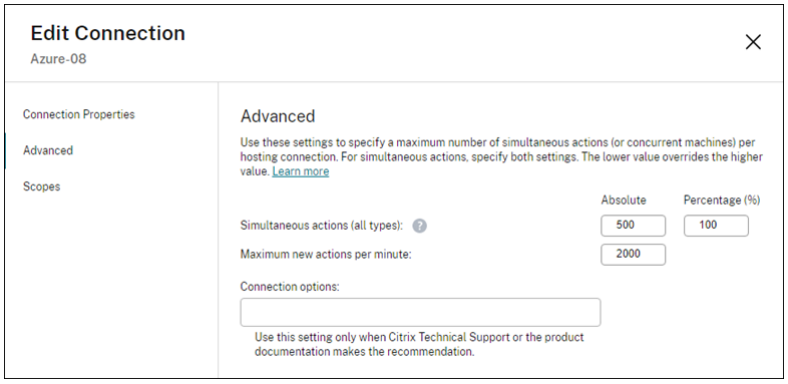
To help mitigate these issues, Citrix DaaS allows you to remove MCS internal throttling to use more of the available request quota from Azure.

We recommend the following optimal settings when powering VMs on or off in large subscriptions, for example, those containing 1,000 VMs:

- Absolute simultaneous operations: 500
- Maximum new operations per minute: 2000
- Max concurrency of operations: 500

Use the Full Configuration interface to configure Azure operations for a given host connection:

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select an Azure-related connection to edit it.
3. In the **Edit Connection** wizard, select **Advanced**.
4. On the **Advanced** page, use the configuration options to specify the number of simultaneous actions and maximum new actions per minute, and any additional connection options.



MCS supports 500 maximum concurrent operations by default. Alternatively, you can use the Remote PowerShell SDK to set the maximum number of concurrent operations.

Use the **PowerShell** property, `MaximumConcurrentProvisioningOperations`, to specify the maximum number of concurrent Azure provisioning operations. When using this property, consider:

- Default value of `MaximumConcurrentProvisioningOperations` is 500.
- Configure the `MaximumConcurrentProvisioningOperations` parameter using the PowerShell command `Set-item`.

Enable Azure AD joined device management

Stale Azure AD joined devices in Azure might prevent new machines from joining Azure AD, causing them to work improperly. To avoid potential issues, you can grant connections permission to manage Azure AD joined devices. With this permission, connections can automatically clean stale Azure AD joined devices.

> **Note:**
>
> Azure AD joined devices can't be deleted from Azure AD when you delete machines or machine catalogs.

1. From **Manage > Full Configuration**, select Hosting in the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.
3. Select **Connection Properties** from the left pane.
4. On the **Connection Properties** page that appears, follow these steps:
    a) Select **Enable Azure AD joined device management**.
    b) Click **Save**.
    c) In the Azure sign-in window that appears, enter your subscription password, and then click **Sign in**.

    After the sign-in completes, you're taken back to the list of hosting connections and resources. Click the connection in the list and then click the **Details** tab in the bottom pane. You can see that the **Azure AD joined device management** field shows **Enabled**.

When you enable Azure AD joined device management with Full Configuration, you must authenticate with Azure AD regardless of the host connection creation method you choose (create new or use existing). The Azure AD built-in **Cloud Device Administrator** role is assigned to the service principal. To adopt the minimal permissions for Azure AD joined device management, you can manually remove the assignment of **Cloud Device Administrator** role from the service principal and create an Azure AD custom role which only includes the minimal permissions and assign it to the service principal.

> **Note:**
>
> - The minimal permissions for Azure AD joined devices management are Azure AD permissions and not the Azure Resource Manager permissions. They cannot be explicitly assigned to a service principal. You must create a custom role in Azure AD which includes those per-

missions and assign it to the service principal. See Create and assign a custom role in Azure Active Directory for details.

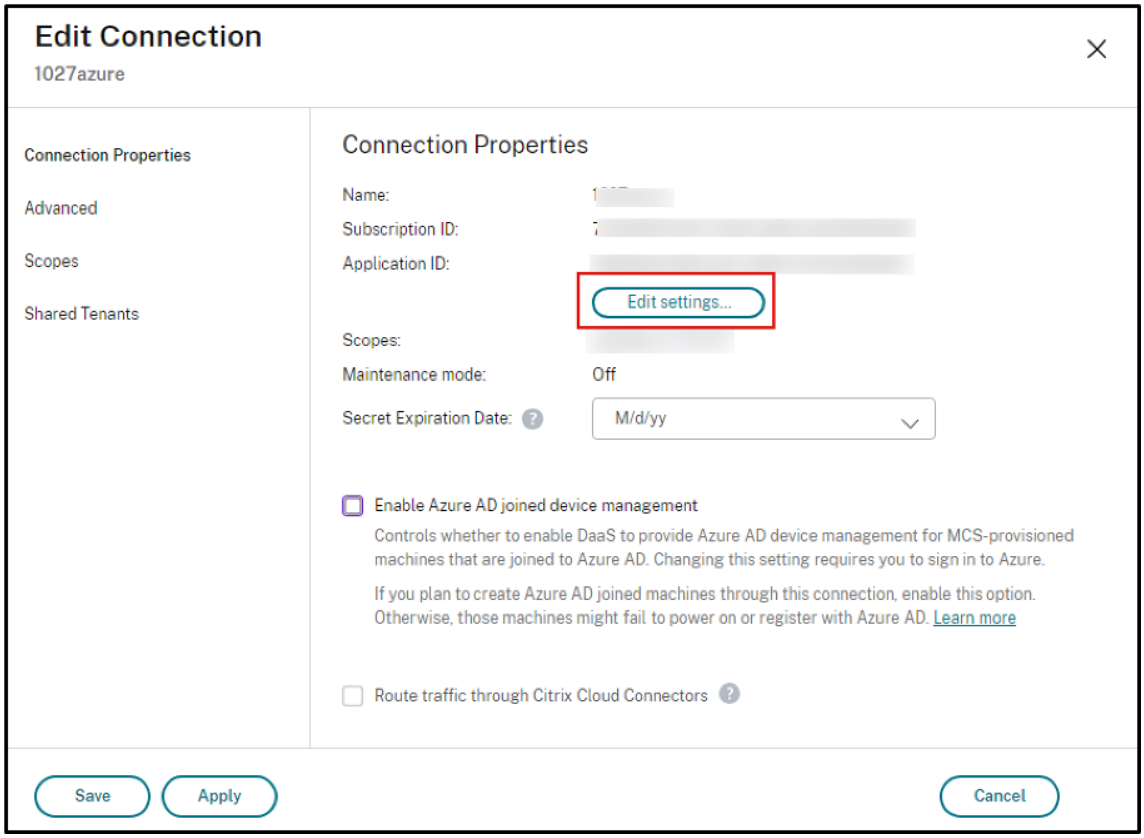
- To create a custom role in Azure AD, you need an Azure AD Premium P1 or P2 license.

Manage service principal of an existing hosting connection

After creating a hosting connection using a service principal, you can choose to edit the hosting connection to have:

- New service principal
- Use another existing service principal

1. From **Manage > Full Configuration**, select **Hosting** from the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.
3. Select **Connection Properties** from the left pane.
4. On the **Connection Properties** page that appears, click **Edit Settings**. You can now choose to create a new service principal or use another existing service principal.



- Click **Create service principal** to create a new service principal. Follow the prompt to log in to your Azure AD user account. Citrix uses the multi-tenant application ID `08b70dc3`

-76c5-4611-ba7d-3312ba36cb2b to create a new service principal for the existing host connection and grant proper permissions.

If you select **Enable Azure AD joined device management** on the **Connection Properties** page, then the Azure AD built-in Cloud Device Administrator role is assigned to the newly created service principal.

- Click **Use existing** to use another existing service principal for that hosting connection. However, there are two scenarios:
  - If you select **Enable Azure AD joined device management**, then you are prompted to log in to your Azure AD user account. Citrix uses the multi-tenant application ID 08b70dc3-76c5-4611-ba7d-3312ba36cb2b to assign the Azure AD built-in Cloud Device Administrator role to the existing service principal.
  - If you do not select **Enable Azure AD joined device management**, then you are not prompted to log in to your Azure AD user account. Enter the application ID and secret for that existing service principal.

To know about enabling Azure AD joined device management, see Enable Azure AD joined device management.

Enable image sharing in Azure

When creating or updating machine catalogs, you can select shared images from different Azure tenants and subscriptions (shared through the Azure Compute Gallery). To enable image sharing within or across tenants, you must make the necessary settings in Azure:

- Share images within a tenant (across subscriptions)
- Share images across tenants

Share images within a tenant (across subscriptions) To select an image in Azure Compute Gallery that belongs to a different subscription, the image must be shared with the service principal (SPN) of that subscription.

For example, if there is a service principal (SPN 1), which is configured in Studio as:

Service principal: SPN 1

Subscription: subscription 1

Tenant: tenant 1

The image is in a different subscription, which is configured in Studio as:

Subscription: subscription 2

Tenant: tenant 1

If you want to share the image in subscription 2 with subscription 1 (SPN 1), go to subscription 2, and share the resource group with SPN1.

The image must be shared with another SPN using Azure role-based access control (RBAC). Azure RBAC is the authorization system used to manage access to Azure resources. For more information on Azure RBAC, see the Microsoft document What is Azure role-based access control (Azure RBAC). To grant access, you assign roles to service principals at resource group scope with the Contributor role. To assign Azure roles, you must have `Microsoft.Authorization/roleAssignments/write` permission, such as User Access Administrator or Owner. For more information on sharing images with another SPN, see the Microsoft document Assign Azure roles using the Azure portal.

Share images across tenants To share images across tenants with Azure Compute Gallery, create an application registration.

For example, if there are two tenants (Tenant 1 and Tenant 2) and you want to share your image gallery with Tenant 1, then:

1. Create an application registration for Tenant 1. For more information, see Create the app registration.
2. Give Tenant 2 access to the application by requesting a sign-in using a browser. Replace `Tenant2 ID` with the tenant ID of Tenant 1. Replace `Application (client)ID` with the application ID of the application registration that you created. When done making the replacements, paste the URL into a browser and follow the sign-in prompts to sign into Tenant 2. For example:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
      client_id=<Application (client) ID>&response_type=code&
      redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   <!--NeedCopy-->
   ```

   For more information, see Give Tenant 2 access.
3. Give the application access to the Tenant 2 resource group. Sign in as Tenant 2 and give the application registration access to the resource group which has the gallery image. For more information, see Authenticate requests across tenants.

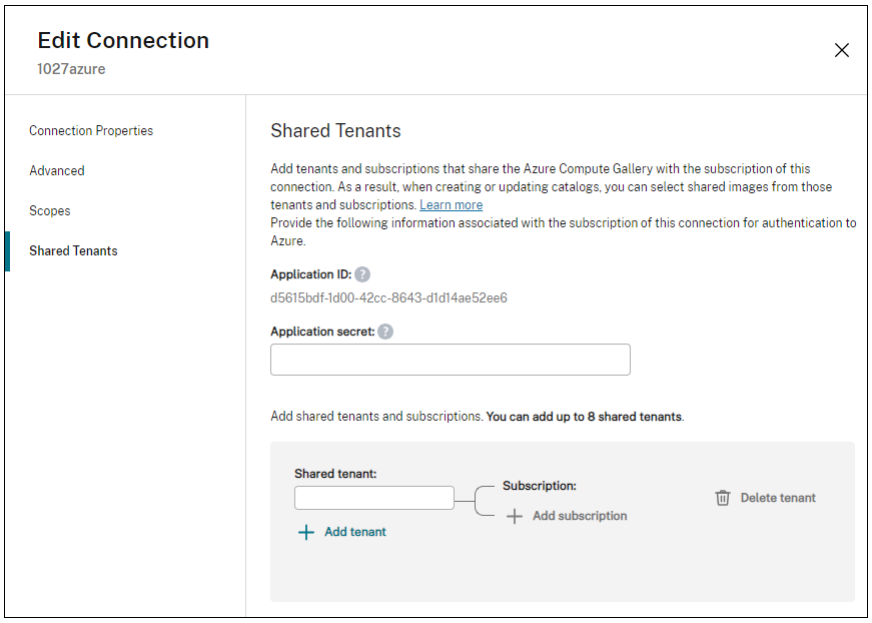
Add shared tenants to a connection using Full Configuration

When creating or updating machine catalogs in the Full Configuration interface, you can select shared images from different Azure tenants and subscriptions (shared through the Azure Compute Gallery). The feature requires that you provide shared tenant and subscription information for associated host connections.

> **Note:**
>
> Make sure you've configured the necessary settings in Azure to enable image sharing across tenants. For more information, see Share images across tenants.

Complete the following steps for a connection:

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.



3. In **Shared Tenants**, do the following:
   a) Provide the application ID and application secret associated with the subscription of the connection. DaaS uses this information to authenticate to Azure AD.
   b) Add tenants and subscriptions that share the Azure Compute Gallery with the subscription of the connection. You can add up to eight shared tenants and eight subscriptions for each tenant.
4. When you are finished, select **Apply** to apply the changes you made and keep the window open, or select **OK** to apply the changes and close the window.

Implement image sharing using PowerShell

This section guides you through the processes of sharing images using PowerShell:

- Select an image from a different subscription
- Update hosting connection custom properties with shared tenant IDs
- Select an image from a different tenant

Select an image from a different subscription You can select an image in Azure Compute Gallery that belongs to a different shared subscription in the same Azure tenant to create and update MCS catalogs using PowerShell commands.

1. In the hosting unit root folder, Citrix creates a new shared subscription folder called `sharedsubscription`.
2. List all shared subscriptions in a tenant.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
<!--NeedCopy-->
```

3. Select one shared subscription, and then list all shared resource groups of that shared subscription.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
<!--NeedCopy-->
```

4. Select a resource group, and then list all galleries of that resource group.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Select a gallery, and then list all image definitions of that gallery.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Select one image definition, and then list all image versions of that image definition.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
<!--NeedCopy-->
```

7. Create and update an MCS catalog using the following elements:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Update hosting connection custom properties with shared tenant IDs Use `Set-Item` to update the hosting connection custom properties with shared tenant IDs and subscription IDs. Add a property `SharedTenants` in `CustomProperties`. The format of `Shared Tenants` is:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

For example:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```

> **Note:**
>
> You can add more than one tenant. Each tenant can have more than one subscription.

Select an image from a different tenant You can select an image in the Azure Compute Gallery that belongs to a different Azure tenant to create and update MCS catalogs using PowerShell commands.

1. In the hosting unit root folder, Citrix creates a new shared subscription folder called `sharedsubscription`.
2. List all shared subscriptions.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
```



```
<!--NeedCopy-->
```

3. Select one shared subscription, and then list all shared resource groups of that shared subscription.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Select a resource group, and then list all galleries of that resource group.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Select a gallery, and then list all image definitions of that gallery.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Select one image definition, and then list all image versions of that image definition.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Create and update an MCS catalog using the following elements:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Create a secure environment for Azure-managed traffic

MCS enables network traffic (API calls from Citrix Cloud to Azure hypervisor) to be routed through Cloud Connectors in your environment. This implementation helps you lock down your Azure subscription to allow network traffic from specific IP addresses. To do this, add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`. After you set the custom properties, you can configure Azure policies to have private disk access to Azure managed disks.

If you configure the Azure policy to create Disk Accesses automatically for each new disk to use private endpoints, you cannot upload or download more than five disks or snapshots at the same time with the same disk access object as enforced by Azure. This limit is for each machine catalog if you configure Azure policy at resource group level, and for all machine catalogs if you configure Azure policy at subscription level.
If you do not configure the Azure policy to create Disk Accesses automatically for each new disk to use private endpoints, the limit of five concurrent operations is not enforced.

> **Note:**
>
> Currently, this feature is not supported for Connector Appliance. For Azure limitations related to this feature, see Restrict import/export access for managed disks using Azure Private Link.

Enable the proxy To enable the proxy, set the custom properties as follows on the host connection:

1. Open a PowerShell window using the Remote PowerShell SDK. For more information, see https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/.
2. Run the following commands:

```
Add-PSSnapin citrix*.
cd XDHyp:\Connections\
dir
<!--NeedCopy-->
```

3. Copy the `CustomProperties` from the connection to a notepad and append property setting `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughConn "Value="True"/>` to the `CustomProperties` to enable the proxy. For example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value="
    4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>
<!--NeedCopy-->
```


4. In the PowerShell window, assign a variable to the modified custom properties. For example:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value
    ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Run `$cred = Get-Credential`. If prompted, provide the connection credentials. The credentials are Azure Application ID and secret.

6. Run `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`.

> **Important:**
>
> If you get a message stating `SubscriptionId` is missing, then replace all double quotes (“) with backtick followed by double quotes (“”) in the custom property. For example:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`" xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
    Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
    Value=`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"
    AuthenticationAuthority`" Value=`"https://login.microsoftonline
    .com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value
    =`"core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"5
    cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"
    ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />
</CustomProperties>
<!--NeedCopy-->
```

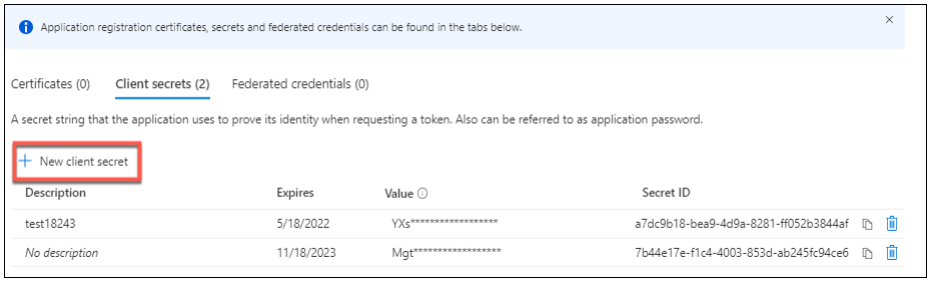
7. Run `dir` to verify the updated `CustomProperties` settings.

Manage the application secret and secret expiration date

Be sure to change the application secret for a connection before the secret expires. You receive an alert on the Full Configuration interface before the secret key expires.

Create an application secret in Azure You can create an application secret for a connection through the Azure portal.

1. Select **Azure Active Directory**.
2. From **App registrations** in Azure AD, select your application.
3. Go to **Certificates & secrets**.
4. Click **Client secrets > New client secret**.



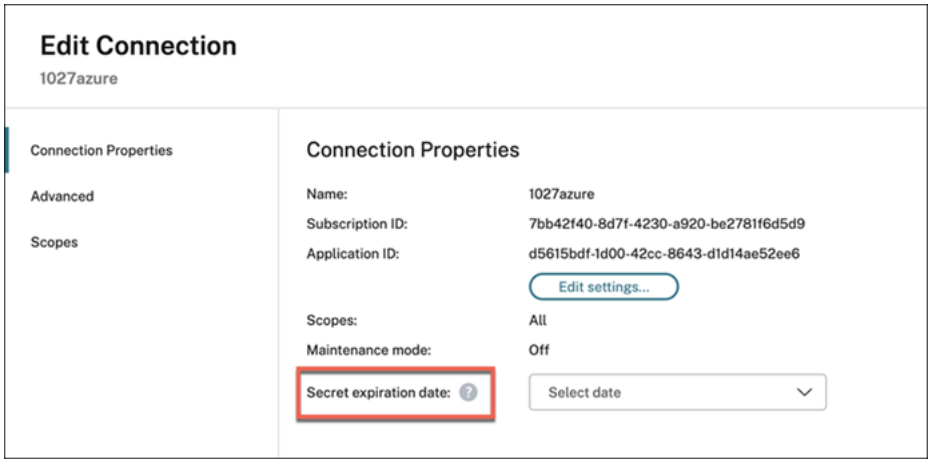
5. Provide a description of the secret and specify a duration. When you're done, select **Add**.

> **Note:**
>
> Be sure to save the client secret because you cannot retrieve it later.

6. Copy the client secret value and the expiration date.
7. In the Full Configuration interface, edit the corresponding connection and replace the content in the **Application secret** and **Secret expiration date** field with the values you copied.

Change the secret expiration date You can use the Full Configuration interface to add or modify the expiration date for the application secret in use.

1. In the **Add Connection and Resources** wizard, right-click a connection, and click **Edit Connection**.
2. On the **Connection Properties** page, click **Secret expiration date** to add or modify the expiration date for the application secret in use.



Required Azure permissions

This section details the minimum permissions and general permissions required for Azure.

Minimum permissions

Minimum permissions give better security control. However, new features that require additional permissions fail if only minimum permissions are given. This section lists minimum permissions by action.

Creating a host connection Add a host connection using the information obtained from Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/tenants/read"
<!--NeedCopy-->
```

Power management of VMs Power on or off the machine instances.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```


Creating, updating, or deleting VMs Create a machine catalog, then add, delete, update machines, and delete the machine catalog.

Following is the list of minimum permissions required when the master images are managed disks or snapshots that are in the same region as the hosting connection.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Features/providers/features/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

You need the following extra permissions based on minimal permissions for the following features:

- If the master image is a VHD in a storage account in the same region as the hosting connection:

  ```
  "Microsoft.Storage/storageAccounts/read",
  "Microsoft.Storage/storageAccounts/listKeys/action",
  <!--NeedCopy-->
  ```

- If the master image is an ImageVersion from the Azure Compute Gallery (formerly Shared Image

Gallery):

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- If the master image is a managed disk, snapshot, or VHD is in a region different from the region of the hosting connection:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
<!--NeedCopy-->
```

- If you use the Citrix-managed resource group:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- If you put the master image in Azure Compute Gallery (formerly Shared Image Gallery) in a shared tenant or subscription:

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
<!--NeedCopy-->
```

- If you use Azure dedicated host support:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- If you use Server Side Encryption (SSE) with Customer Managed Keys (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```


- If you deploy VMs using ARM templates (machine profile):

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
<!--NeedCopy-->
```

- If you use Azure template spec as a machine profile:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Creating, updating, and deleting machines with unmanaged disk Following is the list of minimum permissions required when the master image is VHD and use resource group as provided by admin:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```


Managing Azure AD joined devices Following is the list of minimal permissions required for managing the Azure AD joined devices:

```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```

General permissions

Contributor role has full access to manage all resources. This set of permissions does not block you from getting new features.

The following set of permissions provides the best compatibility going forward although it does include more permissions than needed with the current feature set:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
```



```
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Azure AD permission If you create Azure AD joined machine catalogs, then MCS is responsible for managing the Azure AD devices when you enable Azure AD joined device management. The Azure AD built-in **Cloud Device Administrator** role provides the best compatibility going forward although it does include more permissions than needed with the current feature set.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.

- For Azure-specific information, see Create a Microsoft Azure catalog.

More information

- Create and manage connections and resources
- Microsoft Azure Resource Manager virtualization environments

Connection to Microsoft System Center Virtual Machine Manager

December 11, 2023

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Microsoft System Center Virtual Machine Manager (VMM).

> **Note:**
>
> Before creating a connection to VMM, you need to first finish setting up your VMM as a resource location. See Microsoft System Center Virtual Machine Manager virtualization environments.

Create a connection

If you used MCS to provision VMs, do the following in the connection creation wizard:

- Enter the address as a fully qualified domain name of the host server.
- Enter the credentials for the administrator account that you set up earlier. This account must have permission to create new VMs.
- In the Host Details dialog box, select the cluster or standalone host to use when creating VMs.

  > **Important**
  >
  > Browse for a cluster or standalone host even if you are using a single Hyper-V host deployment.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For creating machine catalogs with MCS on SMB 3 file share, see Create a Microsoft System Center Virtual Machine Manager catalog.

More information

- Create and manage connections and resources
- Microsoft System Center Virtual Machine Manager virtualization environments.

Connection to Nutanix

December 19, 2023

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Nutanix.

> **Note:**
>
> Before creating a connection to Nutanix, you need to first finish setting up your Nutanix account as a resource location. See Nutanix virtualization environments.

Create a connection to Nutanix

The following information is a supplement to the guidance in Create and manage connections. To create a Nutanix connection, follow the general guidance in that article, minding the details specific to Nutanix.

In the **Add Connection and Resources** wizard, select the **Nutanix**connection type on the **Connection** page, and then specify the address and credentials, plus a name for the connection. On the **Network** page, select a network for the hosting unit.

The following connection types are available for selection: **Nutanix AHV**, **Nutanix AHV DRaaS**, and **Nutanix AHV PC**.

- For **Nutanix AHV**, specify the Prism Element (PE) cluster address and credentials.
- For **Nutanix AHV PC**, specify the hypervisor address and credentials.

  > **Note:**
  >
  > Currently, the connection type **Nutanix AHV PC** is only used for creating connection to Nutanix Cloud Cluster (NC2) on Azure. Also, a machine catalog can only be hosted on a single cluster in a NC2 on Azure connection.

- For **Nutanix AHV DRaaS**, specify your address and user name, and then import the public and private keys contained in your Nutanix DRaaS credential files (`.pem`). (Public and private keys are generated in Nutanix DRaaS cloud by Nutanix DRaaS administrators.)

- To import the key, locate your credential file, open it with Notepad (or any text editor), and then copy the content. After that, return to the **Connection** page, select **Import key**, paste the content, and then select **Save**.

Caution: Do not change the credential content or its format.

> **Tip:**
>
> If you deploy machines using Nutanix AHV (Prism Element) as the resource, select the container where the VM's disk resides.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Nutanix specific information, see Create a Nutanix catalog.

More information

- Create and manage connections and resources
- Nutanix virtualization environments
- Nutanix cloud and partner solutions

Connection to Nutanix cloud and partner solutions

December 11, 2023

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Nutanix cloud and partner solutions.

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) supports the following Nutanix cloud and partner solution:

- Nutanix Cloud Clusters on AWS

> **Note:**
>
> - Before creating a connection to Nutanix cloud and partner solution, you must first finish setting up your respective account as a resource location. See Nutanix cloud and partner solutions.

> - For the latest information about setting up Nutanix on-cloud, follow the Nutanix latest guide.

Connect to Nutanix Prism

After you create a Nutanix cluster, connect to Nutanix Prism.
To connect to Nutanix Prism:

1. Create a bastion VM in the 10.0.129.0/24 subnet.
2. RDP into the bastion VM, go to the URL of the **Prism Element** you copied in the previous section.
3. Log in using the default credentials: `admin:nutanix/4u`. Remember to change the password.

Create a VM on the Nutanix Cluster

After connecting to **Nutanix Prism**, create VMs on the Nutanix cluster.

If the VM needs Internet access

1. Go to the AWS console.
2. Create a new subnet 10.0.130.0/24 in the same VPC as the one created by Nutanix CFS.
3. Add a route to the route table of this subnet to direct all none local traffic to the NAT gateway above.
4. RDP into the bastion VM, go to the URL of the **Prism Element** you copied in the previous section and login.
5. Add a new network. Go to **Settings>Network Configuration>Create Subnet**. Use the same subnet 10.0.130.0/24 used in AWS.
6. Create all the VMs (AD, CC, VDA, and so on) in that new subnet.

If the VM does not need Internet access

1. RDP into the bastion VM, go to the URL of the **Prism Element** you copied in the previous section and login.
2. Add a new network. Go to **Settings>Network Configuration>Create Subnet**. Use the subnet 10.0.129.0/24.
3. Create all the VMs (AD, CC, VDA, and so on) in that subnet.

> **Tip:**
>
> Make sure that the time and timezone information in the VMs are set up correctly. This is especially true for AD.

Create host connection

1. From **Manage > Full Configuration**, select **Hosting** in the left pane.
2. Click **Add Connection and Resources**.
3. On the **Connection** screen, select **Create a new Connection**, and in the **Connection address**, enter `https://xxx.xxx.xxx.xxx:9440`.
4. Follow the UI to complete the wizard.

> **Note:**
>
> All connector VMs must have the Nutanix plug-in installed for the Nutanix option to be available in Citrix Studio, even if the plug-ins are not used in the Nutanix zone.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Nutanix specific information, see Create a Nutanix catalog.

More information

- Create and manage connections and resources
- Nutanix virtualization environments
- Nutanix cloud and partner solutions

Connection to VMware

June 6, 2024

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to VMware virtualization environments.

> **Note:**

> Before creating a connection to VMware, you need to first finish setting up your VMware account as a resource location. See VMware virtualization environments.

Required permissions

Create a VMware user account and one or more VMware roles with a set or all permissions listed in this article. Base the roles' creation on the specific level of granularity required over the user's permissions to request the various Citrix DaaS operations at any time. To grant the user-specific permissions at any point, associate them with the respective role, at the data center level at a minimum, with the **Propagate to children** option selected.

The following tables show the mappings between Citrix DaaS operations and the minimum required VMware permissions.

Add connections and resources

SDK	User interface
System.Anonymous, System.Read, and System.View	Added automatically. Can use the built-in read-only role.

Power management

SDK	User interface
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
Datastore.Browse	Datastore > Browse datastore

Provision machines (Machine Creation Services)

To provision machines using MCS, the following permissions are mandatory:

SDK	User interface
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
Virtual machine.Config.Add or remove device	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

SDK	User interface
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot; vSphere 8.0: Virtual machine > Snapshot management > Create snapshot

Image update and rollback

SDK	User interface
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Delete provisioned machines

SDK	User interface
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Storage Profile (vSAN)

To view, create, or delete storage policies during catalog creations on a vSAN datastore, the following permissions are mandatory:

SDK	User interface
StorageProfile.Update	PROFILE-DRIVEN STORAGE > Profile-driven storage update. For vSphere 8: VM storage policies > Update VM storage policies
StorageProfile.View	PROFILE-DRIVEN STORAGE > Profile-driven storage view. For vSphere 8: VM storage policies > View VM storage policies

Tags and Custom Attributes

Tags and custom attributes allow you to attach metadata to the VMs created in vSphere inventory and make it easier to search and filter these objects. To create, edit, assign, and delete tags or categories, the following permissions are mandatory:

SDK	User interface
InventoryService.Tagging.CreateTag	vSphere Tagging > Create vSphere Tag
InventoryService.Tagging.CreateCategory	vSphere Tagging > Create vSphere Tag Category
InventoryService.Tagging.EditTag	vSphere Tagging > Edit vSphere Tag
InventoryService.Tagging.EditCategory	vSphere Tagging > Edit vSphere Tag Category

SDK	User interface
InventoryService.Tagging.DeleteTag	vSphere Tagging > Delete vSphere Tag
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Delete vSphere Tag Category
InventoryService.Tagging.AttachTag	vSphere Tagging > Assign or Unassign vSphere Tag
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Assign or Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

> **Note:**
>
> When MCS creates a machine catalog, it tags the target VMs with special name tags. These tags differentiate the master image from MCS created VMs and prevent using MCS created VMs for image preparation. You can identify the difference by the value of `XdProvisioned` attribute in vCenter. The attribute is set to **True** if MCS creates VMs.

Cryptographic operations

Cryptographic operations privileges control who can perform which type of cryptographic operation on which type of object. vSphere Native Key Provider uses the `Cryptographer.*` privileges. The following minimum permissions are required for cryptographic operations:

> **Note:**
>
> These permissions are required for creating MCS machine catalogs with vTPM equipped VM.

SDK	User interface
Cryptographer.Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographer.AddDisk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographer.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographer.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt

SDK	User interface
Cryptographer.EncryptNew	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographer.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographer.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographer.ReadKeyServersInfo	Privileges > All Privileges > Cryptographic operations > Read KMS information

Provision machines (Citrix Provisioning)

These permissions to clone and deploy a template are required to provision VMs using Citrix Virtual Apps and Desktops Setup Wizard and Export Devices Wizard through the Citrix Provisioning console. Set the permissions while creating a hosting connection.
You need all the permissions from Provision machines (Machine Creation Services) and the following.

SDK	User interface
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
VApp.Export	vApp > Export

> **Note:**
>
> The `VApp.Export` is required for creating MCS machine catalogs using machine profile.

Securing connections to the VMware environment

Using `HTTPS` / `SSL` connections to vCenter requires that the connection is trusted by Citrix DaaS.

There are two options:

- (Recommended) The Citrix DaaS database has the SSL thumbprint installed. This thumbprint is used by Citrix DaaS on each Cloud Connector to trust connections to vCenter.
- (Alternative) Each Cloud Connector trusts the vCenter certificate, and services on the Cloud Connector reuses this trust. This trust can be from:
  - vCenter certificate, issued by the Certificate Authority and trusted by windows, resulting in established trust between Windows and vCenter.
  - vCenter certificate installed on Windows, resulting in established trust between Windows and vCenter.OT

> **Note:**
>
> vCenter certificate and VMware SSL thumbprint are not required for VMware Cloud and its partner solutions.

VMware SSL thumbprint

The VMware SSL thumbprint feature addresses a frequently reported error when creating a host connection to a VMware vSphere hypervisor. Previously, administrators had to manually create a trust relationship between the Citrix-managed Delivery Controllers in the Site and the hypervisor's certificate before creating a connection. The VMware SSL thumbprint feature removes that manual requirement: the untrusted certificate's thumbprint is stored on the Site database so that the hypervisor can be continuously identified as trusted by Citrix DaaS, even if not by the Controllers.

When creating a vSphere host connection, a dialog box allows you to view the certificate of the machine you are connecting to. You can then choose whether to trust it.

The VMware SSL thumbprint can be updated later using PowerShell SDK `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>`.

> **Tip:**
>
> The certificate thumbprint must be written in capital letters.

Obtain and import a certificate

To protect vSphere communications, Citrix recommends that you use HTTPS rather than HTTP. HTTPS requires digital certificates. Citrix recommends you use a digital certificate issued from a certificate authority in accordance with your organization's security policy.

If you are unable to use a digital certificate issued from a certificate authority, and your organization's security policy permits it, you can use the VMware-installed self-signed certificate. Add the VMware vCenter certificate to each Cloud Connector.

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the host file on that server, located at %SystemRoot%/WINDOWS/system32/Drivers/etc/. This step is required only if the FQDN of the computer running vCenter Server is not already present in the domain name system.
2. Obtain the vCenter certificate using any of the following three methods:

   From the vCenter server:

   a) Copy the file rui.crt from the vCenter server to a location accessible on your Cloud Connectors.
   b) On the Cloud Connector, navigate to the location of the exported certificate and open the rui.crt file.

   Download the certificate using a web browser: If you are using Internet Explorer, depending on your user account, you must right-click on Internet Explorer and choose **Run as Administrator** to download or install the certificate.

   a) Open your web browser and make a secure web connection to the vCenter server (for example https://server1.domain1.com).
   b) Accept the security warnings.
   c) Click the address bar displaying the certificate error.
   d) Click **Certificate is not valid**, and then click the **Details** tab.
   e) Click **Export..**
   f) Save the exported certificate.
   g) Navigate to the location of the exported certificate and open the .CER file.

   Import directly from Internet Explorer running as an administrator:

   a) Open your web browser and make a secure web connection to the vCenter server (for example https://server1.domain1.com).
   b) Accept the security warnings.
   c) Click the address bar displaying the certificate error.
   d) View the certificate.

3. Import the certificate into the certificate store on each Cloud Connector.

   a) Click **Install certificate**, select **Local Machine**, and then click **Next**.
   b) Select **Place all certificates in the following store**, and then click **Browse**. On a later supported version: Select **Trusted People** and then click **OK**. Click **Next** and then click **Finish**.

> **Important:**
>
> If you change the name of the vSphere server after installation, you must generate a new self-signed certificate on that server before importing the new certificate.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For VMware specific information, see Create a VMware catalog.

More information

- Create and manage connections and resources
- VMware virtualization environments.
- VMware cloud and partner solutions

Connection to VMware cloud and partner solutions

December 11, 2023

After setting up Azure VMware Solution (AVS) cluster, Google Cloud VMware Engine, and VMware cloud on AWS, create the connections. See Connection to VMware virtualization environments for creating connections.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For VMware specific information, see Create a VMware catalog.

More information

- Create and manage connections and resources
- VMware virtualization environments.
- VMware cloud and partner solutions

Connection to XenServer

April 8, 2024

Create and manage connections and resources provides detailed instructions using the wizard to create a connection. Before establishing a connection to XenServer (formerly Citrix Hypervisor), you need to first finish setting up your XenServer as a host. See Add a resource type or activate an unused domain in Citrix Cloud.

Create a connection to XenServer

When you create a connection to XenServer, you must provide the credentials for a Virtual Machine Power Administrator (VM Power Admin) or higher-level user.

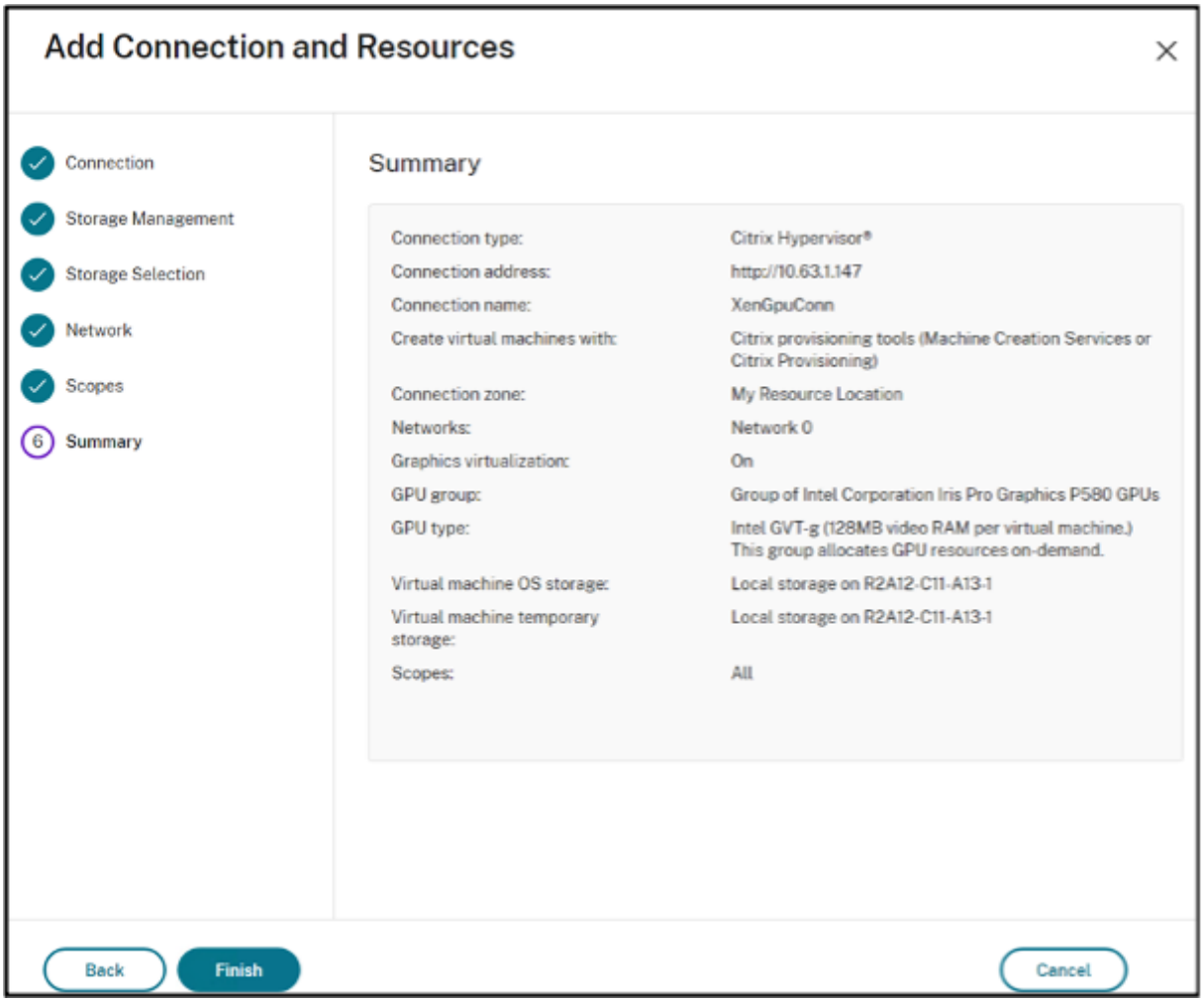
Citrix recommends using HTTPS to secure communications with XenServer. To use HTTPS, you must replace the default TLS certificate installed on XenServer. For more information, see Install a TLS certificate on your server.

You can configure high availability if it is enabled on the XenServer server. Citrix recommends that you select all servers in the pool (from **Edit High Availability**) to allow communication with the XenServer server if the pool master fails.

> **Note:**
>
> If you are using HTTPS and want to configure high-availability servers, do not install a wildcard certificate for all servers in a pool. An individual certificate for each server is required.

When using local storage on one or more XenServer hosts for temporary data storage, make sure that each storage location in the pool has a unique name. (To change a name in XenCenter, right-click the storage and edit the name property.)

If you connect to the XenServer that supports vGPU, you can verify the GPU group and the GPU type in the **Summary** page of the wizard for creating a connection.



Use IntelliCache for XenServer connections

Using IntelliCache, hosted VDI deployments are more cost-effective because you can use a combination of shared storage and local storage. This enhances performance and reduces network traffic. The local storage caches the master image from the shared storage, which reduces the amount of reads on the shared storage. For shared desktops, writes to the differencing disks are written to local storage on the host and not to shared storage.

The important considerations are:

- Shared storage must be NFS when using IntelliCache.
- Citrix recommends that you use a high-performance local storage device to ensure the fastest possible data transfer.

To use IntelliCache, enable IntelliCache as detailed:

- When installing XenServer, select **Enable thin provisioning**. See Install the XenServer host for

information on installing XenServer host from local media. Citrix does not support mixed pools of servers with some servers that have IntelliCache enabled and some servers that do not IntelliCache enabled.

- In Citrix DaaS, IntelliCache is disabled by default. You can change the setting only when creating a XenServer connection. You cannot disable IntelliCache later. When you create a XenServer connection:
  - Select **Shared** as the storage type.
  - Select the **Use IntelliCache** checkbox.

See IntelliCache for more information.

Required XenServer permissions

The XenServer permissions are role-based (RBAC). The Role-Based Access Control (RBAC) feature in XenServer allows you to assign users, roles, and permissions to control who has access to your XenServer and what actions they can perform. The XenServer RBAC system maps a user (or a group of users) to defined roles (a named set of permissions). The roles have associated XenServer permissions to perform certain operations.

For more information, see Role-based access control.

The role hierarchy, in order of increasing permissions is: Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin.

The following section summarizes the minimum role required for each provisioning task.

Creating a host connection

Task	Minimum role required
Add a host connection using the information obtained from XenServer	Read-Only
View users and their assigned role	Read-Only

Power management of VMs

Task	Minimum role required
Power on or off the VMs	VM Operator

Creating, updating, or deleting VMs

Task	Minimum role required
Add or remove VMs to existing snapshots schedules	VM Power Admin
Add, modify, delete snapshot schedules	Pool Operator
Publish master image	Pool Operator (Requires switch-port locking)
Create a machine catalog	Pool Operator: Requires switch-port locking
Add or remove VMs (not GPU enabled VMs)	VM Admin
Add or remove VMs (GPU enabled VMs)	Pool Operator
Add, remove, or configure virtual disk or CD devices	VM Admin
Manage Tags	VM Operator

For more information on RBAC roles and permissions, see RBAC roles and permissions.

For information on switch port locking, see Use switch port locking.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For XenServer specific information, see Create a XenServer catalog.

More information

- Create and manage connections and resources
- XenServer virtualization environments

Create machine catalogs

July 2, 2024

> **Note:**
>
> This article describes how to create catalogs using the Full Configuration interface. If you're using Quick Deploy to create Azure resources, follow the guidance in Create catalogs using Quick

> Deploy.

Collections of physical or virtual machines are managed as a single entity called a machine catalog. Within a machine catalog, all machines share a common operating system type, which can be either multi-session OS or single-session OS, such as Windows or Linux-based systems.

The **Manage > Full Configuration** interface guides you to create the first machine catalog. After you create the first catalog, you create the first delivery group. Later, you can change the catalog you created, and create more catalogs.

Overview

When you create a catalog of VMs, you specify how to provision those VMs. You can use Machine Creation Services (MCS). Or, you can use your own tools to provide machines.

- If you use MCS to provision VMs, you provide an image (or snapshot) to create identical VMs in the catalog. Before you create the catalog, you must set up a hosting connection for the first time to the hypervisor or cloud service of choice and then you must create and configure the master image on the same. Configuring the master image requires tasks such as domain joining when necessary, installing required drivers, applications to be published, and deploying the Virtual Delivery Agent (VDA) on the image.
- After you create the master image, you then create the machine catalog in the **Manage > Full Configuration** interface. You select that image (or a snapshot of an image), specify the number of VMs to create in the catalog, and configure additional information.
- If your machines are already available, you must still create one or more machine catalogs to import these VMs into the catalog.

When using MCS to create the first catalog, you specify a hosting unit that you created previously. Hosting unit provide resource configuration for you to create virtual machine. Later (after you create your first catalog and delivery group), you can change information about that hosting unit or its parent host connection or create more connections and hosting units.

If a Cloud Connector is not operating properly, MCS provisioning operations (such as catalog updates) take longer than usual, and the management interface's performance degrades significantly.

RDS license check

Creation of a machine catalog containing Windows multi-session OS machines includes an automatic check for valid Microsoft RDS licenses. The catalog is searched for a powered-on and registered machine to do the check on.

- If a powered-on and registered machine cannot be found, a warning is displayed, explaining that the RDS licensing check cannot be performed.
- If a machine is found and an error is detected, **Manage > Full Configuration** displays a warning message for the catalog containing the detected issue. To remove an RDS license warning from a catalog (so that it no longer appears in the display), select the catalog. Select **Remove RDS license warning**. When prompted, confirm the action.

VDA registration

A VDA must be registered with a Cloud Connector to be considered when launching brokered sessions. Unregistered VDAs can result in underutilization of otherwise available resources. There are various reasons that a VDA might not be registered, many of which you can troubleshoot. Troubleshooting information is provided in the catalog creation wizard, and after you add a catalog to a delivery group.

In the catalog creation wizard, after you add existing machines, the list of computer account names indicates whether each machine is suitable for adding to the catalog. Hover over the icon next to each machine to display an informative message about that machine.

If the message identifies a problematic machine, you can either remove that machine (using the **Remove** button), or add the machine. For example, if a message indicates that information cannot be obtained about a machine (perhaps because it was never registered), you might choose to add the machine anyway.

For more information about VDA registration troubleshooting, see CTX136668.

MCS catalog creation summary

Here's a brief overview of default MCS actions after you provide information in the catalog creation wizard.

- If you select an image (rather than a snapshot), MCS creates a snapshot.
- MCS creates a full copy of the snapshot and places the copy on each storage location defined in the host connection.
- MCS adds the machines to Active Directory, which creates unique identities.
- MCS creates the number of VMs specified in the wizard, with two disks defined for each VM. In addition to the two disks per VM, full copy of the snapshot or master image is also stored in the same storage location. If you have multiple storage locations defined, each gets the following disk types:
  - The full copy of the snapshot (noted above), which is read-only and shared across the just-created VMs.

  - A unique 16 MB identity disk that gives each VM a unique identity. Each VM gets an identity disk.
  - A unique difference disk to store writes made to the VM. This disk is thin provisioned (if supported by the host storage) and increases to the maximum size of the master image, if necessary. Each VM gets a differencing disk. The difference disk holds changes made during sessions. It is permanent for dedicated desktops. For pooled desktops, it is deleted and a new one created after each restart.

Alternatively, when creating VMs to deliver static desktops, you can specify (on the **Machines** page of the catalog creation wizard) thick (full copy) VM clones. Full clones do not require retention of the master image on every data store. Each VM has its own file.

MCS storage considerations

There are many factors when deciding on storage solutions, configurations, and capacities for MCS. The following information provides proper considerations for storage capacity:

Capacity considerations:

- Disks

  The Delta or Differencing (Diff) Disks consume the largest amount of space in most MCS deployments for each VM. Each VM created by MCS is given at minimum 2 disks upon creation.

  - Disk0 = Diff Disk: contains the OS when copied from the base master image.
  - Disk1 = Identity Disk: 16 MB - contains Active Directory data for each VM.

  As the product evolves, you might have to add more disks to satisfy certain use cases and feature consumption. For example:

  - MCS Storage Optimization creates a write cache style disk for each VM.
  - MCS added the ability to use full clones as opposed to the Delta disk scenario described in the previous section.

  Hypervisor features might also enter into the equation. For example:

  - XenServer IntelliCache creates a Read Disk on local storage for each XenServer. This option saves on IOPS against the image which might be held on the shared storage location.

- Hypervisor overhead

  Different hypervisors use specific files that create overhead for VMs. Hypervisors also use storage for management and general logging operations. Calculate the space to include overhead for:

  - Log files

  - Hypervisor-specific files. For example:
    * VMware adds more files to the **VM storage** folder. See VMware Best Practices.
    * Calculate your total virtual machine size requirements. Consider a virtual machine containing 20 GB for the virtual disk, 16 GB for the swap file, and 100 MB for log files consuming 36.1 GB total.
  - Snapshots for XenServer; Snapshots for VMware.

- Process overhead

  Creating a catalog, adding a machine, and updating a catalog have unique storage implications. For example:

  - Initial catalog creation requires a copy of the base disk to be copied to each storage location.
    * It also requires you to create a Preparation VM temporarily.
  - Adding a machine to a catalog does not require copying of the base disk to each storage location. Catalog creation varies based on the features selected.
  - Updating the catalog to create an extra base disk on each storage location. Catalog updates also experience a temporary storage peak where each VM in the catalog has 2 Diff disks for a certain amount of time.

More considerations:

- **RAM sizing:** Affects the size of certain hypervisor files and disks, including I/O optimization disks, write cache, and snapshot files.
- **Thin / Thick provisioning:** NFS storage is preferred due to the thin provisioning capabilities.

Machine Creation Services (MCS) storage optimization

The Machine Creation Services (MCS) storage optimization feature is also known as MCS I/O. This feature is only available on Azure, GCP, XenServer, VMware, and SCVMM.

- The write cache container is *file-based*, the same functionality found in Citrix Provisioning. For example, the Citrix Provisioning write cache file name is `D:\vdiskdif.vhdx` and the MCS I/O write cache file name is `D:\mcsdif.vhdx`.
- Achieve diagnostic improvements by including support for a Windows crash dump file written to the write cache disk.
- MCS I/O retains the technology *cache in RAM with overflow to hard disk* to provide the most optimal multi-tier write cache solution. This functionality allows an administrator to balance between the cost in each tier, RAM and disk, and performance to meet the desired workload expectation.

Updating the write cache method from *disk-based* to *file-based* requires the following changes:

1. MCS I/O no longer supports RAM only cache. Specify a disk size during machine catalog creation.
2. The VM write cache disk is created and formatted automatically when booting a VM for the first time. Once the VM is up, the write cache file `mcsdif.vhdx` is written into the formatted volume `MCSWCDisk`.
3. The pagefile is redirected to this formatted volume, `MCSWCDisk`. As a result, this disk size considers the total amount of disk space. It includes the delta between the disk size and the generated workload plus the pagefile size. This is typically associated with VM RAM size.

Enable MCS storage optimization updates To enable the MCS I/O storage optimization feature, upgrade the Delivery Controller and the VDA to the latest version of Citrix DaaS.

> **Note:**
>
> If you upgrade an existing deployment which has MCS I/O enabled, no additional configuration is required. The VDA and the Delivery Controller upgrade handle the MCS I/O upgrade.

For information on assigning a drive letter to write-back cache disk, see Assign a specific drive letter to MCS I/O write-back cache disk.

Prepare a master image on the hypervisor or cloud service

The master image contains the operating system, non-virtualized applications, VDA, and other software.

Good to know:

- A master image might also be known as a clone image, golden image, base VM, or base image. Host vendors and cloud service providers may use different terms.
- Ensure that the hypervisor or cloud service has enough processors, memory, and storage to accommodate the number of machines created.
- Configure the correct amount of hard disk space needed for desktops and applications. That value cannot be changed later or in the machine catalog.
- Remote PC Access machine catalogs do not use master images.
- Microsoft KMS activation considerations when using MCS: If your deployment includes 7.x VDAs with a XenServer 6.1 or 6.2, vSphere, or Microsoft System Center Virtual Machine Manager host, you do not need to manually rearm Microsoft Windows or Microsoft Office.

Install and configure the following software on the master image:

- Integration tools for your hypervisor (such as Citrix VM Tools, Hyper-V Integration Services, or VMware tools). If you omit this step, applications and desktops might not function correctly.

- A VDA. Citrix recommends installing the latest version of VDA to allow access to the newest features. Failure to install a VDA on the master image causes the catalog creation to fail.
- Third-party tools as needed, such as antivirus software or electronic software distribution agents. Configure services with settings that are appropriate for users and the machine type (such as updating features).
- Third-party applications that you are not virtualizing. Citrix recommends virtualizing applications. Virtualizing reduces costs by eliminating having to update the master image after adding or reconfiguring an application. Also, fewer installed applications reduce the size of the master image hard disks, which saves storage costs.
- App-V clients with the recommended settings, if you plan to publish App-V applications. The App-V client is available from Microsoft.
- When using MCS, if you localize Microsoft Windows, install the locales and language packs. During provisioning, when a snapshot is created, the provisioned VMs use the installed locales and language packs.

> **Important:**
>
> If you are using MCS, do not run Sysprep on master images.

To prepare a master image:

1. Using your hypervisor's management tool, create a master image and then install the operating system, and all service packs and updates. Specify the number of vCPUs. You can also specify the vCPU value if you create the machine catalog using PowerShell. You cannot specify the number of vCPUs when creating a catalog from **Manage > Full Configuration**. Configure the amount of hard disk space needed for desktops and applications. That value cannot be changed later or in the catalog.
2. Ensure that the hard disk is attached at device location 0. Most standard master image templates configure this location by default, but some custom templates might not.
3. Install and configure the software listed above on the master image.
4. If you are not using MCS, join the master image to the domain where applications and desktops are members. Ensure that the master image is available on the host where the machines are created. If you are using MCS, joining the master image to a domain is not required. The provisioned machines are joined to the domain specified in the catalog creation wizard.
5. Citrix recommends that you create and name a snapshot of your master image so that it can be identified later. If you specify a master image rather than a snapshot when creating a catalog, the management interface creates a snapshot, but you cannot name it.

Volume licensing activation

MCS supports volume licensing activation to automate and manage the activation of Windows operating systems and Microsoft Office. The three models that MCS supports for volume licensing activation are:

- Key Management Service (KMS)
- Active Directory-based activation (ADBA)
- Multiple Activation Key (MAK)

You can change the activation setting after you create the machine catalog.

Key Management Service (KMS)

The KMS is a lightweight service that does not require a dedicated system and can easily be co-hosted on a system that provides other services. This functionality is supported on all Citrix supported Windows versions. During image preparation, MCS does the Microsoft Windows and Microsoft Office KMS rearm. You can skip rearm by running the command `Set-Provserviceconfigurationdata`. For more information on Microsoft Windows KMS Rearm and Microsoft Office KMS Rearm during image preparation, see Machine Creation Services: Image Preparation Overview and Fault-Finding. For more information on KMS activation, see Activate using Key Management Service.

> **Note:**
>
> All machine catalogs created after running the command `Set-Provserviceconfigurationdata` have the same setting as provided in the command.

Active Directory-based activation (ADBA)

ADBA enables you to activate machines through their domain connections. Machines are immediately activated when they join the domain. These machines remain activated as long as they remain joined to the domain and in contact with it. This functionality is supported on all Citrix supported Windows versions except Windows server 2022. For more information on Active directory-based activation, see Activate using Active Directory-based activation.

Multiple Activation Key (MAK)

MAK is a way of activating volume and authenticating the Windows system with the help of the Microsoft server. You must buy the MAK key from Microsoft which is assigned with a fixed number of activation counts. Every time a Windows system is activated, the activation count reduces. There are two ways of activating the system:

- Online Activation: If the Windows system that you want to activate has internet access, the system automatically activates the Windows on installing the product key. This process reduces the activation count by 1 for the corresponding MAK.
- Offline Activation: If the Windows system is not able to connect to the internet to do the online activation, MCS gets a confirmation id and an installation id from the Microsoft server to get the Windows system activated. This way of activation is useful for non-persistent machine catalogs.

> **Note:**
>
> - MCS doesn't support Microsoft Office activation using MAK.
> - Minimum VDA version required is 2303.

Key requirements

- The Delivery Controller must have internet access.
- Create a new catalog if the new image to be updated has a different MAK Key from the original.
- Install the MAK key on the master image. See Deploy MAK Activation for the steps to install MAK Key on a Windows System.
- If you are not using image preparation:
  1. Add the registry DWORD value `Manual` under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
  2. Set the value to `1`.

Activation Counts To view the number of activations remaining for MAK Key or to check if a VM is consuming two or more activations, use the Volume Activation Management Tool (VAMT). See Install VAMT.

Activate the Windows system using MAK To activate the Windows system using MAK:

1. Install the product key on the master image. This step consumes one activation count.
2. Create an MCS machine catalog.
3. If you aren't using image preparation:
   a) Add the registry DWORD value `Manual` under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
   b) Set the value to `1`.

This method disables the option of online activation.

4. Add VMs to the machine catalog.
5. Power on the VMs.
6. Depending on whether it's online or offline activation, the Windows system is activated.

    - If the activation is online, the Windows system is activated after the product key is installed.
    - If the activation is offline, MCS communicates with provisioned VMs to get the activation status of the Windows system. MCS then retrieves a confirmation id and an installed id from the Microsoft server. These IDs are used to activate the Windows system.

Troubleshooting If the provisioned VM is not activated with the installed MAK Key, run `Get-ProvVM` or `Get-ProvScheme` command on a PowerShell window.

- The `Get-ProvScheme` command: See the parameter `WindowsActivationType` associated with the MCS machine catalog from the latest master image.
- The `Get-ProvVM` command. See the parameters `WindowsActivationType`, `WindowsActivationS`, `WindowsActivationStatusErrorCode`, and `WindowsActivationStatusError`.

You can check the error and verify the steps to resolve the issue.

Create a machine catalog using the Full Configuration interface

Before creating a catalog:

- Ensure that you have created a connection to the hypervisor, cloud service, other resource that hosts your machines.
- If you have created a master image to provision machines. Ensure that you have installed a VDA on that master image.

> **Note:**
>
> When you are using a cloud service or hypervisor to host VMs, the catalog creation wizard might contain extra pages specific to that host. For example, when using an Azure Resource Manager master image, the catalog creation wizard contains a **Storage and License Types** page. For host-specific information, see the specific articles as mentioned in Where to go next.

Launch the catalog creation wizard

1. Sign in to Citrix Cloud. In the upper left menu, select **My Services > DaaS**.
2. Select **Manage**.

3. If this is the first catalog being created, you are guided to the correct selection (such as "Set up the machines and create machine catalogs to run apps and desktops"). The catalog creation wizard opens.
4. If you already created a catalog and want to create another, follow these steps:
    a) From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
    b) To organize catalogs using folders, create folders under the default **Machine Catalogs** folder. For more information, see Create a catalog folder.
    c) Select the folder where you want to create the catalog, and then click **Create Machine Catalog**. The catalog creation wizard opens.

The wizard walks you through the pages described in the following sections. The pages you see may differ, depending on the selections you make, and the connection (to a host) you use. Hosts / virtualization resources lists information sources for the supported host types.

Select a machine type

Each catalog must contain machines of only one OS type. Select one of the following on the **Machine Type** page:

- **Multi-session OS:** A multi-session OS catalog provides hosted shared desktops. The machines can be running supported versions of the Windows or Linux operating systems, but the catalog cannot contain both Windows and Linux operating systems.
- **Single-session OS:** A single-session OS catalog provides VDI desktops that you can assign to different users.
- **Remote PC Access:** A Remote PC Access catalog provides users with remote access to their physical office desktop machines. Remote PC Access does not require a VPN to provide security.

Select machine management options

> **Note:**
>
> The page **Machine Management** does not appear if you select **Remote PC Access** on the **Machine Type** page.

The **Machine Management** page indicates how machines are managed and the tool that you want to use to deploy machines.

Select one of the options to indicate how machines must be power managed through the Full Configuration interface:

- **Machines that are power managed (for example, virtual machines or blade PCs)**: This option is available only if you already configured a connection to a hypervisor or cloud service.

- **Machines are not power managed (for example, physical machines)**

If you select the option **Machines that are power managed (for example, virtual machines or blade PCs)**, then select a tool to create VMs:

- **Citrix Provisioning Technology**
  - **Citrix Machine Creation Services (MCS)** Creates a catalog of VMs provisioned and imaged using MCS. MCS copies images cloned from a master image to those VMs.
  - **Citrix Provisioning Services (PVS)** Creates a catalog of VMs provisioned using MCS and imaged using PVS. Those VMs serve as PVS target devices and the PVS server can stream a single shared disk image to them.

    > **Note:**
    >
    > This option is available only for PVS sites registered with Citrix Cloud and is currently limited to Azure resources.

- **Other service or technology** A tool that manages machines already in the data center. Citrix recommends that you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.

> **Note:**
>
> For Linux OS machines, see Create Linux VDAs using Machine Creation Services (MCS).

Select a desktop experience

> **Note:**
>
> The options on the **Desktop Experience** page varies according to the machine type that you select on the **Machine Type** page.

- For **Multi-session OS** machines, users are assigned a random desktop each time they log in. You get the following options on the **Desktop Experience** page:
  - Save changes on the local disk of the machine hosting virtual desktops: Persistent
  - Discard all changes and clear virtual desktops when the user logs off: Non-persistent

  > **Note:**
  >
  > For persistent multi-session machines, changes users make to the desktops will be saved and accessible to all authorized users.

- For single-session OS machines, you get the following options on the **Desktop Experience** page:
  - Connect to a new (random) desktop each time the users log in.

- Connect to the same (static) desktop each time the users log in.

You can further decide whether changes made by users will be saved or discarded after they log off.

Select an image

> **Note:**
>
> - This page appears only if you select **Citrix Machine Creation Services (MCS)** on the **Machine Management** page.
> - The options available on this page vary according to the hypervisor or cloud service.

Follow these steps to complete the settings on the page:

1. Select an image type for the machine catalog, and then select an image. Two types of images are available:

   - **Master image**: A snapshot or VM created as the master image. It undergoes automatic image preparation at the start of catalog creation. If needed, you can add a note for the selected image.

     > **Note:**
     >
     > - When you are using MCS, do not run Sysprep on master images.
     > - If you specify a master image rather than a snapshot, the management interface creates a snapshot, but you cannot name it.
     > - An error message appears if you select a snapshot or VM that is not compatible with the machine management technology you selected earlier in the wizard.
     > - To update images within an image node, select it in the tree, and then click the **Refresh** option at the top right corner. If you don't select any image node, clicking **Refresh** updates all images in the tree. To clear a selected node in the tree, hold **CTRL** and then click the node.

   - **Prepared image**: An image that has undergone image preparation, ready for direct use in VM creation. Opting for prepared images rather than master images for catalog creation ensures faster and more reliable machine catalog creation, along with streamlined image lifecycle management.

   For more information on image preparation, see Machine Creation Service: Image Preparation Overview and Fault-Finding.

2. To inherit VM settings from a machine profile, select **Use a machine profile**, and then select a VM or ARM template spec (specific to Azure) to use as the machine profile.

> **Note:**
>
> Currently, using machine profiles is restricted to Azure, AWS, and GCP VMs.

3. Select the minimum functional level for the catalog. To enable the use of the latest product features, ensure that the master image has the latest VDA version installed.

Configure the machines

> **Note:**
>
> - The title of this page depends on what you selected on the **Machine Management** page: **Machines**, **Virtual Machines**, or **Machines and Users**.
> - This page does not appear if you select **Remote PC Access** on the **Machine Type** page.
> - You can create an empty catalog, which means the catalog contains no machines.

- **When using MCS to create machines:**
  - Specify how many virtual machines to create. Enter **0** (zero) if you do not want to create any. Later, to create VMs for an empty catalog, you can perform **Add machines**.
  - Choose the amount of memory (in MB) each VM has.

    > **Important:**
    >
    > Each created VM has a hard disk. Its size is set in the master image; you cannot change the hard disk size in the catalog.

  - If you indicate on the **Desktop Experience** page that user changes to static desktops should be saved on a separate Personal vDisk, then specify the virtual disk size in GB and the drive letter.
  - If your deployment uses more than one zone (resource location), you can select a zone for the catalog.
  - If you're creating static desktop VMs, select a virtual machine copy mode. See Virtual machine copy mode.
  - If you're creating random non-persistent desktop VMs, you can enable and configure the write-back cache for temporary data on machines to improve I/O performance. For more information, see Configure cache for temporary data.
- **When using other tools to provide machines:**

  Add (or import a list of) machine account names. You can change the account name for a VM after you add or import it. If you have specified static machines on the **Desktop Experience** page, you can optionally specify the user name for use with each VM you add.

> **Tip:**
>
> To add users, you can browse to the users or enter a semicolon-separated list of user names manually. If the users are in Active Directory, enter the names directly. If not, enter the names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`.

After you add or import names, you can use the **Remove** button to delete names from the list while you are still on this wizard page.

- **When using other tools (not MCS):**

  An icon and tooltip for each machine added (or imported) help identify machines that might not be eligible to add to the catalog, or be unable to register with a Cloud Connector.

Virtual machine copy mode The copy mode that you specify on the **Machines** page determines whether MCS creates thin (fast copy) or thick (full copy) clones from the master image. (Default = thin clones)

- Use fast copy clones for more efficient storage use and faster machine creation.
- Use full copy clones for better data recovery and migration support, with potentially reduced IOPS after the machines are created.

Configure cache for temporary data When using MCS to manage random non-persistent machines in a catalog, you can enable write-back cache for machines to improve I/O performance.

Write-back cache is referred to as MCSIO. For more information, see this blog article.

Prerequisites To enable write-back cache, the catalog must meet these requirements:

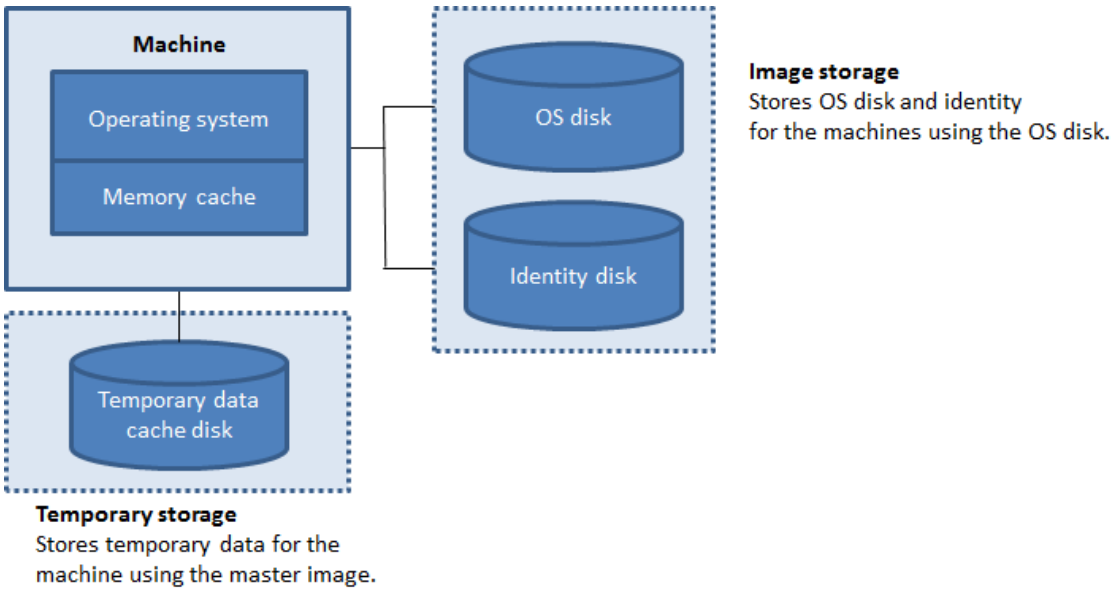
- Uses a connection that specifies storage for temporary data. For more information, see Connections and resources.
- VDAs must be at least version 7.9 and installed with a current MCSIO driver.

  > **Note:**
  >
  > Installing this driver is an option when you install or upgrade a VDA. By default, that driver isn't installed.

- To enable drive letter assignment for disk caches, VMs must meet the following additional requirements:
  - Operating System: Windows
  - VDA version: 2305 or later

Considerations

- Write-back caches come in *Memory* cache and *Disk* cache. By default, their default values differ according to the connection type. Generally, the default values are sufficient for most cases; however, consider the space needed for:
  - Temporary data files created by Windows itself, including the Windows page file.
  - User profile data.
  - ShareFile data that is synced to users' sessions.
  - Data that might be created or copied by a session user or any applications users may install inside the session.



- Configuring the write-back cache with only a disk cache and no memory cache has been deprecated. To enable a cache for temporary data, we recommend selecting **Disk cache size (GB)** and **Memory allocated to cache (MB)** and specifying a size greater than 0 for the memory cache. Temporary data is initially written to the memory cache. When the memory cache reaches its configured limit, the oldest data is moved to the temporary data cache disk.
- The memory cache is part of the total amount of memory on each machine. Therefore, if you enable the **Memory cache size (MB) (recommended)** checkbox, consider increasing the total amount of memory on each machine.
- Changing **Disk cache size (GB)** from its default value can affect performance. The size must match user requirements and the load placed on the machine.

  > **Important:**
  >
  > If the disk cache runs out of space, the user's session becomes unusable.

- If you clear the **Disk cache size** checkbox, no cache disk is created. In this case, specify a **Mem-**

ory allocated to cache value that is large enough to hold all of the temporary data. This is feasible only if large amounts of RAM are available for allocation to each VM.

- If you clear both checkboxes, temporary data is not cached. It is written to the difference disk (located in the OS storage) for each VM. (This is the provisioning action in releases earlier than 7.9.)
- Do not enable caching if you intend to use this catalog to create AppDisks.
- You cannot change the cache values in a machine catalog after it is created.

Using CSV files to bulk add machines If you use the **Full Configuration** management interface, you can bulk add machines by using CSV files. The feature is available to all catalogs except catalogs created through MCS.

A general workflow to use CSV files to bulk add machines is as follows:

1. On the **Machines** page, select **Add CSV File**. The **Add Machines in Bulk** window appears.
2. Select **Download CSV Template**.
3. Fill out the template file.
4. Drag or browse to the file to upload it.
5. Select **Validate** to do validation checks on your import.
6. Select **Import** to complete.

For information about CSV file considerations, see Considerations when using CSV files to add machines.

You can also export machines from a catalog on the same Machines page. The exported CSV of machines can then be used as a template when adding machines in bulk. To export machines:

1. On the **Machines** page, select **Export to CSV file**. A CSV file containing a list of the machines is downloaded.
2. Open the CSV file to add or edit machines as needed. To add machines in bulk using the saved CSV file, see the previous section, Using CSV files to bulk add machines.

> **Note:**
>
> - This feature is not available for Remote PC Access catalogs.
> - Export and import of machines in CSV files is only supported between catalogs of the same type.

Configure NICs for the machines

The page **NICs** does not appear if you select **Remote PC Access** on the **Machine Type** page.

If you plan to use multiple NICs, associate a virtual network with each card. For example, you can assign one card to access a specific secure network, and another card to access a more commonly used network. You can also add or remove NICs from this page.

> **Note:**
>
> For VMWare deployments, when creating a machine catalog using a machine profile, the catalog inherits the NIC configurations from the machine profile. In such cases, if the machine profile has multiple NICs with the same network, then Full Configuration uses the network from the hosting unit for NIC configurations.

Add machine accounts

> **Note:**
>
> This page **Machine Accounts** appears only when you select **Remote PC Access** on the **Machine Type** page.

Add the Active Directory machine accounts or Organizational Units (OUs). Do not use a forward slash (/) in an OU name.

You can choose a previously configured power management connection or select not to use power management. If you want to use power management but a suitable connection has not been configured yet, you can create that connection later and then edit the machine catalog to update the power management settings.

You can also bulk add machines by using CSV files. A general workflow to do that is as follows:

1. On the **Machine Accounts** page, select **Add CSV File**. The **Add Machines in Bulk** window appears.
2. Select **Download CSV Template**.
3. Fill out the template file.
4. Drag or browse to the file to upload it.
5. Select **Validate** to do validation checks on your import.
6. Select **Import** to complete.

For information about CSV file considerations, see Considerations when using CSV files to add machines.

Configure identities for machines in the catalog

> **Note:**
>
> - The page **Machine Identities** appears only when you do not select **Remote PC Access** on

> the **Machine Type** page and select **Citrix Machine Creation Services (MCS)** on the **Machine Management** page.

Each machine in the catalog must have a unique identity. This page lets you configure identities for machines in the catalog. The machines are joined to the identity after they are provisioned. You cannot change the identity type after you create the catalog.

A general workflow to configure settings on this page is as follows:

1. Select an identity from the list.
2. Indicate whether to create accounts or use existing ones, and the location (domain) for those accounts.

You can select one of the following options:

- **On-premises Active Directory**: Machines owned by an organization and signed into with an Active Directory account that belongs to that organization. They exist on-premises.

  > **Note:**
  >
  > By default, the domain where the resource (connection) resides is selected.

- **Azure AD joined**: Machines owned by an organization and signed into with an Azure Active Directory account that belongs to that organization. They exist only in the cloud. For information about the requirements, limitations, and considerations, see Azure Active Directory joined.

  > **Note:**
  >
  > This option requires that the master image meets the operating system prerequisite. For more information, see the Microsoft documentation Microsoft Entra joined devices.

- **Hybrid Azure Active Directory joined**. Machines owned by an organization and signed into with an Active Directory Domain Services account that belongs to that organization. They exist in the cloud and on-premises. For information about the requirements, limitations, and considerations, see Hybrid Azure Active Directory joined.

  > **Note:**
  >
  > - Before you can use hybrid Azure Active Directory join, make sure that your Azure environment meets the prerequisites. See Configure Microsoft Entra hybrid join.
  > - This option requires that the master image meets the operating system prerequisite. For more information, see Microsoft Entra hybrid joined devices.

- **Non-domain-joined**. Machines not joined to any domain. For information about the requirements and limitations, see Non-domain-joined.

> **Important:**
>
> - If you select **On-premises Active Directory** or **Hybrid Azure Active Directory joined** as the identity type, each machine in the catalog must have a corresponding Active Directory computer account.
> - The **Non-domain-joined** identity type requires version 1811 or later of the VDA as the minimum functional level for the catalog. To make it available, update the minimum functional level.
> - The **Azure Active Directory joined** and **Hybrid Azure Active Directory joined** identity types require version 2203 or later of the VDA as the minimum functional level for the catalog. To make them available, update the minimum functional level.

If you create accounts, you must have permission to create computer accounts in the OU where the machines reside. Each machine in the catalog must have a unique name. Specify the account naming scheme for the machines that you want to create. For more information, see Machine account naming scheme.

> **Note:**
>
> Make sure that OU names do not use forward slashes (`/`).

If you use existing accounts, browse to the accounts or click **Import** and specify a `.csv` file containing account names. The imported file content must use the format: `[ADComputerAccount] ADcomputeraccountname.domain`

Ensure that there are enough accounts for all the machines you are adding. The Full Configuration interface manages those accounts. Therefore, either allow that interface to reset the passwords for all the accounts or specify the account password, which must be the same for all accounts.

For catalogs containing physical or existing machines, select or import existing accounts and assign each machine to both an Active Directory computer account and to a user account.

Machine account naming scheme Each machine in a catalog must have a unique name. You must specify a machine account naming scheme when creating a catalog. Use wildcards (hash marks) as placeholders for sequential numbers or letters that appear in the name.

When specifying a naming scheme, consider the following:

- The maximum number of characters allowed is 15.
- The naming scheme must contain at least one wildcard character. You must put all wildcards together.
- The entire name, including wildcards, must contain at least 2 but no more than 15 characters. It must include at least one non-numeric and one # (wildcard) character.

- The name must not include spaces or any of the following characters: ,~!@'$%^&.()} { \/*?"<>|=+[];:_"..
- The name cannot end with a hyphen (-).
- The number of characters increases with the increase in the number of machine accounts. For example, if you create 1,000 machine accounts with the scheme "veryverylong#", the last account name created (veryverylong1000) contains 16 characters that exceeds the number of maximum characters allowed.

You can indicate whether the sequential values are numbers (0-9) or letters (A-Z):

- **0-9**. If selected, the specified wildcards resolve to sequential numbers.

  > **Note:**
  >
  > If there is only one wildcard (#), the account names start with 1. If there are two, the account names start with 01. If there are three, the account names start with 001, and so on.

- **A-Z**. If selected, the specified wildcards resolve to sequential letters.

For example, a naming scheme of PC-Sales-## (with **0-9** selected) results in accounts named PC-Sales-01, PC-Sales-02, PC-Sales-03, and so on.

Optionally, you can specify what the account names start with.

- If you select **0-9**, accounts are named sequentially, starting with the specified numbers. Enter one or more digits, depending on how many wildcards you use in the preceding field. For example, if you use two wildcards, enter two digits or more.
- If you select **A-Z**, accounts are named sequentially, starting with the specified letters. Enter one or more letters, depending on how many wildcards you use in the preceding field. For example, if you use two wildcards, enter two letters or more.

Add domain credentials

Enter the credentials of an administrator who has permission to perform account operations. Detailed steps are as follows:

1. Click Enter credentials. The Windows Security page appears.
2. In the User name field, enter the administrator's SamName, user name, or user SID. Depending on your input:

   - If you enter a SamName, the **Domain** field populates automatically.
   - If you enter a user name or SID, you can limit the user search to a specific domain by entering the domain name or SID in the **Domain** field.

3. Click **Check name** to check whether the user name is valid or unique.
4. In the **Password** field, enter the domain password of the administrator.
5. Click **Done**.

> **Note:**
>
> If the identity type you selected in **Machine Identities** is **Hybrid Azure Active Directory joined**, the credentials you enter must have been granted the `Write userCertificate` permission.

Select a Workspace Environment Management configuration set (optional)

The page **WEM** appears only when you use the Advanced or Premium edition of Citrix DaaS.

Select a Workspace Environment Management (WEM) configuration set to which you want to bind the catalog. A configuration set is a logical container used to organize a set of WEM configurations. Binding a catalog to a configuration set lets you use WEM to deliver the best possible workspace experience to your users.

> **Important:**
>
> - Before you can bind a catalog to a configuration set, you must set up your WEM service deployment. Sign in to Citrix Cloud and then launch the WEM service. For more information, see Get started with Workspace Environment Management service.
> - If you already use WEM, the machines in the catalog that you are about to provision might already be present in a configuration set. For example, through Active Directory. In that case, we recommend that you use Active Directory consistently to perform the configuration and skip this configuration.

If the selected configuration set does not contain settings relating to the basic configuration of WEM, the following option appears:

- **Apply basic settings to configuration set**. The option lets you quickly get started with WEM by applying basic settings to the configuration set. Basic settings include CPU spike protection, auto-preventing CPU spikes, and intelligent CPU optimization. To view the basic settings, click the *here* link. To modify them, use the WEM console.

Upgrade VDA (optional)

> **Important:**
>
> - To ensure a smooth upgrade, make sure that you meet the prerequisites and review known issues before upgrading VDAs to CR or LTSR CU versions. See Upgrade VDAs using the Full

> Configuration interface.
> - When upgrading LTSR VDAs to LTSR Cumulative Update (CU) versions, make sure that the version of the VDA Upgrade Agents running on the VDAs is 7.36.0.7 or later. For more information, see Upgrade VDAs using the Full Configuration interface.

This feature applies to the following machine types:

- MCS-provisioned persistent machines. You deploy them using **Citrix Machine Creation Services** on the **Machine Management** page during catalog creation.
- Machines that are not created using MCS (for example, physical machines). You deploy them using **Other service or technology** on the **Machine Management** page during catalog creation.

For more information about the two options, see Machine management

On the **VDA Upgrade** page, select the VDA version to upgrade to. If specified, the VDAs in the catalog that have the VDA Upgrade Agent installed can upgrade to the selected version —immediately or at a scheduled time.

> **Note:**
>
> - This feature supports upgrading only to the latest VDA. The time at which you create a VDA upgrade schedule or upgrade a VDA determines the latest version of the VDA.
> - After you configure VDA upgrade settings, it might take up to 15 minutes for the **VDA Upgrade** field to reflect the latest status. To show the **VDA Upgrade** column, click the Columns to display icon in the upper right corner, select **Machine Catalog > VDA Upgrade**, and click **Save**.

Choose a VDA track that suits your deployment:

> **Important:**
>
> You can switch between the CR VDA and the LTSR VDA as long as you switch from an earlier version to a later version. You cannot switch from a later version to an earlier version because that is considered a downgrade. For example, you cannot downgrade from 2212 CR to 2203 LTSR (any CU) but you can upgrade from 2112 CR to 2203 LTSR (any CU).

- **Latest CR VDA**. Current Releases (CRs) deliver the latest and most innovative app, desktop, and server virtualization features and functionality.
- **Latest LTSR VDA**. Long Term Service Releases (LTSRs) are recommended for large enterprise production environments that prefer to keep the same base version for an extended period.

After catalog creation, you can upgrade VDAs as needed. For more information, see Upgrade VDAs.

If you want to enable VDA upgrade later, you can return to this page by editing the catalog after catalog creation. For more information, see Configure VDA upgrade settings by editing a catalog.

Review the settings

On the **Summary** page, review the settings you specified. Enter a name and description for the catalog. This information appears in the Full Configuration management interface.

When you're done, select **Finish** to start the catalog creation.

In **Machine Catalogs**, the new catalog appears with an inline progress bar.

To view details of the creation progress:

1. Hover the mouse over the machine catalog.
2. In the tooltip that appears, click **View details**.

   A step-by-step progress graph appears where you can see the following:

   - History of steps
   - Progress and running time of the current step
   - Remaining steps

Create an MCS machine catalog using PowerShell commands

You can also create an MCS machine catalog using PowerShell commands. For more information, see:

- SDKs and APIs
- Manage Citrix DaaS using Remote PowerShell SDKs
- New-ProvScheme

Assign a specific drive letter to an MCS I/O write-back cache disk

You can assign a specific drive letter to an MCS I/O write-back cache disk. This implementation helps you to avoid conflicts between the drive letter of any applications that you use and the drive letter of MCS I/O write-back cache disk. To do this, you can use PowerShell commands. The supported hypervisors are Azure, GCP, VMware, SCVMM, and XenServer.

> **Note:**
>
> This feature requires VDA version 2305 or later.

Limitations

- Applicable to only Windows operating system
- Applicable drive letter for write-back cache disk: E to Z

- Not applicable when Azure temporary disk is used as a write-back cache disk
- Applicable only when you create a new machine catalog

Assign a drive letter to a write-back cache disk To assign a drive letter to write-back cache disk:

1. Open the **PowerShell** window.
2. Run `asnp citrix*`.
3. Create an identity pool if not already created. For information, see Creating a Catalog.
4. Create a provisioning scheme using the `New-ProvScheme` command with the property `WriteBackCacheDriveLetter`. For example:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\\HostingUnits\\name\\virtualprivatecloud.folder\\East
     US.region\\virtualprivatecloud.folder\\abcd-resources.
    resourcegroup\\abcd-resources-vnet.virtualprivatecloud\\
    default.network" }
  `
-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.
   folder\\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
    />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
   ="false" />
```



```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
</CustomProperties>'
<!--NeedCopy-->
```

5. Finish creating the catalog.

Important consideration about setting custom properties

Custom properties must be set correctly at `New-ProvScheme` and `Set-ProvScheme` in GCP and Azure environments. If you specify non-existing custom property or properties, you get the following error message, and the commands fail to run.

```
Invalid property found: <invalid property>. Ensure that the CustomProperties
 parameter supports the property.
```

Important consideration about setting ProvScheme parameters

When you use MCS to create a catalog, you get an error if you:

- Set the following `New-ProvScheme` parameters in unsupported hypervisors when you create a machine catalog:

Parameter	Supported hypervisor
`UseWriteBackCache`	VMware
	Hyper-V
	XenServer
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP

Parameter	Supported hypervisor
`UseFullDiskCloneProvisioning`	AWS VMware Hyper-V XenServer

- Update the following `Set-ProvScheme` parameters after you create the machine catalog:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

Add SIDs while creating virtual machines

You can add the parameter `ADAccountSid` to uniquely identify the machines while creating new virtual machines.

To do this:

1. Create a catalog with the supported identity type.
2. Add machines to the catalog using `NewProvVM`. For example:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
    )  -RunAsynchronously
<!--NeedCopy-->
```

However, you cannot provision a machine with:

- An AD account that is not in the catalog identity pool
- An AD account that is not in available state

Validate configuration before creating an MCS machine catalog

You can validate configuration settings before creating an MCS machine catalog using the parameter `-validate` in `New-ProvScheme` command. After you run this PowerShell command with the parameter, you get an appropriate error message if there is an incorrect parameter used or a parameter has conflict with another parameter. You can then use the error message to resolve the issue and

successfully create an MCS machine catalog using PowerShell. Currently, this feature is applicable to Azure, GCP, and VMware virtualization environments.

> **Note:**
>
> While validating, you must not create an actual MCS machine catalog. You must use the result of the command to fix the errors, and then create a successful catalog. Therefore, while running the `New-ProvScheme` command, use a fake identity pool name.

To validate the configuration, do the following steps:

1. Open a PowerShell window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `New-ProvScheme` command and use the parameter `-validate`. Provide a fake identity pool name for the command to work. For example,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vSanRg\\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
    Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
    FunctionalLevel "L7_20" -Validate
$result.TerminatingError | Format-List -Property *
<!--NeedCopy-->
```

Error message:

```
ErrorData     : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
```



```
Operation    : ValidatingInputs
<!--NeedCopy-->
```

4. After validating the configuration setting, you can create an MCS machine catalog with a real identity pool name and correct parameters.

Where to go next

For information on creating specific hypervisor catalogs, see:

- Create an AWS catalog
- Create a Google Cloud Platform catalog
- Create a Microsoft Azure catalog
- Create a Microsoft System Center Virtual Machine Manager catalog
- Create a Nutanix catalog
- Create a VMware catalog
- Create a XenServer catalog

If this is the first catalog created, you are guided to create a delivery group.

To review the entire configuration process, see Plan and build a deployment.

You can create a Citrix Provisioning catalog using the Full Configuration interface and PowerShell. This implementation provides you the following advantages:

- A single unified console to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning and so on.

Currently, this feature is available only for Azure and VMware workloads. However, in VMware environments, you can currently create the catalogs using only PowerShell commands. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

More information

- Citrix Virtual Apps and Desktops Image Management
- Create and manage connections and resources
- Create machine identities joined catalogs
- Manage machine catalogs

Create an AWS catalog

May 6, 2024

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to AWS virtualization environments.

> **Note:**
>
> Before creating an AWS catalog, you need to finish creating a connection to AWS. See Connection to AWS.

Network setting during image preparation

During image preparation, a preparation virtual machine (VM) is created based on the original VM. This preparation VM is disconnected from the network. To disconnect the network from the preparation VM, a network security group is created to deny all inbound and outbound traffic. This network security group persists and is reused. The network security group's name is `Citrix.XenDesktop.IsolationGroup-GUID`, where GUID is randomly generated.

AWS tenancy

AWS provides the following tenancy options: shared tenancy (the default type) and dedicated tenancy. Shared tenancy means that multiple Amazon EC2 instances from different customers might reside on the same piece of physical hardware. Dedicated tenancy means that your EC2 instances run only on hardware with other instances that you have deployed. Other customers do not use the same piece of hardware.

You can use MCS to provision AWS dedicated hosts by using the Full Configuration interface or PowerShell.

Requirements for provisioning to AWS hosts

- An imported BYOL (bring your own license) image (AMI). With dedicated hosts, use and manage your existing licenses.
- An allocation of dedicated hosts with sufficient utilization to satisfy provisioning requests.
- Enabling **auto-placement**.

Configure AWS dedicated host tenancy using the Full Configuration interface

When you use MCS to create a catalog to provision machines in AWS, the **Machine Catalog Setup > Security** page presents the following options:

- **Use shared hardware**. This setting is suitable for most deployments. Multiple customers share pieces of hardware even though they do not interact with each other. Using shared hardware is the least expensive option for running your Amazon EC2 instances.
- **Use dedicated host**. An Amazon EC2 dedicated host is a physical server with EC2 instance capacity that is fully dedicated, letting you use existing per-socket or per-VM software licenses. Dedicated hosts have preset utilization based on instance type. For example, a single allocated dedicated host of C4 Large instance types is limited to running 16 instances. See the AWS site for more information.
- **Use dedicated instance**. This setting is more suitable for deployments with specific security or compliance requirements. With a dedicated instance, you still enjoy the benefits of having a host separate from other AWS customers but you do not pay for the entire host. You do not need to worry about the capacity of the host but you are charged at a higher rate for the instances.

  This setting is suitable for deployments with licensing restrictions or security requirements that need your use of a dedicated host. With a dedicated host, you own an entire physical host and are billed on an hourly basis. Owning that host lets you spin up as many EC2 instances as that host permits, without more charges.

> **Note:**
>
> You can delete any available preparation identity disk if there is no ongoing catalog creation or image update task.

Configure AWS dedicated host tenancy using the PowerShell

Alternatively, you can provision AWS dedicated hosts through PowerShell. Use the `New-ProvScheme` cmdlet with the parameter `TenancyType` set to `Host`.

Capture AWS instance property

When you create a catalog to provision machines using Machine Creation Services (MCS) in AWS, you select an AMI to represent the master image of that catalog. From that AMI, MCS uses a snapshot of the disk.

> **Tip:**
>
> To use AWS instance property capturing, you must have a VM associated with the AMI.

MCS reads properties from the instance from which the AMI was taken and applies the Identity Access Management (IAM) role and tags of the machine to the machines provisioned for a given catalog. When using this optional feature, the catalog creation process finds the selected AMI source instance, reading a limited set of properties. These properties are then stored in an AWS Launch Template, which is used to provision machines for that catalog. Any machine in the catalog inherits the captured instance properties.

Captured properties include:

- IAM roles: applied to provisioned instances.
- Tags: applied to provisioned instances, their disks, and NICs. These tags are applied to transient Citrix resources, including: S3 bucket and objects, and AMIs, snapshots, and launch templates.

> **Tip:**
>
> The tagging of transient Citrix resources is optional and is configurable using the custom property `AwsOperationalResourcesTagging`. To successfully apply tags and create an AWS catalog with operational resource tagging, do not delete the EC2 instance which was used to create the AMI image.

Capture the AWS instance property

You can use this feature by specifying a custom property, `AwsCaptureInstanceProperties`, when creating a provisioning scheme for an AWS hosting connection:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Refer to the New-ProvScheme for more information.

> **Note:**
>
> The `AwsCaptureInstanceProperties` is deprecated. We recommend using machine profiles to specify machine properties for VMs instead.

Tag AWS operational resource

An Amazon Machine Image (AMI) represents a type of virtual appliance used to create a virtual machine within the Amazon Cloud environment, commonly referred to as EC2. You use an AMI to deploy services that use the EC2 environment. When you create a catalog to provision machines using MCS for AWS, you select the **AMI** to act as the golden image for that catalog.

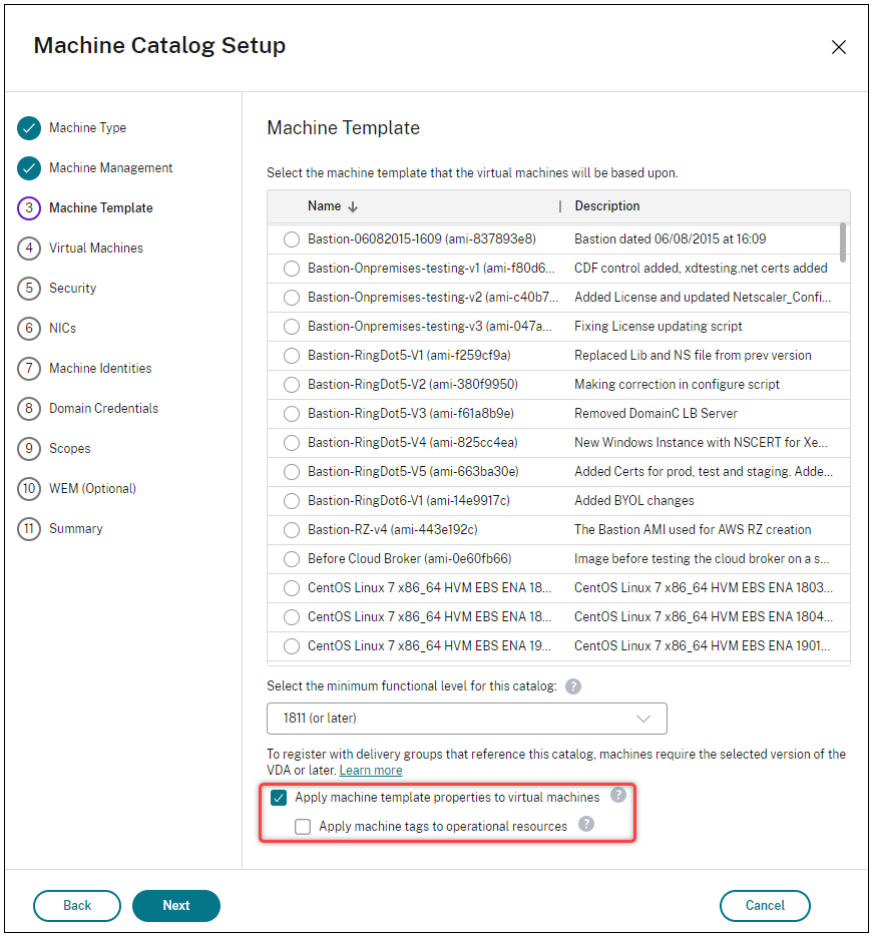
> **Important:**
>
> Creating catalogs by capturing an instance property and a launch template is required for using operational resource tagging.

To create an AWS catalog, you must first create an AMI for the instance you want to be the golden image. MCS reads the tags from that instance and incorporates them into the launch template. The launch template tags are then applied to all Citrix resources created in your AWS environment, including:

- Virtual Machines
- VM disks
- VM network interfaces
- S3 buckets
- S3 objects
- Launch templates
- AMIs

Apply AWS instance properties and tag operational resources in the Full Configuration interface

When creating a catalog to provision machines in AWS by using MCS, you can control whether to apply the IAM role and tag properties to those machines. You can also control whether to apply machine tags to operational resources. You have the following two options:



- **Apply machine template properties to virtual machines**
  - Controls whether to apply the IAM role and tag properties associated with the selected machine template to virtual machines in this catalog.
- **Apply machine tags to operational resources**
  - Controls whether to apply machine tags to every item created in your AWS environment that facilitates provisioning of machines. Operational resources are created as byproducts of catalog creation. They include both temporary and persistent resources, such as preparation VM instance and AMI.

Tag an operational resource using PowerShell

To use PowerShell to tag resources:

1. Open a PowerShell window from the DDC host.
2. Run the command `asnp citrix` to load Citrix-specific PowerShell modules.

To tag a resource for a provisioned VM, use the custom property `AwsOperationalResourcesTagging`. The syntax for this property is:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" ...<standard provscheme parameters
>
```

Create a machine profile-based machine catalog using PowerShell

You can use a machine profile to capture the hardware properties from an EC2 instance (VM) or launch template version and apply them to the provisioned machines. Properties that are captured can include, for example, EBS volume properties, instance type, EBS optimization, CPU options, tenancy type, hibernation capability, and other supported AWS configurations.

You can use an AWS EC2 Instance (VM) or AWS Launch Template version as the machine profile input.

> **Note:**
>
> EBS volume properties are derived only from a machine profile.

Important considerations

The important considerations while creating an MCS machine catalog:

- If you add machine hardware property parameters in the `New-ProvScheme` and `Set-ProvScheme` commands, then the values provided in the parameters overwrites the values in the machine profile.
- If you set `AwsCaptureInstanceProperties` as **`true`** and do not set `MachineProfile` property, then only IAM roles and tags are captured.
- You cannot set both `AwsCaptureInstanceProperties` and `MachineProfile` at the same time.

  > **Note:
  >
  > The `AwsCaptureInstanceProperties` is deprecated.

- If a machine profile is not provided, you must explicitly provide the values of the following properties:
  - Security Group
  - ENI or Virtual Network
- You can enable `AwsOperationalResourcesTagging` only if you enable `AwsCaptureInstancePro` or specify a machine profile.

The important consideration after creating an MCS machine catalog is:

- You cannot change a catalog from a machine profile-based to a non-machine profile-based catalog.

Create a machine catalog using a machine profile

To create a machine catalog using a machine profile:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create an identity pool if not already created. For example,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain abcdf -NamingSchemeType Numeric
<!--NeedCopy-->
```

4. Run New-ProvScheme command. For example:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1
-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
-CleanOnBoot
-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
    demet-ami.0 (ami-0ca813xxxxxx061ef).template'
-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
    -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
    vm'
<!--NeedCopy-->
```

5. Complete creating the catalog.

Update the machine profile

To update the machine profile on a catalog that was initially provisioned with a machine profile, do the following. You can also change the tenancy type and hibernation capability of the machine profile source while editing an MCS machine catalog.

1. Run `Set-ProvScheme` command. For example,

```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
    availabilityzone\citrix-cvad-machineprofile-instance (i-0
    xxxxxxxx).vm"
<!--NeedCopy-->
```


Create a catalog with launch template version using PowerShell

You can create an MCS machine catalog with a launch template version as a machine profile input. You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM.

On the AWS EC2 console, you can provide the instance configuration information of a launch template along with version number. When you specify the launch template version as a machine profile input while creating or updating a machine catalog, the properties from that version of the launch template are copied to the provisioned VDA VMs.

The following properties can be provided using machine profile input or explicitly as parameters in `New-ProvScheme` or `Set-ProvScheme`commands. If they are provided in `New-ProvScheme` or `Set-ProvScheme` commands, they take precedence over the machine profile values of these properties.

- Service Offering
- Networks
- Security Groups
- Tenancy Type

> **Note:**
>
> If service offering is not provided in the machine profile launch template or as a parameter in the `New-ProvScheme` command, you get an appropriate error.

To create a catalog using launch template version as a machine profile input:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Get the list of launch template versions of a launch template. For example:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Create an identity pool if not created. For example:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```


5. Create a provisioning scheme with a launch template version as a machine profile input. For example:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

6. Register a provisioning scheme as a broker catalog. For example:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Complete creating the catalog.

Update the machine profile source

You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM. For example:

- To update the input of a machine profile catalog from a VM to a launch template version:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

- To update the input of a machine profile catalog from a launch template version to a VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
<!--NeedCopy-->
```


Encrypt OS and ID disks

You can create a persistent and non-persistent catalog of VMs with AWS KMS keys (Customer managed key and AWS managed key) that can be used to encrypt OS disk and Identity Disk (ID).

- AWS managed keys are automatically rotated every year.
- Customer managed keys are optional for automatic rotation and can be managed manually.

You can see the following AWS documents for more information on KMS keys:

- AWS KMS concepts
- How automatic key rotation works

For encryption of OS and ID disks, configure one of the following:

- Use a master image that is encrypted (for example, an AMI created from an instance or snapshot that contains a EBS root volume encrypted with KMS key)
- Use a machine profile source (VM or launch template) that contains an encrypted EBS root volume.

Limitations

Consider the following limitations:

- MCS currently supports only one disk on master image AMI.
- You cannot directly encrypt existing unencrypted EBS volumes or snapshots, or modify the KMS key of an existing encrypted volume. To do that, you must:

  1. Create a new snapshot of that volume.
  2. Create a new volume from that snapshot
  3. Encrypt the new volume.

See the following AWS documents:

- Encrypt unencrypted resources
- Limitations of automatic or default encryption of EBS volumes: Automatically encrypt existing and new Amazon EBS volumes.

Create a catalog with disk encryption

You can create an MCS machine catalog with disk encryption using:

- Master image
- Machine profile

Considerations while using machine profile input are:

- The KMS key of the machine profile input takes precedence over the master image's KMS key.
- If no machine profile input is provided, then the KMS key of the master image AMI is used to encrypt the disks of catalog VMs.
- If the machine profile has Block Device Mappings present, then the block devices present in the master image template (AMI) and machine profile must match. For example, if AMI has a device defined on `/dev/sda1`, then the Machine Profile must also have a device defined on `/dev/sda1`.
- If there is no key in the machine profile source and the master image is unencrypted, then disks of catalog VMs are not encrypted.
- When the master image is encrypted, a machine profile source VM or launch template must have an encrypted root volume to be considered a valid input.

Modify an existing catalog

You can modify an existing catalog using the `Set-ProvScheme` PowerShell command to have:

- A machine profile input with a volume containing a new KMS key.
- A master image template AMI encrypted with a new KMS key.

Important considerations:

- The volumes of new VMs added to the catalog are encrypted with the new KMS key.
- To update the encryption settings when there is an existing machine profile, run `Set-ProvScheme` with a new machine profile.
- You cannot modify an existing catalog from having encrypted volumes to unencrypted volumes. You cannot do an image update from an encrypted master AMI to an unencrypted master AMI.

Copy tags on VMs

You can copy tags on NICs, and disks (Identity disk, write back cache disk, and OS disk) that are specified in the machine profile to newly created VMs in an MCS machine catalog. You can specify these tags in any of the machine profile sources (AWS VM instance or AWS launch template version). This feature is applicable to persistent and non-persistent machine catalogs and VMs.

> **Note:**
>
> - On the AWS EC2 console, you cannot see the **Tag Network Interfaces** values under the **Launch Template Version Resource Tags**. However, you can run the PowerShell command `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` to see the tag

> specifications.
> - If a machine profile source (VM or launch template version) has two network interfaces (eni-1 and eni-2), and eni-1 has tag t1 and eni-2 has tag t2, then the VM gets both the two network interfaces' tags.

Filter VM instances using PowerShell

An AWS VM instance that you use as a machine profile VM must be compatible for the machine catalog to create and function correctly. To list the AWS VM instances that can be used as machine profile input VMs, you can use the `Get-HypInventoryItem` command. The command can page and filter the inventory of VMs available on a hosting unit.

Pagination:

Get-HypInventoryItem supports two modes of pagination:

- Paging mode uses the `-MaxRecords` and `-Skip` parameters to return sets of items:
  - `-MaxRecords`: The default is **1**. This controls how many items to return.
  - `-Skip`: The default is **0**. This controls how many items to skip from the absolute beginning (or absolute end) of the list in the hypervisor.
- Scrolling mode uses `-MaxRecords`, `-ForwardDirection`, and `-ContinuationToken` parameters to allow scrolling of the records:
  - `-ForwardDirection`: The default is **True**. This is used along with `-MaxRecords` to return either the next set of matching records or the previous set of matching records.
  - `-ContinuationToken`: The returns the items immediately after (or before if `ForwardDirection` is **false**) but not including the item given in the `ContinuationToken` .

Examples of pagination:

- To return a single record of the machine template with the lowest name. The `AdditionalData` field has the `TotalItemsCount` and the `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
<!--NeedCopy-->
```

- To return 10 records of the machine template with the lowest name:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
<!--NeedCopy-->
```

- To return an array of records ending with the highest name:


```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
<!--NeedCopy-->
```

- To return an array of records starting at the machine template associated with the given `ContinuationToken`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

Filtering:

The following additional optional parameters are supported for filtering. You can combine these parameters with the pagination options.

- `-ContainsName "my_name"`: If the given string matches part of an AMI name, then the AMI is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ‘apollo’
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '` : If an AMI has at least one of these tags, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Note:**
>
> Two tag values are supported. **Not Tagged** tag value matches items which do not have the given tag in their list of tags. **All values** tag value matches items which have the tag regardless of the value of the tag. Otherwise, the match happens only if the item has the tag and the value equals to what is given in the filter.

- `-Id "ami-0a2d913927e0352f3"`: If the AMI matches the given ID, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```


Filtering on AdditionalData parameter:

The `AdditionalData` filter parameter lists templates or VMs based on their capability, service offering, or any property which is in AdditionalData. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
   AdditionalData
<!--NeedCopy-->
```

You can also add a `-Warn` parameter to indicate the incompatible VMs. The VMs are included with an `AdditionalData` field named **Warning**. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
   -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage an AWS catalog.

More information

- Create and manage connections and resources
- Connection to AWS
- Create machine catalogs

Create a Google Cloud Platform catalog

April 12, 2024

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Google cloud environments.

> **Note:**
>
> Before creating a Google cloud platform (GCP) catalog, you need to finish creating a connection to GCP. See Connection to Google cloud environments.

Prepare a master VM instance and a persistent disk

> **Tip:**
>
> Persistent disk is the Google Cloud term for virtual disk.

To prepare your master VM instance, create and configure a VM instance with properties that match the configuration you want for the cloned VDA instances in your planned machine catalog. The configuration does not apply only to the instance size and type. It also includes instance attributes such as metadata, tags, GPU assignments, network tags, and service account properties.

As part of the mastering process, MCS uses your master VM instance to create the Google Cloud *instance template*. The instance template is then used to create the cloned VDA instances that comprise the machine catalog. Cloned instances inherit the properties (except the VPC, subnet, and persistent disk properties) of the master VM instance from which the instance template was created.

After configuring the properties of the master VM instance to your specifics, start the instance and then prepare the persistent disk for the instance.

We recommend that you manually create a snapshot of the disk. Doing so lets you use a meaningful naming convention to track versions, gives you more options to manage earlier versions of your master image, and saves time for machine catalog creation. If you do not create your own snapshot, MCS creates a temporary snapshot for you (which is deleted at the end of the provisioning process).

Enable zone selection

Citrix DaaS supports zone selection. With zone selection, you specify the zones where you want to create VMs. With zone selection, administrators can place sole tenant nodes across zones of their choice. To configure sole tenancy, you must complete the following on Google Cloud:

- Reserve a Google Cloud sole-tenant node
- Create the VDA master image

Reserve a Google Cloud sole-tenant node

To reserve a sole-tenant node, refer to the Google Cloud documentation.

> **Important:**
>
> A node template is used to indicate performance characteristics of the system that is reserved in the node group. Those characteristics include the number of vGPUs, the amount of memory allocated to the node, and the machine type used for machines created on the node. For more information see the Google Cloud documentation.

Create the VDA master image

To deploy machines on the sole-tenant node successfully, you need to take extra steps when creating a master VM image. Machine instances on Google Cloud have a property called *node affinity labels*. Instances used as master images for catalogs deployed to the sole-tenant node require a *node affinity label* that matches the name of the **target node group**. To achieve this, keep the following in mind:

- For a new instance, set the label in the Google Cloud console when creating an instance. For details, see Set a node affinity label when creating an instance.
- For an existing instance, set the label by using the **gcloud** command line. For details, see Set a node affinity label for an existing instance.

> **Note:**
>
> If you intend to use sole tenancy with a shared VPC, see Shared Virtual Private Cloud.

Set a node affinity label when creating an instance To set the node affinity label:

1. In the Google Cloud console, navigate to **Compute Engine > VM instances**.
2. On the **VM instances** page, select **Create instance**.
3. On the **Instance creation** page, type or configure the required information and then select **management, security, disks, networking, sole tenancy** to open the settings panel.
4. On the **Sole tenancy** tab, select **Browse** to view the available node groups in the current project. The **Sole-tenant node** page appears, displaying a list of available node groups.
5. On the **Sole-tenant node** page, select the applicable node group from the list and then select **Select** to return to the **Sole tenancy** tab. The node affinity labels field populates with the information you selected. This setting ensures that machine catalogs created from the instance will be deployed to the selected node group.
6. Select **Create** to create the instance.

Set a node affinity label for an existing instance To set the node affinity label:

1. In the Google Cloud Shell terminal window, use the *gcloud compute instances* command to set a node affinity label. Include the following information in the **gcloud** command:
    - **Name of the VM**. For example, use an existing VM named `s*2019-vda-base.*`
    - **Name of the node group**. Use the node group name you previously created. For example, `mh-sole-tenant-node-group-1`.
    - **The zone where the instance resides**. For example, the VM resides in the `*us-east-1b* zone`.

For example, type the following command in the terminal window:

- `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

For more information about the *gcloud compute instances* command, see the Google Developer Tools documentation at https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Navigate to the **VM instance details** page of the instance and verify that the **Node Affinities** field populates with the label.

Create a machine catalog

> **Note:**
>
> Create your resources before you create a machine catalog. Use the naming conventions established by Google Cloud when configuring machine catalogs. See Bucket and object naming guidelines for more information.

You can create a machine catalog in two ways:

- Full Configuration interface
- PowerShell. See Manage Citrix DaaS using Remote PowerShell SDKs. For information on how to implement specific features using PowerShell, see Use PowerShell

Create a machine catalog using the Full Configuration interface

Follow the guidance in Create machine catalogs. The following description is unique to Google Cloud catalogs.

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select **Create Machine Catalog** in the action bar.
3. On the **Machine Type** page, select **Multi-session OS** and then select **Next**. Citrix DaaS also supports single-session OS.
4. On the **Machine Management** page, select the **Machines that are power managed** and the **Citrix Machine Creation Services** options and then select **Next**. If there are multiple resources, select one from the menu.
5. On the **Image** page, complete these steps as needed, and then click **Next**.

a) Select a snapshot or VM as the master image. If you want to use the sole tenancy functionality, be sure to select an image whose node group property is correctly configured. See Enable zone selection.

b) To use an existing VM as the machine profile, select **Use a machine profile**, and then select the VM.

> **Note:**
>
> Currently, VMs in this catalog inherit the Disk encryption set ID, Machine size, Storage type, and Zone settings from the machine profile.

c) Select the minimum functional level for the catalog.

6. On the **Storage** page, select the type of storage used to contain the operating system for this machine catalog. Each of the following storage options has unique price and performance characteristics. An identity disk is always created using the zonal standard persistent disk.

   - Standard persistent disk
   - Balanced persistent disk
   - SSD persistent disk

   For details about Google Cloud storage options, see Storage options.

7. On the **Virtual Machines** page, specify how many VMs you want to create, view the detailed specification of the VMs, select the Google Cloud machine type, and then select **Next**. If you use sole tenant node groups for machine catalogs, be sure to select **only** the zones where reserved sole tenant nodes are available. See Enable zone selection.

8. On the **Disk Settings** page, you can configure the following settings:

   - Choose whether to enable write-back cache. After enabling write-back cache, you can do the following:
     - Configure the size of the disk and RAM used for caching temporary data. For more information, see Configure cache for temporary data.
     - Select the storage type for the write-back cache disk. The following storage options are available to use for the write-back cache disk:
       * Standard persistent disk
       * Balanced persistent disk
       * SSD persistent disk

       For details about Google Cloud storage options, see Storage options.
     - Select the type for the write-back cache disk.

    * **Use non-persistent write-back cache disk**. If selected, the write-back cache disk does not persist for the provisioned VMs. The disk is deleted during power cycles and any data redirected to the disk will be lost.
    * **Use persistent write-back cache disk**. If selected, the write-back cache disk persists for the provisioned VMs. Enabling this option increases your storage costs.

- When MCS storage optimization (MCS I/O) is enabled, you can choose whether to retain system disks for VDAs during power cycles. For more information, see Enabling MCS storage optimization updates.
- Choose whether to use your own key to protect disk contents. To use the feature, you must first create your own Customer Managed Encryption Keys (CMEKs). For more information, see Using Customer Managed Encryption Keys (CMEK).

  > **Note:**
  >
  > It is available only in the **Manage > Full Configuration** interface.

  After creating the keys, you can select one of those keys from the list. You cannot change the key after you create the catalog. Google Cloud does not support rotating keys on existing persistent disks or images. Therefore, after you provision a catalog, the catalog is tied to a specific version of the key. If that key is disabled or destroyed, the instances and disks encrypted with it become unusable until the key is reenabled or restored.

9. On the **Machine Identities** page, select an Active Directory account and then select **Next**.
   - If you select **Create new Active Directory accounts**, select a domain and then enter the sequence of characters representing the naming scheme for the provisioned VM computer accounts created in the Active Directory. The account naming scheme can contain 1–64 characters, and cannot contain blank spaces, or non-ASCII or special characters.
   - If you select **Use existing Active Directory accounts**, select **Browse** to navigate to the existing Active Directory computer accounts for the selected machines.
10. On the **Domain Credentials** page, select **Enter credentials**, type the user name and password, select **Save**, and then select **Next**.
    - The credential you type must have permissions to perform Active Directory account operations.
11. On the **Scopes** page, select scopes for the machine catalog and then select **Next**.
    - You can select optional scopes or select **custom scope** to customize scopes as needed.
12. On the **Summary** page, confirm the information, specify a name for the catalog, and then select **Finish**.

> **Note:**
>
> The catalog name can contain 1–39 characters, and cannot contain only blank spaces or the characters `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

Machine catalog creation might take a long time to complete. When it completes, the catalog is listed. You can verify that the machines are created on the target node groups in the Google Cloud console.

Import manually created Google Cloud machines

Using this feature, you can:

- Import manually created Google Cloud multi-session OS machines into a Citrix DaaS catalog.
- Remove manually created Google Cloud multi-session OS machines from a Citrix DaaS catalog.
- Use existing Citrix DaaS power management capabilities to power manage Google Cloud Windows multi-session OS machines. For example, set a restart schedule for those machines.

This functionality does not require changes to an existing Citrix DaaS provisioning workflow, nor the removal of any existing feature.

It is recommended that you use MCS to provision machines in Citrix DaaS's Full Configuration interface instead of importing manually created Google Cloud machines.

Shared Virtual Private Cloud

Shared Virtual Private Clouds (VPCs) comprise a host project, from which the shared subnets are made available, and one or more service projects that use the resource. Shared VPCs are desirable options for larger installations because they provide centralized control, usage, and administration of shared corporate Google cloud resources. For more information, see the Google Documentation site.

With this feature, Machine Creation Services (MCS) supports provisioning and managing machine catalogs deployed to Shared VPCs. This support, which is functionally equivalent to the support currently provided in local VPCs, differs in two areas:

- You must grant extra permissions to the Service Account used to create the host connection. This process allows MCS to access and use Shared VPC Resources. See New permissions required.
- You must create two firewall rules, one each for ingress and egress. These firewall rules are used during the image mastering process. See Firewall Rules.

For information on configuring shared VPC, see Configure the shared VPC.

New permissions required

A Google Cloud service account with specific permissions is required when creating the host connection. These additional permissions must be granted to any service accounts used to create Shared VPC based host connections.

> **Tip:**
>
> These additional permissions are not new to Citrix DaaS. They are used to facilitate the implementation of local VPCs. With Shared VPCs, these additional permissions allow access to other shared VPC resources.

A maximum of four extra permissions must be granted to the service account associated with the host connection to support Shared VPC:

- **compute.firewalls.list** - This permission is mandatory. It allows MCS to retrieve the list of firewall rules present on the Shared VPC.
- **compute.networks.list** - This permission is mandatory. It allows MCS to identify the Shared VPC networks available to the service account.
- **compute.subnetworks.list** –This permission is optional depending on how you use VPCs. It allows MCS to identify the subnets within the visible Shared VPCs. This permission is already required when using local VPCs but must also be assigned in the Shared VPC host project.
- **compute.subnetworks.use** - This permission is optional depending on how you use VPCs. It is necessary to use subnet resources in the provisioned machine catalogs. This permission is already required for using local VPCs but must also be assigned in the Shared VPC host project.

When using these permissions, consider that there are different approaches based on the type of permission used to create the machine catalog:

- Project-level permission:
  - Allows access to all Shared VPCs within the host project.
  - Requires the permissions `compute.subnetworks.list` and `compute.subnetworks.use` must be assigned to the service account.
- Subnet-level permission:
  - Allows access to specific subnets within the Shared VPC.
  - Permissions `compute.subnetworks.list` and `compute.subnetworks.use` are intrinsic to the subnet level assignment and therefore do not need to be assigned directly to the service account.

Select the approach that matches your organizational needs and security standards.

> **Tip:**
>
> For more information about the differences between project-level and subnet-level permissions, see Service Project Admins.

Firewall Rules

During the preparation of a machine catalog, a machine image is prepared to serve as the master image system disk for the catalog. When this process occurs, the disk is temporarily attached to a virtual machine. This VM must run in an isolated environment that prevents all inbound and outbound network traffic. This is accomplished through a pair of deny-all firewall rules; one for ingress and one for egress traffic. When using Google Cloud local VCPs, MCS creates this firewall in the local network and applies it to the machine for mastering. After mastering completes, the firewall rule is removed from the image.

We recommend keeping the number of new permissions required to use Shared VPCs to a minimum. Shared VPCs are higher-level corporate resources and typically have more rigid security protocols in place. For this reason, create a pair of firewall rules in the host project on the shared VPC resources, one for ingress and one for egress. Assign the highest priority to them. Apply a new target tag to each of these rules, using the following value:

```
citrix-provisioning-quarantine-firewall
```

When MCS creates or updates a machine catalog, it searches for firewall rules containing this target tag. It then examines the rules for correctness and applies them to the machine used to prepare the master image for the catalog. If the firewall rules are not found, or the rules are found but the rules or their priorities are incorrect, a message similar to the following appears:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag ‘citrix-provisioning-
quarantine-firewall'and proper priority." "Refer to Citrix Documentation
 for details."
```

Configure the shared VPC

Before adding the Shared VPC as a host connection in Citrix DaaS's Full Configuration interface, complete the following steps to add service accounts from the project you intend to provision into:

1. Create an IAM role.
2. Add a service account to the host project IAM role.
3. Add the cloud build service account to the shared VPC.
4. Create firewall rules.

Create an IAM role Determine the access level of the role:

- *Project level access*, or
- A more restricted model using *subnet level access*.

Project level access for IAM role. For the project level IAM role, include the following permissions:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

To create a project level IAM role:

1. In the Google Cloud console, navigate to **IAM & Admin > Roles**.
2. On the **Roles** page, select **CREATE ROLE**.
3. On the **Create Role** page, specify the role name. Select **ADD PERMISSIONS**.
    a) On the **Add permissions** page, add permissions to the role, individually. To add a permission, type the name of the permission in the **Filter table** field. Select the permission and then select **ADD**.
    b) Select **CREATE**.

Subnet-level IAM role. This role omits the addition of the permissions `compute.subnetworks.list` and `compute.subnetworks.use` after selecting **CREATE ROLE**. For this IAM access level, the permissions `compute.firewalls.list` and `compute.networks.list` must be applied to the new role.

To create a subnet level IAM role:

1. In the Google Cloud console, navigate to **VPC network** > **Shared VPC**. The **Shared VPC** page appears, displaying the subnets of the Shared VPC networks that the host project contains.
2. On the **Shared VPC** page, select the subnet that you want to access.
3. In the top-right corner, select **ADD MEMBER** to add a service account.
4. On the **Add members** page, complete these steps:
    a) In the **New members** field, type the name of your service account and then select your service account in the menu.
    b) Select the **Select a role** field and then **Compute Network User**.
    c) Select **SAVE**.
5. In the Google Cloud console, navigate to **IAM & Admin** > **Roles**.
6. On the **Roles** page, select **CREATE ROLE**.
7. On the **Create Role** page, specify the role name. Select **ADD PERMISSIONS**.

a) On the **Add permissions** page, add permissions to the role, individually. To add a permission, type the name of the permission in the **Filter table** field. Select the permission, and then select **ADD**.
b) Select **CREATE**.

Add a service account to the host project IAM role After creating an IAM role, do the following steps to add a service account for the host project:

1. In the Google Cloud console, navigate to the host project and then to **IAM & Admin > IAM**.
2. On the **IAM** page, select **ADD** to add a service account.
3. On the **Add members** page:

   a) In the **New members** field, type the name of your service account and then select your service account in the menu.
   b) Select a role field, type the IAM role you created, and then select the role in the menu.
   c) Select **SAVE**.

The service account is now configured for the host project.

Add the cloud build service account to the shared VPC Every Google Cloud subscription has a service account that is named after the project ID number, followed by `cloudbuild.gserviceaccount`. For example: `705794712345@cloudbuild.gserviceaccount`.

You can determine the project ID number for your project by navigating to **Cloud overview > Dashboard** in the Google Cloud console. The project ID and project number are displayed on the project Dashboard Project info card:

Perform the following steps to add the Cloud Build service account to the Shared VPC:

1. In the Google Cloud console, navigate to the host project and then to **IAM & Admin** > **IAM**.
2. On the **Permissions** page, select **ADD** to add an account.
3. On the **Add members** page, complete these steps:

   a) In the **New members** field, type the name of the Cloud Build service account and then select your service account in the menu.
   b) Select the **Select a role** field, type `Computer Network User`, and then select the role in the menu.
   c) Select **SAVE**.

Create firewall rules As part of the mastering process, MCS copies the selected machine image and uses it to prepare the master image system disk for the catalog. During mastering, MCS attaches the

disk to a temporary virtual machine, which then runs preparation scripts. This VM must run in an isolated environment that prohibits all inbound and outbound network traffic.

To create an isolated environment, MCS requires two *deny all* firewall rules (an ingress rule and an egress rule). Therefore, create two firewall rules (Ingress and Egress) in the *Host Project* as follows:

1. In the Google Cloud console, navigate to the host project and then to **VPC network > Firewall**.
2. On the **Firewall** page, select **CREATE FIREWALL RULE**.
3. On the **Create a firewall rule** page, complete the following:
    - **Name**. Type a name for the rule.
    - **Network**. Select the Shared VPC network to which the ingress firewall rule applies.
    - **Priority**. The smaller the value is, the higher the priority of the rule is. We recommend a small value (for example, 10).
    - **Direction of traffic**. Select **Ingress**.
    - **Action on match**. Select **Deny**.
    - **Targets**. Use the default, **Specified target tags**.
    - **Target tags**. Type `citrix-provisioning-quarantine-firewall`.
    - **Source filter**. Use the default, **IP ranges**.
    - **Source IP ranges**. Type a range that matches all traffic. Type `0.0.0.0/0`.
    - **Protocols and ports**. Select **Deny all**.
4. Select **CREATE** to create the rule.
5. Repeat the steps to create another rule. For **Direction of traffic**, select **Egress**.

Use Customer Managed Encryption Keys (CMEK)

You can use Customer Managed Encryption Keys (CMEK) for MCS catalogs. When using this functionality, you assign the Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` role to the Compute Engine Service Agent. Citrix DaaS account must have the correct permissions in the project where the key is stored. See Assign permissions to Citrix DaaS account. Refer to Helping to protect resources by using Cloud KMS keys for more information.

Your Compute Engine Service Agent is in the following form: `service-<Project _Number >@compute-system.iam.gserviceaccount.com`. This form is different than the default Compute Engine Service Account.

> **Note:**
>
> This Compute Engine Service Account might not appear in the Google Console **IAM Permissions** display. In such cases, use the `gcloud` command as described in Helping to protect resources by using Cloud KMS keys.

Assign permissions to Citrix DaaS account

Google Cloud KMS permissions can be configured in various ways. You can either provide *project level* KMS permissions or *resource level* KMS permissions. See Permissions and roles for more information.

Project level KMS permissions One option is to provide Citrix DaaS account with project-level permissions to browse Cloud KMS resources. To do this, create a custom role, and add the following permissions:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Assign this custom role to your Citrix DaaS account. This allows you to browse regional keys in the relevant project in the inventory.

Resource level KMS permissions For the other option, resource level permissions, in the Google Cloud console, browse to the `cryptoKey` you use for MCS provisioning. Add Citrix DaaS account to a key ring or a key that you use for catalog provisioning.

> **Tip:**
>
> With this option, you cannot browse regional keys for your project in the inventory because Citrix DaaS account does not have project-level list permissions on the Cloud KMS resources. However, you can still provision a catalog using CMEK by specifying the correct `cryptoKeyId` in the `ProvScheme` custom properties. See Create a catalog with CMEK using custom properties.

Rotating customer managed keys

Google Cloud does not support rotating keys on existing persistent disks or images. Once a machine is provisioned it is tied to the key version in use at the time it was created. However, a new version of the key can be created and that new key is used for newly provisioned machines or resources created when a catalog is updated with a new master image.

Important considerations about key rings Key rings cannot be renamed or deleted. Also, you might incur unforeseen charges when configuring them. When deleting or removing a key ring, Google Cloud displays an error message:


```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> **Tip:**
>
> For more information, see Editing or deleting a key ring from the console.

Uniform bucket-level access compatibility

Citrix DaaS is compatible with uniform bucket-level access control policy on Google Cloud. This functionality augments the use of IAM policy that grants permissions to a service account to allow for the manipulation of resources, including storage buckets. With uniform bucket level access control, Citrix DaaS allows you to use an access control list (ACL) to control access to storage buckets or objects stored in them. See Uniform bucket-level access for overview information about Google Cloud uniform bucket-level access. For configuration information, see Require uniform bucket-level access.

Use PowerShell

This section details how to do the following tasks using PowerShell:

- Create a catalog with persistent write-back cache disk
- Improve boot performance with MCSIO
- Create a catalog with CMEK using custom properties
- Create a machine catalog using a machine profile
- Create a machine catalog with machine profile as an instance template
- Create a catalog with shielded VM
- Create Windows 11 VMs on the sole-tenant node

Create a catalog with persistent write-back cache disk

To configure a catalog with persistent write-back cache disk, use the PowerShell command `New-ProvScheme CustomProperties`.

> **Tip:**
>
> Use the PowerShell parameter `New-ProvScheme CustomProperties` only for cloud-based hosting connections. If you want to provision machines using a persistent write-back cache disk for an on-premises solution (for example, XenServer) PowerShell is not needed because the disk persists automatically.

This command supports an extra property, `PersistWBC`, used to determine how the write-back cache disk persists for MCS provisioned machines. The `PersistWBC` property is only used when the `UseWriteBackCache` parameter is specified, and when the `WriteBackCacheDiskSize` parameter is set to indicate that a disk is created.

> **Note:**
>
> This behavior applies to both Azure and GCP where the default MCSIO write-back cache disk is deleted and re-created when power cycling. You can choose to persist the disk to avoid the deletion and recreation of MCSIO write-back cache disk.

Examples of properties found in the `CustomProperties` parameter before supporting `PersistWBC` include:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> **Note:**
>
> This example only applies to Azure. The properties are different in GCP environment.

When using these properties, consider that they contain default values if the properties are omitted from the `CustomProperties` parameter. The `PersistWBC` property has two possible values: **true** or **false**.

Setting the `PersistWBC` property to **true** does not delete the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

Setting the PersistWBC property to **false** deletes the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

> **Note:**
>
> If the PersistWBC property is omitted, the property defaults to **false** and the write-back cache is deleted when the machine is shut down from the management interface.

For example, using the CustomProperties parameter to set PersistWBC to true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Important:**
>
> The PersistWBC property can only be set using the New-ProvScheme PowerShell cmdlet. Attempting to alter the CustomProperties of a provisioning scheme after creation has no impact on the machine catalog and the persistence of the write-back cache disk when a machine is shut down.

For example, set New-ProvSchemeto use the write-back cache while setting the PersistWBC property to true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
```



```
        adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

Improve boot performance with MCSIO

You can improve boot performance for Azure and GCP managed disks when MCSIO is enabled. Use the PowerShell `PersistOSDisk` custom property in the `New-ProvScheme` command to configure this feature. Options associated with `New-ProvScheme` include:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
5 ``````<!--NeedCopy-->
6 ````````Groups" Value="benvaldev5RG3" />
7 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
     />
8 </CustomProperties>
9 <!--NeedCopy-->
```

To enable this feature, set the`PersistOSDisk` custom property to **true**. For example:

```
1 New-ProvScheme
2 -CleanOnBoot
3 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
     /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
     XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
     UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
     StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
     /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
     Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
     =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
     GoldImages.resourcegroup\W10MCSIO-01
     _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8  "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
      CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
```



```
        adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

Create a catalog with CMEK using custom properties

When creating your Provisioning Scheme via PowerShell, specify a `CryptoKeyId` property in `ProvScheme CustomProperties`. For example:

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
        yourCryptoKeyId>" />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

The `cryptoKeyId` must be specified in the following format:

`projectId:location:keyRingName:cryptoKeyName`

For example, if you'd like to use the key `my-example-key` in key ring `my-example-key-ring` in the region `us-east1` and project with ID `my-example-project-1`, your `ProvScheme` custom settings would resemble:

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
        example-project-1:us-east1:my-example-key-ring:my-example-key"
        />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

All MCS provisioned disks and images related to this provisioning scheme use this customer managed encryption key.

> **Tip:**
>
> If you use global keys, the customer properties location must say `global` and not the **region** name, which in the example above is **us-east1**. For example: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:`

> global:my-example-key-ring:my-example-key"/>.

Create a machine catalog using a machine profile

When you create a catalog to provision machines using Machine Creation Services (MCS), you can use a machine profile to capture the hardware properties from a virtual machine and apply them to newly provisioned VMs in the catalog. When `MachineProfile` parameter is not used, the hardware properties are captured from the master image VM or snapshot.
Some properties you define explicitly, for example, `StorageType`, `CatalogZones` and `CryptoKeyId` are ignored from machine profile.

- To create a catalog with a machine profile, use the `New-ProvScheme` command. For example, `New-ProvScheme –MachineProfile "path to VM"`. If you do not specify the `MachineProfile` parameter, hardware properties are captured from the master image VM.
- To update a catalog with a new machine profile, use the `Set-ProvScheme` command. For example, `Set-ProvScheme –MachineProfile "path to new VM"`. This command does not change the machine profile of the existing VMs in the catalog. Only the newly created VMs added to the catalog have the new machine profile.
- You can also update the master image, however, when you update the master image, the hardware properties are not updated. If you want to update the hardware properties, you need to update the machine profile using `Set-ProvScheme` command. These changes will only apply to the new machines in the catalog. For updating the hardware properties of an existing machine, you can use the command `Set-ProvVMUpdateTimeWindow` with `-StartsNow` and `-DurationInMinutes -1` parameters.

  > **Note:**
  >
  > - `StartsNow` indicates that the scheduled start time is the current time.
  > - `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

Create a machine catalog with machine profile as an instance template

You can select a GCP instance template as an input for the machine profile. Instance templates are lightweight resources in GCP, therefore, are very cost effective.

Create a new machine catalog with machine profile as an instance template

1. Open a PowerShell window.

2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Find an instance template in your GCP project using the following command:

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Create a new machine catalog with machine profile as an instance template using New-ProvScheme command:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits\<HostingUnitName>\Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits\<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

   For more information on the New-ProvScheme command, see https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Finish creating the machine catalog using PowerShell commands.

Update a machine catalog to have an instance template as machine profile

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the following command:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits\<HostingUnitName>\
    instanceTemplates.folder\<TemplateName>.template
<!--NeedCopy-->
```

   For information on the Set-ProvScheme command, see https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Create a catalog with shielded VM

You can create an MCS machine catalog with shielded VM properties. A shielded virtual machine is hardened by a set of security controls that provide verifiable integrity of your Compute Engine instances, using advanced platform security capabilities like secure boot, a virtual trusted platform module, UEFI firmware and integrity monitoring.

MCS supports creating the catalog using the machine profile workflow. If you use machine profile workflow, then you must enable the shielded VM properties of a VM instance. You can then use this VM instance as a machine profile input.

Create an MCS machine catalog with shielded VM

1. Enable shielded VM options of a VM instance in Google Cloud console. See Quickstart: Enable Shielded VM options.
2. Create an MCS machine catalog with machine profile workflow by using the VM instance.
   a) Open a PowerShell window
   b) Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
   c) Create an identity pool if not already created.
   d) Run the `New-ProvScheme` command. For example:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
<!--NeedCopy-->
```

3. Finish creating the machine catalog.

Update a machine catalog with a new machine profile

1. Run the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.
    vm
<!--NeedCopy-->
```

To apply the change done in `Set-ProvScheme` to the existing VMs, run the `Set-ProvVMUpdateTimeWindow` command.

1. Run `Set-ProvVMUpdateTimeWindow` command. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Restart the VMs.

Create Windows 11 VMs on the sole-tenant node

You can create Windows 11 VMs in GCP. However, if you install Windows 11 on the master image, then you must enable vTPM during the master image creation process. Also, you must enable vTPM on the machine profile source (VM or instance template).

The key steps to create Windows 11 VMs on the sole-tenant node are:

1. Set up the Google Cloud virtualization environments. For information, see Google Cloud environments.
2. Install VDA. See Install VDAs.
3. Create a connection to Google cloud environments. For information, see Connection to Google cloud environments.
4. Create a Windows 11 Bring Your Own License (BYOL) master image and import the image to Google Cloud. See Create a Windows 11 BYOL master image.
5. Create the machine profile source: Provision VM on the sole-tenant node and enable the vTPM of the source machine profile. See Provision VM on sole-tenant node.
6. Create an MCS machine catalog using the Windows 11 machine profile source enabled with vTPM. The machine profile source must have the same instance type as described in the sole-tenant node. See Create an MCS machine catalog using the Windows 11 machine profile source.

Create a Windows 11 BYOL master image

There are two option to create a Windows 11 BYOL master image and import the master image to Google Cloud:

- Use Google Cloud Cloud Build Tools
- Create the master image on any other hypervisor

Use Google Cloud Cloud Build Tools

1. Upload the Windows 11 ISO, GCP SDK, .NET framework and PowerShell installer files to the GCP storage bucket.
2. Provide the file location in the cloud build `.yaml` file as parameter.
3. Run the following Cloud Build from the command line to build the final Windows 11 image. GCP bootstraps and creates the master image in the selected project using Daisy workflow in GCP and the master image is imported into GCP.

```
1 gcloud compute instances import INSTANCE-NAME--source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
2 <!--NeedCopy-->
```


> **Note:**
>
> Replace all the capital letter text with the actual resource details.

For the complete information, see Create custom Windows BYOL images.

Create the master image on any other hypervisor

1. Create the Windows 11 master image using any other hypervisor.
2. Export the master image in an OVF format to the local machine.
3. Upload the OVF files to the GCP storage bucket using the local gcloud CLI.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
<!--NeedCopy-->
```

4. Run the following Cloud Build from the command line to build the final Windows 11 image. GCP bootstraps and creates the master image in the selected project using Daisy workflow in GCP and the master image is imported into GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
   BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
   --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Note:**
>
> Replace all the capital letter text with the actual resource details.

Provision VM on sole-tenant node

Use sole-tenant nodes to keep your VMs physically separated from VMs in other projects, or to group your VMs together on the same host hardware. For information on the sole-tenant node, see the GCP document Sole-tenancy overview.

For provisioning a VM (machine profile source) on the sole-tenant node, see the GCP document Provision VMs on sole-tenant nodes.

> **Note:**
>
> - Select the same Instance type and region as the node group.
> - Enable vTPM in the Shielded VM section. For more information, see Quickstart: Enable Shielded VM options.
> - Disable the Bitlocker on the source VM.

Create an MCS machine catalog using the Windows 11 machine profile source

You can create an MCS machine catalog to create Windows 11 VMs using the Full Configuration interface or PowerShell commands.

> **Note:**
>
> - For the master image, select the Windows 11 Snapshot or VM.
> - For the machine profile source, select the Windows 11 VM as machine profile. The machine profile source must have the same instance type as described in the sole-tenant node.

For information on using the Full Configuration interface, see Create a machine catalog using the Full Configuration interface.

For information on PowerShell commands, see Create a machine catalog using a machine profile.

After you create the catalog and power on the VMs, you can see the Windows 11 VMs running on the sole tenant node on the Google Cloud console.

Google Cloud Marketplace

You can browse and select images offered by Citrix on Google Cloud Marketplace to create machine catalogs. Currently, MCS supports only the machine profile workflow for this feature.

To search for Citrix VDA VM product through Google Cloud Marketplace, go to https://console.cloud.google.com/marketplace/.

You can use a custom image or a Citrix ready image on Google Cloud Marketplace to update an image of a machine catalog.

> **Note:**
>
> If the machine profile does not contain storage type information, the value is derived from custom properties.

The supported Google Cloud Marketplace images are:

- Windows 2019 Single Session
- Windows 2019 Multi Session
- Ubuntu

Example of using a Citrix ready image as a source for creating a machine catalog:

```
1 New-ProvScheme -ProvisioningSchemeName GCPCatalog \
2 -HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
3 -MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
     win2019-single-vda-v20220819.publicimage \
```



```
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a Google Cloud Platform catalog.

More information

- Create and manage connections and resources
- Connection to Google cloud environments
- Create machine catalogs

Create an HPE Moonshot machine catalog

April 16, 2024

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to HPE Moonshot environments.

> **Note:**
>
> - Create a connection to HPE Moonshot
> - Make sure to have one or more HPE Moonshot nodes available and install VDAs on those nodes.
> - For information about creating the initial HPE Moonshot cartridge image, see the OS Deployment on Moonshot User Guide.

You can create an HPE Moonshot machine catalog using:

- Full Configuration interface
- PowerShell commands

Create a machine catalog using the Full Configuration interface

In the **Machine Catalog Setup** wizard:

1. On the **Operating System** page, select **Multi-session OS** or **Single-session OS**.
2. On the **Machine Management** page, select **Machines that are power managed** and **Another service or technology**.
3. On the **Virtual Machines** page, add machines and their Active Directory machine accounts. You can do either of the following:
   - Click **Add Machines** to add machines manually. The **Select VMs** window appears. Expand the HPE Moonshot chassis connection you created earlier and select the nodes (VMs) you want to add. Then add the associated machine account names.
   - Click **Add CSV File** to bulk add machines. For information about using CSV files to add machines, see Use CSV files to bulk add machines to a catalog.

The **Scopes** and **Summary** pages do not contain HPE Moonshot-specific information.

Create a machine catalog using PowerShell commands

Run the `New-BrokerCatalog` and `New-BrokerMachine` PowerShell commands to create a broker catalog and import machines to the broker catalog.

For example:

```
1 New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage an HPE Moonshot catalog.

More information

- Create and manage connections and resources
- Connection to HPE Moonshot
- Create machine catalogs

Create a Microsoft Azure catalog

May 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Microsoft Azure Resource Manager cloud environments.

> **Note:**
>
> Before creating a Microsoft Azure catalog, you need to finish creating a connection to Microsoft Azure. See Connection to Microsoft Azure.

Create a machine catalog

You can create a machine catalog in two ways:

- Full Configuration interface.
- PowerShell. See Manage Citrix DaaS using Remote PowerShell SDKs. For information on how to implement specific features using PowerShell, see Use PowerShell.

Create a machine catalog using an Azure Resource Manager image in the Full Configuration interface

This information is a supplement to the guidance in Create machine catalogs.

An image can be a disk, snapshot, or an image version of an image definition inside the Azure Compute Gallery that is used to create the VMs in a machine catalog.

Before creating the machine catalog, create an image in Azure Resource Manager.

> **Note:**
>
> - Use of unmanaged disk to provision VM is deprecated.
> - Support for using a master image from a region different from that configured in the host connection is deprecated. Use Azure Compute Gallery to replicate the master image to the desired region.

During image preparation, a preparation virtual machine (VM) is created based on the original VM. This preparation VM is disconnected from the network. To disconnect the network from the preparation VM, a network security group is created to deny all inbound and outbound traffic. The network security group is created automatically once per catalog. The network security group's name is `Citrix-Deny-All-a3pgu-GUID`, where GUID is randomly generated. For example, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

In the machine catalog creation wizard:

1. The **Machine Type** and **Machine Management** pages do not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.
2. On the **Image** page, select an image that you want to use as the master image for all machines in the catalog. The **Select an image** wizard appears. Follow these steps to select an image:

   a) (Applicable only to connections configured with shared images within or across tenants) Select a subscription where the image resides.
   b) Select a resource group.
   c) Navigate to the Azure managed disk, Azure Compute Gallery, or Azure image version.

   When selecting an image, consider the following:

   - Verify that a Citrix VDA is installed on the image.
   - If you select a disk attached to a VM, you must shut down the VM before proceeding to the next step.

   > **Note:**
   >
   > - The subscription corresponding to the connection (host) that created the machines in the catalog is denoted with a green dot. The other subscriptions are those that have the Azure Compute Gallery shared with that subscription. In those subscriptions, only shared galleries are shown. For information about how to configure shared subscriptions, see Share images within a tenant (across subscriptions) and Share images across tenants.
   > - You can create a provisioning scheme using ephemeral OS disk on Windows with trusted launch. When you select an image with trusted launch, then you must select a machine profile with trusted launch that is enabled with vTPM. To create machine catalogs using ephemeral OS disk, see How to create machines using ephemeral OS disks.
   > - When image replication is in progress, you can proceed and select the image as the master image and complete the setup. However, catalog creation might take longer to complete while the image is being replicated. MCS requires the replication to complete within an hour starting from catalog creation. If the replication times out, cata-

> log creation fails. You can verify the replication status in Azure. Try again if the replication is still pending or after the replication completes.
> - You can provision a Gen2 VM catalog by using a Gen2 image to improve boot time performance. However, creating a Gen2 machine catalog using a Gen1 image is not supported. Similarly, creating a Gen1 machine catalog using a Gen2 image is also not supported. Also, any older image that does not have generation information is a Gen1 image.

Choose whether you want VMs in the catalog to inherit configurations from a machine profile. By default, the **Use a machine profile (mandatory for Azure Active Directory)** checkbox is selected. Click **Select a machine profile** to browse to a VM or an ARM template spec from a list of resource groups.

Examples of configurations that VMs can inherit from a machine profile include:

- Accelerated networking
- Boot diagnostics
- Host disk caching (relating to OS and MCSIO disks)
- Machine size (unless otherwise specified)
- Tags placed on the VM

> **Note:**
>
> - When you select a master image for machine catalogs in Azure, the machine profile is filtered based on the master image you selected. For example, the machine profile is filtered based on the Windows OS, security type, hibernation support, and disk encryption set ID of the master image.
> - Using a machine profile with trusted launch as **Security Type** is mandatory when you select an image or snapshot that has trusted launch enabled. You can then enable or disable SecureBoot and vTPM by specifying their values in the Machine Profile. For information about Azure trusted launch, see https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Validate the ARM template spec to make sure whether it can be used as a machine profile to create a machine catalog. For information on creating an Azure template spec, see Create an Azure template spec.

There are two ways to validate the ARM template spec:

- After you select the ARM template spec from the resource group list, click **Next**. Error messages appear if the ARM template spec has errors.
- Run one of the following PowerShell commands:


```
- Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath
   <string>
- Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath
   <string>
```

For example:

```
1  Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
      InventoryPath machineprofile.folder/vdi01-d-rg.
      resourcegroup/VDD-templ-spec.templatespec/1.5.
      templatespecversion
2  <!--NeedCopy-->
```

After you create the catalog, you can view the configurations that the image inherits from the machine profile. On the **Machine Catalogs** node, select the catalog to view its details in the lower pane. Then, click the **Template Properties** tab to view machine profile properties. The **Tags** section displays up to three tags. To view all tags placed on the VM, click **View all**.

If you want MCS to provision VMs on an Azure dedicated host, enable the **Use a host group** checkbox and then select a host group from the list. A host group is a resource that represents a collection of dedicated hosts. A dedicated host is a service that provides physical servers that host one or more virtual machines. Your server is dedicated to your Azure subscription, not shared with other subscribers. When you use a dedicated host, Azure ensures that your VMs are the only machines running on that host. This feature is suitable for scenarios where you must meet regulatory or internal security requirements. To learn more about host groups and considerations for using them, see Provision VMs on Azure dedicated hosts.

> **Important:**
>
> - Only host groups that have Azure auto-placement enabled are shown.
> - Using a host group changes the **Virtual Machines** page offered later in the wizard. Only machine sizes that the selected host group contains are shown on that page. Also, Availability Zones are selected automatically and not available for selection.

3. The **Storage and License Types** page appears only when you use an Azure Resource Manager image.

   You have the following storage types to use for the machine catalog:

   - **Premium SSD**. Offers a high-performance, low-latency disk storage option suitable for VMs with I/O-intensive workloads.
   - **Standard SSD**. Offers a cost-effective storage option that is suitable for workloads that require consistent performance at lower IOPS levels.
   - **Standard HDD**. Offers a reliable, low-cost disk storage option suitable for VMs that run latency-insensitive workloads.

- **Azure ephemeral OS disk**. Offers a cost-effective storage option that reuses the local disk of the VMs to host the operating system disk. Alternatively, you can use PowerShell to create machines that use ephemeral OS disks. For more information, see Azure ephemeral disks. Consider the following when using an ephemeral OS disk:
  - Azure ephemeral OS disk and MCS I/O cannot be enabled at the same time.
  - To update machines that use ephemeral OS disks, you must select an image whose size does not exceed the size of the VM's cache disk or temporary disk.
  - You cannot use the **Retain VM and system disk during power cycles** option offered later in the wizard.

> **Note:**
>
> The identity disk is always created using Standard SSD irrespective of the storage type that you choose.

The storage type determines which machine sizes are offered on the **Virtual Machines** page of the wizard. MCS configures premium and standard disks to use Locally Redundant Storage (LRS). LRS makes multiple synchronous copies of your disk data within a single data center. Azure ephemeral OS disks use the local disk of the VMs to store the operating system. For details about Azure storage types and storage replication, see the following:

- Introduction to Azure Storage
- Azure premium storage: Design for high performance
- Azure Storage redundancy

Select whether to use existing Windows licenses or Linux licenses:

- Windows licenses: Using Windows licenses along with Windows images (Azure platform support images or custom images) lets you run Windows VMs in Azure at a reduced cost. There are two types of licenses:
  - **Windows Server license**. Lets you use your Windows Server or Azure Windows Server licenses, allowing you to use Azure Hybrid Benefits. For details, see https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Azure Hybrid Benefit reduces the cost of running VMs in Azure to the base compute rate, waiving the cost of extra Windows Server licenses from the Azure gallery.
  - **Windows Client license**. Lets you bring your Windows 10 and Windows 11 licenses to Azure, allowing you to run Windows 10 and Windows 11 VMs in Azure without the need for extra licenses. For details, see Client Access Licenses and Management Licenses.
- Linux licenses: With bring-your-own-subscription (BYOS) Linux licenses, you do not have to pay for the software. The BYOS charge only includes the compute hardware fee. There are two types of licenses:

- **RHEL_BYOS**: To use RHEL_BYOS type successfully, enable Red Hat Cloud Access on your Azure subscription.
- **SLES_BYOS**: The BYOS versions of SLES include support from SUSE.

See the following:

- Verify the Windows license
- Configure the Linux license

See the following documents to understand License types and their benefits:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery is a repository for managing and sharing images. It lets you make your images available throughout your organization. We recommend that you store an image in Azure Compute Gallery when creating large non-persistent machine catalogs because doing that enables faster resets of VDA OS disks. After you select **Place prepared image in Azure Compute Gallery**, the **Azure Compute Gallery settings** section appears, letting you specify more Azure Computer Gallery settings:

- **Ratio of virtual machines to image replicas**. Lets you specify the ratio of virtual machines to image replicas that you want Azure to keep. By default, Azure keeps a single image replica for every 40 non-persistent machines. For persistent machines, that number defaults to 1,000.
- **Maximum replica count**. Lets you specify the maximum number of image replicas that you want Azure to keep. The default is 10.

For information on Azure Compute Gallery, see Azure Compute Gallery.

4. On the **Virtual Machines** page, indicate how many VMs you want to create and the machine size. After catalog creation, you can change the machine size by editing the catalog.
5. The **NICs** page does not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.
6. On the **Disk Settings** page, choose whether to enable write-back cache. With the MCS storage optimization feature enabled, you can configure the following settings when creating a catalog. These settings apply to both Azure and GCP environments.

   After enabling write-back cache, you can do the following:

   - Configure the size of the disk and RAM used for caching temporary data. For more information, see Configure cache for temporary data.

- Select the storage type for the write-back cache disk. The following storage options are available to use for the write-back cache disk:
  - Premium SSD
  - Standard SSD
  - Standard HDD
- Choose whether you want the write-back cache disk to persist for the provisioned VMs. Select **Enable write-back cache** to make the options available. By default, **Use non-persistent write-back cache disk** is selected.
- Select the type for the write-back cache disk.
  - **Use non-persistent write-back cache disk**. If selected, the write-back cache disk is deleted during power cycles. Any data redirected to it will be lost. If the VM's temporary disk has sufficient space, it is used to host the write-back cache disk to reduce your costs. After catalog creation, you can check whether the provisioned machines use the temporary disk. To do so, click the catalog and verify the information on the **Template Properties** tab. If the temporary disk is used, you see **Non-persistent Write-back Cache Disk** and its value is **Yes (using VM's temporary disk)**. If not, you see **Non-persistent Write-back Cache Disk** and its value is **No (not using VM's temporary disk)**.
  - **Use persistent write-back cache disk**. If selected, the write-back cache disk persists for the provisioned VMs. Enabling the option increases your storage costs.
- Choose whether to retain VMs and system disks for VDAs during power cycles.

  Retain VM and system disk during power cycles. Available when you've selected **Enable write-back cache**. By default, VMs and the system disks are deleted on shutdown and recreated on startup. If you want to reduce VM restart times, select this option. Keep in mind that enabling this option also increases storage costs.
- Choose whether to **Enable storage cost saving**. If enabled, save storage costs by downgrading the storage disk to Standard HDD when the VM shuts down. The VM switches to its original settings on restart. The option applies to both storage and write-back cache disks. Alternatively, you can also use PowerShell. See Change the storage type to a lower tier when a VM is shut down.

  > **Note:**
  >
  > Microsoft imposes restrictions on changing the storage type during VM shutdown. It's also possible that Microsoft will block storage type changes in the future. For more information, see this Microsoft article.

- Choose whether to encrypt data on machines in this catalog and which encryption key to use. Server-side encryption with a customer-managed key (CMK) lets you manage en-

cryption at a managed disk level and protect data on the machines in the catalog. Default settings are inherited from either the machine profile or the master image, with the profile taking priority:

- If you're using a *machine profile* with a *CMK*, the **Use the following key to encrypt data on each machine** option is auto-selected and defaults to the key from the *machine profile*.
- If you're using a *machine profile* with a Platform Managed Key (PMK) and the *master image* is *CMK* encrypted, the **Use the following key to encrypt data on each machine** option is auto-selected and defaults to the key from the master image.
- If you're *not* using a *machine profile* and the *master image* is *CMK* encrypted, the **Use the following key to encrypt data on each machine** option is auto-selected and defaults to the key from the *master image*.

For more information, see Azure server side encryption.

7. On the **Resource Group** page, choose whether to create resource groups or use existing groups.

   - If you choose to create resource groups, select **Next**.
   - If you choose to use existing resource groups, select groups from the **Available Provisioning Resource Groups** list.

   > **Note:**
   >
   > Select enough groups to accommodate the machines you're creating in the catalog. A message appears if you choose too few. You might want to select more than the minimum required if you plan to add more VMs to the catalog later. You can't add more resource groups to a catalog after the catalog is created.

   For more information, see Azure resource groups.

8. On the **Machine Identities** page, choose an identity type and configure identities for machines in this catalog. If you select the VMs as **Azure Active Directory joined**, you can add them to an Azure AD security group. Detailed steps are as follows:

   a) From the **Identity type** field, select **Azure Active Directory joined**. The **Azure AD security group (optional)** option appears.
   b) Click **Azure AD security group: Create new**.
   c) Enter a group name, and then click **Create**.
   d) Follow the onscreen instructions to sign in to Azure.
   If the group name doesn't exist in Azure, a green icon appears. Otherwise, an error message appears requesting you to enter a new name.
   e) To add the security group to an assigned security group, select **Join an assigned security group as a member**, and then click **Select a group** to choose an assigned group to join.

f) Enter the machine account naming scheme for the VMs.

After catalog creation, Citrix DaaS accesses Azure on your behalf and creates the security group and a dynamic membership rule for the group. Based on the rule, VMs with the naming scheme specified in this catalog are automatically added to the security group.

Adding VMs with a different naming scheme to this catalog requires you to sign in to Azure. Citrix DaaS can then access Azure and create a dynamic membership rule based on the new naming scheme.

When deleting this catalog, deleting the security group from Azure also requires signing in to Azure.

> **Note:**
>
> To rename the Azure AD security group after catalog creation, edit the catalog and go to **Azure AD Security Group** from the left navigation. Names of Azure AD security groups must not contain the following characters: `@ "\ / ; : # . * ? = < > | [ ] ( )'`.

- The **Domain Credentials** and **Summary** pages do not contain Azure-specific information. Follow the guidance in the Create Machine Catalogs article.

Complete the wizard.

Create an Azure template spec

You can create an Azure template spec in the Azure portal and use it in the Full configuration interface and PowerShell commands to create or update an MCS machine catalog.

To create an Azure template spec for an existing VM:

1. Go to the Azure portal. Select a resource group, and then select the VM and network interface. From **...** menu on the top, click **Export template**.
2. Clear **Include parameters** checkbox if you want to create a template spec for catalog provisioning.
3. Click **Add to library** to modify the template spec later.
4. On the **Importing template** page, enter the required information such as **Name**, **Subscription**, **Resource Group**, **Location**, and **Version**. Click **Next: Edit Template**.
5. You also need a network interface as an independent resource if you want to provision catalogs. Therefore, you must remove any `dependsOn` specified in the template spec. For example:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
```



```
],
<!--NeedCopy-->
```

6. Create **Review+Create** and create the template spec.
7. On the **Template Specs** page, verify the template spec you created. Click the template spec. On the left panel, click **Versions**.
8. You can create a new version by clicking **Create new version**. Specify a new version number, make changes to the current template spec, and click **Review + Create** to create the new version of the template spec.

You can get information about the template spec and template version using the following PowerShell commands:

- To get information about the template spec, run:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- To get information about the template spec version, run:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
<!--NeedCopy-->
```

Use a template spec in creating or updating a catalog

You can create or update an MCS machine catalog using a template spec as a machine profile input. To do this, you can use the Full Configuration interface or PowerShell commands.

- Using the **Full configuration** interface: See Create a machine catalog using an Azure Resource Manager image in Full Configuration interface.
- For PowerShell: See Use template spec in creating or updating a catalog using PowerShell

Provision machines into specified Availability Zones

You can provision machines into specific Availability Zones in Azure environments. You can achieve that using the Full Configuration interface or PowerShell.

> **Note:**

> If no zones are specified, MCS lets Azure place the machines within the region. If more than one zone is specified, MCS randomly distributes the machines across them.

Configure Availability Zones in the Full Configuration interface

When creating a machine catalog, you can specify Availability Zones into which you want to provision machines. On the **Virtual Machines** page, select one or more Availability Zones where you want to create machines.

There are two reasons that no Availability Zones are available: The region has no Availability Zones or the selected machine size is unavailable.

For information on configuring using PowerShell command, see Configure Availability Zones using PowerShell.

Azure ephemeral disks

An Azure ephemeral disk allows you to repurpose the cache disk or temporary disk to store the OS disk for an Azure-enabled virtual machine. This functionality is useful for Azure environments that require a higher performant SSD disk over a standard HDD disk. For information on creating a catalog with an Azure ephemeral disk, see Create a catalog with an Azure ephemeral disk.

> **Note:**
>
> Persistent catalogs do not support ephemeral OS disks.

Ephemeral OS disks require that your provisioning scheme use managed disks and an Azure Compute Gallery. For more information, see Azure shared image gallery.

Store an ephemeral OS temporary disk

You have the option of storing an ephemeral OS disk on the VM temp disk or a resource disk. This functionality enables you to use an ephemeral OS disk with a VM that either doesn't have a cache, or has insufficient cache. Such VMs have a temp or resource disk to store an ephemeral OS disk, such as Ddv4.

Consider the following:

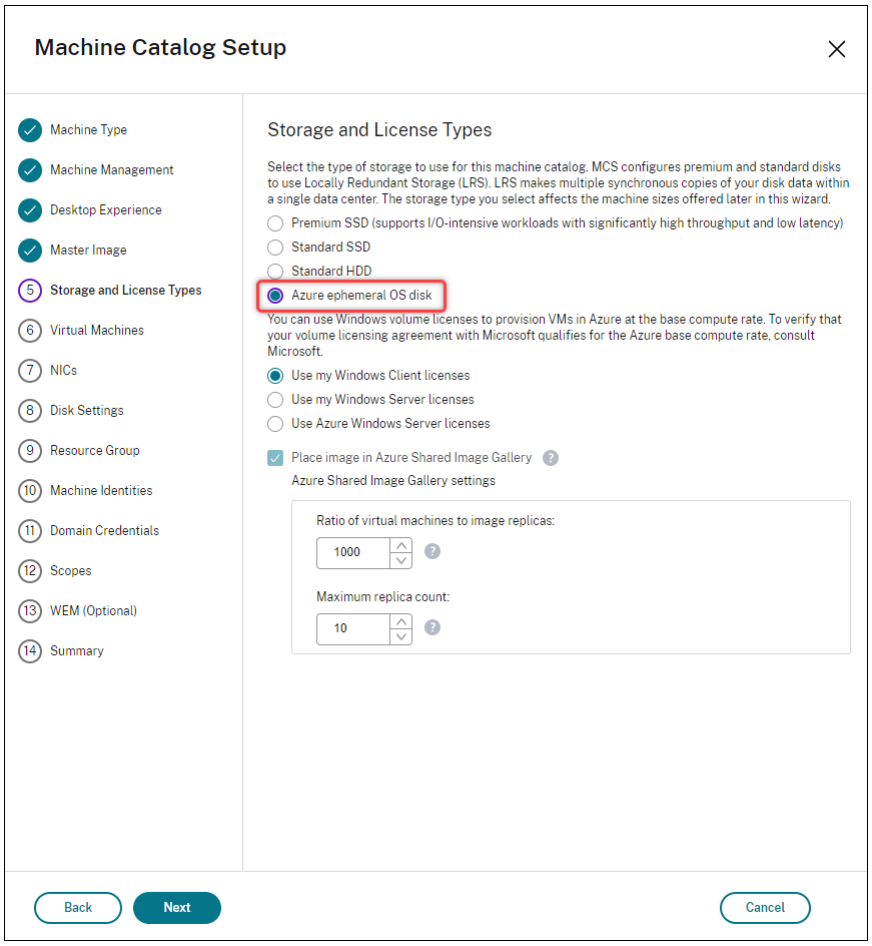
- An ephemeral disk is stored either in the VM cache disk, or the VMs temporary (resource) disk. The cache disk is preferred over the temporary disk, unless the cache disk is not large enough to hold the contents of the OS disk.
- For updates, a new image that is larger than the cache disk but smaller than the temp disk results in replacing the ephemeral OS disk with the VM's temp disk.

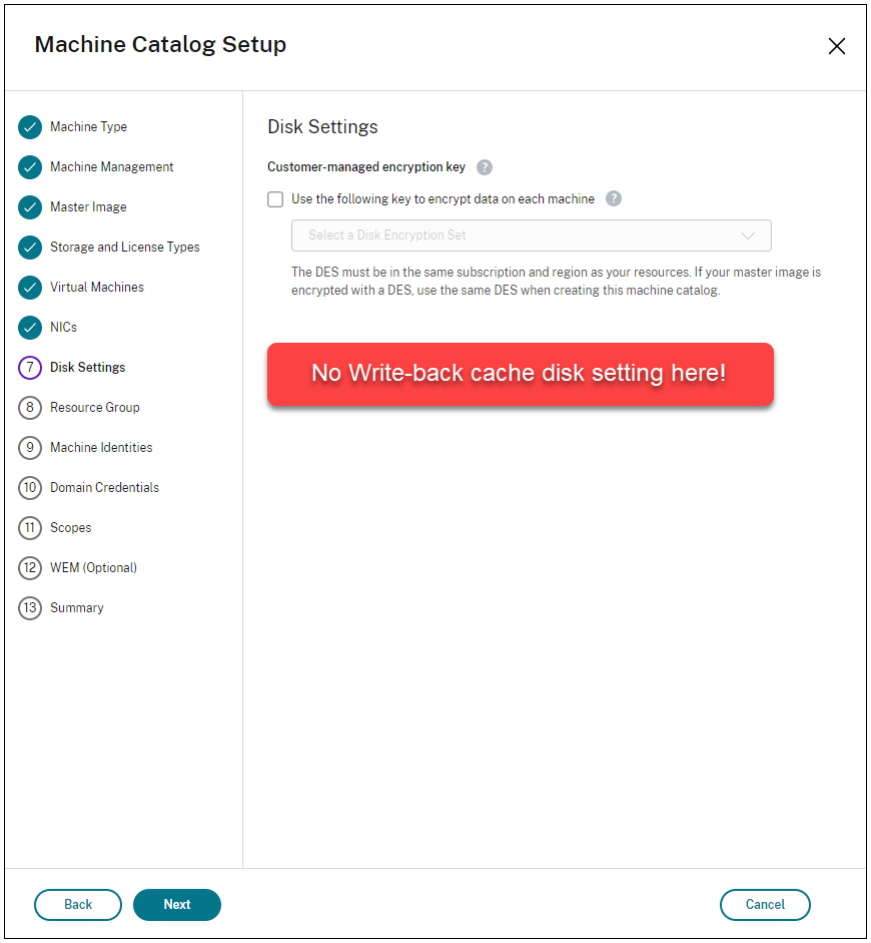
Azure ephemeral disk and Machine Creation Services (MCS) storage optimization (MCS I/O)

Azure ephemeral OS disk and MCS I/O cannot be enabled at the same time.

The important considerations are as follows:

- You cannot create a machine catalog with both ephemeral OS disk and MCS I/O enabled at the same time.
- In the **Machine Catalog Setup** wizard, if you select **Azure ephemeral OS disk** on the **Storage and License Types** page, you do not get the option for write-back cache disk settings on the **Disk Settings** page.





- The PowerShell parameters (`UseWriteBackCache` and `UseEphemeralOsDisk`) set to **true** in `New-ProvScheme` or `Set-ProvScheme` fails with proper error message.
- For existing machine catalogs created with both features enabled, you can still:
  - update a machine catalog.
  - add or delete VMs.
  - delete a machine catalog.

Azure Compute Gallery

Use Azure Compute Gallery (formerly Shared Image Gallery) as a published image repository for MCS provisioned machines in Azure. You can store a published image in the gallery to accelerate the creation and hydration of OS disks, improving start and application launch times for non-persistent VMs. Azure Compute Gallery contains the following three elements:

- Gallery: Images are stored here. MCS creates one gallery for each machine catalog.
- Gallery Image Definition: This definition includes information (operating system type and state,

Azure region) about the published image. MCS creates one image definition for each image created for the catalog.

- Gallery Image Version: Each image in an Azure Compute Gallery can have multiple versions, and each version can have multiple replicas in different regions. Each replica is a full copy of the published image. Citrix DaaS creates one Standard_LRS image version (version 1.0.0) for each image with the appropriate number of replicas in the catalog's region, based on the number of machines in the catalog, the configured replica ratio, and the configured replica maximum.

> **Note:**
>
> Azure Compute Gallery functionality is only compatible with managed disks. It is not available for legacy machine catalogs.

For more information, see Azure shared image gallery overview.

Access images from Azure Compute Gallery

When selecting an image to use for creating a machine catalog, you can select images you created in the Azure Compute Gallery. These images appear in the list of images on the **Image** page of the Machine Catalog Setup wizard.

For these images to appear, you must:

1. Set up Citrix DaaS.
2. Connect to the Azure Resource Manager.
3. In the Azure portal, create a resource group. For details, see Create an Azure Shared Image Gallery using the portal.
4. In the resource group, create an Azure Compute Gallery.
5. In the Azure Compute Gallery, create an image definition.
6. In the image definition, create an image version.

For information on configuring the Azure Compute Gallery, see Configure Azure Compute Gallery.

Conditions for Azure temporary disk to be eligible for write-back cache disk

You can use the Azure temporary disk as write-back cache disk only if all the following conditions are satisfied:

- The write-back cache disk must non-persist as the Azure temporary disk is not appropriate for persistent data.
- The chosen Azure VM size must include a temporary disk.
- The ephemeral OS disk is not required to be enabled.

- Accept to place the write-back cache file on Azure temporary disk.
- The Azure temporary disk size must be greater than the total size of (write-back cache disk size + reserved space for paging file + 1 GB buffer space).

Non-persistent write-back cache disk scenarios

The following table describes three different scenarios when a temporary disk is used for write-back cache while creating a machine catalog.

Scenario	Outcome
All conditions to use a temporary disk for write-back cache are satisfied.	The WBC file `mcsdif.vhdx` is placed on the temporary disk.
Temporary disk has insufficient space for write-back cache usage.	A VHD disk 'MCSWCDisk'is created and WBC file `mcsdif.vhdx` is placed on this disk.
Temporary disk has sufficient space for write-back cache usage but `UseTempDiskForWBC` is set to false.	A VHD disk 'MCSWCDisk'is created and WBC file `mcsdif.vhdx` is placed on this disk.

See the following PowerShell topics:

- Create a machine catalog with non-persistent write-back cache disk
- Create a machine catalog with persistent write-back cache disk

Azure server-side encryption

Citrix DaaS supports customer-managed encryption keys for Azure managed disks through Azure Key Vault. With this support you can manage your organizational and compliance requirements by encrypting the managed disks of your machine catalog using your own encryption key. For more information, see Server-side encryption of Azure Disk Storage.

When using this feature for managed disks:

- To change the key that the disk is encrypted with, you change the current key in the `DiskEncryptionSet`. All resources associated with that `DiskEncryptionSet` change to be encrypted with the new key.
- When you disable or delete your key, any VMs with disks using that key automatically shut down. After shutting down, the VMs are not usable unless the key is enabled again or you assign a new key. Any catalog using the key cannot be powered on, and you cannot add VMs to it.

Important considerations when using customer-managed encryption keys

Consider the following when using this feature:

- All resources related to your customer-managed keys (Azure Key Vaults, disk encryption sets, VMs, disks, and snapshots) must reside in the same subscription and region.
- Disks, snapshots, and images encrypted with customer-managed keys cannot move to another resource group and subscription.
- Refer to the Microsoft site for limitations on disk encryption sets per region.

> **Note:**
>
> See Quickstart: Create a Key Vault using the Azure portal for information on configuring Azure server-side encryption.

Azure Customer-managed encryption key

When creating a machine catalog, you can choose whether to encrypt data on the machines provisioned in the catalog. Server-side encryption with a customer-managed encryption key lets you manage encryption at a managed disk level and protect data on the machines in the catalog. A Disk Encryption Set (DES) represents a customer-managed key. To use this feature, you must first create your DES in Azure. A DES is in the following format:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Select a DES from the list. The DES you select must be in the same subscription and region as your resources.

If you create a catalog with an encryption key and later disable the corresponding DES in Azure, you can no longer power on the machines in the catalog or add machines to it.

See Create a machine catalog with customer-managed key.

Azure disk encryption at host

You can create an MCS machine catalog with encryption at host capability. Currently, MCS supports only the machine profile workflow for this feature. You can use a VM or a template spec as an input for a machine profile.

This encryption method does not encrypt the data through the Azure storage. The server hosting the VM encrypts the data and then the encrypted data flows through the Azure storage server. Hence, this method of encryption encrypts data end to end.

Restrictions:

Azure disk encryption at the host is:

- Not supported for all Azure machine sizes
- Incompatible with Azure disk encryption

For more information, see:

- Create a machine catalog with encryption at host capability.
- Retrieve encryption at host information from a machine profile

Double encryption on managed disk

You can create a machine catalog with double encryption. Any catalogs created with this feature have all disks server side encrypted with both platform and customer-managed keys. You own and maintain the Azure Key Vault, Encryption Key, and the Disk Encryption Sets (DES).

Double encryption is platform-side encryption (default) and customer-managed encryption (CMEK). Therefore, if you are a high security sensitive customer who is concerned about the risk associated with any encryption algorithm, implementation, or a compromised key, you can opt for this double encryption. Persistent OS and data disks, snapshots, and images are all encrypted at rest with double encryption.

> **Note:**
>
> - You can create and update a machine catalog with double encryption using the Full Configuration interface and PowerShell commands.
> - You can use non-machine profile-based workflow or machine profile-based workflow for creating or updating a machine catalog with double encryption.
> - If you use non-machine profile-based workflow to create a machine catalog, you can reuse the stored `DiskEncryptionSetId`.
> - If you use a machine profile, you can use a VM or template spec as a machine profile input.

Limitations

- Double encryption is not supported for Ultra Disks or Premium SSD v2 disks.
- Double encryption is not supported on unmanaged disks.
- If you disable a Disk Encryption Set key associated with a catalog, then the VMs of the catalog are disabled.
- All resources related to your customer-managed keys (Azure Key Vaults, disk encryption sets, VMs, disks, and snapshots) must be in the same subscription and region.
- You can only create up to 50 disk encryption sets per region per subscription.

See the following PowerShell topics:

- Create a machine catalog with double encryption
- Convert an unencrypted catalog to use double encryption
- Verify the catalog is double encrypted

Azure resource groups

Azure provisioning resource groups provide a way to provision the VMs that provide applications and desktops to users. You can add existing empty Azure resource groups when you create an MCS machine catalog, or have new resource groups created for you. For information about Azure resource groups, see the Microsoft documentation.

Azure Resource Group Usage

There is no limit on the number of virtual machines, managed disks, snapshots, and images per Azure Resource Group. (The limit of 240 VMs per 800 managed disks per Azure Resource Group has been removed.)

- When using a full-scope service principal to create a machine catalog, MCS creates only one Azure Resource Group and uses that group for the catalog.
- When using a narrow scope service principal to create a machine catalog, you must supply an empty, pre-created Azure Resource Group for the catalog.

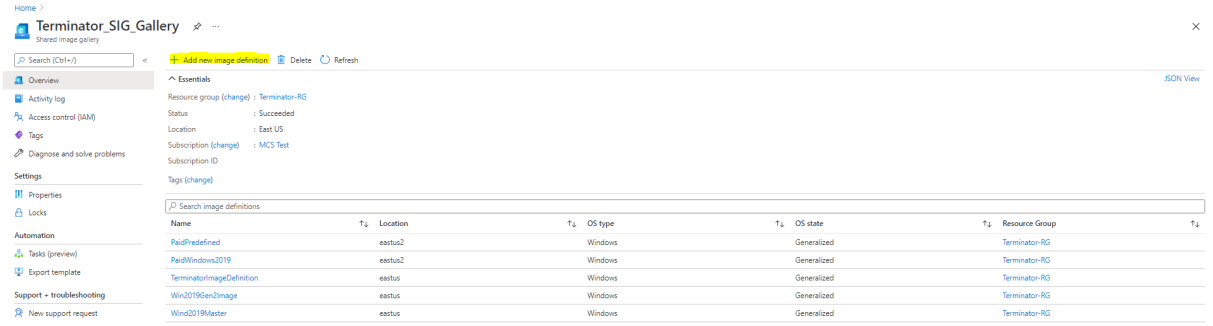
Azure Marketplace

Citrix DaaS supports using a master image on Azure that contains plan information to create a machine catalog. For more information, see Microsoft Azure Marketplace.

> **Tip:**
>
> Some images found on the Azure Marketplace, like the standard Windows Server image, do not append plan information. Citrix DaaS feature is for paid images.

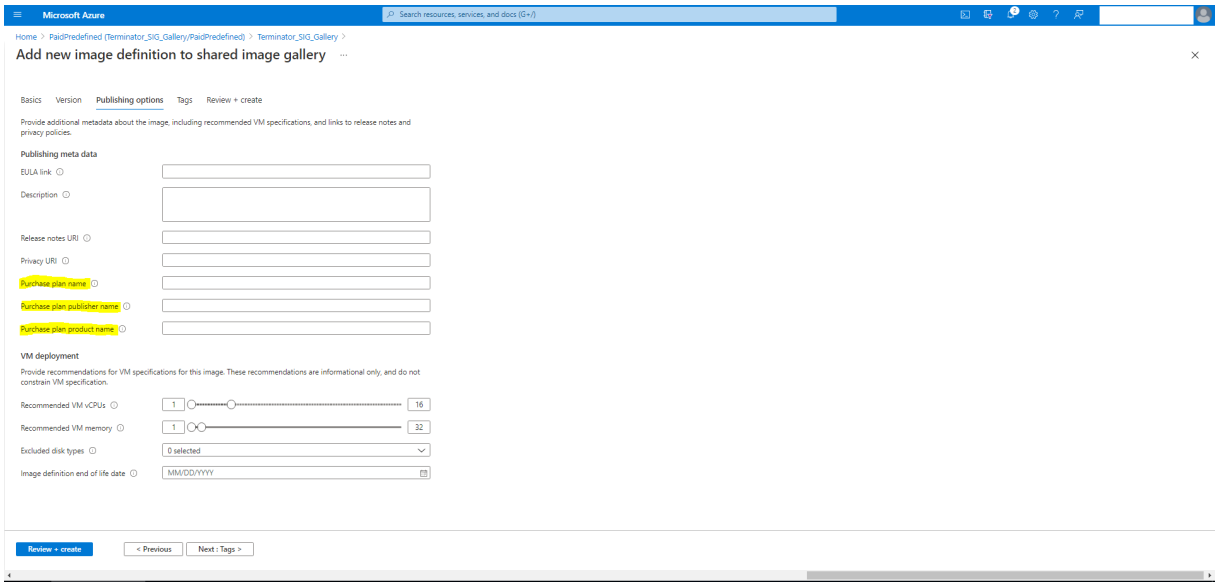
Ensure that the image created in Azure Compute Gallery contains Azure plan information

Use the procedure in this section to view Azure Compute Gallery images in the Full configuration interface. These images can optionally be used for a master image. To put the image into an Azure Compute Gallery, create an image definition in a gallery.

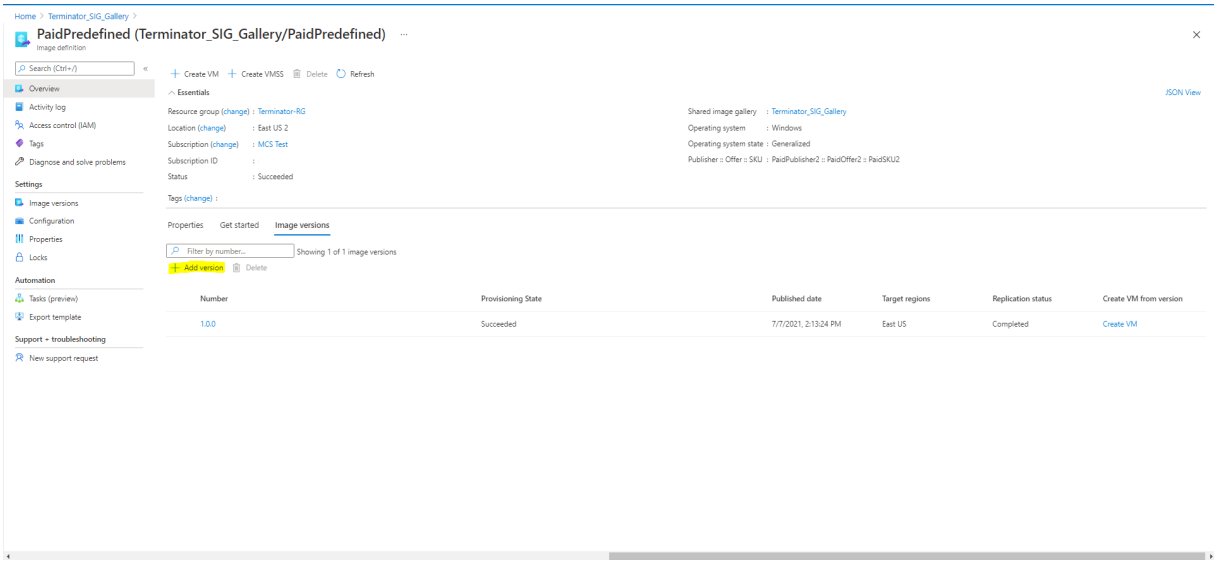


In the **Publishing options** page, verify the purchase plan information.

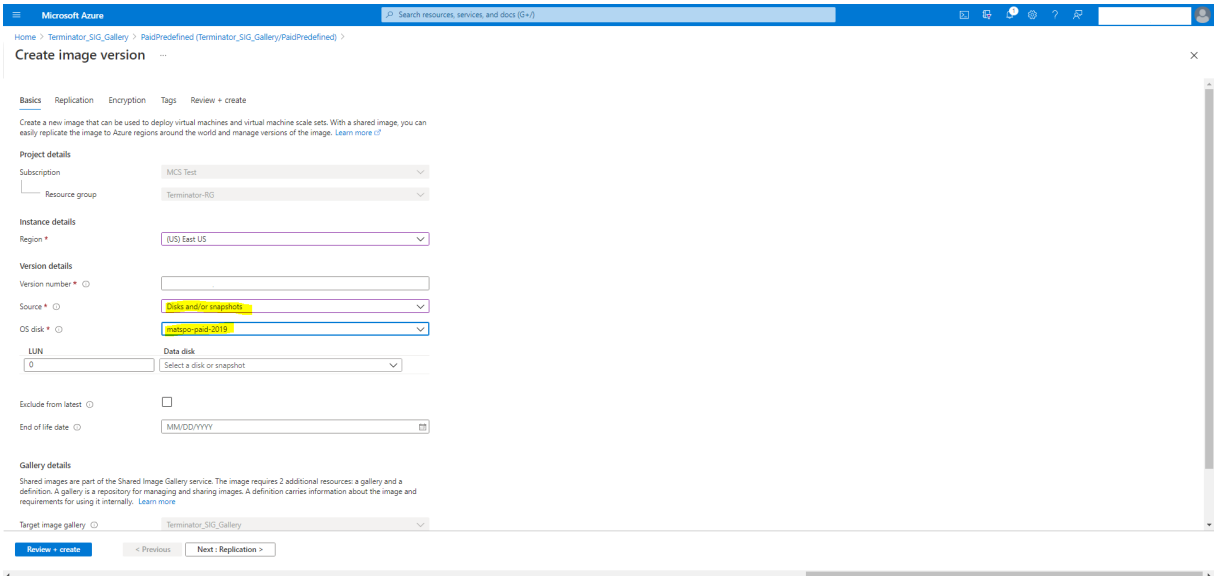
The purchase plan information fields are initially empty. Populate those fields with the purchase plan information used for the image. Failure to populate purchase plan information can cause the machine catalog process to fail.



After verifying the purchase plan information, create an image version within the definition. This is used as the master image. Click **Add version**:



In the **Version details** section, select the image snapshot or managed disk as the source:



Provision catalog VMs with Azure Monitor Agent installed

Azure monitoring is a service which you can use to collect, analyze, and act on telemetry data from your Azure and on-premises environments.

Azure Monitor Agent (AMA) collects monitoring data from compute resources like virtual machines and delivers the data to Azure monitor. It currently supports the collection of Event Logs, Syslog, and Performance metrics and sends it to Azure Monitor Metrics and Azure Monitor Logs data sources.

To enable monitoring by uniquely identifying the VMs in monitoring data, you can provision the VMs of an MCS machine catalog with AMA installed as an extension.

Requirements

- Permissions: Ensure that you have the minimum Azure permissions as specified in About Azure permissions and the following permissions to use Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Data Collection Rule: Set up a data collection rule in the Azure portal. For information about setting up a DCR, see Create a data collection rule. A DCR is platform specific (Windows or Linux). Ensure that you create a DCR as per the required platform.
  The AMA uses Data Collection Rules (DCR) to manage the mapping between the resources, such as VMs, and data sources, like Azure Monitor Metrics and Azure Monitor Logs.
- Default Workspace: Create a workspace in the Azure portal. For information on creating a workspace, see Create a Log Analytics workspace. When you collect logs and data, the information is stored in a workspace. A workspace has a unique workspace ID and resource ID. The workspace name must be unique for a given resource group. After you create a workspace, configure data sources and solutions to store their data in the workspace.
- Whitelisted the monitor extension: The extensions `AzureMonitorWindowsAgent` and `AzureMonitorLinuxAgent` are Citrix defined whitelisted extensions. To view the list of whitelisted extensions, use the PowerShell command, `Get-ProvMetadataConfiguration` .
- Master Image: Microsoft recommends removing extensions from an existing machine before creating a new machine from it. If the extensions are not removed, it might lead to leftover files and unexpected behavior. For more information, see If the VM is recreated from an existing VM.

For information on creating a catalog with AMA enabled using PowerShell, see Provision catalog VMs with AMA enabled.

Azure confidential VMs

Azure confidential computing VMs ensure that your virtual desktop is encrypted in memory and protected in use.

You can use MCS to create a catalog with Azure confidential VMs. You must use the machine profile workflow to create such a catalog. You can use both VM and ARM template spec as a machine profile input.

Important considerations for confidential VMs

The important considerations for supported VM sizes and creating machine catalog with confidential VMs are as follows:

- Supported VM sizes: Confidential VMs support the following VM sizes:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Create machine catalogs with confidential VMs.
  - You can create a machine catalog with Azure Confidential VMs using the Full Configuration interface and PowerShell commands.
  - You must use machine profile-based workflow for creating a machine catalog with Azure Confidential VMs. You can use a VM or template spec as a machine profile input.
  - The master image and the machine profile input must be both enabled with the same confidential security type. The security types are:
    * VMGuestStateOnly: Confidential VM with only VM guest state encrypted
    * DiskWithVMGuestState: Confidential VM with both OS disk and VM guest state encrypted with platform managed key or customer managed key. Both normal and Ephemeral OS disk can be encrypted.
  - You can get confidential VM information of various resource types such as managed disk, snapshot, Azure Compute Gallery image, VM, and ARM template spec using the AdditionalData parameter. For example:

    ```
    PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
       \image.folder\username-dev-testing-rg.resourcegroup\
       username-dev-tsvda.vm).AdditionalData
    <!--NeedCopy-->
    ```

    The additional data fields are:

    * DiskSecurityType
    * ConfidentialVMDiskEncryptionSetId
    * DiskSecurityProfiles

    To get the confidential computing property of a machine size, run the following command: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

The additional data field is `ConfidentialComputingType`.

- You cannot change the master image or machine profile from confidential to non-confidential security type, or from non-confidential to confidential security type.
- You get appropriate error messages for any incorrect configuration.

Prepare master images and machine profiles

Before creating a set of confidential VMs, follow these steps to prepare a master image and a machine profile for them:

1. In the Azure portal, create a confidential VM with specific settings, such as

   - **Security Type**: Confidential virtual machines
   - **Confidential OS disk encryption**: Enabled.
   - **Key management**: Confidential disk encryption with a platform-managed key
     For more information about creating confidential VMs, see this Microsoft article.

2. Prepare the master image on the VM created. Install the necessary applications and VDA on the created VM.

   > **Note:**
   >
   > Creating confidential VMs using VHD is not supported. Instead, use Azure Compute Gallery, managed disks, or snapshots for this purpose.

3. Create the machine profile using either of these ways:

   - Use the existing VM created in step 1 if it possesses the needed machine properties.
   - If you opt for an ARM template spec as the machine profile, create the template spec as needed. Specifically, configure parameters that meet your confidential VM requirements, such as *SecurityEncryptionType* and *diskEncryptionSet* (for customer-managed key). For more information, see Create an Azure template spec.

     > **Note:**
     >
     > - Ensure the master image and the machine profile have the same security key type.
     > - To create confidential VMs requiring confidential OS disk encryption with a customer-managed key, make sure that the disk encryption set IDs in both the master image and the machine profile are identical.

Create confidential VMs using Full Configuration or PowerShell commands

To create a set of confidential VMs, create a machine catalog using a master image and a machine profile derived from a desired confidential VM.

To create the catalog using Full Configuration, follow the steps described in Create machine catalogs. Keep the following considerations in mind:

- On the **Image** page, select a master image and a machine profile you've prepared for the confidential VM creation. The machine profile selection is mandatory and only profiles that match the same security encryption type as the selected master image are available for selection.
- On the **Virtual Machines** page, only machine sizes that support confidential VMs appear for selection.
- On the **Disk Settings** page, you can't specify the disk encryption set because it's inherited from the selected machine profile.

Use PowerShell

This section details how to do the following tasks using PowerShell:

- Use template spec in creating or updating a catalog using PowerShell
- Enable Azure VM extensions
- Machine catalogs with trusted launch
- Use machine profile property values
- Configure Availability Zones using PowerShell
- Provision VMs on Azure dedicated hosts
- Configure storage types
- Enable zone-redundant storage
- Capture diagnostic settings on VMs and NICs from a machine profile
- Verify the Windows license
- Configure the Linux license
- Create a machine catalog with an Azure ephemeral disk
- Configure Azure Compute Gallery
- Create or update a catalog with multiple NICs per VM
- Create a machine catalog with non-persistent write-back cache disk
- Create a machine catalog with persistent write-back cache disk
- Improve boot performance with MCSIO
- Create a machine catalog with customer-managed encryption key
- Create a machine catalog with encryption at host capability
- Create a machine catalog with double encryption
- Page file location determination

- Page file setting scenarios
- Specify page file setting
- Modify page file settings
- Provision catalog VMs with AMA enabled
- Create a catalog using Azure Spot VMs
- Copy tags on all resources

Use template spec in creating or updating a catalog using PowerShell

You can create or update an MCS machine catalog using a template spec as a machine profile input. To do this, you can use the Full Configuration interface or PowerShell commands.

For Full Configuration interface, see Create a machine catalog using an Azure Resource Manager image in Full Configuration interface.

Using PowerShell commands:

1. Open the **PowerShell** window.
2. Run `asnp citrix*`.
3. Create or update a catalog.

    - To create a catalog:

        a) Use the `New-ProvScheme` command with a template spec as a machine profile input. For example:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
    image.folder/fgthj.resourcegroup/nab-ws-
    vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

        b) Finish creating the catalog.

    - To update a catalog, use `Set-ProvScheme` command with a template spec as a machine profile input. For example:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
    Us.region/vm.folder/MasterDisk.vm'
MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/testing.templatespec/V1.
    templatespecversion'
```



```
3   [-ProvisioningSchemeName] <String>
4   [-CustomProperties <String>][-ServiceOffering <String>] [-
       PassThru]
5   [<CommonParameters>]
6   <!--NeedCopy-->
```

Enable Azure VM extensions

After you select the ARM template spec, run the following PowerShell commands to work with Azure VM extensions:

- To view the list of supported Azure VM extensions: `Get-ProvMetadataConfiguration`
- To add more VM extensions: `Add-ProvMetadataConfiguration`. For example, `Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  If you try to add any of the following, the command fails with an error message:

  - Citrix defined extension.
  - Existing user defined extension.
  - Unsupported configuration keys. Currently, the supported configuration key is `Extension`.
- To remove extensions from the list: `Remove-ProvMetadataConfiguration`. You can remove the extensions that you added.

Machine catalogs with trusted launch

To successfully create a machine catalog with trusted launch, use:

- A machine profile with trusted launch
- A VM size that supports trusted launch
- A Windows VM version that supports trusted launch. Currently, Windows 10, Windows 11, Windows Server 2016, 2019, and 2022 support trusted launch.

> **Important:**
>
> MCS supports creating a new catalog with trusted launch enabled VMs. However, to update an existing persistent catalog and existing VMs, you have to use the Azure portal. You cannot update trusted launch of a non-persistent catalog. For more information, see the Microsoft document Enable Trusted launch on existing Azure VMs.

To view the Citrix DaaS offering inventory items, and to determine whether the VM size supports trusted launch, run the following command:

1. Open a PowerShell window.
2. Run **asnp citrix*** to load the Citrix-specific PowerShell modules.
3. Run the following command:

```
$s = (ls XDHyp:\HostingUnits\<name of hosting unit>\
   serviceoffering.folder\"<VM size>".serviceoffering)
<!--NeedCopy-->
```

4. Run `$s | select -ExpandProperty Additionaldata`
5. Check the value of the `SupportsTrustedLaunch` attribute.
   - If `SupportsTrustedLaunch` is **True**, the VM size supports trusted launch.
   - If `SupportsTrustedLaunch` is **False**, the VM size does not support trusted launch.

As per Azure's PowerShell, you can use the following command to determine the VM sizes that support trusted launch:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

The following are examples that describe whether the VM size supports trusted launch after you run the Azure PowerShell command.

- *Example 1*: If the Azure VM supports only Generation 1, that VM does not support trusted launch. Therefore, the `TrustedLaunchDisabled` capability is not displayed after you run the Azure PowerShell command.
- *Example 2*: If the Azure VM supports only Generation 2 and the `TrustedLaunchDisabled` capability is **True**, the Generation 2 VM size is not supported for trusted launch.
- *Example 3*: If the Azure VM supports only Generation 2 and the `TrustedLaunchDisabled` capability is not displayed after you run the PowerShell command, the Generation 2 VM size is supported for trusted launch.

For more information on trusted launch for Azure virtual machines, see the Microsoft document Trusted launch for Azure virtual machines.

Create a machine catalog with trusted launch

1. Create a master image enabled with trusted launch. See the Microsoft documentation Trusted launch VM Images.
2. Create a VM or template spec with security type as **trusted launch virtual machines**. For more information on creating a VM or template spec, see the Microsoft document Deploy a trusted launch VM.

3. Create a machine catalog using the Full Configuration interface or PowerShell commands.

   - If you want to use the Full configuration interface, see Create a machine catalog using an Azure Resource Manager image in the Full Configuration interface.
   - If you want to use PowerShell commands, use the `New-ProvScheme` command with the VM or the template spec as a machine profile input. For the complete list of commands to create a catalog, see Creating a catalog.

     Example of `New-ProvScheme` with VM as machine profile input:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
-MachineProfile "XDHyp:\HostingUnits\<adnet>\machineprofile.
    folder\<def.resourcegroup>\<machine profile vm.vm>"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

     Example of `New-ProvScheme` with template spec as machine profile input:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

Errors while creating machine catalogs with Trusted launch

You get appropriate errors in the following scenarios while creating a machine catalog with trusted launch:

Scenario	Error
If you select a machine profile while creating an unmanaged catalog	`MachineProfileNotSupportedForUnmanagedCata`
If you select a machine profile that supports Trusted launch while creating a catalog with unmanaged disk as the master image	`SecurityTypeNotSupportedForUnmanagedDisk`
If you do not select a machine profile while creating a managed catalog with a master image source with Trusted launch as the security type	`MachineProfileNotFoundForTrustedLaunchMaste`
If you select a machine profile with a security type different from the security type of the master image	`SecurityTypeConflictBetweenMasterImageAndMa`
If you select a VM size that does not support Trusted launch but use a master image that supports Trusted launch while creating a catalog	`MachineSizeNotSupportTrustedLaunch`

Use machine profile property values

The machine catalog uses the following properties that are defined in the custom properties:

- Availability zone
- Dedicated Host Group Id
- Disk Encryption Set Id
- OS type
- License type
- Storage type

If these custom properties are not defined explicitly, then the property values are set from the ARM template spec or VM, whichever is used as the machine profile. In addition, if `ServiceOffering` is not specified, then it is set from the machine profile.

> **Note:**
>
> If some of the properties are missing from the machine profile and not defined in the custom properties, then the default values of the properties take place wherever applicable.

The following section describes some scenarios at `New-ProvScheme` and `Set-ProvScheme` when `CustomProperties` either have all the properties defined or values are derived from the MachineProfile.

- New-ProvScheme Scenarios
  - MachineProfile has all the properties and CustomProperties are not defined. Example:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    The following values are set as custom properties for the catalog:

    ```
    Get-ProvScheme | select CustomProperties
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
    <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
       -value>"/>
    <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
       " Value="<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="
       DedicatedHostGroupId" Value="<mpA-value>"/>
    <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
       value>"/>
    </CustomProperties>
    <!--NeedCopy-->
    ```

  - MachineProfile has some properties and CustomProperties are not defined. Example: MachineProfile only has LicenseType and OsType.

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    The following values are set as custom properties for the catalog:

    ```
    Get-ProvScheme | select CustomProperties
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
       -value>"/>
    <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpA-value>"/>
    </CustomProperties>
    <!--NeedCopy-->
    ```

  - Both MachineProfile and CustomProperties define all properties. Example:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
     $CustomPropertiesA
    ```


Custom properties take priority. The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId
   " Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="
   DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<
   CustomPropertiesA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Some properties are defined in MachineProfile and some properties are defined in CustomProperties. Example:
  - CustomProperties define LicenseType and StorageAccountType
  - MachineProfile define LicenseType, OsType, and Zones

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
   -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
   value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Some properties are defined in MachineProfile and some properties are defined in CustomProperties. In addition, ServiceOffering is not defined. Example:

* CustomProperties define StorageType
* MachineProfile define LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
    serviceoffering.folder\<explicit-machine-size>.
    serviceoffering"
<!--NeedCopy-->
```

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder\<explicit-machine-size>.
    serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- If the OsType is in neither in the CustomProperties nor in the MachineProfile, then:
  * The value is read from the master image.
  * If the master image is an unmanaged disk, the OsType is set to Windows. Example:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

The value from the master image is written to the custom properties, in this case Linux.

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="OSType" Value="
    Linux"/>
</CustomProperties>
<!--NeedCopy-->
```

- Set-ProvScheme Scenarios
  - An existing catalog with:

    * CustomProperties for `StorageAccountType` and OsType
    * MachineProfile `mpA.vm` that defines zones

- Updates:

    * MachineProfile mpB.vm that defines StorageAccountType
    * A new set of custom properties $CustomPropertiesB that defines LicenseType and OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

The following values are set as custom properties for the catalog:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6       </CustomProperties>
7  <!--NeedCopy-->
```

- An existing catalog with:

    * CustomProperties for `StorageAccountType` and OsType
    * MachineProfile `mpA.vm` that defines StorageAccountType and LicenseType

- Updates:

    * A new set of custom properties $CustomPropertiesB that defines StorageAccountType and OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

The following values are set as custom properties for the catalog:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<mp-A-value>"/>
```



```
</CustomProperties>
<!--NeedCopy-->
```

- An existing catalog with:
  - CustomProperties for `StorageAccountType` and OsType
  - MachineProfile `mpA.vm` that defines Zones
- Updates:
  - A MachineProfile mpB.vm that defines StorageAccountType and LicenseType
  - `ServiceOffering` is not specified

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder\<value-from-machineprofile>.
   serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

Configure Availability Zones using PowerShell

Using PowerShell, you can view the Citrix DaaS offering inventory items by using `Get-Item`. For example, to view the *Eastern US region* `Standard_B1ls` service offering:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
   name\East US.region\serviceoffering.folder\Standard_B1ls.
   serviceoffering"
<!--NeedCopy-->
```

To view the zones, use the `AdditionalData` parameter for the item:

```
$serviceOffering.AdditionalData
```

If Availability Zones are not specified, there is no change in how machines are provisioned.

To configure Availability Zones through PowerShell, use the **Zones** custom property available with the `New-ProvScheme` operation. The **Zones** property defines a list of Availability Zones to provision machines into. Those zones can include one or more Availability Zones. For example, `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` for Zones 1 and 3.

Use the `Set-ProvScheme` command to update the zones for a provisioning scheme.

If an invalid zone is provided, the provisioning scheme is not updated, and an error message appears providing instructions on how to fix the invalid command.

> **Tip:**
>
> If you specify an invalid custom property, the provisioning scheme is not updated and a relevant error message appears.

Outcome of using host groups and Azure availability zones at the same time

There is a pre-flight check to assess whether the creation of a machine catalog will be successful based on the availability zone specified in the custom property and the host group's zone. Catalog creation fails if the availability zone custom property does not match the host group's zone.

For information on configuring availability zones through PowerShell, see Configuring Availability Zones through PowerShell.

For information on Azure dedicated hosts, see Azure dedicated hosts.

The following table describes the various combinations of availability zone and host group zone and which ones result in successful or failed creation of a machine catalog.

Host group zone	Availability zone in custom property	Machine catalog creation outcome
Specified. For example, host group is in Zone 1	Not specified	Successful. Machines are created in the host group's zone
Specified. For example, host group is in Zone 1	Same zone as host group zone. For example, zone in the custom property is set to 1	Successful. Machines are created in Zone 1
Specified. For example, host group is in Zone 1	Different from the host group zone. For example, zone in the custom property is set to 2	As the specified availability zone and the host group's zone do not match, catalog creation fails with a relevant error during pre-flight checks

Host group zone	Availability zone in custom property	Machine catalog creation outcome
Specified. For example, host group is in Zone 1	Multiple zones specified. For example, zones in the custom properties are set to 1,2 or 2,3	As the specified availability zone and the host group's zone do not match, catalog creation fails with a relevant error during pre-flight checks
Not specified. For example, zone of the host group is None	Not specified	As the specified availability zone and the host group's zone match (that is, no zone), catalog creation is successful. Machines are not created in any zone
Not specified. For example, zone of the host group is None	Specified. For example, zones in the custom property are set to one or multiple zones	Because the specified availability zone and the host group's zone do not match, catalog creation fails with a relevant error during pre-flight checks

Provision VMs on Azure dedicated hosts

You can use MCS to provision VMs on Azure dedicated hosts. Before provisioning VMs on Azure dedicated hosts:

- Create a host group.
- Create hosts in that host group.
- Ensure that there is sufficient host capacity reserved for creating catalogs and virtual machines.

You can create a catalog of machines with host tenancy defined through the following PowerShell script:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

When using MCS to provision virtual machines on Azure dedicated hosts, consider:

- A *Dedicated host* is a catalog property and cannot be changed once the catalog is created. Dedicated tenancy is currently not supported on Azure.
- A pre-configured Azure host group, in the region of the hosting unit, is required when using the `HostGroupId` parameter.
- Azure auto-placement is required. This functionality makes a request to onboard the subscription associated with the host group. For more information, see VM Scale Set on Azure Dedicated Hosts - Public Preview. If auto-placement is not enabled, MCS throws an error during catalog creation.

Configure storage types

Select different storage types for virtual machines in Azure environments that use MCS. For target VMs, MCS supports:

- OS disk: premium SSD, SSD, or HDD
- Write-back cache disk: premium SSD, SSD, or HDD

When using these storage types, consider the following:

- Ensure that your VM supports the selected storage type.
- If your configuration uses an Azure ephemeral disk, you do not get the option for write-back cache disk setting.

> **Tip:**
>
> `StorageType` is configured for an OS type and storage account. `WBCDiskStorageType` is configured for write-back cache storage type. For a normal catalog, `StorageType` is required. If `WBCDiskStorageType` is not configured, the `StorageType` is used as the default for `WBCDiskStorageType`.

If WBCDiskStorageType is not configured, then StorageType is used as the default for WBCDiskStorageType

Configure storage types for VMs

To configure storage types for VMs, use the `StorageType` parameter in `New-ProvScheme`. To update the value of the `StorageType` parameter in an existing catalog to one of the supported storage types use `Set-ProvScheme` command.

The following is an example set of the `CustomProperties` parameter in a provisioning scheme:


```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>'
<!--NeedCopy-->
```

Enable zone-redundant storage

You can select zone-redundant storage during catalog creation. It synchronously replicates your Azure managed disk across multiple availability zones, which allows you to recover from a failure in one zone by utilizing the redundancy in others.

You can specify **Premium_ZRS** and **StandardSSD_ZRS** in the storage type custom properties. ZRS storage can be set using existing custom properties or through the **MachineProfile** template. ZRS storage is also supported with `Set-ProvVMUpdateTimeWindow` command with `-StartsNow` and `-DurationInMinutes -1` parameters. You can change existing VMs from LRS to ZRS storage.

> **Note:**
>
> - `StartsNow` indicates that the scheduled start time is the current time.
> - `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

Limitations:

- Supported only for managed disks
- Supported only with premium and standard solid-state drives (SSD)
- Not supported with `StorageTypeAtShutdown`
- Available only in certain regions.
- Performance of Azure drops when creating ZRS disks at scale. Therefore, for the first power on, turn on the machines in smaller batches (less than 300 machines at a time)

Set zone-redundant storage as the disk storage type

You can select zone-redundant storage during the initial catalog creation, or you can update your storage type in an existing catalog.

Select zone-redundant storage using PowerShell commands

When creating a new catalog in Azure using the `New-ProvScheme` Powershell command, use `Standard_ZRS` as the value in the `StorageAccountType`.
For example:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

When setting this value, it is validated by a dynamic API that determines if it can be used properly. The following exceptions can occur if the use of ZRS is not valid for your catalog:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: The StorageTypeAtShutdown custom property cannot be used with ZRS storage.
- **StorageAccountTypeNotSupportedInRegion**: This exception occurs if you try to use ZRS Storage in an Azure Region that does not support ZRS.
- **ZrsRequiresManagedDisks**: You can use zone-redundant storage only with managed disks.

You can set the disk storage type using the following custom properties:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Note:**
>
> During catalog creation, the machine profile's OS disk `StorageType` is used if the custom properties are not set.

Capture diagnostic settings on VMs and NICs from a machine profile

You can capture diagnostic settings on VMs and NICs from a machine profile while creating a machine catalog, updating an existing machine catalog, and updating existing VMs.

You can create a VM or template spec as a machine profile source.

Key steps

1. Set up required IDs in Azure. You must provide these IDs in the template spec.
    - Storage account
    - Log analytics workspace
    - Event hub namespace with the standard tier pricing

2. Create machine profile source.
3. Create a new machine catalog, update an existing catalog, or update existing VMs.

Set up required IDs in Azure

Set up one of the following in Azure:

- Storage account
- Log analytics workspace
- Event hub namespace with the Standard tier pricing

Set up a storage account Create a standard storage account in Azure. In the template spec, give the full resourceId for the storage account as the `storageAccountId`.

Once VMs are set up to log data to the storage account, the data can be found under the `insights-metrics-pt1m` container.

Set up a log analytics workspace Create a log analytics workspace. In the template spec, give the full resourceId for the log analytics workspace as the workspaceId.

Once VMs are set up to log data to the workspace, data can be queried under Logs in Azure. You can run the following command in Azure under Logs to show a count of all the metrics logged by a resource:

```
AzureMetrics | summarize Count=count()by ResourceId
```

Set up an event hub Do the following to set up an event hub in the Azure portal:

1. Create an event hub namespace with the standard tier pricing.
2. Create an event hub underneath the namespace.
3. Navigate to **Capture** under the event hub. Switch ON the toggle to capture with the Avro output type.
4. Create a new container in an existing storage account to capture the logs.
5. In the template spec, specify the `eventHubAuthorizationRuleId` in the following format: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Specify the name of the event hub.

Once VMs are set up to log data to the event hub, the data is captured into the configured storage container.

Create a machine profile source

You can create a VM or template spec as a machine profile source.

Create a VM based machine profile with diagnostic settings If you want to create a VM as your machine profile, then first set up diagnostic settings on the template VM itself. You can refer to the detailed instructions provided in the Microsoft documentation Diagnostic settings in Azure Monitor.

You can run the following commands to verify that there are now diagnostic settings associated with the VM or NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
<!--NeedCopy-->
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
<!--NeedCopy-->
```

Create a template spec-based machine profile with diagnostic settings If you want to use a VM that already has diagnostic settings enabled and export it into an ARM template spec, these settings won't be automatically included within the template. You must manually add or modify diagnostic settings within the ARM template.

However, if you want a VM as your machine profile, MCS ensures that the critical diagnostic settings are accurately captured and applied to the resources within your MCS catalog.

1. Create a standard template spec that defines a VM and NICs.
2. Add additional resources to deploy the diagnostic settings according to the spec: Microsoft.Insights diagnosticSettings. For scope, reference either a VM or NIC that's in the template by name with a partial ID. For example, for creating diagnostic settings attached to a VM named test-VM in the template spec, specify the scope as:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   <!--NeedCopy-->
   ```

3. Use the template spec as a machine profile source.

Create or update a catalog with diagnostic settings

After you create a machine profile source, you can now create a machine catalog using `New-ProvScheme` command, update an existing machine catalog using `Set-ProvScheme` command, and update existing VMs using `Request-ProvVMUpdate` command.

Verify the Windows license

You can verify that the provisioned VM is using the licensing benefit by running the following PowerShell command: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- For the Windows Server license type, verify that the license type is **Windows_Server**. More instructions are available at https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- For the Windows Client license type, verify that the license type is **Windows_Client**. More instructions are available at https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Alternatively, you can use the `Get-Provscheme` PowerShell SDK to do the verification. For example: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. For more information about this cmdlet, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

Configure the Linux license

With bring-your-own-subscription (BYOS) Linux licenses, you do not have to pay for the software. The BYOS charge only includes the compute hardware fee. There are two types of licenses:

- **RHEL_BYOS**: To use RHEL_BYOS type successfully, enable Red Hat Cloud Access on your Azure subscription.
- **SLES_BYOS**: The BYOS versions of SLES include support from SUSE.

You can set the LicenseType value to Linux options at `New-ProvScheme` and `Set-ProvScheme`.

Example of setting LicenseType to RHEL_BYOS at `New-ProvScheme`:

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog" -
     RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties '<
     CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
      Value="true" /><Property xsi:type="StringProperty" Name="
     StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
     StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
      xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
     xsi:type="StringProperty" Name="LicenseType" Value="RHEL_BYOS" /></
     CustomProperties>'
2 <!--NeedCopy-->
```

Example of setting LicenseType to SLES_BYOS at `Set-ProvScheme`:


```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
     '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
    xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
    CustomProperties>'
<!--NeedCopy-->
```

> **Note:**
>
> If `LicenseType` value is empty, then the default values are Azure Windows Server License or Azure Linux License, depending on OsType value.

Example of setting LicenseType to empty:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
     '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /></
    CustomProperties>'
<!--NeedCopy-->
```

Create a machine catalog with an Azure ephemeral disk

To provision ephemeral OS disks using `New-ProvScheme`, consider the following constraints:

- The VM size used for the catalog must support ephemeral OS disks.
- The size of the cache or temporary disk associated with the VM size must be greater than or equal to the size of the OS disk.
- The temporary disk size must be greater than the cache disk size.

Also consider these contraints when:

- Creating the provisioning scheme
- Modifying the provisioning scheme
- Updating the image

To use ephemeral disks, you must set the custom property `UseEphemeralOsDisk` to **true** when running `New-ProvScheme`.

> **Note:**
>
> If the custom property `UseEphemeralOsDisk` is set to **false** or a value is not specified all provisioned VDAs continue to use a provisioned OS disk.

The following is an example set of custom properties to use in the provisioning scheme:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
             }
 ,
            {

                "Name": "LicenseType",
                "Value": "Windows_Server"
             }
 ,
            {

                "Name": "UseEphemeralOsDisk",
                "Value": "true"
             }

        ],
<!--NeedCopy-->
```


Configure an ephemeral disk for an existing catalog

To configure an Azure ephemeral OS disk for an existing catalog, use the `UseEphemeralOsDisk` parameter in `Set-ProvScheme`. Set the value of the `UseEphemeralOsDisk` parameter to **true**.

> **Note:**
>
> To use this feature, you must also enable the parameters `UseManagedDisks` and `UseSharedImageGallery`.

For example:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
    "true" />
<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
    true" />
</CustomProperties>'
<!--NeedCopy-->
```

Configure Azure Compute Gallery

Use the `New-ProvScheme` command to create a provisioning scheme with Azure Compute Gallery support. Use the `Set-ProvScheme` command to enable or disable this feature for a provisioning scheme and to change the replica ratio and replica maximum values.

Three custom properties were added to provisioning schemes to support the Azure Compute Gallery feature:

`UseSharedImageGallery`

- Defines whether to use the Azure Compute Gallery to store the published images. If set to **True**, the image is stored as an Azure Compute Gallery image, otherwise the image is stored as a snapshot.
- Valid values are **True** and **False**.
- If the property is not defined, the default value is **False**.

`SharedImageGalleryReplicaRatio`

- Defines the ratio of machines to gallery image version replicas.
- Valid values are integer numbers greater than 0.

- If the property is not defined, default values are used. The default value for persistent OS disks is 1000 and the default value for non-persistent OS disks is 40.

`SharedImageGalleryReplicaMaximum`

- Defines the maximum number of replicas for each gallery image version.
- Valid values are integer numbers greater than 0.
- If the property is not defined, the default value is 10.
- Azure currently supports up to 10 replicas for a gallery image single version. If the property is set to a value greater than that supported by Azure, MCS attempts to use the specified value. Azure generates an error, which MCS logs then leaves the current replica count unchanged.

> **Tip:**
>
> When using Azure Compute Gallery to store a published image for MCS provisioned catalogs, MCS sets the gallery image version replica count based on the number of machines in the catalog, the replica ratio, and the replica maximum. The replica count is calculated by dividing the number of machines in the catalog by the replica ratio (rounding up to the nearest integer value) and then capping the value at the maximum replica count. For example, with a replica ratio of 20 and a maximum of 5, 0–20 machines have one replica created, 21–40 have 2 replicas, 41–60 have 3 replicas, 61–80 have 4 replicas, 81+ have 5 replicas.

Use case: Updating the Azure Compute Gallery replica ratio and replica max

The existing machine catalog uses Azure Compute Gallery. Use the `Set-ProvScheme` command to update the custom properties for all existing machines in the catalog and any future machines:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
2 <!--NeedCopy-->
```

Use Case: Converting a snapshot catalog to an Azure Compute Gallery catalog

For this use case:

1. Run `Set-ProvScheme` with the `UseSharedImageGallery` flag set to **True**. Optionally include the `SharedImageGalleryReplicaRatio` and `SharedImageGalleryReplicaMaximum` properties.
2. Update the catalog.
3. Power cycle the machines to force an update.

For example:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Tip:**
>
> The parameters `SharedImageGalleryReplicaRatio` and `SharedImageGalleryReplicaMaximum` are not required. After the `Set-ProvScheme` command completes the Azure Compute Gallery image has not yet been created. Once the catalog is configured to use the gallery, the next catalog update operation stores the published image in the gallery. The catalog update command creates the gallery, the gallery image, and the image version. Power cycling the machines updates them, at which point the replica count is updated, if appropriate. From that time, all existing non-persistent machines are reset using the Azure Compute Gallery image and all newly provisioned machines are created using the image. The old snapshot is cleaned up automatically within a few hours.

Use Case: Converting an Azure Compute Gallery catalog to a snapshot catalog

For this use case:

1. Run `Set-ProvScheme` with the `UseSharedImageGallery` flag set to **False** or not defined.
2. Update the catalog.
3. Power cycle the machines to force an update.

For example:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
```



```
      Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
      UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
      Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
<!--NeedCopy-->
```

> **Tip:**
>
> Unlike updating from a snapshot to an Azure Compute Gallery catalog, the custom data for each machine is not yet updated to reflect the new custom properties. Run the following command to see the original Azure Compute Gallery custom properties: `Get-ProvVm -ProvisioningSchemeName catalog-name`. After the `Set-ProvScheme` command completes the image snapshot has not yet been created. Once the catalog is configured to not use the gallery, the next catalog update operation stores the published image as a snapshot. From that time, all existing non-persistent machines are reset using the snapshot and all newly provisioned machines are created from the snapshot. Power cycling the machines updates them, at which point the custom machine data is updated to reflect that `UseSharedImageGallery` is set to **False**. The old Azure Compute Gallery assets (gallery, image, and version) are automatically cleaned up within a few hours.

Create or update a catalog with multiple NICs per VM

MCS supports multiple NICs per VM. You can associate multiple NICs on a VM to multiple subnets, however, those subnets must be in the same virtual network (VNet). You can use PowerShell command to:

- Create a catalog with multiple NICs on a VM
- Update an existing catalog configuration to have multiple NICs on a VM so that newly created VMs have multiple NICs
- Update an existing VM to have multiple NICs

You can create or update a non-machine profile-based machine catalog and machine profile-based machine catalog to have multiple NICs on a VM. Currently, for a machine profile-based machine catalog, you can only have the same number of NICs as specified in the machine profile source.

Properties such as accelerated networking and network security group are derived from the machine profile source.

> **Note:**
>
> The VM size must support the same number of NICs and corresponding accelerated networking, otherwise you get an error.

You can retrieve the maximum number of NICs associated with a selected VM size. A PowerShell property called `MaxNetworkInterfaces` displays the maximum NIC count when you run the Power-

Shell `get-item` command with the `AdditionalData` parameter.

Retrieve the maximum NIC count

To retrieve the maximum NIC count:

1. Open a **PowerShell** window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` to list all available VM sizes.
4. Run `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`
5. Check `MaxNetworkInterfaces` to know the maximum NIC count.

Create a catalog with multiple NICs on a VM

To create a catalog with multiple NICs on a VM, do the following:

1. Open a PowerShell window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create an identity pool if not already created.
4. Create the provisioning scheme:
   - If creating a non-machine profile-based machine catalog, run `New-ProvScheme` command with `NetworkMappings` parameter. You can add multiple subnets to the parameter `NetworkMappings`. For example:

     ```
     New-Provscheme -NetworkMappings @{
     "0"="subnetpath1";"1"="subnetpath1" }

     <!--NeedCopy-->
     ```

   - If creating a machine profile-based machine catalog:
     a) Create a VM in Azure to have multiple NICs. For information, see Create and manage a Windows virtual machine that has multiple NICs. You can also create a new VM, and then attach a network interface in the Networking page of Azure portal.
     b) Run `New-ProvScheme` command with the VM as a machine profile input.

     > **Note:**
     >
     > When creating a machine profile-based machine catalog, the count of `NetworkMappings` must be the same as the `NetworkInterfaceCount` of the machine profile. The `NetworkInterfaceCount` can be retrieved from `AdditionalData` of `Get-`


```
item -Path "machine profile path".
```

5. Finish creating the catalog.

Update a catalog to have multiple NICs on a VM

To update a catalog to have multiple NICs on a VM, do the following:

1. Open a **PowerShell** window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Update the provisioning scheme:
   - If creating a non-machine profile-based machine catalog, run the `Set-ProvScheme` command with `NetworkMappings` parameter. You can add multiple subnets to parameter `NetworkMappings`. For example:

     ```
     Set-Provscheme -NetworkMappings @{
     "0"="subnetpath1";"1"="subnetpath1" }

     <!--NeedCopy-->
     ```

   - If creating a machine catalog based on a machine profile:
     a) Create a VM in Azure to have multiple NICs. For information, see Create and manage a Windows virtual machine that has multiple NICs.
     b) Run `Set-ProvScheme` command with the VM as a machine profile input.

Update an existing VM to have multiple NICs on a VM

You can also update an existing VM using `Set-ProvVMUpdateTimeWindow` and also perform power cycle on existing VM during the update time window. For more information on updating an existing VM, see Update provisioned machines to current provisioning scheme state.

Create a machine catalog with non-persistent write-back cache disk

To configure a catalog with non-persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`. The custom properties are:

- `UseTempDiskForWBC`. This property indicates whether you are accepting to use the Azure temporary storage to store the write-back cache file. This must be configured to true when running `New-ProvScheme` if you want to use the temporary disk as write-back cache disk. If this property is not specified, the parameter is set to False by default.

For example, using the `CustomProperties` parameter to set `UseTempDiskForWBC` to true:

```
    -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.
       com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
       XMLSchema-instance"> `
    <Property xsi:type="StringProperty" Name="PersistWBC" Value="false
       "/> `
    <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
       false"/> `
    <Property xsi:type="StringProperty" Name="PersistVm" Value="false
       "/> `
    <Property xsi:type="StringProperty" Name="StorageAccountType" Value
       ="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value
       ="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="LicenseType" Value="
       Windows_Client"/> `
    <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
       ="true"/> `
    </CustomProperties>'
<!--NeedCopy-->
```

> **Note:**
>
> After you commit the machine catalog to use Azure local temporary storage for write-back cache file, it cannot be changed to use VHD later.

Create a machine catalog with persistent write-back cache disk

To configure a catalog with persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`.

> **Tip:**
>
> Use the PowerShell parameter `New-ProvScheme CustomProperties` only for cloud-based hosting connections. If you want to provision machines using a persistent write-back cache disk for an on-premises solution (for example, XenServer) PowerShell is not needed because the disk persists automatically.

This parameter supports an extra property, `PersistWBC`, used to determine how the write-back cache disk persists for MCS provisioned machines. The `PersistWBC` property is only used when the `UseWriteBackCache` parameter is specified, and when the `WriteBackCacheDiskSize` parameter is set to indicate that a disk is created.

> **Note:**
>
> This behavior applies to both Azure and GCP where the default MCSIO write-back cache disk is deleted and re-created when power cycling. You can choose to persist the disk to avoid the dele-

> tion and recreation of MCSIO write-back cache disk.

Examples of properties found in the `CustomProperties` parameter before supporting `PersistWBC` include:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> **Note:**
>
> This example only applies to Azure. The properties are different in the GCP environment.

When using these properties, consider that they contain default values if the properties are omitted from the `CustomProperties` parameter. The `PersistWBC` property has two possible values: **true** or **false**.

Setting the `PersistWBC` property to **true** does not delete the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

Setting the `PersistWBC` property to **false** deletes the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

> **Note:**
>
> If the `PersistWBC` property is omitted, the property defaults to **false** and the write-back cache is deleted when the machine is shut down from the management interface.

For example, using the `CustomProperties` parameter to set `PersistWBC` to true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```


> **Important:**
>
> The `PersistWBC` property can only be set using the `New-ProvScheme` PowerShell cmdlet. Attempting to alter the `CustomProperties` of a provisioning scheme after creation has no impact on the machine catalog and the persistence of the write-back cache disk when a machine is shut down.

For example, set `New-ProvScheme`to use the write-back cache while setting the `PersistWBC` property to true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
   true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value
   =`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"
   benvaldev5RG3`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
   " />
</CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Improve boot performance with MCSIO

You can improve boot performance for Azure and GCP managed disks when MCSIO is enabled. Use the PowerShell `PersistOSDisk` custom property in the `New-ProvScheme` command to configure this feature. Options associated with `New-ProvScheme` include:


```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
</CustomProperties>
<!--NeedCopy-->
```

To enable this feature, set the`PersistOSDisk` custom property to **true**. For example:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Create a machine catalog with customer-managed encryption key

If you want to create a machine catalog using PowerShell commands, where the encryption key is a customer-managed key, do the following:

1. Open a PowerShell window.

2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Enter `cd xdhyp:/`.
4. Enter `cd .\HostingUnits\(your hosting unit)`.
5. Enter cd diskencryptionset.folder.
6. Enter dir to get the list of the Disk Encryption Sets.
7. Copy the Id of a Disk Encryption Set.
8. Create a custom property string to include the Id of the Disk Encryption Set. For example:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
    org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"
    False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
    =`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. Create an identity pool if not already created. For example:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. Run the New-ProvScheme command: For example:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits\<adnet>\machineprofile.folder
    \<def.resourcegroup>\<machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```


11. Finish creating the machine catalog.

Create a machine catalog with encryption at host capability

To create a machine catalog with encryption at host capability

1. Check if the subscription has the encryption at host feature enabled or not. To do this, see https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. If not enabled, you must enable the feature for the subscription. For information on enabling the feature for your subscription, see https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Check if a particular Azure VM size supports encryption at host or not. To do this, in a PowerShell window, run one of the following:

```
PS XDHyp:\Connections\<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Create a VM or a template spec, as an input for machine profile, in the Azure portal with encryption at host enabled.
   - If you want to create a VM, select a VM size that supports encryption at host. After you create the VM, the VM property **Encryption at host** is enabled.
   - If you want to use a template spec, assign the parameter `Encryption at Host` as **true** inside `securityProfile`.
4. Create an MCS machine catalog with machine profile workflow by either selecting a VM or a template spec.
   - OS disk / Data Disk: Gets encrypted through Customer-managed key and Platform-managed key
   - Ephemeral OS Disk: Gets encrypted only through Platform-managed key
   - Cache Disk: Gets encrypted through Customer-managed key and Platform-managed key

   You can create the machine catalog using the Full Configuration interface or running PowerShell commands.

Retrieve encryption at host information from a machine profile

You can retrieve the encryption at host information from a machine profile when you run the PowerShell command with the `AdditionalData` parameter. If `EncryptionAtHost` parameter is **True**,

it indicates that the encryption at host is enabled for the machine profile.

For example: When the machine profile input is a VM, run the following command:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
<!--NeedCopy-->
```

For example: When the machine profile input is a template spec, run the following command:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
<!--NeedCopy-->
```

Create a machine catalog with double encryption

You can create and update a machine catalog with double encryption using the Full Configuration interface and PowerShell commands.

The detailed steps on how to create a machine catalog with double encryption are:

1. Create an Azure Key Vault and DES with Platform-managed and customer-managed keys. For information on how to create an Azure Key Vault and a DES, see Use the Azure portal to enable double encryption at rest for managed disks.
2. To browse available Disk Encryption Sets in your hosting connection:

   a) Open a **PowerShell** window.
   b) Run the following PowerShell commands:

      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName (ex. azure-east)`
      v. `cd diskencryptionset.folder`
      vi. `dir`

   You can use an Id of the `DiskEncryptionSet` to create or update a catalog using custom properties.
3. If you want to use machine profile workflow, create a VM or template spec as a machine profile input.

   - If you want to use a VM as a machine profile input:

     a) Create a VM in Azure Portal.

b) Navigate to **Disks>Key management** to encrypt the VM directly with any `DiskEncryptionSetID`.

- If you want to use a template spec as a machine profile input:

a) In the template, under `properties>storageProfile>osDisk>managedDisk`, add `diskEncryptionSet` parameter and add the id of the double encryption DES.

4. Create the machine catalog.

- If using the Full Configuration interface, do one of the following in addition to the steps in Create machine catalogs.

  - If you do not use a machine-profile based workflow, on the **Disk Settings** page, select **Use the following key to encrypt data on each machine**. Then, select your double encryption DES from the drop-down list. Continue creating the catalog.
  - If using the machine profile workflow, on the **Image** page, select a master image (or prepared image) and a machine profile. Make sure that the machine profile has a disk encryption set id in its properties.

  All machines created in the catalog are double encrypted by the key associated with the DES that you selected.

- If using PowerShell commands, do one of the following:

  - If not using machine profile-based workflow, add the custom property `DiskEncryptionSetId` in the `New-ProvScheme` command. For example:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/
    xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" />
<Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
    DiskEncryptionSetId" Value="/subscriptions/12345678-
    xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
    providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
```



```
14  -ServiceOffering "Redacted"
15  <!--NeedCopy-->
```

- If using machine profile-based workflow, use a machine profile input in the New-ProvScheme command. For example:

```
1   New-ProvScheme -CleanOnBoot
2   -HostingUnitName azure-east
3   -IdentityPoolName aio-ip
4   -InitialBatchSizeHint 1
5   -MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
       \abc.resourcegroup\fgb-vda-snapshot.snapshot
6   -NetworkMapping @{
7   "0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
       folder\apa-resourceGroup.resourcegroup\apa-
       resourceGroup-vnet.virtualprivatecloud\default.network"
        }
8
9   -ProvisioningSchemeName aio-test
10  -MachineProfile XDHyp:\HostingUnits\azure-east\
       machineprofile.folder\abc.resourcegroup\abx-mp.
       templatespec\1.0.0.templatespecversion
11  <!--NeedCopy-->
```

Finish creating a catalog using the remote PowerShell SDK. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. All machines created in the catalog are double encrypted by the key associated with the DES you selected.

Convert an unencrypted catalog to use double encryption

You can update a machine catalog's encryption type (using custom properties or machine profile).

- If not using machine profile-based workflow, add the custom property DiskEncryptionSetId in the Set-ProvScheme command. For example:

```
1   Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2   -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
       .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
       /2001/XMLSchema-instance">
3   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
       resourceGroups/Sample-RG/providers/Microsoft.Compute/
       diskEncryptionSets/SampleEncryptionSet" />
4   </CustomProperties>'
5   <!--NeedCopy-->
```

- If using machine profile-based workflow, use a machine profile input in the Set-ProvScheme command. For example:


```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Once successful, all new VMs that you add in your catalog are double encrypted by the key associated with the DES you selected.

Verify the catalog is double encrypted

- In the Full Configuration interface:
  1. Navigate to **Machine Catalogs**.
  2. Select the catalog that you want to verify. Click the **Template Properties** tab located near the bottom of the screen.
  3. Under **Azure Details**, verify the Disk Encryption Set ID in **Disk Encryption Set**. If the catalog's DES Id is blank, the catalog is not encrypted.
  4. In the Azure Portal, verify that the encryption type of the DES associated with the DES Id is platform-managed and customer-managed keys.
- Using the PowerShell command:
  1. Open the **PowerShell** window.
  2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
  3. Use `Get-ProvScheme` to get the information of your machine catalog. For example:

     ```
     Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
     <!--NeedCopy-->
     ```

  4. Retrieve the DES Id custom property of the machine catalog. For example:

     ```
     <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
         Value="/subscriptions
        /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
        -RG/providers/Microsoft.Compute/diskEncryptionSets/
        SampleEncryptionSet" />
     <!--NeedCopy-->
     ```

  5. In the Azure Portal, verify that the encryption type of the DES associated with the DES Id is platform-managed and customer-managed keys.

Page file location determination

The page file location is determined according to the following scenario:

> **Note:**
>
> The default page file location is OS disk.

Scenario	Location
Page file setting is specified in the custom properties	As specified in the custom properties
Ephemeral OS disk or hibernation is enabled	OS disk
VM has a temporary disk	Temporary disk
MCS IO is enabled	WBC disk

Page file setting scenarios

The following table describes some of the possible scenarios of page file setting during image preparation and provisioning scheme update:

During	Scenario	Outcome
Image preparation	You set the source image page file on the temporary disk, while the VM size that you specify in the provisioning scheme has no temporary disk	The page file is placed on the OS
Image preparation	You set the source image page file on the OS disk, while the VM size that you specify in the provisioning scheme has a temporary disk	The page file is placed on the temporary disk
Image preparation	You set the source image page file on the temporary disk and enable the ephemeral OS disk in the provisioning scheme	The page file is placed on the OS disk
Provisioning scheme update	You attempt to update the provisioning scheme when the VDA version is earlier than 2311	Modifies the page file setting with a warning

During	Scenario	Outcome
Provisioning scheme update	You attempt to update the provisioning scheme when the VDA version is 2311 or later	Determines the page file location as per Page file location determination

Specify page file setting

Using PowerShell commands, you can specify page file settings, including the location and size. This overrides the page file settings determined by MCS as per Page file location determination. You can do this by running the following `New-ProvScheme` command during machine catalog creation.

Important considerations

Consider the folloiwng before proceeding with the catalog creation:

- You must provide all the custom properties ('PageFileDiskDriveLetterOverride', 'InitialPageFileSizeInMB', and 'MaxPageFileSizeInMB') in the `New-ProvScheme` command or none of them.
- This feature is not supported through Citrix Studio.
- The initial page file size must be between 16 MB and 16777216 MB.
- The maximum page file size must be greater than or equal to the initial page file size and less than 16777216 MB.
- You can set both the initial page file size and maximum page file size to zero at the same time.

> **Note:**
>
> You can modify the page file settings of the newly added VMs of an existing catalog, without updating the master image. To modify the page file settings, you need VDA version 2311 or later. You can modify the page file settings using the PowerShell commands. For more information, see Modify page file settings.

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
    zijincloud-resources.resourcegroup\
    CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk
    " `
-NetworkMapping @{
```



```
 "0"="XDHyp:\\HostingUnits\\zijinnet\\virtualprivatecloud.folder\\East
    US.region\\virtualprivatecloud.folder\\neal-zijincloud-resources.
    resourcegroup\\neal-zijincloud-resources-vnet.virtualprivatecloud\\
    default.network" }
  `
-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.
    folder\\Standard_B2ms.serviceoffering" `
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

Modify page file settings

You can modify the page file settings of the newly added VMs to an existing catalog without updating the master image. Currently, this feature is applicable to only Azure environments.

To modify the page file settings, you need VDA version 2311 or later. You can modify the page file settings using the PowerShell commands.

Following are the various page file settings that you can modify in the Azure environment:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

Modify the page file settings of an existing catalog

To modify the page file settings of an existing machine catalog, run the `Set-ProvScheme` command. In this case, the updates are applied only to the new VMs added to the catalog. For example:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
```



```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   StandardSSD_LRS" />
<Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="D" />
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048" />
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
   ="8196" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
<Property  xsi:type="StringProperty" Name="Zones" Value="1" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
   test-group1" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Note:**
>
> If you enable the write back cache and try to set the `PageFileDiskDriveLetterOverride` to `C:` using the PowerShell command, MCS IO driver automatically redirects the page file to a correct disk drive and not `C:`.

Provision catalog VMs with AMA enabled

1. Set up a machine profile template.
   - If you want to use a VM as a machine profile template:
     a) Create a VM on the Azure portal.
     b) Power on the VM.
     c) Add the VM to the data collection rule under **Resources**. This invokes agent installation on the template VM.

     > **Note:**
     >
     > If you must create a Linux catalog, set up a Linux machine.

   - If you want to use template spec as a machine profile template:
     a) Set up a template spec.
     b) Add the following extension and data collection rule association to the generated template spec:

     ```
     {

     ```



```
"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "description": "Association of data collection rule.
           Deleting this association will break the data
          collection for this Arc server.",
     "dataCollectionRuleId": "/subscriptions/<azure-
        subscription>/resourcegroups/<azure-resource-group
        >/providers/microsoft.insights/datacollectionrules
        /<azure-data-collection-rule>"
      }

     }

<!--NeedCopy-->
```

Note:

If you have a data collection rule setup with a Microsoft Sentinel data connector, you can simply add `dataCollectionRuleAssociation` in the template spec in the same manner as a regular DCR association. The catalog VMs can then show up in the Sentinel DCR and the AMA would be installed on those VMs. For information on the

> best practices for data collection rule creation, see Best practices for data collection rule creation and management in Azure Monitor.

2. Create or update an existing MCS machine catalog.

   - To create a new MCS catalog:

     a) Select that VM or template spec as a machine profile in the Full Configuration interface.
     b) Proceed with the next steps to create the catalog.

   - To update an existing MCS catalog, use the following PowerShell commands. In this case, only the new VMs get the updated machine profile template.

     ```
     Set-ProvScheme -ProvisioningSchemeName "name"
     -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
        folder\abc.resourcegroup\ab-machine-profile.vm"
     <!--NeedCopy-->
     ```

   - To update existing VMs with the updated machine profile template, run `Set-ProvScheme`, and then run `Set-ProvVMUpdateTimeWindow`:

     ```
     Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
         "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.
        resourcegroup\ab-machine-profile.vm"
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
         -StartsNow -DurationInMinutes -1
     <!--NeedCopy-->
     ```

3. Power on catalog VMs.
4. Go to the Azure portal and check if the monitor extension is installed on the VM and the VM is showing up under DCR's Resources. After a few minutes monitoring data is displayed on the Azure Monitor.

Troubleshooting

For information in troubleshooting guidance for Azure Monitor Agent, see the following:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Create a catalog using Azure Spot VMs

Azure Spot VMs allow you to take advantage of Azure's unused computing capacity at a significant cost savings. However, the ability to allocate an Azure Spot VM depends on the current capacity and pricing. Therefore, Azure might evict your running VM, fail to create the VM, or fail to power on the VM as per the Eviction policy. Therefore, Azure Spot VMs are good for some non-critical applications and desktops. For more information, see Use Azure Spot Virtual Machines.

Limitations

- All VM sizes aren't supported for Azure Spot VMs. For more information, see Limitations.

  You can run the following PowerShell command to check whether a VM size supports Spot VMs or not. If a VM size supports Spot VM, then `SupportsSpotVM` is **True**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
     folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  <!--NeedCopy-->
  ```

- Currently, Azure Spot VMs do not support hibernation.

Requirement

While creating the machine profile source (VM or template spec) for Azure Spot VMs catalog, you must select Azure Spot Instance (if using VM) or set `priority` as `Spot` (if using template spec).

Steps to create a catalog using Azure Spot VMs

1. Create a machine profile source (VM or launch template).
   - For creating a VM using the Azure portal, see Deploy Azure Spot Virtual Machines using the Azure portal.
   - For creating a template spec, add the following properties under **resources > type: Microsoft.Compute/virtualMachines > properties** in the template spec. For example:

     ```
     "priority": "Spot",
     "evictionPolicy": "Deallocate",
     "billingProfile": {

     "maxPrice": 0.01
      }

     <!--NeedCopy-->
     ```


> **Note:**
>
> - Eviction policy can be **Deallocate** or **Delete**.
>   - For non-persistent VMs, MCS always sets the eviction policy as **Delete**. If the VM is evicted, it is deleted along with any non-persistent disks (For example, OS disk). Any persistent disks (for example, Identity disk) are not deleted. However, an OS disk is persistent if the catalog type is persistent or the `PersistOsDisk` custom property is set to True. Similarly, a WBC disk is persistent if the `PersistWbc` custom property is set to **True**.
>   - For persistent VMs, MCS always sets the eviction policy as Deallocate. If the VM is evicted, it is deallocated. No changes are made to the disks.
> - The maximum price is the price that you are willing to pay per hour. If you are using **Capacity Only**, then this is **-1**. The maximum price can only be null, -1, or a decimal greater than zero. For more information, see Pricing.

2. You can run the following PowerShell command to check if a machine profile is Azure Spot VM enabled or not. If the `SpotEnabled` parameter is **True** and `SpotEvictionPolicy` is set to **Deallocate** or **Delete**, then the machine profile is Azure Spot VM enabled. For example,

   - If the machine profile source is a VM, run the following command:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
       AdditionalData
   <!--NeedCopy-->
   ```

   - If the machine profile source is a template spec, run the following command:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
       templatespec\14.0.0-spot-delete.templatespecversion").
       AdditionalData
   <!--NeedCopy-->
   ```

3. Create a machine catalog using a machine profile with `New-ProvScheme` PowerShell command.

You can update a catalog using the `Set-ProvScheme` command. You can also update existing VMs using the PowerShell command `Set-ProvVmUpdateTimeWindow`. The machine profile is updated on the next power on.

Evictions on a running Azure Spot VM

If the computing capacity is unavailable or the price per hour is higher than the maximum price as configured, Azure evicts a running Spot VM. By default, you are not notified of an eviction. The VM simply

freezes and the VM is evicted. Microsoft recommends using Scheduled Events to monitor evictions. See Continuously monitor for eviction. You can also run scripts from within a VM to get a notification before the eviction. For example, Microsoft has a polling script in Python ScheduledEvents.cs.

Troubleshooting

- You can see Spot VM properties in the provisioned VM's customMachineData using the `Get-ProvVM` command. If the priority field is set to **Spot**, then Spot is in use.
- You can check if a VM is using Spot in Azure Portal:
  1. Find the VM in the Azure Portal.
  2. Go to the **Overview** page.
  3. Scroll down to the bottom and locate the **Azure Spot** section.
     - If Spot is not in use, then this field is empty.
     - If Spot is in use, the **Azure Spot** and **Azure Spot eviction policy** fields are set.

1. You can check the billing profile or maximum price per hour for the VM on the Configuration page.

Copy tags on all resources

You can copy tags specified in a machine profile to all the resources such as, multiple NICs and disks (OS disk, Identity disk, and write-back cache disk) of a new VM or an existing VM in a machine catalog. The machine profile source can be a VM or an ARM template spec.

> **Note:**
>
> You must add the policy on the tags (See Assign policy definitions for tag compliance) or add the tags in a machine profile source to retain the tags on the resources.

Prerequisites

Create the machine profile source (VM or ARM template spec) to have tags on VM, disks, and NICs of that VM.

- If you want to have a VM as a machine profile input, then apply tags on the VM and all the resources in the Azure portal. See Apply tags with Azure portal.
- If you want to have ARM template spec as a machine profile input, then add the following tag block under each resource.


```
 "tags": {

"TagC": "Value3"
 }
,
<!--NeedCopy-->
```

> **Note:**
>
> You can have a maximum of one disk and at least one NIC in the template spec.

Copy tags to the resources of a VM in a new machine catalog

1. Create a non-persistent or persistent catalog with a VM or ARM template spec as a machine profile input.
2. Add a VM to the catalog and power it on. You must see the tags specified in the machine profile copied to the corresponding resources of that VM.

   > **Note:**
   >
   > You get an error if there is a mismatch in the number of NICs provided in the machine profile and the number of NICs you want the VMs to use.

Modify tags on the resources of an existing VM

1. Create a machine profile with the tags on all the resources.
2. Update the existing machine catalog with the updated machine profile. For example:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
<!--NeedCopy-->
```

3. Turn off the VM on which you want to apply the updates.
4. Request a scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
<!--NeedCopy-->
```

5. Turn on the VM.
6. You must see the tags specified in the machine profile copied to the corresponding resources.

> **Note:**
>
> You get an error if there is a mismatch in the number of NICs provided in the machine profile and the number of NICs provided in the `Set-ProvScheme`.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a Microsoft Azure catalog.

More information

- Create and manage connections and resources
- Connection to Microsoft Azure Resource Manager
- Create machine catalogs

Create a Microsoft System Center Virtual Machine Manager catalog

July 2, 2024

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Microsoft System Center Virtual Machine Manager (VMM) virtualization environments.

> **Note:**
>
> Before creating a VMM catalog, you need to finish creating a connection to VMM. See Connection to Microsoft System Center Virtual Machine Manager.

Create a master VM

- Install a VDA on the master VM, and select the option to optimize the desktop. This improves performance.
- Take a snapshot of the master VM to use as a backup.
- Create virtual desktops.

MCS on SMB 3 file shares

For machine catalogs created with MCS on SMB 3 file shares for VM storage, credentials must meet the following requirements to ensure that calls from the XenServer Communications Library (HCL) connect successfully to SMB storage.

- VMM user credentials must include full read write access to the SMB storage.
- Storage-virtual disk operations during VM lifecycle events are performed through the Hyper-V server using the VMM user credentials.

For more information on SMB 3, see Overview of file sharing using the SMB 3 protocol in Windows Server.

When using VMM 2012 SP1 with Hyper-V on Windows Server 2012: When using SMB as storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Cloud Connector to individual Hyper-V machines. For more information, see CTX137465.

Using a standard PowerShell V3 remote session, the HCL in the Cloud Connector uses CredSSP to open a connection to the Hyper-V machine. This feature passes Kerberos-encrypted user credentials to the Hyper-V machine, and the PowerShell commands in the session on the remote Hyper-V machine run with the credentials provided (in this case, those of the VMM user), so that communication commands to storage work correctly.

The following tasks use PowerShell scripts that originate in the HCL. The scripts are then sent to the Hyper-V machine to act on the SMB 3.0 storage.

Consolidate Master Image: An image creates a new MCS provisioning scheme (machine catalog). It clones and flattens the master VM ready for creating new VMs from the new disk created (and removes dependency on the original master VM).

ConvertVirtualHardDisk on the root\virtualization\v2 namespace

Example:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2
    ";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

Create differencing disk: Creates a differencing disk from the image generated by consolidating the image. The differencing disk is then attached to a new VM.

CreateVirtualHardDisk on the root\virtualization\v2 namespace

Example:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2
    ";
```



```
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

Upload identity disks: The HCL cannot directly upload the identity disk to SMB storage. Therefore, the Hyper-V machine must upload and copy the identity disk to the storage. Because the Hyper-V machine cannot read the disk from the Cloud Connector, the HCL must first copy the identity disk through the Hyper-V machine as follows.

1. The HCL uploads the Identity to the Hyper-V machine through the administrator share.
2. The Hyper-V machine copies the disk to the SMB storage through a PowerShell script running in the PowerShell remote session.

   A folder is created on the Hyper-V machine and the permissions on that folder are locked for the VMM user only (through the remote PowerShell connection).
3. The HCL deletes the file from the administrator share.
4. When the HCL completes the identity disk upload to the Hyper-V machine, the remote PowerShell session copies the identity disks to SMB storage, and then deletes it from the Hyper-V machine.

The identity disk folder is recreated if deleted to make it available for reuse.

Download identity disks: As with uploads, the identity disks pass through the Hyper-V machine to the HCL. The following process creates a folder that has only VMM user permissions on the Hyper-V server if it does not exist.

1. The HyperV machine copies the disk from the SMB storage to local Hyper-V storage using a PowerShell script running in the PowerShell V3 remote session.
2. HCL reads the disk from the Hyper-V machine's administrator share into memory.
3. HCL deletes the file from the administrator share.

Create a catalog with a machine profile

You can use a machine profile to create and update an MCS machine catalog in System Center Virtual Machine Manager (SCVMM) environments. You can also enable nested virtualization and vTPM.

Important considerations

- Master image can only be a snapshot and not a VM.
- You can only use VM as the machine profile source.
- You can configure VTPM from the Hyper-V console and not from the SCVMM console.

- If the master image has vTPM enabled, then you must enable the vTPM on the machine profile source.
- vTPM is only supported on Generation 2 machines.
- The following parameters overwrite the values captured in a machine profile if provided separately:
  - VMCpuCount
  - VMMemoryMB
  - Disk storage
- You can update an existing catalog using the `Set-ProvScheme` command.
- You can update the memory and disk cache sizes after creating the MCS catalogs when MCSIO is enabled.

Steps to create a catalog using a machine profile

1. Create a VM to be a machine profile source. For more information, see Provision virtual machines in the VMM fabric. You cannot change the **Generation** once selected.
   - If you want to enable nested virtualization, select the **Enable Nested Virtualization** checkbox on the **Select Source** page.
   - If you want to enable vTPM, then after you create the VM, log in to the Hyper-V host and find your VM under the **Hyper-V Manager**. Right-click the VM, then go to **Settings**. Under **Security**, select the **Enable Trusted Platform Module** checkbox.
2. Open a **PowerShell** window.
3. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
4. Create a Broker catalog. This catalog is populated with machines which are about to be created.
5. Create an identity pool. This becomes a container for AD accounts created for the machines that are to be created.
6. Create a provisioning scheme with the machine profile. For example:

```
1 New-ProvScheme -HostingUnitName "<hostingunit name>"
2 -IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<
     path to the checkpoint/snapshot>"
3 -ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<
     path to the machine profile VM>"
4 <!--NeedCopy-->
```

7. Updates the Broker catalog with the unique Id of the provisioning scheme.
8. Create and add VMs to the catalog.

You can update an existing catalog using the Set-ProvScheme command. For example:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
    "XDHyp:\<path to the machine profile VM>"
<!--NeedCopy-->
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a Microsoft System Center Virtual Machine Manager catalog.

More information

- Create and manage connections and resources
- Connection to Microsoft System Center Virtual Machine Manager
- Create machine catalogs

Create a Nutanix catalog

February 1, 2024

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Nutanix virtualization environments.

> **Note:**
>
> Before creating a Nutanix catalog, you need to finish creating a connection to Nutanix. See Connection to Nutanix.

Create a machine catalog using a Nutanix snapshot

The snapshot you select is the template used to create the VMs in the catalog. Before creating the catalog, create images and snapshots in Nutanix. For more information, see the Nutanix documentation.

In the catalog creation wizard:

- The **Operating System** and **Machine Management** pages do not contain Nutanix-specific information.

- The **Container** or **Cluster and Container** page is unique to Nutanix.
  - If you deploy machines by using Nutanix AHV XI as the resources, on the **Container** page, select a container where the VMs' identity disks will be placed.
  - If you deploy machines by using Nutanix AHV Prism Central (PC) as the resources, you see the **Cluster and Container** page. Select which cluster to use for the deployment of VMs and then a container.
- On the **Image** page, select the image snapshot. Use the Acropolis console to rename your snapshots if needed. If you rename snapshots, restart the catalog creation wizard to see a refreshed list.
- On the **Virtual Machines** page, indicate the number of virtual CPUs and the number of cores per vCPU.
- On the **NICs** page, select the NIC type to filter associated networks. This option is available only for Nutanix AHV PC connections. There are two NIC types: **VLAN** and **OVERLAY**. Select one or more NICs that the master image contains and then select an associated virtual network for each NIC.
- The **Machine Identities**, **Domain Credentials**, **Scopes**, and **Summary** pages do not contain Nutanix-specific information.

Limitation

When creating an MCS catalog with Nutanix host connection (specifically, Nutanix AHV plugin 2.7.1 and Nutanix AHV plugin 2.5.1), the hard disk size of provisioned VMs are incorrectly displayed on the Full Configuration interface.

- Nutanix AHV plugin 2.7.1: The size displayed is much smaller (1 GB) than the real storage size.
- Nutanix AHV plugin 2.5.1: The size displayed is much smaller (32 GB) than the real storage size.

However, this works as designed if the master image VM is a snapshot in VM.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs.

More information

- Create and manage connections and resources

- Connection to Nutanix
- Connection to Nutanix cloud and partner solutions
- Create machine catalogs

Create a VMware catalog

July 2, 2024

Create machine catalogs describes the wizards that create a machine catalog.

> **Note:**
>
> Before creating a VMware catalog, you need to finish creating a connection to VMware. See Connection to VMware.

Create a machine catalog using a machine profile

You can create an MCS machine catalog using a machine profile. The source of the machine profile input is a VMware template. The machine profile captures the hardware properties from a VMware template and applies them to the newly provisioned VMs in the catalog.

> **Note:**
>
> - Master image input (snapshot) and machine profile input (VMware template) must either be both vTPM enabled or both vTPM disabled. This rule applies to both `New-ProvScheme` and `Set-ProvScheme`.
> - If the master image is vTPM enabled, then the VMware template can only come from the same VM source as the master image.
> - Encrypted storage policy only supports full clone.

The VMware template in the machine profile must exist during the catalog life cycle to allow provisioning of VMs to the catalog. Without a VMware template, you cannot provision new VMs. When a VMware template gets deleted, you must supply a new template using the `Set-ProvScheme` command.

- MCS captures properties of a VMware template. You can create a new VMware template referencing stored properties of the VMware template using the `Get-Provscheme` command.
- Alternatively, if the machine catalog and provisioned VMs exist, then an MCS provisioned machine can also be used to create a new VMware template.
- When MCSIO is enabled, you can update the memory and disk cache sizes after creating the MCS catalogs.

Based on different OS, you can create a machine catalog with different configurations:

- If Windows 11 is installed on the master image, then it is a requirement to have vTPM enabled for the master image. Therefore, the VMware template, which is a source of machine profile, must have vTPM attached to it.
- If Windows 10 is installed on the master image with no vTPM attached, then you can create a machine catalog with non-vTPM VMware template as source for machine profile.

There is another configuration where you can create a machine catalog using full copy disk mode with machine profile template applied with encrypted storage policy.

To create a machine catalog using PowerShell commands with machine profile as input:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the following commands:

   - To create a machine catalog with vTPM attached VMware template as a source for machine profile input and windows11 installed master image:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\<hosting unit name>\\<network name>.
    network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<
    template name>.template"
-TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
```



```
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
   ProvisioningType 'MCS'
-Scope @()  -SessionSupport "SingleSession"
-ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- To create a machine catalog with non-vTPM VMware template as source for machine profile and Windows10 installed master image:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\<hosting unit name>\\<string>.
   network" }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"  -Description "<string>"  -
   IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()  -SessionSupport "
   SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```


- To create a machine catalog using Full copy disk mode with machine profile template applied with encrypted storage policy:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\<hosting unit name>\\<string>.
    network" }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
     -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<
    template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
-UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
    ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- To update a machine profile, use the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -
    IdentityPoolName 'name' -MachineProfile 'XDHyp:\
    HostingUnits\<hosting unit name>\<template name>.template
<!--NeedCopy-->
```


Check for multiple NICs

You get various error messages during the pre-flight checks for multiple NICs when using a machine profile and the `NetworkMapping` parameter in the `New-ProvScheme` and `Set-ProvScheme` commands.

The pre-flight checklist for multiple NICs is as follows:

- Only NIC count from the machine profile template is used and validated. The network to which these NICs point towards is not used or validated against the hosting unit networks.
- If the NIC count in the machine profile template is greater than the number of networks in the hosting unit, you get an error message.
- If the NIC count in the machine profile template is zero, you get an error message.
  When the NIC count in the machine profile template is one, then:
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- When the NIC count in the machine profile template is greater than 1, or the hosting unit network count is greater than 1, then:
  - Valid network mapping is required in the command, and it should provide mapping for each NIC (that is, NetworkMapping count should be same as the machine profile NIC count).
  - Multiple NICs cannot be mapped to the same network in the hosting unit.
  - `NetworkMapping` count and machine profile NIC count must be less than or equal to the hosting unit network count.
  - `NetworkMapping` must be provided for each id from 0 to n-1, where n is the number of network adapters in the machine profile template.

Troubleshooting

If the catalog fails to create, see CTX294978.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a VMware catalog.

More information

- Create and manage connections and resources
- Connection to VMware
- Connection to VMware cloud and partner solutions
- Create machine catalogs

Create a XenServer catalog

July 2, 2024

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to XenServer (formerly Citrix Hypervisor) virtualization environments.

> **Note:**
>
> Before creating a XenServer catalog, you need to finish creating a connection to XenServer. See Connection to XenServer.

Create a machine catalog using a GPU-capable XenServer

GPU-capable machines require a dedicated master image. Those VMs require video card drivers that support GPUs. Configure GPU-capable machines to allow the VM to operate with software that uses the GPU for operations.

1. In XenCenter, create a VM with standard VGA, networks, and vCPU.
2. Update the VM configuration to enable GPU use (either Passthrough or vGPU).
3. Install a supported operating system and enable RDP.
4. Install Citrix VM Tools and NVIDIA drivers.
5. Turn off the Virtual Network Computing (VNC) Admin Console to optimize performance, and then restart the VM.
6. You are prompted to use RDP. Using RDP, install the VDA and then restart the VM.
7. Optionally, create a snapshot for the VM as a baseline template for other GPU master images.
8. Using RDP, install customer-specific applications that are configured in XenCenter and use GPU capabilities.

Create a machine profile-based machine catalog using PowerShell

When you create a catalog to provision machines using MCS, you can use a machine profile to capture the hardware properties from a virtual machine and apply them to newly provisioned VMs in the cata-

log. If the `MachineProfile` parameter is not used, the hardware properties are captured from the master image VM or snapshot.

> **Note:**
>
> Currently, you can use only a snapshot as a machine profile input.

You can update the memory and disk cache sizes after creating the MCS catalogs when MCSIO is enabled. You can explicitly configure the following parameters to overwrite the values of the parameters in the machine profile input:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Create a catalog with a machine profile

1. Open the PowerShell window.
2. Run `asnp citrix*`.
3. Create an identity pool. The identity pool is a container for the Active Directory (AD) accounts for the VMs to be created. For example:

```
1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
    IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
    -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
2 <!--NeedCopy-->
```

4. Create the required AD computer accounts in Active Directory.

```
1 $password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
2 New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

5. Run the `New-ProvScheme` command to create a catalog. For example:

```
1 New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
3 </CustomProperties>'
```



```
4 -MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
     vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
     " -Scope @() -SecurityGroup @()
5 -MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
     ExampleMachineProfile.vm\ExampleSnapshot.snapshot"
6 <!--NeedCopy-->
```

6. Register provisioning scheme as a broker catalog. For example:

```
1 $ConfigZone = Get-ConfigZone | Where-Object {
2   $_.Name -eq "xxxxxx"  }
3
4 New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
     Description "Machine profile catalog" -ProvisioningSchemeId
     fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
     SessionSupport MultiSession -PersistUserChanges Discard -
     ZoneUid ($ConfigZone.Uid)
5 <!--NeedCopy-->
```

7. Add VMs to the catalog.

Update a catalog with a new machine profile

> **Note:**
>
> - The `Set-ProvScheme` command in this case does not change the machine profile of the existing VMs in the catalog. Only the newly created VMs added to the catalog have the new machine profile.
> - You cannot convert a machine profile-based machine catalog to non-machine profile-based machine catalog.

To update a catalog with a new machine profile:

1. Run the `Set-ProvScheme` command. For example:

```
1 Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
     MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
     ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
     snapshot"
2 <!--NeedCopy-->
```

   For more information on the Set-ProvScheme command, see Set-ProvScheme.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a XenServer catalog.

More information

- Create and manage connections and resources
- Connection to XenServer
- Create machine catalogs

Create catalogs of different join types

June 16, 2023

Using MCS, you can provision machines as non-domain-joined, on-premises AD joined, Azure AD joined, or hybrid Azure AD joined.

For information about how to configure machine identities in the Full Configuration interface, see Create machine catalogs.

For specific information on how to create machine identities joined catalogs, see the following:

- Create Azure Active Directory joined catalogs
- Create Microsoft Intune enabled catalogs
- Create Hybrid Azure Active Directory joined catalogs
- Create Non-domain-joined catalogs

Create Azure Active Directory joined catalogs

February 1, 2024

This article describes how to create Azure Active Directory (AD) joined catalogs using Citrix DaaS.

For information on requirements, limitations, and considerations, see Azure Active Directory joined.

Before you create the machine catalog, you need the following:

1. New resource location
    - Navigate to the Citrix Cloud admin UI > upper left hamburger menu > **Resource Locations**.
    - Click **+ Resource Location**.
    - Enter a name for the new resource location and click **Save**.
2. Create a hosting connection. See Create and manage connections section for details. When deploying machines on Azure, see Connection to Azure Resource Manager.

3. To consistently delete stale Azure AD devices and allow new devices to join Azure AD, you can assign the Cloud Device Administrator role to the provisioning service principal. If you do not delete the Azure stale AD devices, then the corresponding non-persistent VM stays in the initializing state until you manually remove it from the Azure AD portal. To do this, enable Azure AD joined device management of host connections using Full Configuration Interface or perform the following steps:

   a) Sign in to the Azure portal and navigate to **Azure Active Directory > Roles and administrators**.

   b) Search for **Cloud Device Administrator** built-in role and click **Add assignments** to assign the role to the service principal of the application used by the hosting connection.

   c) Use the Citrix Remote PowerShell SDK to run the following commands to get the existing `CustomProperties` of the hosting connection. The `${ HostingConnectionName }` refers to the name of the hosting connection.

      i. Open a **PowerShell** window.

      ii. Run `asnp citrix*` to load the Citrix-specific **PowerShell** modules.

      iii. Run the following command to get the existing custom properties of the hosting connection.

```
(Get-Item -LiteralPath XDHyp:\Connections\${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

      iv. Copy the CustomProperties from the connection to a notepad and append property setting `<Property xsi:type="StringProperty"Name="AzureAdDeviceManagement"Value="true"/>`.

      v. In the **PowerShell** window, assign a variable to the modified custom properties. For example, `$UpdatedCustomProperties='<CustomProperties ...</CustomProperties>'`.

      vi. Set the custom property back to the hosting connection:

```
Set-Item -LiteralPath XDHyp:\Connections\${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```


vii. Run the command `(Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName } ).CustomProperties` to verify the updated custom property settings.

You can create Azure AD joined catalogs by using the Full Configuration interface or **PowerShell**.

Use the Full Configuration interface

The following information is a supplement to the guidance in Create machine catalogs. To create Azure AD joined catalogs, follow the general guidance in that article, minding the details specific to Azure AD joined catalogs.

In the catalog creation wizard:

1. On the **Image** page:
   - Select 2106 or later as the functional level.
   - Select **Use a machine profile** and select the appropriate machine from the list.
2. On the **Machine Identities** page, select **Azure Active Directory joined**. The created machines are owned by an organization and are signed into with an Azure AD account that belongs to that organization. They exist only in the cloud.

   > **Note:**
   >
   > - The **Azure Active Directory joined** identity type requires version 2106 or later as the minimum functional level for the catalog.
   > - The machines are joined to the Azure AD domain associated with the tenant to which the hosting connection is bound.

3. Users must be granted explicit access in Azure to log into the machines using their AAD credentials. See Azure Active Directory joined section for more details.

Use PowerShell

The following are **PowerShell** steps equivalent to operations in Full Configuration. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

The difference between on-premises AD joined catalogs and Azure AD joined ones lies in the creation of the identity pool and the provisioning scheme.

To create an identity pool for Azure AD joined catalogs:


```
New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
    WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
    NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
    -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
<!--NeedCopy-->
```

To create a provisioning scheme for Azure AD joined catalogs, the **MachineProfile** parameter is required in New-ProvScheme:

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
    schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.
    w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty
    `" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageType`" Value=`"StandardSSD_LRS`" /><
    Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
    Windows_Server`" /></CustomProperties>" -HostingUnitName "
    AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
    InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
    AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
    MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
    azuread-rg.resourcegroup\azuread-
    small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
     US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
    azuread-vnet.virtualprivatecloud\Test_VNET.network" }
  -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
     Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
     \AzureResource\serviceoffering.folder\Standard_DS1_v2.
     serviceoffering"
<!--NeedCopy-->
```

All other commands used to create Azure AD joined catalogs are the same as for traditional on-premises AD joined catalogs.

View the status of the Azure AD join process

In the Full Configuration interface, the status of the Azure AD join process is visible when Azure AD joined machines in a delivery group are in a powered-on state. To view the status, use Search to identify those machines and then for each check **Machine Identity** on the **Details** tab in the lower pane. The following information can appear in **Machine Identity**:

- Azure AD joined
- Not yet joined to Azure AD

> **Note:**
>
> If the machines fail to be in Azure AD joined state, they do not register with the Delivery Controller.

> Their registration status appears as **Initialization.**

Also, using the Full Configuration interface, you can learn why machines are unavailable. To do that, click a machine on the **Search** node, check **Registration** on the **Details** tab in the lower pane, and then read the tooltip for additional information.

Delivery Group

See Create delivery groups section for details.

Enable Rendezvous

Once the delivery group has been created, you can enable Rendezvous. See Rendezvous V2 for details.

Troubleshoot

If machines fail to be Azure AD joined, do the following:

- Check if the system assigned managed identity is enabled for the machines. MCS-provisioned machines must have this enabled automatically. The Azure AD join process fails without system assigned managed identity. If the system assigned managed identity is not enabled for MCS-provisioned machines, possible reason is:
  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `AzureAD`. You can verify this by running `Get-AcctIdentityPool`.
- For catalogs that use master images with VDA version 2206 or earlier, check the provisioning status of **AADLoginForWindows** extension for the machines. If the **AADLoginForWindows** extension does not exist, possible reasons are:
  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `AzureAD`. You can verify this by running `Get-AcctIdentityPool`.
  - The **AADLoginForWindows** extension installation is blocked by Azure policy.
- To troubleshoot **AADLoginForWindows** extension provisioning failures, you can check logs under `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` on the MCS-provisioned machine.

> **Note:**
>
> MCS does not rely on the `AADLoginForWindows` extension to join a VM to Azure AD when using a master image with VDA version 2209 or later. In this case, the `AADLoginForWindows` extension will not be installed on the MCS-provisioned machine. Therefore, `AADLoginForWindows` extension provisioning logs can't be collected.

- Check the Azure AD join status and debug logs by running `dsregcmd /status` command on the MCS-provisioned machine.
- Check Windows event logs under **Application and Services Logs > Microsoft > Windows > User Device Registration**.
- Check if Azure AD device management is correctly configured by running `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }`.

  Ensure that the value of:

  - `AzureAdDeviceManagement` property in `CustomProperties` is **true**
  - `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` property in metadata is **true**

  If `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` is **false**, it indicates that the `ServicePrincipal` of the application used by the hosting connection is not granted with sufficient permissions to perform Azure AD device management. To resolve this, assign the `ServicePrincipal` with the **Cloud Device Administrator** role.

Azure Active Directory dynamic security group

Dynamic group rules place the VMs in the catalog to a dynamic security group based on the naming scheme of the machine catalog.

If the naming scheme of the machine catalog is Test### (where, # means number), Citrix creates the dynamic membership rule ^*Test[0-9]{3}$* in the dynamic security group. Now, if the name of the VM created by Citrix is anything from Test001 to Test999, then the VM is included in the dynamic security group.

> **Note:**
>
> If the name of the VM created by you manually is anything from Test001 to Test999, then also the VM is included in the dynamic security group. This is one of the limitations of the dynamic security group.

The dynamic security group feature is useful when you want to manage the VMs by Azure Active Directory (Azure AD). This is also useful when you want to apply Conditional Access policies or distribute apps from Intune by filtering the VMs with Azure AD dynamic security group.

You can use **PowerShell** commands to:

- Create a machine catalog with Azure AD dynamic security group
- Enable security group feature for an Azure AD catalog
- Delete a machine catalog with Azure AD joined device security group

> **Important:**
>
> - To create a machine catalog with Azure AD dynamic security group, add machines to the catalog, and delete the machine catalog, you must have Azure AD access token. For information on getting the Azure AD access token, see https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/.
> - To request an access token in Azure AD, Citrix requests the **Group.ReadWrite.All** permission for Microsoft Graph API. An Azure AD user who has tenant-wide admin consent permission can grant **Group.ReadWrite.All** permission for Microsoft Graph API. For information on how to grant tenant-wide admin consent to an application in Azure Active Directory (Azure AD), see the Microsoft document https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/.

Create a machine catalog with Azure AD dynamic security group

1. In the machine catalog setup user interface of the web-based console, on the **Machine Identities** page, select **Azure Active Directory joined**.
2. Log in to Azure AD.
3. Get the access token to MS Graph API. Use this access token as a value of `$AzureADAccessToken` parameter when you run the **PowerShell** commands.
4. Run the following command to verify if the dynamic security group name exists in the tenant.

```
Get-AcctAzureADSecurityGroup
 –AccessToken  $AzureADAccessToken
 –Name "SecurityGroupName"
<!--NeedCopy-->
```

5. Create a machine catalog using the Tenant ID, access token, and dynamic security group. Run the following command to create an IdentityPool with `IdentityType=AzureAD` and create a dynamic security group in Azure.

```
New-AcctIdentityPool
-AllowUnicode
```



```
-IdentityPoolName "SecurityGroupCatalog"
-NamingScheme "SG-VM-###"
-NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
-WorkgroupMachine
-IdentityType "AzureAD"
-DeviceManagementType "None"
-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupName "SecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Enable security group feature for an Azure AD catalog

You can enable the dynamic security feature for an Azure AD catalog that was created without the dynamic security group feature enabled. To do this:

1. Manually create a new dynamic security group. You can also reuse an existing dynamic security group.
2. Log in to Azure AD, and get the access token to MS Graph API. Use this access token as a value of `$AzureADAccessToken` parameter when you run the **PowerShell** commands.

   > **Note:**
   >
   > For information on the permissions required by the Azure AD user, see https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/.

3. Run the following command to connect the identity pool to the created Azure AD dynamic security group.

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

If you update the naming scheme, Citrix updates the naming scheme to a new membership rule. If you delete the catalog, membership rule gets deleted, and not the security group.

Delete a machine catalog with Azure AD joined device security group

When you delete a machine catalog, the Azure AD joined device security group is also deleted.

To delete the Azure AD dynamic security group, do the following:

1. Log in to Azure AD.
2. Get the access token to MS Graph API. Use this access token as value of `$AzureADAccessToken` parameter when you run the **PowerShell** commands.
3. Run the following command:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Create an Azure AD dynamic security group under an existing Azure AD assigned security group

You can create an Azure AD dynamic security group under an existing Azure AD assigned security group. You can do the following:

- Get security group information.
- Get all Azure AD assigned security groups that are synced from on-premises AD server or the assigned security groups to which Azure AD roles can be assigned.
- Get all Azure AD dynamic security groups.
- Add Azure AD dynamic security group as a member of Azure AD assigned group.
- Remove the membership between Azure AD dynamic security group and Azure AD assigned security group when Azure AD dynamic security group is deleted along with the machine catalog.

You can also see explicit error messages when any of the operations fail.

Requirement:

You must have the access token to the MS Graph API when you run the **PowerShell** commands.

To get the access token:

1. Open Microsoft graph explorer and log in to Azure AD.
2. Make sure you have consent to **Group.ReadWrite.All** and **GroupMember.ReadWrite.All** permissions.
3. Get access token from Microsoft graph explorer. Use this access token when you run the **PowerShell** commands.

To get security group information by group id:

1. Get the access token.
2. Find group object id from Azure portal.
3. Run the following **PowerShell** command in the **PowerShell** console:


```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
<!--NeedCopy-->
```

To get security groups by group display name:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```

To get security groups whose display name contains a substring:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

To get all Azure AD assigned security groups that are synced from on-premises AD server or the assigned security groups to which Azure AD roles can be assigned:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

To get all Azure AD dynamic security groups:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

To get Azure AD assigned security groups with maximum record count:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

To add Azure AD dynamic security group as a member of Azure AD assigned security group:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

To get Azure AD assigned security group members:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> **Note:**
>
> `Get-AcctAzureADSecurityGroupMember` provides you only the direct members of the security group type under Azure AD assigned security group.

To remove the membership between Azure AD dynamic security group and Azure AD assigned security group when Azure AD dynamic security group is deleted along with machine catalog:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```


Modify Azure AD dynamic security group name

You can modify the Azure AD dynamic security group name associated with a machine catalog. This modification makes the security group information stored in Azure AD identity pool object to be consistent with the information stored in Azure portal.

> **Note:**
>
> The Azure AD dynamic security groups do not include security groups synced from on-premises AD and other group types like Office 365 group.

You can modify the Azure AD dynamic security group name using Full Configuration interface and **PowerShell** commands.

To modify the Azure AD dynamic security group name using **PowerShell**:

1. Open the **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific **PowerShell** modules.
3. Run the command `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`.

You get appropriate error messages if the Azure AD dynamic security group name cannot be modified.

Create Microsoft Intune enabled catalogs

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

This article describes how to create Microsoft Intune enabled catalogs using Citrix DaaS. You can enable Microsoft Intune by using the Full Configuration interface or PowerShell.

For information on requirements, limitations, and considerations, see Microsoft Intune.

Use the Full Configuration interface

The following information is a supplement to the guidance in Create machine catalogs. This feature requires the selection of **Azure Active Directory joined** in **Machine Identities** during catalog creation. Follow the general guidance in that article, minding the details specific to this feature.

In the catalog creation wizard:

- On the **Machine Identities** page, select **Azure Active Directory joined** and then **Enroll the machines in Microsoft Intune**. If enabled, enroll the machines in Microsoft Intune for management.

Use PowerShell

The following are PowerShell steps equivalent to operations in Full Configuration.

To enroll machines in Microsoft Intune using the Remote PowerShell SDK, use the `DeviceManagementType` parameter in `New-AcctIdentityPool`. This feature requires that the catalog is Azure AD joined and that Azure AD possesses the correct Microsoft Intune license. For example:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
     IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
     AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
     NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
     ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Troubleshoot

If machines fail to enroll in Microsoft Intune, do the following:

- Check if the MCS-provisioned machines are Azure AD joined. The machines fail to enroll in Microsoft Intune if they are not Azure AD joined. See https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html to troubleshoot Azure AD join issues.
- Check if your Azure AD tenant is assigned with the appropriate Intune license. See https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses for license requirements of Microsoft Intune.
- For catalogs that use master images with VDA version 2206 or earlier, check the provisioning status of **AADLoginForWindows** extension for the machines. If the **AADLoginForWindows** extension does not exist, possible reasons are:
  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `AzureAD` or `DeviceManagementType` is not set to `Intune`. You can verify this by running `Get-AcctIdentityPool`.
  - The **AADLoginForWindows** extension installation is blocked by Azure policy.

- To troubleshoot **AADLoginForWindows** extension provisioning failures, you can check logs under `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` on the MCS provisioned machine.

  > **Note:**
  >
  > MCS does not rely on the `AADLoginForWindows` extension to join a VM to Azure AD and enroll to Microsoft Intune when using a master image with VDA version 2209 or later. In this case, the `AADLoginForWindows` extension will not be installed on the MCS-provisioned machine. Therefore, `AADLoginForWindows` extension provisioning logs can't be collected.

- Check Windows event logs under **Application and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.

Create Hybrid Azure Active Directory joined catalogs

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

This article describes how to create Hybrid Azure Active Directory (AD) joined catalogs using Citrix DaaS.

You can create Azure AD joined catalogs by using the Full Configuration interface or PowerShell.

For information on requirements, limitations, and considerations, see Hybrid Azure Active Directory joined.

Use the Full Configuration interface

The following information is a supplement to the guidance in Create machine catalogs. To create hybrid Azure AD joined catalogs, follow the general guidance in that article, minding the details specific to hybrid Azure AD joined catalogs.

In the catalog creation wizard:

- On the **Machine Identities** page, select **Hybrid Azure Active Directory joined**. The created machines are owned by an organization and are signed into with an Active Directory Domain Services account that belongs to that organization. They exist in the cloud and on-premises.

> **Note:**
>
> If you select **Hybrid Azure Active Directory joined** as the identity type, each machine in the catalog must have a corresponding AD computer account.

Use PowerShell

The following are PowerShell steps equivalent to operations in Full Configuration. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

The difference between on-premises AD joined catalogs and hybrid Azure AD joined ones lies in the creation of the identity pool and the machine accounts.

To create an identity pool along with the accounts for hybrid Azure AD joined catalogs:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

> **Note:**
>
> `$password` is the matching password for an AD user account with Write Permissions.

All other commands used to create hybrid Azure AD joined catalogs are the same as for traditional on-premises AD joined catalogs.

View the status of the hybrid Azure AD join process

In the Full Configuration interface, the status of the hybrid Azure AD join process is visible when hybrid Azure AD joined machines in a delivery group are in a powered-on state. To view the status, use Search to identify those machines and then for each check **Machine Identity** on the **Details** tab in the lower pane. The following information can appear in **Machine Identity**:

- Hybrid Azure AD joined

- Not yet joined to Azure AD

> **Note:**
>
> - You might experience delayed hybrid Azure AD join when the machine initially powers on. This is caused by the default machine identity sync interval (30 minutes of Azure AD Connect). The machine is in hybrid Azure AD joined state only after the machine identities are synced to Azure AD through Azure AD Connect.
> - If machines fail to be in hybrid Azure AD joined state, they are not registered with the Delivery Controller. Their registration status appears as **Initialization**.

Also, using the Full Configuration interface, you can learn why machines are unavailable. To do that, click a machine on the **Search** node, check **Registration** on the **Details** tab in the lower pane, and then read the tooltip for additional information.

Troubleshoot

If machines fail to be hybrid Azure AD joined, do the following:

- Check if the machine account has been synced to Azure AD through the Microsoft Azure AD portal. If synced, **Not yet joined to Azure AD** appears, indicating pending registration status.

  To sync machine accounts to Azure AD, make sure:

  - The machine account is in the OU that is configured to be synced with Azure AD. Machine accounts without the **userCertificate** attribute are not synced to Azure AD even they are in the OU that is configured to be synced.
  - The attribute **userCertificate** populates in the machine account. Use Active Directory Explorer to view the attribute.
  - Azure AD Connect must have been synced at least once after the machine account is created. If not, manually run the `Start-ADSyncSyncCycle -PolicyType Delta` command in the PowerShell console of the Azure AD Connect machine to trigger an immediate sync.

- Check if the Citrix managed device key pair for hybrid Azure AD join is correctly pushed to the machine by querying the value of **DeviceKeyPairRestored** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentCo**

  Verify that the value is 1. If not, possible reasons are:

  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `HybridAzureAD`. You can verify this by running `Get-AcctIdentityPool`.
  - The machine is not provisioned using the same provisioning scheme of the machine catalog.

  - The machine is not joined to the local domain. Local domain joined is a prerequisite of the hybrid Azure AD join.

- Check diagnostic messages by running the `dsregcmd /status /debug` command on the MCS-provisioned machine.
  - If hybrid Azure AD join is successful, **AzureAdJoined** and **DomainJoined** are **YES** in the output of the command line.
  - If not, refer to the Microsoft documentation to troubleshoot the issues: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.
  - If you get the error message **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, then run the following PowerShell command to repair the user certificate:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
   UserCertificate
<!--NeedCopy-->
```

For more information about the user certificate issue, see CTX566696.

Create non-domain-joined catalogs

November 1, 2022

This article describes how to create non-domain-joined catalogs using Citrix DaaS.

For information on requirements, limitations, and considerations, see Non-domain-joined.

Before you create the machine catalog, you need the following:

1. New resource location
   - Navigate to the Citrix Cloud admin UI > upper left hamburger menu > **Resource Locations**.
   - Click **+ Resource Location**.
   - Enter a name for the new resource location and click **Save**.
2. Create a hosting connection. See Create and manage connections section for details.

Using Citrix DaaS, you can create catalogs based on workgroups or non-domain-joined machines. Creating non-domain-joined machines depends on how the account identity pool is created. The account identity pool is the mechanism used by MCS to create and track machine names during catalog provisioning.

You can create non-domain-joined catalogs by using the Full Configuration interface or PowerShell.

Use the Full Configuration interface

The following information is a supplement to the guidance in Create machine catalogs. To create non-domain-joined catalogs, follow the general guidance in that article, minding the details specific to non-domain-joined catalogs.

In the catalog creation wizard:

- On the **Machine Identities** page, select **Non-domain-joined**. The created machines are not joined to any domain.

> **Note:**
>
> The **Non-domain-joined** identity type requires version 1811 or later of the VDA as the minimum functional level for the catalog. To make it available, update the minimum functional level if necessary.

Use PowerShell

The following are PowerShell steps equivalent to operations in Full Configuration.

You can create an identity pool for non-domain-joined catalogs using the Remote PowerShell SDK.

For example, in previous releases, all Active Directory fields were supplied in a single instance:

```
1 New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
     IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
     -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
     Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

MCS now uses new PowerShell parameters, **WorkgroupMachine** and **IdentityType**, to create an identity pool for non-domain-joined catalogs. Using the same example as above, the parameters eliminate the need to specify all AD-specific parameters including domain administrator credentials:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
     WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
     NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
     ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

All other commands used to create non-domain-joined catalogs are the same as for the traditional on-premises Active Directory joined catalogs.

Manage machine catalogs

June 27, 2024

> **Note:**
>
> This article describes how to manage catalogs using the Full Configuration interface and PowerShell commands. If you created the catalog using the Quick Deploy interface, and continue using that interface to manage the catalog, then follow Manage catalogs in Quick Deploy.

Introduction

You can add or remove machines from a machine catalog, and rename, change the description, or manage a catalog's Active Directory computer accounts.

Catalog maintenance can also include the tasks of making sure that each machine has the latest OS updates, antivirus software updates, operating system upgrades, or configuration changes.

- Catalogs containing pooled random machines created using Machine Creation Services (MCS) maintain machines by updating the image used in the catalog and then updating the machines. This method lets you update large numbers of user machines efficiently.
- For catalogs containing static, permanently assigned machines, you can manage the image or template that those catalogs currently use but only the machines you add to the catalogs later are created using the new image or template.
- For Remote PC Access catalogs, you manage updates to users' machines outside of the Full Configuration management interface. Perform this task individually or collectively using third-party software distribution tools.

For information about creating and managing connections to host hypervisors and cloud services, see Create and manage connections and resources.

> **Note:**
>
> MCS does not support Windows 10 IoT Core and Windows 10 IoT Enterprise. Refer to the Microsoft site for more information.

About persistent instances

When updating the master image for an MCS catalog containing persistent machines, any new machines added to the catalog use the updated image. Existing machines continue to use the original master image. The process of updating an image is done the same way for any other type of catalog. Consider the following:

- With persistent disk catalogs, the pre-existing machines are not updated to the new image, but any new machines added to the catalog use the new image.
- For non-persistent disk catalogs, the machine image is updated the next time only if the machine is restarted within Studio or PowerShell. If the machine is restarted from the hypervisor outside of Studio, the disk is not reset.
- For catalogs that do not persist, if you want different images for different machines, the images must reside in separate catalogs.

Manage machine catalogs

You can manage a machine catalog in two ways:

- Using Full Configuration interface
- Using PowerShell

Use Full Configuration interface

This section details how you can manage catalogs using the Full Configuration interface:

- View catalog details
- Add machines to a catalog
- Delete machines from a catalog
- Edit a catalog
- Rename a catalog
- Delete a catalog
- Manage Active Directory computer accounts in a catalog
- Change the master image for a catalog
- Change the functional level or undo the change
- Clone a catalog
- Organize catalogs using folders
- Configure auto-upgrade for VDAs
- Manage configuration set for a catalog
- Retry catalog creation
- (Non-Citrix provisioned VDAs only) Generate and manage enrollment tokens

View catalog details

1. Use the search function to locate a specific machine catalog. Refer to Search for instances for instructions.
2. From the search results, select a catalog as necessary.

3. Refer to the following table for descriptions of the catalog columns.
4. Click a tab in the bottom details pane for more information about this catalog.

Column	Description
Machine Catalog	The name and the allocation type of the catalog. Allocation types include: Random: Machines in the catalog are allocated to a user randomly. Permanent: Machines in the catalog are allocated to a user permanently.
Machine Type	The supported session type of the machines in the catalog. Possible values include: OS type: Multi-session OS (Virtual); User data: Discard. OS type: Multi-session OS (Virtual); User data: On local disk OS type: Single-session OS (Remote PC Access) OS type: Single-session OS (Virtual); User data: Discard OS type: Single-session OS (Virtual); User data: On local disk
Machine Count	The machine count in the catalog and the provisioning methods include: Machine creation services (MCS machine), Manual, and Citrix provisioning services.
Allocated Count	The number of machines in the catalog assigned to a delivery group.
Folder	The location of the catalog within the **Machine Catalogs** tree. It displays the name of the folder that the catalog is in (including the trailing backslash), or − if the catalog is at the root level.
VDA Upgrade	VDA Upgrade State. Possible values include: Not configured, Scheduled, Available, and Up to date.
Image Status	The image update status of the catalog. Applicable only to non-persistent machine catalogs. Possible values include: Fully updated, Partially updated, Pending updates, Preparing

Add machines to a catalog

Before you start:

- Make sure the virtualization host (hypervisor or cloud service provider) has sufficient processors, memory, and storage to accommodate the additional machines.
- Make sure that you have enough unused Active Directory computer accounts. If you are using existing accounts, the number of machines you can add is limited by the number of accounts available.
- If you use the Full Configuration management interface to create Active Directory computer accounts for the additional machines, you must have appropriate domain administrator permission.

> **Tip:**
>
> If the Citrix DaaS account used to add machines to the machine catalog has restricted AD permissions, add all Cloud Connectors you intend to use in the **Log on to..** screen.

To add machines to a catalog:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a machine catalog and then select **Add machines** in the action bar.
3. On the **Virtual Machines** page, select the number of virtual machines to add.
4. On the **Machine Identities** page, configure the settings as follows:
    - Select an identity from the list.
    - If applicable, indicate whether to create accounts or use existing ones, and the location (domain) for those accounts.

      If there are insufficient existing Active Directory accounts for the number of VMs you are adding, select the domain and location where the accounts are created.

      If you use existing Active Directory accounts, browse to the accounts or select **Import** and specify a `.csv` file containing account names. Make sure that there are enough accounts for all the machines you are adding. The Full Configuration interface manages these accounts. Allow that interface to reset the passwords for all the accounts, or specify the account password, which must be the same for all accounts.
    - If this identity pool is used by other catalogs, you can't change it to a different pool using Full Configuration. Instead, use the **Set-ProvScheme** PowerShell cmdlet. For more information, see the Citrix Virtual Apps and Desktops SDK Documentation.
    - Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters appear. For example, a naming scheme of PC-Sales-## (with 0-9 selected) results in computer accounts named PC-Sales-01, PC-Sales-02, PC-Sales-03, and so on.
    - Optionally, you can specify what the account names start with.

When specifying what the account names start with, be aware of the following scenario: If the starting numbers or letters are already in use, the first account created is named using the nearest unused numbers or letters thereafter.

See Manage the sequence number of the machine name to customize the sequence number of machines, which are deployed using MCS, through PowerShell commands.

5. On the **Domain Credentials** page, select **Enter credentials** and enter user credentials with sufficient permissions to create machine accounts.

The machines are created as a background process, and can take much time when creating many machines. Machine creation continues even if you close the Full Configuration management interface.

Use CSV files to bulk add machines to a catalog

You can bulk add machines by using CSV files. The feature is available for all catalogs except catalogs provisioned through MCS.

To bulk add machines to a catalog, complete the following steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a machine catalog and then select **Add Machines** in the action bar. The **Add Machines** window appears.
3. Select **Add CSV File**. The **Add Machines in Bulk** window appears.
4. Select **Download CSV Template**.
5. Fill out the template file.
6. Drag or browse to the file to upload it.
7. Select **Validate** to perform validation checks on your import.
8. Select **Import** to complete the process.

Considerations when using CSV files to add machines

> **Note:**
>
> - For non-Active Directory users, you must type their names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`.
> - VM names are case sensitive. When entering VM paths, make sure that you enter the VM names correctly.

When editing the CSV template file, keep the following in mind:

- The feature gives you more flexibility to bulk add machines through a CSV file. In the file, you can add only machines (for use with user auto-assignments) or add machines along with user assignments. Type your data in the following format:

  - For machine account and user name (samName) pairs:
    - Domain\ComputerName1, Domain\Username1
    - Domain\ComputerName2, Domain\Username1;Domain\Username2
    - Domain\ComputerName3, AzureAD:username
  - For machine accounts only:
    - Domain\ComputerName1
    - Domain\ComputerName2
  - For VM and user name pairs:
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer
  - For VMs only:
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer

    For example:
    `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    where,

    - `xpace-scale` is the ConnectionName: The name of the connection that you entered in **Full Configuration > Hosting > Add Connections and Resources**. For more information, see Create a connection and resources.
    - `East US.region` is the RegionName: The name of the region with `.region` as extension.
    - `wsvdaV3-2.vm` is the VMName: The name of the virtual machine with `.vm` as extension.

- The maximum number of machines that a file can contain is 1,000. To import more than 1,000 machines, spread them across different files and then import those files one by one. We recommend that you import no more than 1,000 machines. Otherwise, catalog creation can take a long time to complete.

You can also export machines from a catalog on the same **Add Machines** page. The exported CSV of machines can then be used as a template when adding machines in bulk. To export machines:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a machine catalog and then select **Add Machines** in the action bar. The **Add Machines** window appears.
3. Select **Export to CSV file**. A CSV file containing a list of the machines is downloaded.

4. Open the CSV file to add or edit machines as needed. To add machines in bulk using the saved CSV file, see the previous section, Use CSV files to bulk add machines to a catalog.

> **Note:**
>
> - This feature is not available for Remote PC Access and MCS-provisioned catalogs.
> - Export and import of machines in CSV files is only supported between catalogs of the same type.

Enroll machines to catalogs using the WebSocket VDA enrollment tool

The WebSocket VDA enrollment tool facilitates token-based enrollment for VDA machines. This tool helps you convert a connection to a WebSocket connection by adding the VDA to the machine catalog using the enrollment token.

> **Note:**
>
> This tool is designed to enroll VDA machines that haven't been enrolled in any machine catalog.

Follow the instructions to run the enrollment tool:

1. Log in to the VDA.
2. Locate the tool `EnrollMachine.exe`, in `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Run the tool with the appropriate input parameters. For example, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

The following table describes the input parameters of the enrollment tool:

Parameter Name	Required	Description	Example
`-websocket_token_stdin`	Yes	Reads the enrollment token.	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		Reads the enrollment token directly from the command line parameter.	`.\EnrollMachine.exe -websocket_token_string:<token>`

Parameter Name	Required	Description	Example
-websocket_token_file:[token-file-path]		Reads the enrollment token from the path provided.	.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt
log:[log-file-path]	No	Shows the Enrollment tool logs.	.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]
-help	No	Shows a brief help text.	.\EnrollMachine.exe -help

After successful enrollment, you will receive a success message on the tool and in the logs. Ensure to sign in to the Full Configuration to verify that the VDA machine is added to the catalog and that the status of the machine is registered.

Troubleshooting By default, you can find the logs of the enrollment tool at:

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

If you have specified a different path for the logs, you can use `log:[log-file-path]` to retrieve your logs.

The following table lists the codes returned by the enrollment tool:

Code	String	Description
0	Success	VDA is successfully added to the machine catalog.
-1	InvalidArgument	The input parameter in the enrollment token is invalid.
-2	BrokerAgentNotFound	The broker agent service is not found.
-3	TokenInvalid	The token entered is invalid.

Code	String	Description
-4	TokenMissingRequiredClaims	The required claims for the token are missing, for example, CustomerId, or Enrollment URIs.
-5	InternalError	A general error has occurred.
-6	TimedOut	The task has timed out.
-7	FailedToDetermineMachineADJoinedStatus	The service that returns the machine AD joined status failed.
-8	ADMachineFailedToFindSid	The service that returns the AD machine Sid failed.
-9	EnrollRequestFailed	The request failed due to an HTTP error.
-10	EnrollResponseMissingRequiredFields	The enrollment tool response is missing the parameter `VirtualSiteId`.
-11	InsufficientPermission	You do not have the required permission to run the task.
-12	FailedToDetermineMachineAadJoinedStatus	The service that checks the machine AD join status throws an error.
-13	AadMachineFailedToFindDeviceId	The additional parameter `AAD device id` added by the system is empty.
-14	AadDeviceIdNotValid	The additional parameter `AAD device id` added by the system is not a valid guid.
-15	NoValidMacAddress	Invalid MAC address.
-16	FailedToGetComputerHostName	Failed to get the computer host name to set the additional parameter `VdaInstanceName`.
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Failed to open the VDA registry key to write the list of Delivery controllers.
-18	Failed Token reached the max count	Failed Token reached the max count.

Delete machines from a catalog

After you delete a machine from a machine catalog, users can no longer access it, so before deleting a machine, ensure that:

- User data is backed up or no longer required.
- All users are logged off. Turning on maintenance mode stops new connections from being made to a machine.
- Machines are powered off.

To delete machines from a catalog:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **View Machines** in the action bar.
3. Select one or more machines and then select **Delete** in the action bar.
4. If you are deleting persistent machines from the catalog, choose whether to delete them from the hypervisor or cloud service as well. If you choose to delete them, indicate whether to retain, disable, or delete their Active Directory accounts.

When you delete persistent machines from an Azure Resource Manager catalog, the machines and associated resource groups are deleted from Azure, even if you choose to retain them.

When you delete non-persistent machines from a catalog, they are automatically deleted from the hypervisor or cloud service.

Edit a catalog

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Edit Machine Catalog** in the action bar.
3. On the **Scopes** page, change the scopes.
4. On the **NIC** page, perform the following actions:

    - To change the subnet mapping of an NIC, select a network from the **Associated Network** field.
    - To add a subnet mapping, select **Add NIC**, select a network from the **Associated Network** field, and click **Save**.

    Only those subnets present in the host associated with the catalog appear in the **Associated Network** field.

    You can only add NIC to Azure machine catalogs without machine profiles.

> **Note:**
>
> - For AWS machine catalogs, you cannot map the same subnet to more than one NIC.
> - For machine catalogs with machine profiles, the number of NICs on the catalog must be equal to the number of NICs on the machine profile.
> - This feature is not supported for IBM Cloud hypervisors.
> - This feature is supported only for Nutanix Prism Element in case of Nutanix hypervisors.

5. On the **VDA Upgrade** page, change or select the VDA version to upgrade to. For more information, see VDA upgrade.
6. You might see additional pages depending on the catalog type.

   For catalogs created using an Azure Resource Manager image, the following pages are visible. Keep in mind that changes you make apply only to machines you add to the catalog later. Existing machines remain unchanged.

   - On the **Virtual Machines** page, change the machine size and availability zones where you want to create machines.

     > **Note:**
     >
     > – Only machine sizes that the catalog supports are shown.
     > – If necessary, select **Show only machine sizes used in other machine catalogs** to filter the machine size list.

   - On the **Machine Profile** page, choose whether to use or change a machine profile.
   - (Only when the catalog is configured with a dedicated group host) On the **Dedicated host group** page, choose whether to change a host group.
   - On the **Storage and License Types** page, choose whether to change the storage type, license type, and Azure Computer Gallery settings (available only when **Place prepared image in Azure Gallery** is in use).

     > **Note:**
     >
     > If the newly selected setting doesn't support the current machine size, a warning dialog box appears, informing you that changing the setting will reset the machine size setting. If you choose to continue, a red dot appears next to the **Virtual Machines** menu, prompting you to select a new machine size.

   For more information about settings available on the pages, see Create a machine catalog using an Azure Resource Manager image.

   For Remote PC Access catalogs, the following pages are visible:

- On the **Power Management** page, change the power management settings and select a power management connection.
- On the **Organizational Units** page, add or remove Active Directory OUs.

7. On the **Description** page, change the catalog description.
8. Click **Apply** to apply the changes you made and click **Save** to exit.

Rename a catalog

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Rename Machine Catalog** in the action bar.
3. Enter the new name.

Delete a catalog

Before deleting a catalog, ensure that:

- All users are logged off and no disconnected sessions are running.
- Maintenance mode is turned on for all machines in the catalog so that new connections cannot be made.
- All machines in the catalog are powered off.
- The catalog is not associated with a delivery group. In other words, the delivery group does not contain machines from the catalog.

To delete a catalog:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Delete Machine Catalog** in the action bar.
3. If the catalog contains persistent machines, indicate whether to delete those machines from the hypervisor or cloud service as well. If you choose to do so, choose whether to retain, disable, or delete their Active Directory computer accounts.
4. If necessary, select **Hide progress** to run the deletion in the background.

> **Note:**
>
> - When you delete an Azure Resource Manager catalog, the associated machines and resource groups are deleted from Azure, even if you choose to retain them.
> - When you delete a catalog containing non-persistent machines, those machines are deleted from the hypervisor or cloud service.
> - When the hypervisor or cloud service is unreachable during catalog deletion, both catalog and VM deletion fail. If needed, you can choose to delete the VM records only from your

> Citrix site database. To do so, select the machine catalog in the **Machine Catalogs** node, and then perform the deletion shown on the **Troubleshoot** tab. Keep in mind that this action leaves the VMs intact on the host.

Manage Active Directory computer accounts in a catalog

To manage Active Directory accounts in a machine catalog, you can:

- Free unused machine accounts by removing Active Directory computer accounts from single-session and multi-session catalogs. Those accounts can then be used for other machines.
- Add accounts so that when more machines are added to the catalog, the computer accounts are already in place. Do not use a forward slash (/) in an OU name.

To manage Active Directory accounts:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Manage AD accounts** in the action bar.
3. Choose whether to add or delete computer accounts. If you add accounts, specify what to do with the account passwords: either reset them all or enter a password that applies to all accounts.

   You might reset passwords if you do not know the current account passwords; you must have permission to perform a password reset. If you enter a password, the password is changed on the accounts as they are imported. If you delete an account, choose whether the account in an Active Directory is to be kept, disabled, or deleted.

You can also indicate whether Active Directory accounts are to be retained, disabled, or deleted when you remove machines from a catalog or delete a catalog.

Change the master image for a catalog

We recommend that you save copies or snapshots of images before you change the master image for a catalog. The database keeps a historical record of the images used with each machine catalog. If users encounter problems with the new image you deployed to their desktops, you can roll it back to the previous version, minimizing user downtime. Do not delete, move, or rename images. Otherwise, you cannot roll back the master image.

> **Important:**
>
> When changing the master image for a persistent catalog, consider the following: only machines

> you add to the catalog later are created using the new image. We do not roll out the new image to existing machines in the catalog.

After a machine is updated, it restarts automatically.

Update or create an image

Before you change the master image for a catalog, prepare a new image on your host hypervisor by either updating an existing image or creating one.

1. On your hypervisor or cloud service provider, take a snapshot of the current VM and give the snapshot a meaningful name. This snapshot can be used to roll back the master image.
2. If necessary, power on the image, and log on.
3. Install updates or make any required changes to the image.
4. If the image uses a Personal vDisk, update the inventory.
5. Power off the VM.
6. Take a snapshot of the VM, and give the snapshot a meaningful name that is recognized when you change the master image.

> **Note:**
>
> Although you can create a snapshot using the management interface, we recommend that you create a snapshot using the hypervisor management console, and then select that snapshot in the Full Configuration management interface. This enables you to provide a meaningful name and description rather than an automatically generated name. For GPU images, you can change the image only through the XenServer XenCenter console.

Change the master image

To roll out a new master image to all machines in a catalog:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Change Master Image** in the action bar.
3. On the **Image** page, select the host and the image you want to roll out.

   > **Tip:**
   >
   > For an MCS-created catalog, you can annotate its image by adding a note for the image. A note can contain up to 500 characters. Each time you change the master image, a note-related entry is created whether you add a note. If you update a catalog without adding a

> note, the entry appears as null (-). To view note history for the image, select the catalog, click **Template Properties** in the low pane, and then click **View note history**.

4. On the **Rollout Strategy** page, choose when the machines in the machine catalog are changed with the new image: on the next shutdown or immediately.

   > **Note:**
   >
   > The **Rollout Strategy** page is not available for persistent VMs because rollout is only applicable to non-persistent VMs.

5. Verify the information on the **Summary** page and then select **Finish**. Each machine restarts automatically after it is updated.

   To track the progress of the update, locate the catalog in **Machine Catalogs** to view the inline progress bar and the step-by-step progress graph. For a non-persistent catalog, you can track its image update statuses through the **Image Update** column, including **Fully updated**, **Partially updated**, **Pending update**, and **Preparing image**.

   > **Tip:**
   >
   > To show the **Image Update** column, select the **Columns to Display** icon in the action bar, select **Machine Catalog > Image Status**, and then click **Save**.

If you are updating a catalog using the PowerShell SDK, you can specify a hypervisor template (`VMTemplates`), as an alternative to an image or a snapshot of an image.

Rollout strategy

Changing the image on the next shutdown will immediately affect any machines not currently in use, that is, machines that do not have an active user session. A system that is in use receives the update when the current active session ends.

> **Note:**
>
> Rollout strategy is only applicable to non-persistent VMs.

Consider the following:

- New sessions cannot be launched until the update has completed on applicable machines.
- For single-session machines, machines are immediately updated when the machine is not in use, or when users are not logged in.
- For a multi-session OS with child machines, reboots do not occur automatically. They must be manually shut down and restarted.

> **Tip:**
>
> Limit the number of machines being rebooted by using the advanced settings for a host connection. Use these settings to modify the actions taken for a given catalog; advanced settings vary depending on the hypervisor.

Roll back the master image

After you roll out an updated or new image, you can roll it back. This might be necessary if issues occur with the newly updated machines. When you roll back, machines in the catalog are rolled back to the last working image. Any new features that require the newer image are no longer available. As with the rollout, rolling back a machine includes a restart.

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select the catalog and then select **Roll Back Master Image** in the action bar.
3. Specify when to apply the earlier image to machines, as described for the rollout operation.

The rollback is applied only to machines that need to be reverted. For machines that have not been changed to the new or updated image (for example, machines with users who have not logged off), users do not receive notification messages and are not forced to log off.

To track the rollback progress, locate the catalog in **Machine Catalogs** to view the inline progress bar and the step-by-step progress graph.

You cannot roll back in certain scenarios, including the following. (The **Roll Back Master Image** option is not visible).

- You do not have permission to roll back.
- The catalog was not created using MCS.
- The catalog was created using an image of the OS disk.
- The snapshot used to create the catalog has become corrupted.
- User changes to the machines in the catalog do not persist.
- Machines in the catalog are running.

Change the functional level or undo the change

Change the functional level for the machine catalog after you upgrade the VDAs on the machines to a newer version. We recommend upgrading all VDAs to the latest version to enable access to all the newest features.

Before changing the functional level for a machine catalog:

- Start the upgraded machines so that they register with Citrix DaaS. This lets the management interface determine that the machines in the catalog need upgrading.

To change the functional level for a catalog:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select the catalog. The **Details** tab in the lower pane displays version information.
3. Select **Change Functional Level**. If the management interface detects that the catalog needs to change the functional level, it displays a message. Follow the prompts. If one or more machines cannot be changed, a message explains why. To ensure that all machines function properly. We recommend you resolve those issues before clicking **Change**.

After the catalog upgrade completes, you can revert the machines to their previous VDA versions by selecting the catalog and then selecting **Undo Functional Level Change** in the action bar.

Clone a catalog

Before cloning a catalog, be aware of the following considerations:

- You cannot change settings associated with operating system and machine management. The cloned catalog inherits those settings from the original.
- Cloning a catalog can take some time to complete. If necessary, select **Hide progress** to run the cloning in the background.
- The cloned catalog inherits the name of the original and has a suffix Copy. You can change the name. See Rename a catalog.
- After cloning completes, be sure to assign the cloned catalog to a delivery group.
- You can create an empty catalog by cloning. During catalog cloning, you can set the number of machines to zero for MCS-provisioned catalogs and add no machines for non-MCS-provisioned catalogs.

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Clone** in the action bar.
3. In the **Clone Selected Machine Catalog** window, view the settings for the cloned catalog and configure settings as applicable. Select **Next** to proceed to the next page.
4. On the **Summary** page, view a summary of the settings and select **Finish** to start cloning.
5. If necessary, select **Hide progress** to run the cloning in the background.

Organize catalogs using folders

You can create folders to organize catalogs for easy access. For example, you can organize catalogs by image type or by organization structure.

> **Tip:**
>
> You can set your preferred default view (folder or list view) for the Machine Catalogs node by clicking the **Folder** icon on the top right of the action bar.

Required roles

By default, you need to have the following built-in role to create and manage catalog folders: Cloud Administrator, Full Administrator, or Machine Catalog Administrator. If necessary, you can customize roles for creating and managing catalog folders. For more information, see Required permissions.

Create a catalog folder

Before you start, first plan how to organize your catalogs. Consider the following:

- You can nest folders up to five levels deep (excluding the default root folder).
- A catalog folder can contain catalogs and subfolders.
- All nodes in **Full Configuration** (such as the **Machine Catalogs** and the **Applications** nodes) share a folder tree in the backend. To avoid name conflicts with other nodes when renaming or moving folders, we recommend you give different names to first-level folders in different nodes.

To create a catalog folder, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. In the folder hierarchy, select a folder and then select **Create Folder** in the **Action** bar.
3. Enter a name for the new folder, and then click **Done**.

> **Tip:**
>
> If you create a folder in an unintended location, you can drag it to the correct location.

Move a catalog

You can move a catalog between folders. Detailed steps are as follows:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. View catalogs by folder. You can also turn on **View all** above the folder hierarchy to view all catalogs at a time.
3. Right-click a catalog and then select **Move Machine Catalog**.
4. Select the folder to which you want to move the catalog, and then click **Done**.

> **Tip:**
>
> You can drag a catalog to a folder.

Manage catalog folders

You can delete, rename, and move catalog folders.

You can delete a folder only if it and its subfolders don't contain catalogs.

To manage a folder, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. In the folder hierarchy, select a folder, and then select an action in the **Action** bar as needed:
   - To rename the folder, select **Rename Folder**.
   - To delete the folder, select **Delete Folder**.
   - To move the folder, select **Move Folder**.
3. Follow the onscreen instructions to complete the remaining steps.

Required permissions

The following table lists the permissions required to do actions on catalog folders.

Action	Required permissions
Create catalog folders	Create Machine Catalog Folder
Delete catalog folders	Remove Machine Catalog Folder
Move catalog folders	Move Machine Catalog Folder
Rename catalog folders	Edit Machine Catalog Folder
Move catalogs to folders	Edit Machine Catalog Folder and Edit Machine Catalog Properties

Configure auto-upgrade for VDAs

> **Important:**
>
> - To ensure a smooth upgrade, make sure that you meet the prerequisites and review known issues before upgrading VDAs to CR or LTSR CU versions. See Upgrade VDAs using the Full Configuration interface.

> - When upgrading LTSR VDAs to LTSR Cumulative Update (CU) versions, make sure that the version of the VDA Upgrade Agents running on the VDAs is 7.36.0.7 or later. For more information, see Upgrade VDAs using the Full Configuration interface.
> - You can switch between the CR VDA and the LTSR VDA as long as you switch from an earlier version to a later version. You cannot switch from a later version to an earlier version because that is considered a downgrade. For example, you cannot downgrade from 2212 CR to 2203 LTSR (any CU) but you can upgrade from 2112 CR to 2203 LTSR (any CU).
> - You can also upgrade VDAs using PowerShell. See Upgrade VDAs using PowerShell.

With the feature, you can do the following:

- Upgrade VDAs on a per-catalog basis
- Edit or cancel a scheduled VDA upgrade
- Configure VDA upgrade settings after catalog creation
- Upgrade VDAs on a per-machine basis

> **Note:**
>
> - When you schedule VDA upgrades for a catalog, only VDAs in the catalog that have the VDA Upgrade Agent installed can be upgraded.
> - Upgrading a VDA fails when the machine is in maintenance mode or when a session is running on the machine.

Supported machine types

This feature applies to the following machine types:

- MCS-provisioned persistent machines (AD joined, Azure AD joined, and non-domain-joined). You deploy them using **Citrix Machine Creation Services** on the **Machine Management** page during catalog creation.
- Remote PC Access machines
- Citrix HDX Plus for Windows 365 machines
- Other persistent machines provisioned using non-Citrix provisioning services or technologies. You add those machines into DaaS for management by using **Other service or technology** on the **Machine Management** page during catalog creation.

For more information about the **Citrix Machine Creation Services** and **Other service or technology** options, see Machine management.

> **Note:**

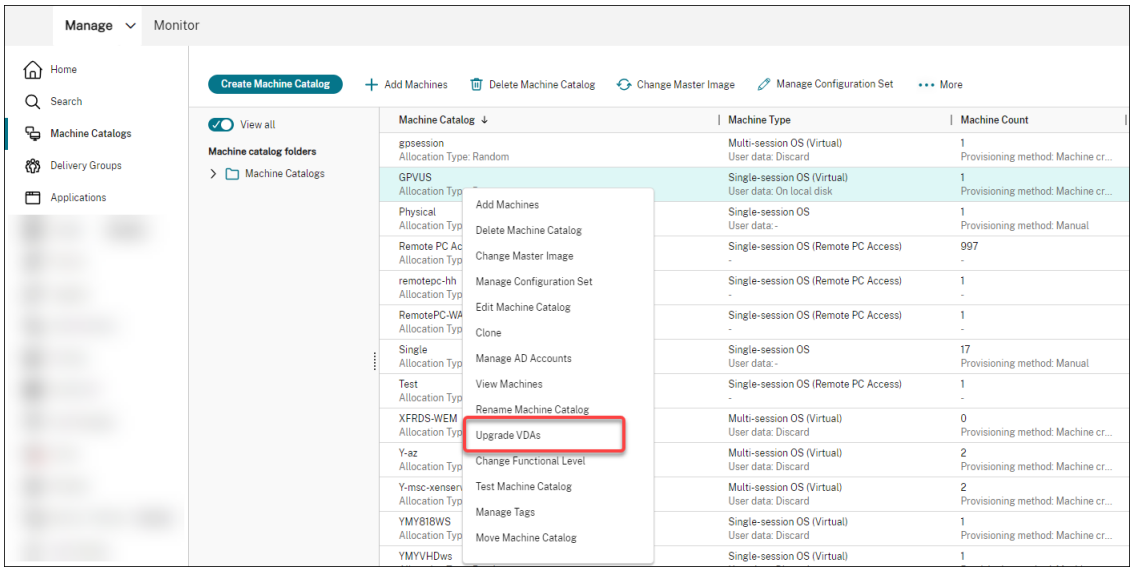
> For MCS-provisioned machines, only static persistent machines are supported. Random machines are not supported even if they are persistent.

Upgrade VDAs on a per-catalog basis

> **Note:**
>
> When scheduling VDA upgrades for a catalog, be aware that all machines in the catalog will be included in the upgrade scope. Therefore, we recommend backing up those machines before initiating the upgrade.

After enabling VDA upgrade for a catalog, you can upgrade VDAs in the catalog immediately or schedule upgrades for the catalog. To do that, follow these steps:

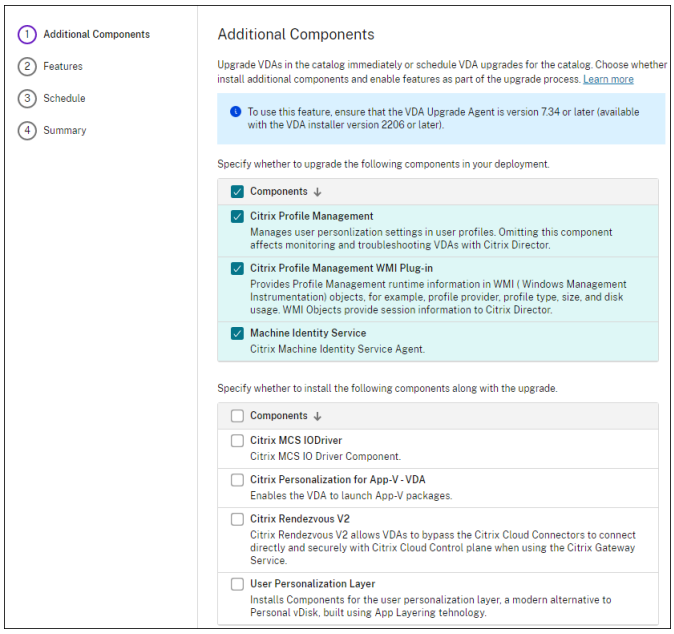
1. From **Manage > Full Configuration**, select **Machine Catalogs**.
2. Select the catalog and then **Upgrade VDAs** from the contextual menu or action bar. (Right-click to display the contextual menu.) The VDA Upgrade window appears.



3. Choose whether to upgrade additional components in your deployment. You can also choose to install certain components in addition to the upgrade. If a component requires configuration, you must click the **Configure** button and configure the component's settings to continue. After configuring, you can click **Edit** to change the configuration.

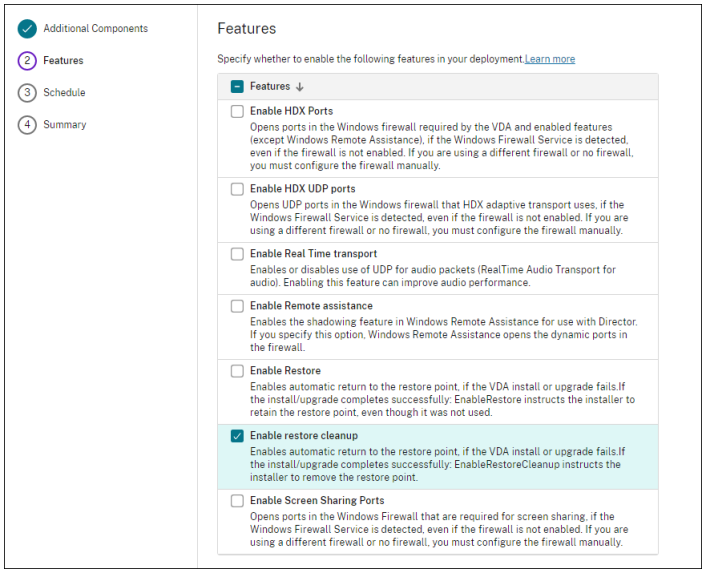
> **Important:**
>
> - To use the additional components feature, make sure that your VDA Upgrade Agent is version 7.34 or later, which is included in the VDA installer version 2206 or later.
>
> **Note:**

- If you choose not to upgrade a component, the component remains intact in your deployment.
- For a complete list of additional components, see Install VDAs.



4. Click **Next**.
5. Choose whether to enable any of the listed features. Click **Next**.

> **Note:**
>
> By default, the **Enable restore cleanup** check box is selected. We recommend enabling the restore feature. With the feature enabled, a system restore point is created before the upgrade starts. The restore point is deleted after the successful installation of the VDA. For more information, see Restore on install or upgrade failure.



6. Choose whether to upgrade the VDAs immediately or at a scheduled time.

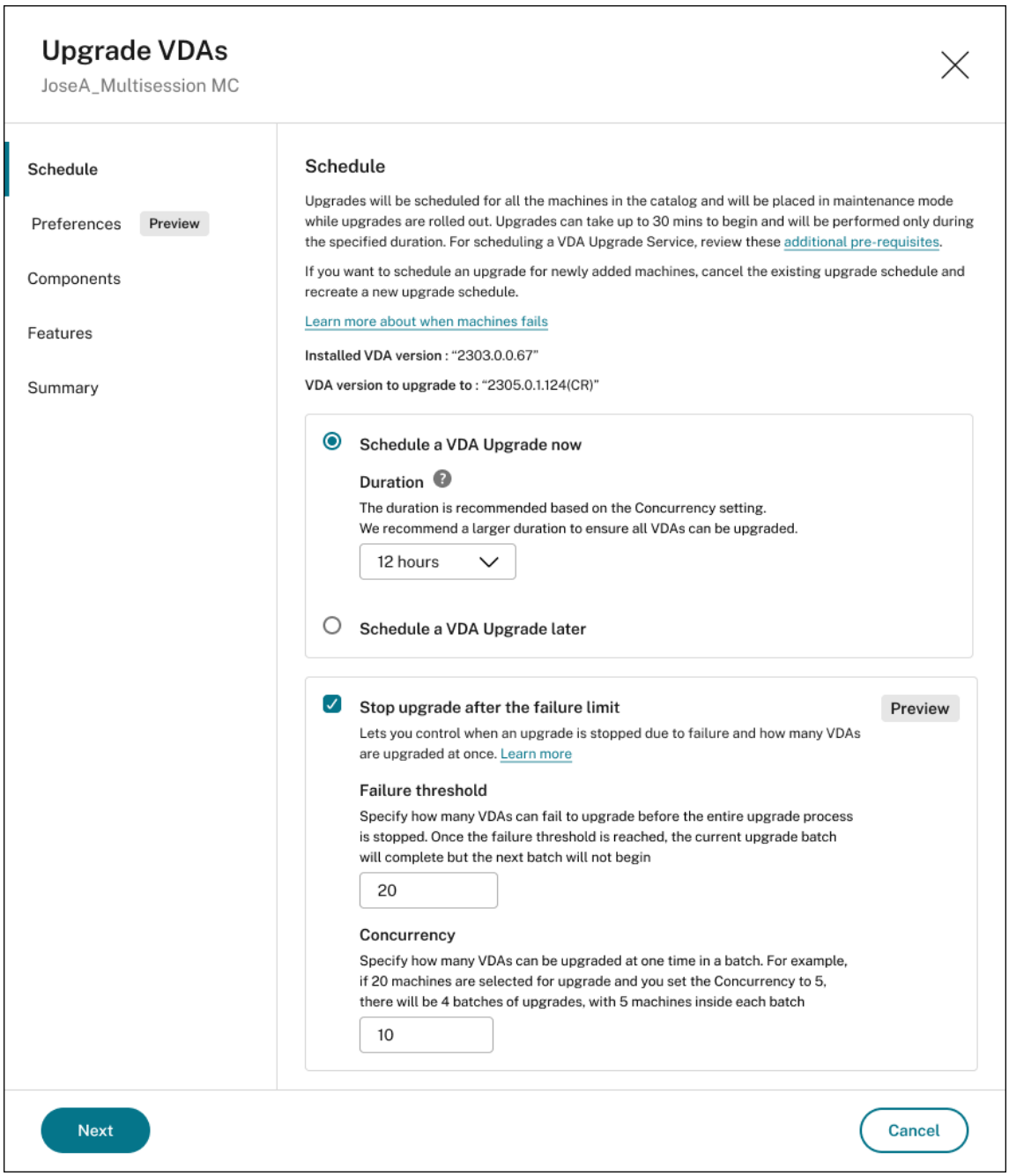
   - To upgrade the VDAs immediately, select **Upgrade now** and then specify a duration.

     A duration is the amount of time, in hours, after which the VDA Upgrade Service stops initiating additional upgrades. Upgrades in progress will run to completion. During that time, DaaS starts to upgrade the VDAs when they become eligible (for example, no active sessions anymore).

     The more VDAs that must be upgraded, the longer this duration is. We recommend selecting a large value (for example, 12 hours). Otherwise, depending on the number of the VDAs, there might still be VDAs that DaaS is unable to upgrade within this window.

   - To schedule the upgrades, select **Upgrade later** and then specify when you want the upgrades to occur.

     You can schedule the upgrades only for the next seven days. Upgrades you schedule apply only to the machines that are currently in the catalog. If you add machines to the catalog later but want to upgrade them as well, cancel the scheduled upgrade and then recreate a schedule.



7. Select the **Stop upgrade after the failure limit (Tech Preview)** option.

   Behaviour illustration

   - Failure Threshold and Concurrency Level must be greater than Zero.
   - Failure Threshold and Concurrency Level must be lesser than or equal to the Total Number of machines being scheduled for Upgrade

Failure Threshold	Concurrency Level	Behavior
Provided	Not Provided or input 0	FailureThreshold is applied and ConcucrrencyLevel is decided by the load balancer as before.
Not Provided or input 0	Provided	FailureThreshold defaults to 10000 (Max Machines Per catalog) and ConcucrrencyLevel is used for batching.
Not Provided or input 0	Not Provided or input 0	The Default behavior is applicable with concurrency levels updated by the load balancer.

8. Enter the **FailureThreshold**.

   > **Note:**
   >
   > Failure Threshold is the number of failures after which the VUS halts any pending upgrade installation from subsequent batches that are not picked up by the upgrade agent.

9. Enter the **Concurrency**.

   > **Note:**
   >
   > Concurrent Upgrade is the number of VMs that can concurrently upgrade at any point within the upgrade window.

10. Click **Next**.

    > **Note:**
    >
    > ExitOnError is incompatible with **Enable Restore** or **Enable Restore and Cleanup** and may not work as intended.

11. Review your choices on the **Summary** page, then click **Finish** to apply your settings and exit the window.

> **Note:**
>
> - The **Upgrade VDAs** option is available only after you enable VDA upgrade for the catalog. To enable VDA upgrade, edit the catalog.
> - All machines in the catalog are placed in maintenance mode while upgrades are rolled out. Upgrades can take up to 30 minutes to begin and will be performed only during the speci-

> fied time period.

On the **Machine Catalogs** node, the **VDA Upgrade** column provides VDA upgrade information for the catalog. The following information can appear:

> **Tip:**
>
> To show the **VDA Upgrade** column, select **Columns to Display** in the action bar, select **Machine Catalog > VDA Upgrade**, and then click **Save**.

- **Available**: A new VDA version is available.
- **Scheduled**: The VDA upgrade has been scheduled.
- **Not configured**: Appears when you have not enabled VDA upgrade for the catalog.
- **Up to date**: The catalog's VDAs are up to date.
- **Unknown**: Unable to get information necessary for VDA upgrade. There are multiple possible reasons:
  - The VDA was in use during the upgrade window.
  - The number of upgrades in progress reached the maximum limit of 500.
  - The VDA Upgrade Agent was unresponsive during the upgrade window. Ensure that the agent is running on the VDA and can communicate with Citrix DaaS.
  - Unable to perform upgrade validation checks. See VDA upgrade requirement.

You can also view the status of VDA upgrades for a catalog. To do that, click the catalog and then check the **VDA Upgrade State** information on the **Details** tab. The following information can appear:

- **Not scheduled**: You have enabled VDA upgrade for the catalog but have not set up an upgrade schedule.
- **Scheduled**: You have created an upgrade schedule for the catalog. For example, if you set the schedule to start at `09:00 PM, December 14, 2030`, information appears as follows: Scheduled for `December 14, 2030 09:00 PM UTC`.
- **In progress**: VDA upgrades have started.
- **Canceled**: You have canceled the scheduled upgrade.
- **Failed**: The catalog contains one or more machines whose VDA upgrades were not successful.
- **Successful**: All VDAs in the catalog were upgraded successfully.

You can also troubleshoot VDA upgrade issues with recommended actions for a catalog. To do that, click the catalog and then go to the **Troubleshoot** tab.

To quickly drill-down to catalogs that have a specific VDA upgrade state, you can use filters. For more information, see Use Search in the Full Configuration management interface.

Be aware of the following considerations:

- The **VDA Upgrade** or **VDA Upgrade State** filter is available for use only with the following filters: **Name** and **Machine Catalog**.

- When you use the **VDA Upgrade** or the **VDA Upgrade State** filter, **Errors** and **Warnings** in the upper right corner become unavailable.

Edit or cancel a scheduled VDA upgrade

After you schedule the upgrades for a catalog, you might want to edit or cancel the scheduled upgrade. To do that, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs**.
2. Select the catalog and then **Edit Scheduled VDA Upgrade** in the action bar. The Edit VDA Upgrade window appears, showing information about the installed VDA version and VDA version to upgrade to.
3. Choose whether to edit or cancel the scheduled upgrade.
    - To cancel the upgrade, click **Cancel scheduled upgrade**. Remember: Canceling the scheduled upgrade does not force the upgrade in progress to stop.
4. Click **Done** to exit the window.

Configure VDA upgrade settings by editing a catalog

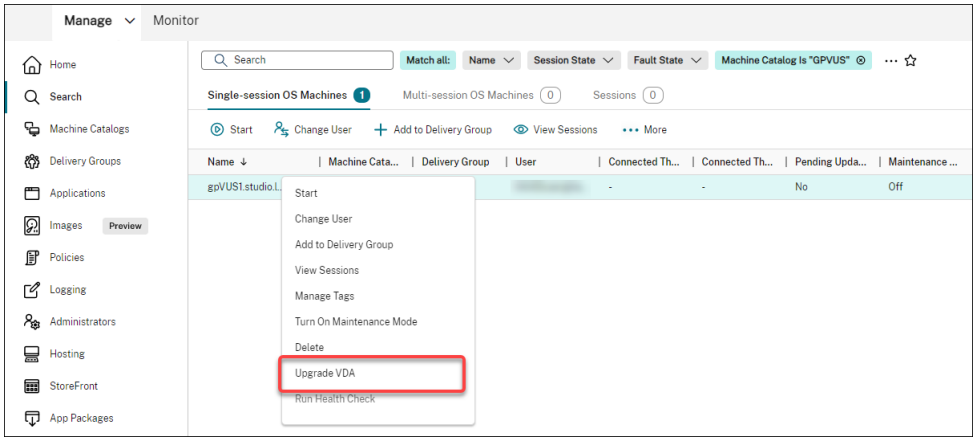
After catalog creation, you can configure VDA upgrade settings by editing the catalog. Before you start editing, consider the following:

- Verify that all machines in the catalog are on the same VDA (CR or LTSR) track. Otherwise, certain VDA upgrades will fail. For example, if you select **Latest LTSR VDA**, CR VDA upgrades will fail.
- Upgrades to some of the machines in the catalog might have started. You cannot modify upgrades that are already in progress. Upgrades in progress continue. Those that have not yet started will upgrade to the specified version.

Upgrade VDAs on a per-machine basis

After enabling VDA upgrade for a catalog, you can upgrade the catalog's VDAs one by one or in batches. To do that, follow these steps:

1. From **Manage > Full Configuration**, select **Search**.
2. Select one or more machines and then **Upgrade VDA** from the contextual menu or action bar. (Right-click to display the contextual menu.)



Note:

- For the **Upgrade VDA** option to be available, make sure that you have enabled VDA upgrade for the catalog where the selected machines reside and that those machines have the VDA Upgrade Agent installed. To enable VDA upgrade for it, edit the catalog.
- Machines will be placed in maintenance mode while upgrades are rolled out. Upgrades can take up to 30 minutes to begin.
- If your selection contains machines for which VDA upgrades are not available or whose upgrades are pending (scheduled, in progress, or awaiting upgrades), we will skip upgrades for those machines.

On the **Search** node, you can add the **VDA Upgrade** column. For information about how to add a custom column, see Customize columns to display. The column is useful. It provides VDA upgrade information for the machine. The following information can appear:

- **Available**: A new VDA version is available.
- **Scheduled**: The VDA upgrade has been scheduled.
- **Not configured**: Appears when you have not enabled VDA upgrade for the machine.
- **Up to date**: The VDA is up to date.
- **Unknown**: Information about the VDA upgrade is not yet available.

You can also view the status of the VDA upgrade for a machine. To do that, click the machine and then check the **VDA Upgrade State** information on the **Details** tab. The following information can appear:

- **Unknown**: Unable to get information necessary for VDA upgrade. There are multiple possible reasons:
  - The VDA was in use during the upgrade window.
  - The number of upgrades in progress reached the maximum limit of 500.
  - The VDA Upgrade Agent was unresponsive during the upgrade window. Ensure that the agent is running on the VDA and can communicate with Citrix DaaS.

  - Unable to perform upgrade validation checks. See VDA upgrade requirement.

- **Scheduled**: You have set up an upgrade schedule. For example, if you set the schedule to start at `09:00 PM, December 14, 2030`, information appears as follows: Scheduled for `December 14, 2030 09:00 PM UTC`.
- **Awaiting upgrade**: The machine is placed in maintenance mode, awaiting the upgrade. (Make sure that users have logged out of their session so that the upgrade can proceed.)
- **In progress**: The VDA upgrade has started.
- **Upgrade failed**: Attempts to upgrade the VDA failed.
- **Validation failed**: Attempts to validate VDA upgrade settings failed.
- **Canceled**: The upgrade for the machine has been canceled.
- **Successful**: The VDA was upgraded successfully.

You can also troubleshoot VDA upgrade issues with recommended actions for a machine. To do that, click the machine and then go to the **Troubleshoot** tab.

To quickly drill down to machines that have a specific VDA upgrade state, you can use filters. For more information, see Use Search in the Full Configuration management interface. Be aware of the following considerations:

- The **VDA Upgrade** or **VDA Upgrade State** filter is available for use only with the following filters: **Name** and **Machine Catalog**.
- When you use the **VDA Upgrade** or the **VDA Upgrade State** filter, **Errors** and **Warnings** in the upper right corner become unavailable.

Manage configuration set for a catalog

Before you start, make sure that you have set up your WEM service deployment. For more information, see Get started with Workspace Environment Management service.

> **Note:**
>
> By default, if you have the Cloud Administrator, Full Access Administrator, or Machine Catalog Administrator role, you can manage configuration sets for catalogs. If necessary, you can allow roles to manage configuration sets by granting them the **Manage configuration sets** permission.

Bind a catalog to a configuration set

> **Important:**
>
> If your Citrix DaaS and WEM service instances do not reside in the same region, you cannot bind a catalog to a configuration set. In that case, migrate your WEM service to the same region as Citrix DaaS.

To bind a catalog to a configuration set, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs**.
2. Select the machine catalog and then **Manage configuration set** in the action bar. The **Manage configuration set** window appears.
3. Select a WEM configuration set to which you want to bind the catalog.

   > **Note:**
   >
   > If the selected configuration set does not contain settings relating to the basic configuration of WEM, the **Apply basic settings to configuration set** option appears. We recommend that you select the option to apply basic settings to the configuration set.

4. Click **Save** to save your change.

Switch to a different configuration set

To switch to a different configuration set for a catalog, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs**.
2. Select the machine catalog and then **Manage configuration set** in the action bar. The **Manage configuration set** window appears.
3. Select a different WEM configuration set to which you want to bind the catalog.
4. Click **Save** to save your change.

Unbind a catalog from the configuration set

To unbind a catalog from the configuration set, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs**.
2. Select the machine catalog and then **Manage configuration set** in the action bar. The **Manage configuration set** window appears.
3. Click the X icon on the right-hand side of the selected configuration set.
4. Click **Save** to save your change.

Retry catalog creation

> **Note:**
>
> This feature applies only to MCS catalogs.

Failed catalogs are marked with an error icon. To see the details, go to the **Troubleshoot** tab of each catalog. Before retrying catalog creation, be aware of the following considerations:

- Check the troubleshooting information first and resolve the issues. The information describes the issues found and provides recommendations for resolving them.
- You cannot change settings associated with Operating system and machine management. The catalog inherits those settings from the original.
- The creation can take some time to complete. If necessary, select **Hide progress** to run the creation in the background.

To retry creating a catalog, do the following:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select the catalog and then go to its **Troubleshoot** tab.
3. Click the retry hyperlink to retry creating the catalog.
4. In the wizard that appears, change settings where necessary. If there is no need to make changes, you can go to the **Summary** page directly.
5. After you finish, select **Finish** to start the creation.

(Non-Citrix provisioned VDAs only) Generate and manage enrollment tokens

After you decide to adopt token-based enrollment for non-Citrix provisioned machines, generate tokens on a per-machine catalog basis, and then share them with VDA installation administrators.

An enrollment token features:

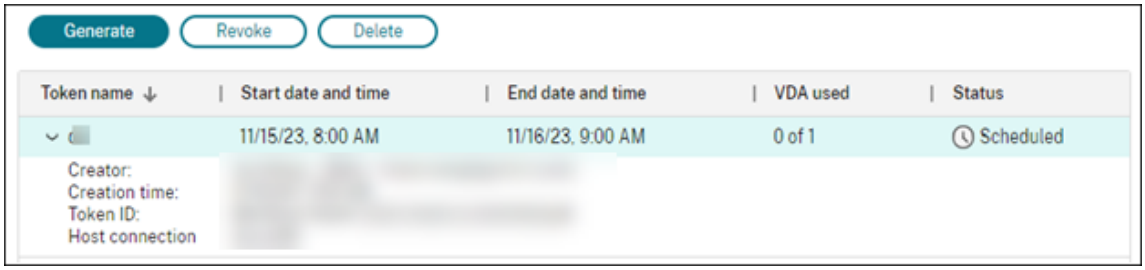
- Registration range: 1 to 100 VDA machines
- Validity period: up to 14 days

To generate a token for a catalog using Full Configuration, follow these steps:

1. In **Full Configuration > Machine Catalogs**, locate a non-MCS-provisioned catalog, which has **Provisioning method: Manual** displayed in the **Machine Count** column.
2. Right-click the catalog, and then select **Manage Enrollment Tokens**.
3. On the **Generate enrollment token** page that appears, provide the following token information:
    - Type a name for the token.
    - Enter its validity period. The period must be no more than 14 days. The token is valid only for the specified period.
    - (Optional) Select a host connection for power management of VDAs enrolled with the token. Options include all host connections under this catalog's zone.
    - Enter the token usage limits (between 1–100).

4. Click **Generate**.
5. In the **Token successfully generated** window that appears, copy the token and save it in a safe place, or click **Download** to download it to the **Downloads** folder.

   A token record appears in the token list.



6. Share the token with VDA installation administrators.

   For more information about how to install VDA and a token on machines, see Install VDAs.

Manage tokens

You have two options to revoke a token and make it unavailable for VDA enrollment:

- Revoke: Revoke the token but retain it in the list for logging purposes.
- Delete: Revoke the token and delete it from the list.

> **Note:**
>
> Expired tokens are automatically deleted in 14 days.

Use PowerShell

This section details how you can manage catalogs using PowerShell:

- Use PowerShell to check VDA upgrade status and VDA version
- Manage the sequence number of the machine name
- Enable one-time restart schedule
- Add descriptions to an image
- Reset OS disk
- Repair the identity information of active computer accounts
- Change the network setting for an existing machine catalog
- Manage versions of a machine catalog
- Change cache configuration of an existing machine catalog
- Convert a non-machine profile-based machine catalog to machine profile-based machine catalog

- Retrieve warnings and errors associated with a catalog
- Delete machines without hypervisor access
- VDA update support via local file share access

Use PowerShell to check VDA upgrade status and VDA version

Use the `Get-VusCatalog` PowerShell command to check the VDA upgrade status. Suppose that the catalog name is `wuhanTestMC1`. You can type the following in the command prompt:

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`

```
PS C:\Users\hanw> Get-VusCatalog -Name  wuhanTestMC1


CancelledUpgrades           : 0
DurationInHours             : 8
FailedUpgrades              : 0
InProgressUpgrades          : 0
LastStateChangeInUtc        : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades       : 100
Name                        : wuhanTestMC1
ProvisioningType            : MCS
ScheduledTimeInUtc          : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades : 0
SessionSupport              : SingleSession
StateId                     : UpgradeSuccessful
SuccessfulUpgrades          : 1
TotalMachines               : 1
Uid                         : 12
UpgradeState                : UpgradeAvailable
UpgradeType                 : CR
UpgradeVersion              : 2112.0.0.32068
Uuid                        : 339e7bce-271b-4c37-9a1c-bce287008b65
```

In this example, `UpgradeState` is `UpgradeAvailable`, meaning that VDA upgrade is enabled for the catalog. `StateId` is `UpgradeSuccessful`, meaning that the catalog has been successfully upgraded to 2112.0.0.32068 (`UpgradeVersion`).

Use the `Get-BrokerMachine` PowerShell command to get the current VDA version.


```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

Use the `Get-VusAvailableVdaVersion` PowerShell command to get the latest VDA version.

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```


Manage the sequence number of the machine name

To customize the sequence number of machines, which are deployed using MCS, through PowerShell commands, do the following:

1. Open Powershell as an administrator on the Delivery Controller.
2. Run the command `asnp citrix*` to load the Citrix modules.
3. Run the following command to check the start count for the identity pool of the catalog:

   ```
   Get-AcctIdentityPool -IdentityPoolName xxx
   <!--NeedCopy-->
   ```

   The `IdentityPoolName` is the name of the catalog.
4. If you want to set this count to a different value, run the following command and specify the StartCount as X:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
   <!--NeedCopy-->
   ```
5. Add the machines to the catalog so that the machines are created with the required count.
6. After creating the machines, run the following command to set it back to the original value Y:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
   <!--NeedCopy-->
   ```

Enable a one-time restart schedule

If you want to enable one-time restart schedule using PowerShell, use the following `BrokerCatalogRebootSch` PowerShell commands to create, modify, and delete a restart schedule:

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

Example:

- To create a restart schedule of the VMs in the catalog named **BankTellers** to begin on Feb 3, 2022, between 2 AM and 4 AM.

  ```
  New-BrokerCatalogRebootSchedule -Name BankTellers
  -CatalogName BankTellers
  -StartDate "2022-02-03"
  ```



```
-StartTime "02:00"
-Enabled $true
-RebootDuration 120
<!--NeedCopy-->
```

- To create a restart schedule of the VMs in the catalog having UID 17 to begin on Feb 3, 2022, between 1 AM and 5 AM. Ten minutes before the restart, each VM is set to display a message box with the title: **WARNING: Reboot pending**, and the message: **Save your work**, in every user session.

```
New-BrokerCatalogRebootSchedule
-Name 'Update reboot'
-CatalogUid 17
-StartDate "2022-02-03"
-StartTime "01:00" -Enabled $true -RebootDuration 240
-WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
<!--NeedCopy-->
```

- To rename the catalog restart the schedule named **Old Name** to **New Name**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
    Name"
<!--NeedCopy-->
```

- To display all catalog restart schedules with UID 1, and then rename the catalog reboot schedule with the UID 1 to **New Name**.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- To set the catalog restart schedule named **Accounting** to display a message with the title **WARNING: Reboot pending, and the message, Save your work**, ten minutes before the restart of each VM. The message appears in every user session on that VM.

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- To display all restart schedules that are disabled, and then enable all disabled restart schedules.

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
   BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- To set the catalog restart schedule with UID 17 to display the message: **Rebooting in %m% minutes** in fifteen, ten, and five minutes before the restart of each VM.


```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
    %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- To configure the time zone for the catalog named **MyCatalog**.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

Add descriptions to an image

You can add informative descriptions about changes related to image updates for machine catalogs. Use this feature to add a description when creating a catalog, or when you update an existing master image for a catalog. You can also display information for each master image in the catalog. This functionality is useful for administrators who want to add descriptive labels when updating a master image used by a catalog, for example, *Office 365 installed*. Use the following commands to add or view image descriptions:

- `NewProvScheme`. A new parameter, `masterImageNote` enables you to add a note to an image. For example:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
    XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
    XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`. Use this parameter to publish the note. For example:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
    MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
    snapshot -MasterImageNote "Visual Studio 2019 installed"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`. Display information for each image. For example:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

```



```
Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed
<!--NeedCopy-->
```

Reset OS disk

Use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. Currently, this feature is applicable to Azure, Google Cloud, SCVMM, VMware, and XenServer virtualization environments.

To successfully run the PowerShell command, make sure that:

- The target VMs are in a persistent MCS catalog.
- The MCS machine catalog is functioning properly. This implies that the provisioning scheme and host exist, and the provisioning scheme has correct entries.
- Hypervisor is not in maintenance mode.
- Target VMs are powered-off and in maintenance mode.

Perform the following steps to reset the OS disk:

1. Open a **PowerShell** window.
2. Run asnp citrix* to load the Citrix-specific PowerShell modules.
3. Run the PowerShell command `Reset-ProvVMDisk` in any one of the following ways:
   - Specify the list of VMs as a comma-separated list, and perform the reset on each VM:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
         ,"def") -OS
     <!--NeedCopy-->
     ```

   - Specify the list of VMs as an output from `Get-ProvVM` command, and perform the reset on each VM:

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
         "abc" -OS
     <!--NeedCopy-->
     ```

   - Specify a single VM by name:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS
     <!--NeedCopy-->
     ```

   - Create separate reset tasks for each of the VMs returned by the `Get-ProvVM` command. This is less efficient because each task will perform the same redundant checks, such as hypervisor capability check, connection check for each VM.


```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. A confirmation prompt appears that lists the VMs to be reset along with a warning message that it is an unrecoverable operation. If you do not provide an answer and press **Enter**, no further action takes place.

   You can run the PowerShell command `-WhatIf` to print the action it would take and exit without performing the action.

   You can also bypass the confirmation prompt using one of the following methods:

   - Provide the `-Force` parameter:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Force
     <!--NeedCopy-->
     ```

   - Provide the `-Confirm:$false` parameter:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Confirm:$false
     <!--NeedCopy-->
     ```

   - Before running the `Reset-ProvVMDisk`, change `$ConfirmPreference` to 'None':

     ```
     PS C:\Windows\system32> $ConfirmPreference='None'
     PS C:\Windows\system32> $ConfirmPreference
     None
     PS C:\Windows\system32> Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -VMName "abc" -OS
     <!--NeedCopy-->
     ```

   > **Note:**
   >
   > Do not take VMs out of the maintenance mode or power them on until the completion of the reset process.

5. Run `Get-ProvTask` to get the status of the tasks returned by `Reset-ProvVMDisk` command.

Repair the identity information of active computer accounts

You can reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent MCS machine catalogs.

> **Note:**
>
> Currently, the feature is supported only for Azure and VMware virtualization environments.

Conditions

Ensure the following to successfully reset the identity disk:

- Turn off and set the VM to maintenance mode
- Do not include the parameter -OS in the PowerShell command

Reset identity information

To reset identity information:

1. Open the **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Reset the identity information.

    - To reset only the machine password and trust keys, run the following commands in the following order:

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
       PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
       $password -Target IdentityInfo
    <!--NeedCopy-->
    ```

    The description of the parameters used in the command are as follows:

    - `IdentityAccountName`: The name of the identity account that must be repaired.
    - `PrivilegedUserName`: User account that has write permission on identity provider (AD or Azure AD).
    - `PrivilegedUserPassword`: Password for PrivilegedUserName.
    - `Target`: Target for the repair action. It can be IdentityInfo to repair account password/trust key, and UserCertificate to repair user certificate attributes of Hybrid Azure AD joined machine identities.

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
       > -Identity -ResetIdentityInfo
    <!--NeedCopy-->
    ```

    `ResetIdentityInfo` parameter resets the following:

    - Password and trust keys: If the VM is AD domain joined (for Citrix DaaS only)

  - Trust keys only: If the VM is not AD domain joined (for Citrix DaaS only)
  - Password only: If the VM is AD domain joined (for Citrix Virtual Apps and Desktops only)

- To reset all configuration of the identity disk, run the following commands in the following order:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
   PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
   $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. Type **y** to confirm the action. You can also skip the confirmation prompt using the `-Force` parameter. For example:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
   Identity -Force
<!--NeedCopy-->
```

5. Run `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` to check the updated identity disk setting. The attributes of the identity disk (for example, `IdentityDiskId`) must be updated. The `StorageId` and `IdentityDiskIndex` must not change.

Change the network setting for an existing machine catalog

You can change the network setting for an existing machine catalog so that the new VMs are created on the new subnetwork. Use the parameter `-NetworkMapping` in the `Set-ProvScheme` command to change the network setting.

To change the network setting for an existing provisioning scheme, do the following:

1. In the PowerShell window, run the command `asnp citrix*` to load the PowerShell modules.
2. Run `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` to get to the network path that you want to change.
3. Assign a variable to the new network setting. For example:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```


4. Run `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Run `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` to verify the new network setting for the existing provisioning scheme.

Manage versions of a machine catalog

When an MCS machine catalog is updated with the `Set-ProvScheme` command, the current configuration is saved as a version. You can then manage the various versions of the machine catalog using PowerShell commands. You can:

- See the list of versions of a machine catalog
- Use any previous version to update the machine catalog
- Manually delete a version if it is not used by a VM of that machine catalog
- Change the maximum number of versions to be retained by the machine catalog (default is 99)

A version includes the following information of a machine catalog:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Run the following commands (provided as examples) to manage the various versions of a machine catalog.

- To see the configuration details of the various versions of a machine catalog:

```
1  Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
2  <!--NeedCopy-->
```

- To see the configuration details of a particular version of a machine catalog:

```
1  Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
       Version 2
2  <!--NeedCopy-->
```

- To see the total number of versions associated with a machine catalog:

  ‘‘‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- To use any previous version to update the machine catalog:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- To manually delete a version if it is not used by a VM of that machine catalog:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 3
```

- To set the maximum number of versions to be retained by the machine catalog (default is 99). This setting is applied across all the catalogs. For example, in this case, a maximum of 15 versions will be retained for all the MCS provisioned catalogs.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
```

If the number of versions reaches the maximum number of versions, then a new version cannot be created if older versions are in use by any of the VMs in the machine catalog. In that case, do one of the following:

- Increase the limit of the maximum number of versions to be retained by the machine catalog.
- Update some VMs that are on older versions so that those older versions are no longer referenced by any VMs, and can be deleted.

Change cache configuration of an existing machine catalog

After creating a non-persistent catalog with MCSIO enabled, you can use the `Set-ProvScheme` command to modify the following parameters:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

This feature is currently applicable to:

- GCP and Microsoft Azure environments, and
- a non-persistent catalog with MCSIO enabled

Requirements

The requirements to modify the cache configuration are:

- Update to the latest version of VDA (2308 or later).
- Enable the parameter `UseWriteBackCache` for the existing machine catalog. Use `New-ProvScheme` to create a machine catalog with `UseWriteBackCache` enabled. For example:


```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
    HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
```

Change the cache configuration

Run the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
```

> **Note:**
>
> - The value of `WriteBackCacheDiskSize` must be more than zero because at least 1 GB of cache disk storage is required.
> - The value of `WriteBackCacheMemorySize` must be less than the machine catalog memory size.
> - These changes only affect new VMs added to the catalog after the change is made. Existing VMs are not affected by these changes.

Convert a non-machine profile-based machine catalog to a machine profile-based machine catalog

You can use a VM, template spec (in case of Azure), or launch template (in case of AWS) as a machine profile input to convert a non-machine profile-based machine catalog to machine profile-based machine catalog. New VMs added to the catalog take property values from the machine profile.

> **Note:**
>
> An existing machine profile-based machine catalog cannot be changed to a non-machine profile-based machine catalog.

To do this:

1. Create a persistent or non-persistent machine catalog with VMs and without a machine profile.
2. Open the **PowerShell** window.

3. Run the `Set-ProvScheme` command to apply the property values from the machine profile to the new VMs added to the machine catalog. For example:

   - In the case of Azure:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
       -MachineProfile XDHyp:\HostingUnits\<HostingUnitName>\
       machineprofile.folder\<ResourceGroupName>\<
       TemplateSpecName>\<VersionName>
   ```

   - In the case of AWS:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
       -MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\<
       launch-template>.launchtemplate\<launch-template-version>.
       launchtemplateversion"
   ```

Retrieve warnings and errors associated with a catalog

You can get historical errors and warnings to understand issues with your MCS machine catalog and fix those issues.

Using PowerShell commands, you can:

- Get a list of errors or warnings
- Change the warning state from **New** to **Acknowledged**
- Delete the errors or warnings

To run the PowerShell commands:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.

To get a list of errors and warnings:

Run `Get-ProvOperationEvent` command.

- With no parameters: Gets all errors and warnings
- With `LinkedObjectType` and `LinkedObjectUid` parameter: Gets all errors and warnings associated with a specific provisioning scheme
- With `EventId` parameter: Gets a specific error or warning that matches this event ID
- With `Filter` parameter: Gets errors or warnings by a customized filter

To change the state of errors or warnings from **New** to **Acknowledged**:

Run `Confirm-ProvOperationEvent` command.

- With `EventId` parameter: Sets the state of a specific error or warning that matches this event ID. You can get the `EventId` of a specific error or warning as an output from `Get-ProvOperationEvent` command
- With `LinkedObjectType` and `LinkedObjectUid` parameters: Sets the state of all the errors and warnings associated with a specific provisioning scheme
- With `All` parameter: Sets the state of all errors and warnings as **Acknowledged**

To delete the errors or warnings:

Run `Remove-ProvOperationEvent` command.

- With `EventId` parameter: Removes a specific error or warning that matches this event ID. You can get the `EventId` of a specific error or warning as an output from `Get-ProvOperationEvent` command
- With `LinkedObjectType` and `LinkedObjectUid` parameters: Removes all errors and warnings associated with a specific provisioning scheme
- With `All` parameter: Removes all errors and warnings

For more information, see Citrix PowerShell SDK.

Delete machines without hypervisor access

When deleting a VM or a provisioning scheme, MCS needs to remove tags from the VM, and sometimes from the base disk as well, so that the resources included in the deletion options are no longer tracked or identified by MCS. However, some of these resources are only accessible through hypervisor. Use the `PurgeDBOnly` option in `Remove-ProvVM` PowerShell to delete VM resource objects such as VM, base disk, image in ACG, and so on from the database even when there is no hypervisor access.

This option is enabled on:

- all supported hypervisors
- persistent and non-persistent VMs

Limitations

You cannot use the commands -PurgeDBOnly and -ForgetVM at the same time.

Use the PurgeDBOnly command

When running the PowerShell command `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` the deletion operation might fail in the following scenarios:

- The host connection is in maintenance mode
- Invalid credentials
- Authentication failure
- Unauthorized operation
- The hypervisor is unreachable

> **Note:**
>
> Remove-provVM -ForgetVM targets only persistent VMs. If one of the VMs in the list is non-persistent, the operation fails.

When the operation fails because the hypervisor is unreachable, the following prompt appears:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Use the `-PurgeDBOnly` option in the `Remove-ProvVM` PowerShell command to delete references of a VM from MCS database. For example,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

VDA Update Support via Local File Share Access (Tech Preview)

Specify the VDA installer location through PowerShell cmdlets which reduces your effort from providing network rules to allow each VDA to go and fetch the new VDA installer from the Citrix Managed Azure CDN.

PowerShell cmdlets

Two new optional parameters added to **New-VusCatalogSchedule** and **New-VusMachineUpgrade** cmdlets that allow you to use installers from a local file share

- **VdaWorkstationPackageUri** - to specify the UNC path to the workstation OS VDA installer
- **VdaServerPackageUri** - to specify the UNC path to the server OS VDA installer

Prerequisites

- VDA Upgrade Agent to version 7.40.0.35 or later (using the VDA installer version 2311 or later)
- Virtual Apps and Desktops Remote PowerShell SDK version 7.40 or newer (released on Jan 10, 2024 or later)
- Remote PowerShell SDK version 7.42 or later (released after Feb 16, 2024)

How to Set File Share Permissions

The network shares containing VDA installer packages must have read access for the VDA Upgrade Agent service which runs as Local System (NT AUTHORITY\SYSTEM principal).

- **Domain-Joined file share permission**

  When the VDA machine is domain-joined, then the **Local System** account (VUA runs as Local System), uses computer credentials when accessing network shares.

  The least privilege permission can be set by granting the **Read** access to Domain Computers.

  1. Choose people on your network who you want to share the file with.
  2. Click **Advanced Sharing Settings** and turn on **File and Printer Sharing**.

- **Non-Domain Joined file share permission**

  When the VDA machine is non-domain joined, then the **Local System** account (VUA runs as Local System), uses **ANONYMOUS LOGON** when accessing network shares.

  1. Select a shared folder.
  2. Disable the password protection.
     a) Go to Folder **Properties**.
     b) Select **Network and Sharing Center**.
     c) Turn off **Password Protected Sharing**.
  3. Click **Advanced Sharing** to grant a share permission.
     a) Select **Permissions**.
     b) Grant a **Read** share permission to **ANONYMOUS LOGON**.
  4. Select the **Security Tab** to grant folder permissions
     a) Click **Edit** to add permissions to the shared folder
     b) Select the shared folder to grant folder permissions to **ANONYMOUS LOGON**.
  5. Click **Advanced** to turn on **File and Printer Sharing**.
  6. Add the shared folder name to **Network Access Security Policy**.

  > **Note:**
  >
  > Restart your machine for the change to take effect immediately.

VDA Updates from a Local File Share

1. Download the VDA installer and place it in the shared file.

> **Note:**
>
> With Virtual Upgrade Service, you can select from either the Current Release track or the LTSR track.
>
> **For Example:** If the machine catalog is set to Current Release that is 2311, and the VDA version is 2305, you must upgrade the VDA to version 2311.

a) Navigate to the **Downloads** page on our website.
b) Select **Citrix Virtual Apps and Desktops** as the product.
c) Select **Citrix Virtual Apps and Desktops 7 2311, All Editions**.
d) Select the VDA installer from the **Components that are on product ISO but also packaged separately** expandable.

2. Select the relevant VDA installer based on the catalog type.

   - Download the **Multi-session OS VDA installer** if the catalog type is **multi session**
   - Download the **Single-session OS VDA installer** if the catalog type is **single session**
   - Download the **Single-session OS Core Services VDA installer** if the catalog type is **Remote PC Access**

> **Note:**
>
> The version of the file share installer has to **exactly** match the version of the latest installer version published by VUS to the cloud.

Troubleshoot

- For machines with `Power State Unknown` status, see CTX131267 for guidance.
- To fix VMs that continuously show an unknown power state, see How to fix VMs that continuously show an unknown power state.
- If a Cloud Connector is not operating properly, MCS provisioning operations (such as catalog updates) take longer than usual and the management console performance degrades significantly.

Where to go next

For information on managing specific hypervisor catalogs, see:

- Manage an AWS catalog
- Manage a Google Cloud Platform catalog
- Manage a Microsoft Azure catalog
- Manage a Microsoft System Center Virtual Machine Manager catalog

- Manage a VMware catalog
- Manage a XenServer catalog

‘‘

Manage an AWS catalog

December 11, 2023

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to AWS cloud environments.

> **Note:**
>
> Before managing an AWS catalog, you need to finish creating an AWS catalog. See Create an AWS catalog.

Remove tags

When you create a catalog or a VM, tags are created on the following resources:

- Virtual machine
- Root disk volume
- Identity disk volume
- Elastic network interface (ENI)
- Root disk image (AMI)
- Launch template
- Snapshot of AMI or root disk

You can remove VMs and machine catalogs from Citrix database and remove Citrix-created tags. You can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and Citrix-created tags from a single VM or a list of VMs from a machine catalog.

  > **Note:**
  >
  > With the `ForgetVM` parameter, the VMs are removed from the Citrix's provisioning scheme database, however, the VMs continue to remain in the hypervisor.

- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and resources from a machine catalog.

To do this:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Unlock the VM before removing the VMs. For example:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
<!--NeedCopy-->
```

4. Run one of the following commands to remove VMs, machine catalog, and Citrix-created tags from resources.

   - Run `Remove-ProvVM` with `ForgetVM` to remove VMs from Citrix database and Citrix-created tags from VMs. For example:

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
    >" -ForgetVM
<!--NeedCopy-->
```

   - Run `Remove-ProvScheme` to remove machine catalog from Citrix database and resources from a machine catalog. For example:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
    ForgetVM
<!--NeedCopy-->
```

5. Verify that the VM is removed from the Delivery Controller, but, not from the hypervisor.

   a) Run `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"`. This must return nothing.

   b) Go to AWS EC2 console. You must see the VMs, however, the Citrix-created tags are now removed. Citrix-created tags from the following resources are removed:

      - Virtual machine
      - Root disk volume
      - Identity disk volume
      - ENI

6. If you remove the machine catalog, verify that the catalog is removed from the Delivery Controller.

   a) Run `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. This must return an error.

   b) Verify in AWS EC2 console that the following resources are removed.

      - Root disk image (AMI)

- Launch template
- Snapshot of AMI or root disk

Identify resources created by MCS

Following are the tags that MCS adds to the resources on AWS platform. The tags in the table are represented as "key":"value".

Resource name	Tag
ID disk	"Name": "VMName_IdentityDisk" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Image	"XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"Description": "XD Nic" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"Name": "VMName_rootDisk" "XdConfig": "XdProvisioned=True" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true] "Citrix Resource": "" [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"Name": "Preparation - CatalogName - xxxxxxxxxx" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true] "Citrix Resource": ""

Resource name	Tag
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
Published snapshot	“XdConfig”: “XdProvisioned=true”
	If not a snapshot for Volume Worker AMI, then “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Template	[when AwsCaptureInstanceProperties = true] “XdConfig”: “XdProvisioned=true”
	[when AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
	[when AwsCaptureInstanceProperties = true] “CitrixResource”: “”
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
VM in catalog	“XdConfig”: “XdProvisioned=true”
	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
	[when AwsCaptureInstanceProperties = true] “CitrixResource”: “”
	[when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx”
	[when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n”
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
Volume worker AMI	“XdConfig”: “XdProvisioned=true”
Volume worker bootstraper	“Name”: “XenDesktop Temp”
	“XdConfig”: “XdProvisioned=true”
	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

Resource name	Tag
Volume worker instance	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “” “Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true”

More information

- Create and manage connections and resources
- Connection to AWS
- Create machine catalogs
- Create an AWS catalog
- Manage machine catalogs

Manage a Google Cloud Platform catalog

February 1, 2024

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Google cloud environments.

> **Note:**
>
> Before managing a Google Cloud Platform catalog, you need to finish creating a Google Cloud Platform catalog. See Create a Google Cloud Platform catalog.

Add machines to a catalog

To add machines to a catalog, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select the machine catalog to which you want to add machines.
3. Select **Add Machines** in the action bar.
4. On the **Virtual Machines** page, specify the number of machines you want to add and then select **Next**.

5. On the **Machine Identities** page, select an Active Directory account and then select **Next**.
6. On the **Domain Credentials** page, select **Enter credentials**, type the user name and password, select **Save**, and then select **Next**.
7. On the **Summary** page, confirm the information and then select **Finish**.

Update machines

This feature can be useful in cases where you want to update your master image or the minimum functional level.

To update machines, follow these steps:

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select the machine catalog that contains machines you want to update.
3. Select **Change Master Image** in the action bar.
4. On the **Image** page, select a VM and the minimum functional level for the catalog and then select **Next**.
5. On the **Rollout Strategy** page, specify when you want to update the machines and then select **Next**.
6. On the **Summary** page, confirm the information and then select **Finish**.

Roll back a machine update

To roll back a machine update, follow these steps:

> **Important:**
>
> Do not rename, delete, or move master images. Otherwise you cannot roll back the update.

1. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
2. Select the machine catalog where you want to roll back the machine update.
3. Select **Roll Back Master Image** in the action bar.
4. On the **Overview** page, confirm the information and then select **Next**.
5. On the **Rollout Strategy** page, configure the rollout strategy and then select **Next**.
6. On the **Summary** page, confirm the information and then select **Finish**.

Power management

Citrix DaaS lets you do the power management of Google Cloud machines. Use the **Search** node in the navigation pane to locate the machine you want to power manage. The following power actions are available:

- Delete
- Start
- Restart
- Force Restart
- Shut Down
- Force Shutdown
- Add to Delivery Group
- Manage Tags
- Turn On Maintenance Mode

You can also power manage Google Cloud machines by using Autoscale. To do so, add the Google Cloud machines to a Delivery Group and then enable Autoscale for that Delivery Group. For more information about Autoscale, see Autoscale.

Update provisioned machines using PowerShell

The `Set-ProvScheme` command changes the provisioning scheme. However, it does not affect existing machines. Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can now apply the current provisioning scheme to an existing persistent or non-persistent machine or set of machines. Currently, in GCP, the property updates supported by this feature are Machine profile, Service offering and Custom catalog settings.

You can update:

- A single VM
- A list of specific VMs or all existing VMs associated with a provisioning scheme ID
- A list of specific VMs or all existing VMs associated with a provisioning scheme name

To update the existing VMs:

1. Check the configuration of the existing machines. For example,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Update the provisioning scheme. For example,

   - Updating machine profile

```
`Set-ProvScheme  –ProvisioningSchemeName "my-catalog"  –
    MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

   - Updating service offering


```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering " XDHyp:\HostingUnits\<hosting-unit>\
    serviceoffering.folder\<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Check if the current property of the VM matches the current provisioning scheme, and if there is any pending update action on the VM. For example,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

You can also find machines with a particular version. For example,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Update existing machines.

- To update all the existing machines:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- To update a list of specific machines:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
<!--NeedCopy-->
```

- To update machines based on the output of `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Note:**
>
> - `StartsNow` indicates that the scheduled start time is the current time.
> - `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

5. Find machines with an update scheduled. For example,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
```



```
<!--NeedCopy-->
```

6. Restart the machines. At the next power-up, property changes are applied to the existing machines. You can check the updated status using the following command:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

Change disk related custom properties of an existing catalog

You can change the following disk related custom properties of an existing catalog and existing VMs of the catalog:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Note:**
>
> - `StorageType` property is for OS disk
> - `PersistOsDisk` property can be set only for non-persistent catalog with write-back cache enabled

This implementation helps you to select different storage types for different disks even after you create a catalog and thus, balances pricing associated with different storage types.

To do this, use PowerShell commands `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow`:

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
3. Run `Get-ProvVM -VMName <VM name>` to get the custom properties.
4. Change the custom properties string:
   a) Copy the custom properties to a Notepad and change the custom properties.
   b) In the **PowerShell** window, paste the modified custom properties from Notepad and assign a variable to the modified custom properties. For example:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
```



```
<Property xsi:type="StringProperty" Name="CatalogZones" Value
    ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
    true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
    ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Update the existing catalog. For example:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
    CustomProperties $cp
<!--NeedCopy-->
```

6. Update the existing VMs. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Restart the VMs. At the next power up, custom property changes are applied to the existing VMs.

Protect accidental machine deletion

Citrix DaaS lets you protect MCS resources on the Google Cloud to prevent accidental deletion. Configure the provisioned VM by setting the `deletionProtection` flag to TRUE.

By default, VMs provisioned through MCS or Google Cloud plug-in are created with InstanceProtection enabled. The implementation is applicable to both persistent and non-persistent catalogs. The non-persistent catalogs are updated when the instances get re-created from the template. For existing persistent machines, you can set the flag in the Google Cloud console. For more information about setting the flag, see the Google Documentation site. New machines added to persistent catalogs are created with `deletionProtection` enabled.

If you attempt to delete a VM instance for which you have set the `deletionProtection` flag, the request fails. However, if you are granted the permission `compute.instances.setDeletionProtection` or assigned the IAM **Compute Admin** role, you can reset the flag to allow the resource to be deleted.

Identify resources created by MCS

Following are the tags that MCS adds to the resources on GCP platform. The tags in the table are represented as "key":"value".

Resource name	Tag
ID disk	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Image	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Preparation VM	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Published snapshot	"CitrixResource": "internal"
Storage bucket	"CitrixResource": "internal"
Template	"CitrixResource": "internal"
VM in catalog	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". The plug-in also adds this label for MCS provisioned VMs: "citrix-provisioning-scheme-id": "provSchemeId". You can use this label to filter by catalog in the GCP console.
WBC disk	"CitrixResource": "internal" CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

> **Note:**
>
> A VM is not visible in the Citrix inventory if a **CitrixResource** tag is added to identify it as a resource

> created by MCS. You can remove or rename the tag to make it visible.

More information

- Create and manage connections and resources
- Connection to Google cloud environments
- Create machine catalogs
- Create a Google Cloud Platform catalog
- Manage machine catalogs

Manage an HPE Moonshot catalog

April 16, 2024

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to HPE Moonshot catalog.

> **Note:**
>
> Before managing a HPE Moonshot catalog, you need to finish creating a HPE Moonshot catalog. See Create an HPE Moonshot machine catalog.

Power management

Citrix DaaS lets you do power management of HPE Moonshot machines. Use the **Search** node in the navigation pane to locate the machine you want to power manage. The following power actions are available:

- Start
- Shut Down
- Force Shutdown
- Restart
- Reset

> **Note:**
>
> **Suspend** and **Resume** power actions are not supported.

More information

- Create and manage connections and resources
- Connection to HPE Moonshot
- Create machine catalogs
- Create an HPE Moonshot machine catalog
- Manage machine catalogs

Manage a Microsoft Azure catalog

April 16, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Microsoft Azure Resource Manager cloud environments.

> **Note:**
>
> Before managing a Microsoft Azure catalog, you need to finish creating a Microsoft Azure catalog. See Create a Microsoft Azure catalog.

Change the storage type to a lower tier when a VM is shut down

You can save storage costs by switching the storage type of a managed disk to a lower tier when you shut down a VM. To do this, use the `StorageTypeAtShutdown` custom property.

The storage type of the disk changes to a lower tier (as specified in the `StorageTypeAtShutdown` custom property) when you shut down the VM. After you power on the VM, the storage type changes back to the original (as specified in `StorageType` custom property or `WBCDiskStorageType` custom property).

> **Important:**
>
> - The disk does not exist until the VM is powered on at least once. Therefore, you cannot change the storage type when you first power on the VM.
> - A VM might take a little longer to start after you change the storage type to a lower tier.

Requirements

- Applicable to a managed disk. This implies that you set the custom property `UseManagedDisks` to true.
- Applicable to a persistent and non-persistent catalog with a persistent OS disk. This implies that you set the custom property `persistOsDisk` to true.
- Applicable to a non-persistent catalog with a persistent WBC disk. This implies that you set the custom property `persistWBC` to true.

Restriction

- As per Microsoft, you can only change the disk type twice per day. See the Microsoft document. As per Citrix, the `StorageType` update happens whenever there is a Start or Deallocate action for the VM. Therefore, limit the number of power actions per VM to twice per day. For example, one power action in the morning to start the VM and one in the evening to deallocate the VM.

Change the storage type to a lower tier

Before proceeding with the steps, see the Requirements and Restrictions.

1. Add the custom property `StorageTypeAtShutdown`, set the value to Standard_LRS (HDD), and create a catalog using `New-ProvScheme`. For information on creating a catalog using PowerShell, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Note:**
   >
   > If `StorageTypeAtShutdown` has any value other than empty or Standard_LRS (HDD), the operation fails.

   Example of setting custom properties while creating a persistent catalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS “  />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```



```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> '
<!--NeedCopy-->
```

Example of setting custom properties while creating a non-persistent catalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.
    com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
    Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
    />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> '
<!--NeedCopy-->
```

> **Note:**
>
> When you use a machine profile, the custom property takes precendence over the property defined in `MachineProfile`.

2. Shut down the VM and check the storage type of the VM in Azure portal. The storage type of the disk changes to a lower tier, as specified in the `StorageTypeAtShutdown` custom property.
3. Turn on the VM. The storage type of the disk switches back to the storage type mentioned in:
   - `StorageType` custom property for OS disk
   - `WBCDiskStorageType` custom property for WBC disk only if you specify it in `CustomProperties`. Otherwise, it switches back to the storage type mentioned in `StorageType`.

Apply `StorageTypeAtShutdown` to an existing catalog

Before proceeding with the steps, see the Requirements and Restrictions.

Use `Set-ProvScheme` to apply `StorageTypeAtShutdown` to the new VMs added to an existing catalog.

Example of setting custom properties while adding a VM to an existing catalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties> '

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

Change the storage type of existing VMs to a lower tier on shutdown

Before proceeding with the steps, see the Requirements and Restrictions.

You can save storage costs by changing the storage type of existing VMs to a lower tier when the VMs are shut down.

To change the Storage type of existing machines in a catalog to a lower tier when the VMs are shut down:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `Get-Provscheme -ProvisioningSchemeName $CatalogName`.

4. Change the custom properties string.

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Update the provisioning scheme of the existing catalog. The update applies to new VMs added after running `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Update the existing VMs to enable `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. When you power on the machines next time, the `StorageTypeAtShutdown` property of the machines is updated. The storage type changes at the next shutdown.

8. Run the following command to view the `StorageTypeAtShutdown` value for each VM in a catalog.

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
       ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

Update provisioned machines to current provisioning scheme state

The `Set-ProvScheme` command changes the provisioning scheme. However, it does not affect existing machines. Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can apply the current provisioning scheme to an existing persistent or non-persistent machine or set of machines. You can also schedule a time slot for the configuration updates of the existing MCS provisioned machines. Any power on or restart during the scheduled time slot applies a scheduled provisioning scheme update to a machine. Currently, in Azure, you can update `ServiceOffering`,

`MachineProfile` and the following custom properties:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Note:**
>
> - You can only update `StorageType`, `WBCDiskStorageType`, and `IdentityDiskStorageType` custom properties for a catalog using managed disk in Azure environments.
> - If you run `Set-ProvVMUpdateTimeWindow` twice, then the most recent command takes effect.

You can update:

- A single VM
- A list of specific VMs or all existing VMs associated with a provisioning scheme ID
- A list of specific VMs or all existing VMs associated with a provisioning scheme name (machine catalog name)

After you make the following changes to the provisioning scheme, VM instance gets recreated for persistent catalogs in Azure:

- Change the `MachineProfile`
- Remove `LicenseType`
- Remove `DedicatedHostGroupId`

> **Note:**
>
> The OS disk of existing machines along with all its data remains as is and a new VM is attached to the disk.

Before updating the existing VMs:

1. Check the configuration of the existing machines. For example,

```
1 Get-ProvScheme | select ProvisioningSchemeName,
     ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

2. Update the provisioning scheme. For example,

- With VM as a machine profile input:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\
    machineprofile.folder\<resource-group>.resourcegroup\<
    virtual-machine>.vm"
<!--NeedCopy-->
```

- With template spec as a machine profile input:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\
    machineprofile.folder\<resource-group>.resourcegroup\<
    template-spec>.templatespec\<template-spec-version>.
    templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits\<hosting-unit>\
    serviceoffering.folder\<service-offering>.serviceoffering"
<!--NeedCopy-->
```

- With just service offering:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits\<hosting-unit>\
    serviceoffering.folder\<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Check if the current property of the VM matches the current provisioning scheme, and if there is any pending update action on the VM. For example,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

You can also find machines with a particular version. For example,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

To request updates for existing machines to apply at the next restart:

1. Run the following commands to update existing machines and have the updates apply at the next restart.

- To update all the existing machines. For example,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- To update a list of specific machines. For example,


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

- To update machines based on the output of Get-ProvVM. For example,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Note:**
>
> - `StartsNow` indicates that the scheduled start time is the current time.
> - `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

2. Find machines with an update scheduled. For example,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Restart the machines. At the next power up, property changes are applied to the existing machines. You can check the updated status using the following command. For example,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

To schedule a VM to update to the latest provisioning settings next time it starts in the scheduled time window:

1. Run the following commands:

   - To schedule an update with start time as the current time:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

   - To schedule an update on a weekend:

```
 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName " my-
    catalog " -VMName " vm1 " -StartTimeInUTC " 10/15/2022
    9:00am " -DurationInMinutes (New - TimeSpan - Days 2).
    TotalMinutes
<!--NeedCopy-->
```


> **Note:**
>
> - `VMName` is optional. If not specified, the update is scheduled for the entire catalog.
> - Instead of `StartTimeInUTC`, use `StartsNow` to indicate that the schedule start time is the current time.
> - `DurationInMinutes` is optional. Default is 120 minutes. A negative number (for example, –1) indicates no upper bound on schedule's time window.

2. Check the update status.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Power on the VM. If you power on the machine after the scheduled time slot, configuration update is not applied. If you power on the machine within the scheduled time slot,

   - If the machine is powered off, and
     - you do not power on the machine, configuration update is not applied
     - you power on the machine, configuration update is applied
   - If the machine is powered on, and
     - you do not restart the machine, configuration update is not applied
     - you restart the machine, configuration update is applied

To cancel the configuration update:

You can also cancel a configuration update of a single VM, multiple VMs, or an entire catalog. To cancel a configuration update:

1. Run `Clear-ProvVMUpdateTimeWindow`. For example:

   - To cancel the configuration update scheduled for a single VM:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName " my-
    catalog " -VMName " vm1 "
<!--NeedCopy-->
```

   - To cancel the configuration update scheduled for multiple VMs:

```
 Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
     catalog" -VMName "vm1","vm2"
<!--NeedCopy-->
```

> **Note:**
>
> The VMs must be from the same catalog.

Update properties of individual VMs

You can update properties of individual VMs in a persistent MCS machine catalog using the PowerShell command `Set-ProvVM`. However, the updates are not applied immediately. You must set the time window using the PowerShell command `Set-ProvVMUpdateTimeWindow` for the updates to apply.

This implementation helps you to manage individual VMs efficiently without updating the entire machine catalog. Currently, this feature is applicable only to the Azure environment.

Currently, the properties that you can update are:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Using this feature, you can:

- Update the properties of a VM
- Retain the properties updated on a VM after the machine catalog is updated
- Revert the configuration updates applied to a VM

Before updating properties of a VM:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Check the configuration of the existing machine catalog. For example:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Check the configuration of the VM on which you want to apply the updates. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Update properties of a VM

Do the following to update the properties on a VM:

1. Turn off the VM on which you want to apply the updates.
2. Update the properties of the VM. For example, if you want to update storage type (`StorageType`) custom property of the VM, run the following:


```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

You can update properties of two VMs in a machine catalog simultaneously. For example:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

> **Note:**
>
> The updates are not applied immediately.

3. Get the list of properties that are specified to be updated and the configuration version. For example:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

Check the property value of `Version` and the properties to be updated (in this case, `StorageType`).

4. Check the configuration version. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Check the property value of `ProvVMConfigurationVersion`. The update is not yet applied. The VM is still in the old configuration.

5. Request scheduled update. For example:

```
 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
 <!--NeedCopy-->
```

For more information on scheduled updates, see Update provisioned machines to current provisioning scheme state.

> **Note:**
>
> Any pending provisioning scheme update is also applied.

6. Restart the VM. For example:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Check the configuration version. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Check the property value of `ProvVMConfigurationVersion`. The update is now applied. The VM now has the new configuration.

8. To apply further configuration updates on the VM, turn off the VM, and repeat the steps.

Retain the properties updated on a VM after the machine catalog is updated

Do the following to retain the properties updated on a VM:

1. Turn off the VM on which you want to apply the updates.
2. Update the machine catalog. For example, if you want to change the VM size (`ServiceOffering`) and storage type (`StorageType`), run the following:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. Get the configuration details of the machine catalog. For example:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

   The `ProvisioningSchemeVersion` is now incremented by one. The VM size and storage type are also updated.

4. Update the properties of the VM. For example, provide a machine profile to the VM.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\
    machineprofile.folder\<resource-group>.resourcegroup\<template-
    spec>.templatespec\<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```


> **Note:**
>
> The machine profile input has a tag and a different VM size (`ServiceOffering`) specified.

5. Get the list of properties that the VM will have after merging the configuration updates on the VM with the machine catalog updates. For example:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Note:**
>
> Any updates on the VM will override the updates done on the machine catalog.

6. Request scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Restart the VM. For example:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

   The VM keeps its updated VM size as derived from the machine profile. The tag values as specified in the machine profile are also applied to the VM. However, the storage type is derived from the latest provisioning scheme.

8. Get the configuration version of the VM. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   The `ProvisioningSchemeVersion` and `ProvVMConfigurationVersion` now shows the latest version.

Revert the configuration updates applied to a VM

1. After applying the updates to a VM, turn off the VM.
2. Run the following command to remove the updates that are applied on the VM. For example:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```


3. Request scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Restart the VM. For example:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Check the configuration version of the VM. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   The `ProvVMConfigurationVersion` value is now the configuration version of the machine catalog.

Change disk encryption

You can change the disk encryption in Azure virtualization environments and do the following:

- Create an MCS machine catalog with disk encryption set (DES) that is different from the master image DES using the `New-ProvScheme` command. For example:

```
$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
    subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/
    testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-
    diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
<!--NeedCopy-->
```

- Change the disk encryption type from one DES key to another DES key of an existing MCS machine catalog and existing VMs using `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow` commands. After you restart the VMs, you can see the updated DES key. For example:


```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Update an MCS machine catalog and VM that was not previously CMEK enabled to have customer-managed encryption key (CMEK) encryption (DES), disk encryption at host, or double encryption using `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow` commands. For information on different encryption types, see Azure server side encryption, Azure disk encryption at host, and Double encryption on managed disk.
- Update an existing MCS machine catalog and VMs to be non-encrypted that was previously encrypted using `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow` commands. For example:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Enable disk encryption with private endpoint (an MCS machine catalog that used a host connection enabled with `ProxyHypervisorTrafficThroughConnector`). For more information on `ProxyHypervisorTrafficThroughConnector`, see Create a secure environment for Azure-managed traffic. For information on how to enable disk encryption with private endpoints, see Enable disk encryption with private endpoint.

Enable disk encryption with private endpoint

As per the Azure limitation, currently, you can't have server-side encryption with customer-managed keys for private endpoints. However, you can update an existing MCS machine catalog and VMs with private endpoints to be encrypted with the DES key.

Update an existing machine catalog with private endpoints The detailed steps to update an existing machine catalog with private endpoints are as follows:

1. Create a catalog without disk encryption through `ProxyHypervisorTrafficThroughConnector`. For more information on `ProxyHypervisorTrafficThroughConnector`, see Create a secure environment for Azure-managed traffic.
2. Run `Set-ProvScheme` to update the catalog with `DiskEncryptionSetId`.

   > **Note:**
   >
   > `DiskEcryptionSetId` can be configured through `CustomProperties` or `MachineProfile`. When it is defined in both `CustomProperties` and `MachineProfile`, the properties defined in `CustomProperties` are applied.

   Example when using `CustomProperties`:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1"/>
   </CustomProperties>'
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

   Example when using MachineProfile: Use a VM that has disk encryption enabled or a template spec with disk encryption settings:

   ```
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
       folder\testrg.resourcegroup\new-template.vm"
   <!--NeedCopy-->
   ```

   Alternatively, you can update a machine profile using the Full Configuration interface.
3. Run `Set-ProvVMUpdateTimeWindow` to update existing catalog VMs. For example:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
       VMName azu01, azu02 -StartsNow -DurationInMinutes -1
   <!--NeedCopy-->
   ```
4. After you restart the VMs, you can see the updated disk encryption on the VM's disks in Azure portal.
5. Run `Set-ProvScheme` to unset the disk encryption before adding new catalog VMs.

> **Note:**
>
> This step is required because you are updating a private endpoint catalog. If you do not do this step, then you will get errors while trying to add new VMs to the catalog.

For example:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Add new VMs to the catalog.

Update individual catalog VMs The detailed steps to update individual catalog VMs are as follows:

1. Create a catalog without disk encryption through `ProxyHypervisorTrafficThroughConnector`. For more information on `ProxyHypervisorTrafficThroughConnector`, see Create a secure environment for Azure-managed traffic.
2. Run `Set-ProvVM` to update catalog VM with `DiskEncryptionSetId`.

> **Note:**
>
> The `DiskEcryptionSetId` can be configured through either `CustomProperties` or `MachineProfile`.

Example when using `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1" />
</CustomProperties>'
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    CustomProperties $customProperties
<!--NeedCopy-->
```

Example when using MachineProfile:


```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
<!--NeedCopy-->
```

3. Run `Set-ProvVMUpdateTimeWindow` to update existing catalog VMs. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. After you restart the VMs, you can see the updated disk encryption on the VMs disks in Azure portal.
5. Add new VMs to the catalog.

Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition

You can display information for an Azure VM, including OS disk and type, snapshot and gallery image definition. This information is displayed for resources on the master image when a machine catalog is assigned. Use this functionality to view and select either a Linux or Windows image. A PowerShell property, `TemplateIsWindowsTemplate`, was added to the `AdditionDatafield` parameter. This field contains Azure-specific information: VM type, OS disk, gallery image information, and OS type information. Setting `TemplateIsWindowsTemplate` to **True** indicates that the OS type is Windows; setting `TemplateIsWindowsTemplate` to **False** indicates that the OS type is Linux.

> **Tip:**
>
> Information displayed by the `TemplateIsWindowsTemplate` PowerShell property is derived from the Azure API. Sometimes, this field might be empty. For example, a snapshot from a data disk does not contain the `TemplateIsWindowsTemplate` field because the OS type cannot be retrieved from a snapshot.

For example, set the Azure VM `AdditionData` parameter to **True** for Windows OS type using PowerShell:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
```



```
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM templates

You can display region name information for an Azure VM, managed disks, snapshots, Azure VHD, and ARM templates. This information is displayed for the resources on the master image when a machine catalog is assigned. A PowerShell property called `RegionName` displays the region name information when you run the PowerShell command with the `AdditionalData` parameter.

For example, use the following PowerShell command to get a VM information in Azure.

```
PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).
    AdditionalData
Key Value
HardDiskSizeGB 127
ResourceGroupName HU-DEV-TESTING-RG
RegionName East US
TemplateIsWindowsTemplate True
LicenseType
ServiceOfferingDescription Standard_B2ms
ServiceOfferingMemory 8192
ServiceOfferingCores 2
SupportedMachineGenerations Gen1,Gen2
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SecurityType
SecureBootEnabled
VTpmEnabled
<!--NeedCopy-->
```

Identify resources created by MCS

Following are the tags that MCS adds to the resources on Azure platform. The tags in the table are represented as “key”:”value”.

Resource name	Tag
ID disk	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Image	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

Resource name	Tag
	“CitrixResource”: “Internal”
NIC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
OS disk	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Preparartion VM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Published snapshot	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Resource group	“CitrixResource”: “Internal” CitrixSchemaVersion: 2.0 “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Storage account	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
WBC disk	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”

> **Note:**
>
> A VM is not visible in the Citrix inventory if a **CitrixResource** tag is added to identify it as a resource created by MCS. You can remove or rename the tag to make it visible.

Remove tags

When you create a catalog or a VM, tags are created on the following resources:

- Resource group
- Virtual machine
- OS disk
- Identity disk
- Network interface
- Storage account

You can remove VMs and machine catalogs from Citrix database and remove tags. You can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and tags from a single VM or a list of VMs from a machine catalog.
- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and tags from an entire machine catalog.

This feature is only applicable to persistent VMs.

To do this:

1. Open a **PowerShell** window.
2. Run **asnp citrix*** to load the Citrix-specific PowerShell modules.
3. Run `Remove-ProvVM` to delete VMs from Citrix database and tags from VMs.
   For example:

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
<!--NeedCopy-->
```

4. Run `Remove-ProvScheme` to delete machine catalog from Citrix database and tags from machine catalogs. For example:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
<!--NeedCopy-->
```

> **Note:**
>
> After you use `ForgetVM` parameter in `Remove-ProvScheme`, MCS deletes all snapshots including base disk snapshot if the provisioning scheme is present in either bring your own resource group (BYORG) or Citrix managed resource group.

More information

- Create and manage connections and resources
- Connection to Microsoft Azure
- Create machine catalogs

- Create a Microsoft Azure catalog
- Manage machine catalogs

Manage a Microsoft System Center Virtual Machine Manager catalog

December 11, 2023

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Microsoft System Center Virtual Machine Manager (VMM) virtualization environments.

> **Note:**
>
> Before managing a VMM catalog, you need to finish creating a VMM catalog. See Create a Microsoft System Center Virtual Machine Manager catalog.

Identify resources created by MCS

Following are the tags that MCS adds to the resources on SCVMM platform. The tags in the table are represented as "key":"value".

Resource name	Tag
Preparation VM	Tag string: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" Custom property entry: "XdConfig:" XdProvisioned=True"
VM in catalog	Tag string: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" Custom property entry: "XdConfig:" XdProvisioned=True"

More information

- Create and manage connections and resources
- Connection to Microsoft System Center Virtual Machine Manager
- Create machine catalogs
- Create a Microsoft System Center Virtual Machine Manager catalog
- Manage machine catalogs

Manage a VMware catalog

May 9, 2024

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to VMware virtualization environments.

> **Note:**
>
> Before managing a VMware catalog, you need to finish creating a VMware catalog. See Create a VMware catalog.

Update the folder ID of a machine catalog

You can update the folder ID of an MCS machine catalog by specifying the `FolderId` in the custom properties of `Set-ProvScheme` command. The VMs created after updating the folder ID are created under this new folder ID. If this property is not specified in `CustomProperties`, then VMs are created under the folder where the master image is located.

Perform the following steps to update the folder ID of a machine catalog.

1. Open a Web browser and enter the URL for the **vSphere Web Client**.
2. Enter the credentials and click **Login**.
3. Create a VM placement folder in **vSphere Web Client**.
4. Open a PowerShell window.
5. Run **asnp citrix*** to load the Citrix-specific PowerShell modules.
6. Specify the `FolderID` in the `CustomProperties` of `Set-ProvScheme`. In this example, the folder ID value is `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
2 <!--NeedCopy-->
```

7. Add a VM to the machine catalog using Studio.
8. Check the new VM on vSphere Web Client. The new VM is created under the new folder.

Find the folder ID using PowerShell commands

Use the Powershell command `Get-HypConfigurationDataForItem` to find the folder ID for an existing folder in a VMware Hypervisor.

Create a hosting connection and resource group for a VMware Hypervisor. Then, perform the following steps to find the folder ID of a folder on that hypervisor.

1. Determine the `XDHyp` path to the root of the vm folder tree. For example:

```
XDHyp:\Connections\VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

2. Use `Get-HypConfigurationDataForItem` to retrieve the tree structure. For example:

```
Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\
    VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

3. Run the following command to identify the folder ID from the output XML. In this example, look for the folder ID of `ExampleFolder` in the XML output.

```
$result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:\
    Connections\VMwareConn\Datacenter.datacenter
$result.VmPlacementFolder
<!--NeedCopy-->
```

XML output:

```
<?xml version="1.0" encoding="utf-16"?>
<CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Name>vm</Name>
<Id>group-v4</Id>
<SubFolder>
<CtxVmPlacementFolder>
  <Name>vCLS</Name>
  <Id>group-v75</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>MyOtherFolder</Name>
  <Id>group-v1110</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>ExampleFolder</Name>
  <Id>group-v4658</Id>
  <SubFolder />
</CtxVmPlacementFolder>
</SubFolder>
</CtxVmPlacementFolder>
```



```
<!--NeedCopy-->
```

Find the folder ID in vSphere

Access the MOB on any ESXi or vCenter server system to find the folder ID of the VMs.

The Managed Object Browser (MOB) is a web-based server application available inbuilt in all ESX/ESXi and vCenter server systems. This vSphere utility allows you to view detailed information about objects like VMs, datastores, and resource pools.

1. Open a web browser and enter `http://x.x.x.x/mob`, where x.x.x.x is the IP address of the vCenter Server or ESX/ESXi host. For example, https://10.60.4.70/mob.
2. On the **Home** page of MOB, click the value of the property **content**.
3. Click the value of the **rootFolder**.
4. Click the value of the **childEntity**.
5. Click the value of the **vmFolder**.
6. You can find the folder ID in the value of the **childEntity**.

Storage migration of VMs

You can move the disk storage of existing VMs from an old storage to a new storage. During migration, MCS retains the VM capabilities such as power management, reset OS disk, and so on. You can also add new VMs to the machine catalog using the new disk storage. To do this, use the PowerShell command `Move-ProvVMDisk`.

Currently, you can only migrate full clone persistent VMs.

The new storage must satisfy the following conditions:

- It must be within the same cluster of the old storage.
- The host on which the VM is running must have access to both the old and new datastores.

You can do the following tasks:

- Migrate the disk storage
- Deprecate the old storage

Migrate the disk storage

To migrate the disk storage:

1. Add a new storage to an existing hosting unit. Change the old storage to **Superseded**. You can do this using the Full Configuration interface or PowerShell commands.

- If using the Full Configuration interface, see Edit storage.
- If using PowerShell commands:
  - Run `Add-Hyphostingunitstorage` to add the new storage to the existing hosting unit.
  - Run `Set-Hyphostingunitstorage` with **Superseded** as true to disable new VM creation in the old storage.

2. Turn off the VMs and turn on the **Maintenance Mode**.
3. Move disk storage of the VMs to the new storage and update the storage information. For example:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

4. Get the task ID of the migration. For example:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

5. Check the status of the migration.

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: Provides the list of VMs with successful disk migration, including the VMs that are already migrated to the new storage.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines` : Provides the list of VMs with failed migration.
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: Provides the list of VMs whose migration has not yet started.
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: Provides the updated VM properties after the migration. Check the properties such as `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage`, and `LastBootTime`.

After migrating the disks of MCS created VMs with snapshot, you might see the warning **Consolidation is required in the VSphere Client**. To consolidate and avoid data loss:

1. Take a VMware VM backup. For example, transfer all VM files into another folder on a datastore.
2. After you see the warning, click **Consolidate**, and then click **OK** to confirm the consolidation.

Deprecate the old storage

To deprecate the old storage after VMs disk migration:

1. Get the information about the base disks and machine count in each disk storage of the hosting unit. For example:

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
       xxxxx
   $result
   $result.ProvResourceInStorage | Format-List -Property *
   <!--NeedCopy-->
   ```

   After a successful migration, MCS automatically removes the stale base disk and there are no machines in the old storage. Therefore, after running the command, make sure that there are no machines and base disk in the old storage.

2. Run `Remove-Hyphostingunitstorage` to entirely remove the old storage from the hosting unit. You can also use the Full Configuration interface to remove the old storage.

Identify resources created by MCS

Following are the tags that MCS adds to the resources on VMware platform. The tags in the table are represented as "key":"value".

Resource name	Tag
Preparation VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True"
VM in catalog	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True"

More information

- Create and manage connections and resources
- Connection to VMware
- Create machine catalogs
- Create a VMware catalog
- Manage machine catalogs

Manage a XenServer catalog

December 12, 2023

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to XenServer virtualization environments.

> **Note:**
>
> Before managing a XenServer catalog, you need to finish creating a XenServer catalog. See Create a XenServer catalog.

Identify resources created by MCS

When the Machine Creation Services (MCS) generates resources like disks, it assigns a ProvisioningScheme ID tag for better utilization of those resources.

Tags are helpful to administrators as they can better manage and organize the resources. For example, if resources, like unused disks, are tagged, then administrators can easily identify where the resource is created, making the cleanup process efficient.

Following are the tags that MCS adds to the resources on XenServer platform. The tags in the table are represented as "key":"value".

Resource name	Tag
Copy of disk on each network or local storage (on-prem only)	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ID disk	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Preparation VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM in catalog	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBC disk	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Retrieve information about provisioning scheme

To retrieve detailed information about the provisioning scheme, you can execute the following PowerShell commands. Replace `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx` with the actual Provisioning Scheme ID:

1. Replace the placeholder ID with your actual Provisioning Scheme ID

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Retrieve detailed information about the provisioning scheme:

```
Get-ProvisioningScheme -Id $provisioningSchemeId
<!--NeedCopy-->
```

Retrieve list of resources created by MCS

Run the following commnds to get a comprehensive list of resources created by MCS.

1. Replace the placeholder ID with your actual Provisioning Scheme ID.

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Retrieve the entire list of resources created by MCS.

```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
   ConvertTo-JSON -Depth 6
<!--NeedCopy-->
```

   After execution, you get the following output:

   - The name and ID of the provisioning scheme.
   - A list of provisioning image versions within the provisioning scheme. Each entry includes:
     - The image name and ID.
     - The Disk ID and Storage ID of the disk.
   - A list of provisioning VMs. Each entry includes:
     - The OS disk ID and parent disk ID of the OS disk .
     - The Storage ID of the OS disk.
     - The Identity disk and its Storage ID.

More information

- Create and manage connections and resources

- Connection to XenServer
- Create machine catalogs
- Create a XenServer catalog
- Manage machine catalogs

Power Management

November 8, 2023

With Citrix DaaS, you can power manage MCS-provisioned VMs across various supported hypervisors and cloud services. The power management operation provides you:

- Optimal user experience
- Cost management and power savings

The power actions available are:

- Start
- Shut down
- Restart
- Suspend
- Resume
- Force restart
- Force shutdown

> **Note:**
>
> - For a non-persistent VM, power cycle (shutdown/start and restart) results in OS disk getting reset.
> - Power action capabilities and behaviors vary depending on hypervisors or cloud services.

The article covers key power management features associated with certain supported hypervisors.

- Power manage AWS VMs
- Power manage Azure VMs

Power manage AWS VMs

April 24, 2024

For information on required permissions, see About AWS permissions.

Instance Hibernation

The hibernation process stores the in-memory state of the instance, along with its private, and elastic IP addresses, allowing it to pick up exactly where it left off.

When an instance is instructed to hibernate, it writes the in-memory state to a file in the root EBS volume, and then shuts itself down. An Amazon EBS volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive. Encrypt the root EBS volume of the instance. The encryption ensures proper protection for sensitive data when it is copied from memory to the EBS volume. For information on EBS encryption, see Amazon EBS encryption.

Following are the limitations of the supported instance hibernation:

- Instance memory (RAM) of only up to 150 GB is supported
- UEFI boot mode is not supported
- The General Purpose SSD and Provisioned IOPS SSD are only supported as EBS volume types.

Create hibernation supported VMs

To create hibernation supported VMs:

1. Create a host connection. See Connection to AWS.
2. Launch an instance with EBS root encrypted and the **Stop-Hibernate** property enabled. For more information, see:
   - Instance lifecycle
   - Amazon EBS encryption
   - Hibernation prerequisites
   - Enable hibernation for an instance
   - Hibernate your On-Demand Instance or Spot Instance
3. Use this instance as a master image to create an AMI.
4. Prepare the master image:
   a) Install a VDA on the master image. Citrix recommends installing the latest version to allow access to the newest features. Failure to install a VDA on the master image causes the catalog creation to fail. For more information on how to install a VDA, see Install VDAs.
   b) Join the master image to the domain where applications and desktops are members. Ensure that the master image is available on the host where the machines are created.
5. Create an AMI from that instance. For information on creating an AMI from an instance, see Create an AMI from an Amazon EC2 Instance.

6. Create a machine catalog using `New-ProvScheme` command. Set the `AwsCaptureInstancePropert` custom property as **True**. For information on enabling AWS instance properties in the Full configuration interface, see Applying AWS instance properties and tagging operational resources in the Full Configuration interface.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

   For information on creating machine catalog using PowerShell commands, see https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

VMs that can be hibernated are created if:

- You select an AMI created from a master image that has the **Stop-Hibernate** property enabled.
- The master VM is domain joined and has the VDA installed.
- You select the correct VM size (service offering) that can handle hibernation.

The **New-ProvScheme** command fails with an appropriate error message if:

- The master VM is hibernation enabled but the service offering is not capable of handling hibernation.
- If the master VM is not domain joined and has no VDA installed.

Hibernation status of service offerings and AMI

To get the hibernation status of the service offerings and AMI (templates), run the following commands:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

Update service offering of an existing hibernation supported provisioning scheme

1. Run the `Set-ProvScheme` command. For example,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
    String>
<!--NeedCopy-->
```

The system displays an exception message if the service offering is not compatible.

Create machine catalog with hibernation support

When creating machine catalogs, you can use a machine profile that supports hibernation.

1. In the catalog creation wizard, follow the instructions till the selection of the machine profile.
2. On the **Machine Template** page, click **Select a machine profile** and select a machine profile.
3. On the **Virtual Machine** page, click the **Edit** icon and select a VM.

> **Note:**
>
> If the machine profile is hibernation enabled, the system displays only those VMs that can be hibernated.

4. Follow the onscreen instructions to complete all settings. The **Summary** page displays the hibernation status of the catalog.

> **Note:**
>
> In the edit machine catalog, when you change the machine profile to a hibernation-enabled one, you are be asked to reconfigure your VMs accordingly.

Update machine catalog that supports hibernation

If you try to update an existing machine catalog with a machine catalog that does not support hibernation, the update fails with an appropriate error message.

Power management of hibernated VMs

You can do the following power management operations on the hibernated VMs:

1. Suspend the VM from the running state.
2. Resume VM from the suspended state.
3. Restart VM from the suspended state.

To see the power management options, in the **Manage > Full Configuration** interface, right-click the hibernated VMs.

You can also see the power state as **Suspending** and **Suspended** for each VM as per the power operations you perform on the VMs.

Power manage Azure VMs

June 6, 2024

For information on required permissions, see Required Azure permissions.

Azure on-demand provisioning

With Azure on-demand provisioning, VMs are created only when Citrix DaaS initiates a power-on action, after the provisioning completes.

When you use MCS to create machine catalogs in the Azure Resource Manager, the Azure on-demand provisioning feature:

- Reduces your storage costs
- Provides faster catalog creation

When you create an MCS catalog, the Azure portal displays the network security groups, network interfaces, base images, and identity disks in the resource groups.

The Azure portal does not show a VM until Citrix DaaS initiates a power-on action for it. Then, the VM's status in the Full Configuration interface changes to **On**. There are two types of machines with the following differences:

- For a pooled machine, the operating system disk and write-back cache exist only when the VM exists. When you shut down a pooled machine in the console, the VM is not visible in the Azure portal. There's a significant storage cost saving if you routinely shut down machines (for example, outside of working hours).
- For a dedicated machine, the operating system disk is created the first time the VM is powered on. The VM in the Azure portal remains in storage until the machine identity is deleted. When you shut down a dedicated machine in the console, the VM is still visible in the Azure portal.

> **Note:**
>
> Support for Azure catalogs created before the on-demand provisioning feature ("legacy"catalogs) is deprecated. Therefore, recreate the Azure legacy catalog VMs. The catalogs are then

> provisioned as on-demand that saves storage cost.

Preserving a provisioned virtual machine when power cycling

Choose whether to preserve a provisioned virtual machine when power cycling. Use the PowerShell parameter `New-ProvScheme CustomProperties`. This parameter supports an extra property, `PersistVm`, used to determine if a provisioned virtual machine persists when power cycled. Set the `PersistVm` property to **true** to persist a virtual machine when powered off, or set the property to **false** to ensure that the virtual machine is not preserved when powered off.

> **Note:**
>
> The `PersistVm` property only applies to a provisioning scheme with the properties `CleanOnBoot` and `UseWriteBackCache` enabled. If the `PersistVm` property is not specified for non-persistent virtual machines, they're deleted from the Azure environment when powered off.

In the following example, the `New-ProvScheme CustomProperties` parameter sets the `PersistVm`property to **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
   resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

In the following example, the `New-ProvScheme CustomProperties` parameter preserves the write-back cache by setting `PersistVM` to **true**:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
```



```
        StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
        Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
        false`" /><Property xsi:type=`"StringProperty`" Name=`"
        PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
        StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
        type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
        resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
        LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
5   -HostingUnitName "demo"
6   -IdentityPoolName "NonPersistent-MCSIO-PersistVM"
7   -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
        resourcegroup\demo-snapshot.snapshot"
8   -NetworkMapping @ {
9   "0"="XDHyp:\HostingUnits\demo\\virtualprivatecloud.folder\East US.
        region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
        .virtualprivatecloud\default.network" }
10
11  -ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
12   -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
        Standard_B2ms.serviceoffering" -UseWriteBackCache
13   -WriteBackCacheDiskSize 127
14   -WriteBackCacheMemorySize 256
15   <!--NeedCopy-->
```

> **Tip:**
>
> The `PersistVm` property determines whether to preserve a provisioned virtual machine. The `PersistOsdisk` property determines whether to persist the OS disk. To preserve a provisioned virtual machine, preserve the OS disk first. You cannot delete the OS disk without first deleting the virtual machine. You can use the `PersistOsdisk` property without using specifying the `PersistVm` parameter.

Customize power on behavior at storage type change failure

At power on, the storage type of a managed disk can fail to change to the desired type due to a failure on Azure. In these scenarios, the VM would remain off with a failure message sent to you. However, you can either choose to power on the VM even when storage cannot be restored to its configured type or choose to keep the VM powered off.

- If you configure the custom property `FailSafeStorageType` as **true** (default setting) or do not specify it in `New-ProvScheme` or `Set-ProvScheme` commands:
  - On power on, the VM powers on with the incorrect storage type.
  - On shutdown, the VM remains off with the incorrect storage type.
- If you configure the custom property `FailSafeStorageType` as **false** in `New-ProvScheme` or `Set-ProvScheme` commands:

- On power on, the VM remains off with the incorrect storage type.
- On shutdown, the VM remains off with the incorrect storage type.

To create a machine catalog to include `FailSafeStorageType` custom property:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create an identity pool if not already created.
4. Add the custom property in `New-ProvScheme`. For example:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
     Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Create the machine catalog. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

To update an existing machine catalog so to include `FailSafeStorageType` custom property. This update does not affect existing VMs.

1. Update the custom property in `Set-ProvScheme` command. For example:

```
    Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
    <CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
        machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
        instance`">
    <Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
        Premium_LRS`" />
```



```
    <Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
        `" Value=`"Premium_LRS`" />
    <Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
        Value=`"false`" />
    </CustomProperties>"
    <!--NeedCopy-->
```

To apply the change done in Set-ProvScheme to the existing VMs, run the `Request-ProvVMUpdate` command.

1. Run the Request-ProvVMUpdate command. For example:

```
Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
    List-Of-Vm-Names>
<!--NeedCopy-->
```

2. Restart the VMs.

Create hibernation-capable VMs

In Azure environments, you can create an MCS machine catalog that supports hibernation. Using this feature, you can suspend a VM, and then reconnect to the previous state of the VM when a user signs in again.

The hibernation capability applies to the following:

- Single-session OS
- Persistent and non-persistent VMs
- Static and random (pooled) VDI desktops

You can resume to the same session after you hibernate a VM, irrespective of whether the VDI desktop is static or random.

In this section, see the following:

- Prerequisites
- Limitations
- Create and manage a hibernation-capable machine catalog
- Create a machine catalog for existing hibernation-capable VMs
- Enable hibernation on existing MCS-provisioned VMs
- Check the hibernation property
- Power management of VMs (Manual and Automated)

Prerequisites to use hibernation

To use hibernation, make sure to complete the following tasks:

- Install the Azure VM Agent on the master image for both Windows and Linux. The page file of the Windows image can be on the temporary disk. MCS sets the page file location to the C: drive in the base disk when hibernation is enabled on the machine catalog.
- MCS automatically sets the hibernation property for the generated resources. You do not need to configure properties of the master resources to support hibernation.
- Use a VM size in your subscription that supports hibernation.
- Create a hibernation-capable machine profile (VM or template spec) so that VMs inherit the hibernation-capability. To create the VM, see Getting started with hibernation.

  > **Note:**
  >
  > As per Microsoft, you can deploy hibernation enabled VMs from an OS disk. This feature is supported for certain regions currently and will be available for all the regions soon. For more information, see Deploy hibernation enabled VMs from an OS disk.

  To create the template spec, do the following:

  1. Open the Azure Portal. Choose a VM whose configuration you want to use in the template. Select **Export template** in the left pane.
  2. Clear the **Include parameters** checkbox. Copy the context and save it as a JSON file, for example, `VMExportTemplate.json`.
  3. Ensure that the parameter `hibernationEnabled` is **`true`** on the template. If the parameter is not **`true`**, check the VM configuration that you used. You can specify a supported VM size in the template file. However, you can also specify the machine size while creating the catalog.
  4. Add the template for the network interface resource to the JSON file `VMExportTemplate.json`. As a result, you have an ARM template file having two resources.
  5. Select **Azure Portal > Template specs > Import template > Choose local template file** to import this template file as an ARM template spec.
  6. After the ARM Template specification is created, you can use it as a machine profile.

  > **Note:**
  >
  > It might take a few minutes to sync to Citrix Studio.

For more information, see the Microsoft document Prerequisites to use hibernation.

Limitations

- Only single-session OS machine catalogs (persistent and non-persistent) are supported.
- Ephemeral OS disks and MCS I/O features do not support Azure hibernation.

- Hibernation might fail during the Automatic Windows updates.

For more information, see the Microsoft document.

Create and manage a hibernation-capable machine catalog

To create hibernation-capable VMs, you can create and manage a hibernation-capable machine catalog using:

- Full Configuration interface, or
- PowerShell commands

Create a catalog using the Full Configuration interface

1. Sign in to Citrix Cloud. In the upper left menu, select **My Services > DaaS**.
2. From **Manage > Full Configuration**, select **Machine Catalogs** in the left pane.
3. Select **Create Machine Catalog**. The catalog creation wizard opens.
4. On the **Machine Type** page, select the **Single-session OS** machine type for this catalog.
5. On the **Machine Management** page, select the settings as follows:
   a) Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
   b) Select **Citrix Machine Creation Services (MCS)**.
6. On the **Desktop Experience** page, select the random or static desktop experience as needed.
7. On the **Image** page, select a master image. Select the checkbox **Use a machine profile** and select a machine profile that supports hibernation. Click the tooltip to know if a machine profile supports hibernation.
8. On the **Storage and License Types** page, select the storage and license to use for this catalog.
9. On the **Virtual Machines** page, select the count of VMs, VM size, and availability zone.

   > **Note:**
   >
   > The machine sizes that support hibernation are only shown for your selection. The GPU VM series are in preview.

10. On the **NICs** page, add the NICs you want the VMs to use.
11. On the **Disk Settings** page, select the storage type and size of the write-back cache disk.
12. On the **Resource Group** page, select the resource group to provision VMs.

13. On the **Machine Identities** page, select **Create new Active Directory accounts**. Then, specify an account naming scheme.
14. On the **Domain Credentials** page, click **Enter credentials**. Enter your domain credentials to perform account creation in the target Active Directory domain.
15. On the **Summary** page, enter a name for the machine catalog, and then click **Finish**.

When the MCS machine catalog creation is complete, locate the catalog in the catalog list, and then click the **Template Properties** tab. The value of the parameter **Hibernation** must be **Supported**.

If you want to edit a machine catalog, consider the following restrictions:

- If the current machine catalog supports hibernation, you can't:
  - Change the VM size to a hibernate-incapable one.
  - Change the machine profile to a hibernate-incapable one.
- If the current machine catalog does not support hibernation, you can't:
  - currently, change the machine profile to a hibernate-capable one using the Full Configuration interface. However, you can do so using the PowerShell commands. See Enable hibernation on existing MCS-provisioned VMs.

Create a machine catalog for managing existing hibernation-capable VMs If you already have hibernation-capable VMs and want to suspend and resume them, create a machine catalog to import those VMs for power management.

> **Note:**
>
> You can create a machine catalog containing both hibernation-capable and incapable VMs. However, if you want hibernation-related functionality, you must create the machine catalog with only hibernation-capable VMs.

To create a catalog for existing hibernation-capable VMs using the Full Configuration interface, follow the on-screen instructions to complete the steps and pay attention to the following key settings:

1. On the **Machine Management** page, select **Machines that are power managed**, and then select **Other service or technology** as the way of deploying machines.
2. On the **Virtual Machines** page, add or import only the hibernation-capable VMs.

Create a machine catalog using PowerShell commands After you meet all the requirements to use hibernation, you can create a hibernation-capable machine catalog using the `New-ProvScheme` command. For information on how to create a catalog using the Remote PowerShell SDK, see Manage Citrix DaaS using Remote PowerShell SDKs.

While creating the catalog, you can check whether a VM size and machine profile supports hibernation or not using the following PowerShell commands:

- For the VM size, run the following command and check whether the property `supportsHibernation` is **True**. For example,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
    VirtualNetwork> \serviceoffering.folder") | select Name,
    AdditionalData | ConvertTo-Json
<!--NeedCopy-->
```

- For the machine profile, run the following command and check whether the property `supportsHibernation` is **True**. For example,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
    VirtualNetwork> \machineprofile.folder\abc.resourcegroup")|
    select Name, AdditionalData|ConvertTo-Json
<!--NeedCopy-->
```

If you want to edit a machine catalog, consider the following restrictions:

- If the current machine catalog supports hibernation, you can't:
  - Change the VM size to a hibernate-incapable one
  - Change the machine profile to a hibernate-incapable one
- If the current machine catalog does not support hibernation, you can't:
  - currently, change the machine profile to a hibernate-capable one using the Full Configuration interface. However, you can do so using the PowerShell commands. See Enable hibernation on existing MCS-provisioned VMs.

For information on how to modify VM size and machine profile of a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Enable hibernation on existing MCS-provisioned VMs

You can enable Azure hibernation on existing:

- Windows MCS-provisioned VMs of a machine catalog created without a temporary disk.
- Linux MCS-provisioned VMs of a machine catalog created with and without a temporary disk.

> **Note:**

> - The existing MCS-provisioned VMs must have an Azure VM agent installed.
> - Currently, you can only use the PowerShell command to enable this feature.

To do this:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load Citrix-specific PowerShell modules.
3. Check the configuration of the existing machines. For example:

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Enable hibernation on this machine catalog using the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
   folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. Request update on existing VMs in a machine catalog.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
   String[]
<!--NeedCopy-->
```

6. Restart the VMs to trigger updates on the existing VMs. For example:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

Check hibernation property

You can check the hibernation property of a machine catalog, VM, and a broker machine using the PowerShell commands:

- To check the hibernation property of a provisioning scheme, run the following PowerShell commands. The `HibernationEnabled` parameter must be `True`.

```
  (Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
     VMMetadata -join "" |  ConvertFrom-Json | Select
     HibernationEnabled
  <!--NeedCopy-->
```

- To check the hibernation property of a provisioning VM, run the following PowerShell commands. The `SupportsHibernation` parameter must be `True`.


```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- To check the hibernation capacity of a broker machine, run the following PowerShell commands. The **Suspend** and **Resume** power actions indicate hibernation capability.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

Power management of hibernation-capable VMs

You can perform the following power management operations on the hibernation-capable VMs:

- **Suspend** VM from the running state
- **Resume** VM from the suspended state
- **Force shut** down VM from a suspended state
- **Force restart** the VM from the suspended state

See the following for more information:

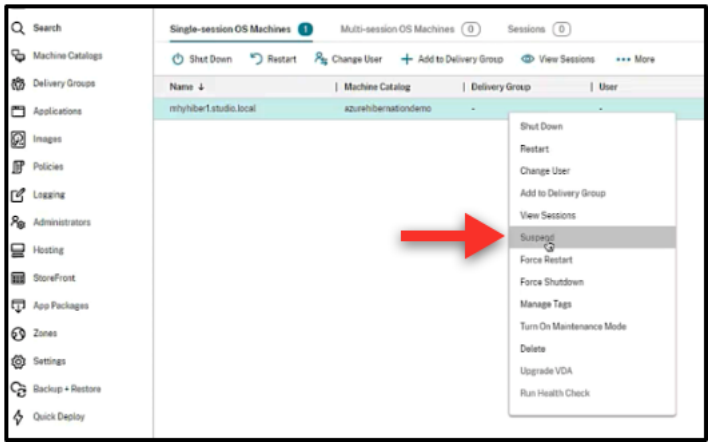
- Suspend
- Resume

Suspend You can suspend a VM using one of the following ways:

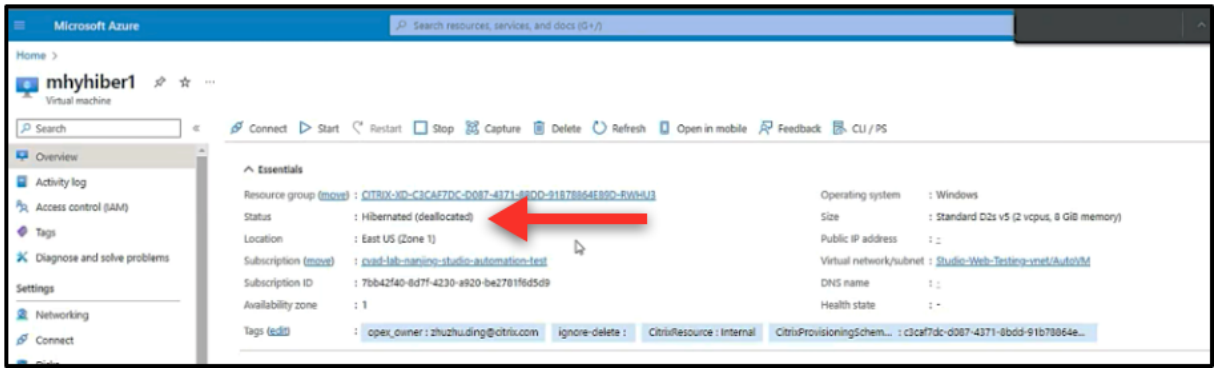
- **Manually** using the Full Configuration interface
- **Automatically** using the timeout policy: For more information, see Miscellaneous settings.

To manually suspend a VM:

1. Right-click the VM, and select **Suspend**. Click **Yes** to confirm the action. The **Power State** changes from **Suspending** to **Suspended**.

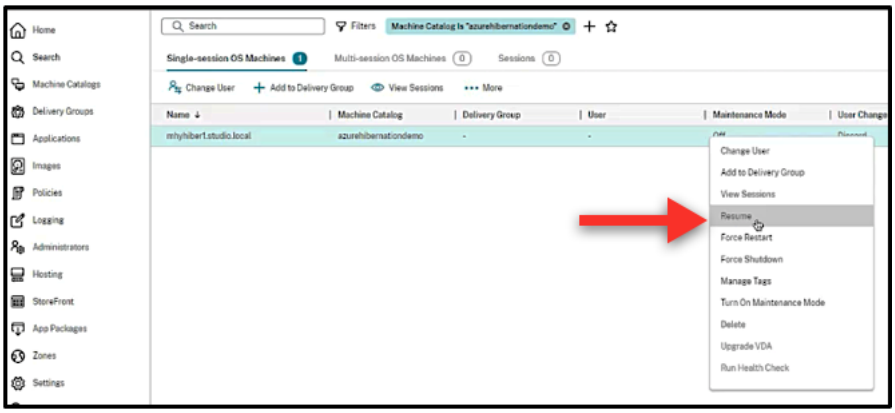


You can check the status of the VM in the Azure portal.

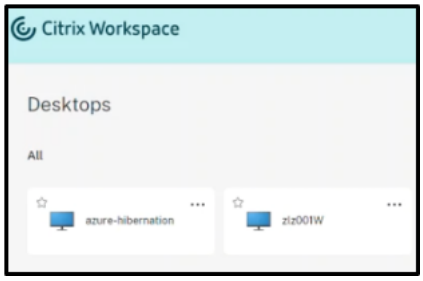


Resume To resume a hibernated VM, use one of the following ways:

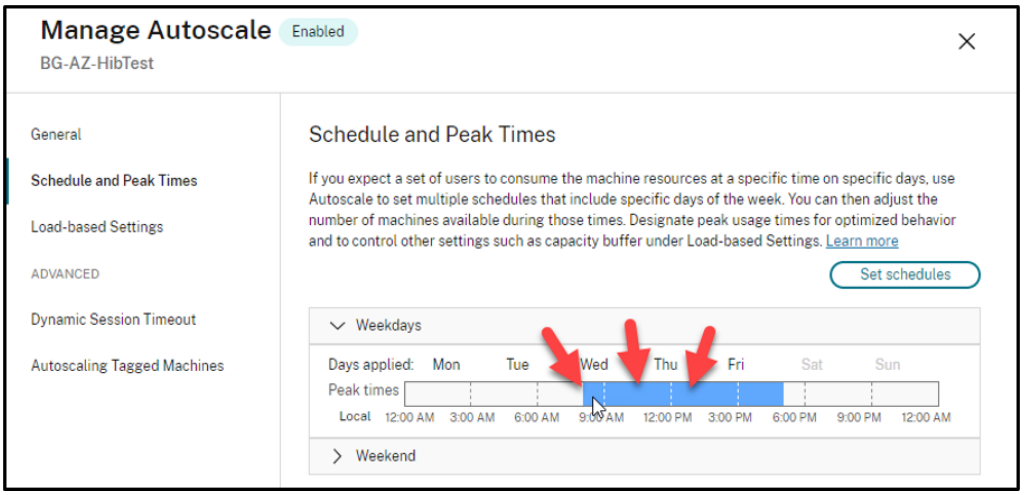
- **Manually**:
  - Administrators can resume the VM using the Full Configuration interface.



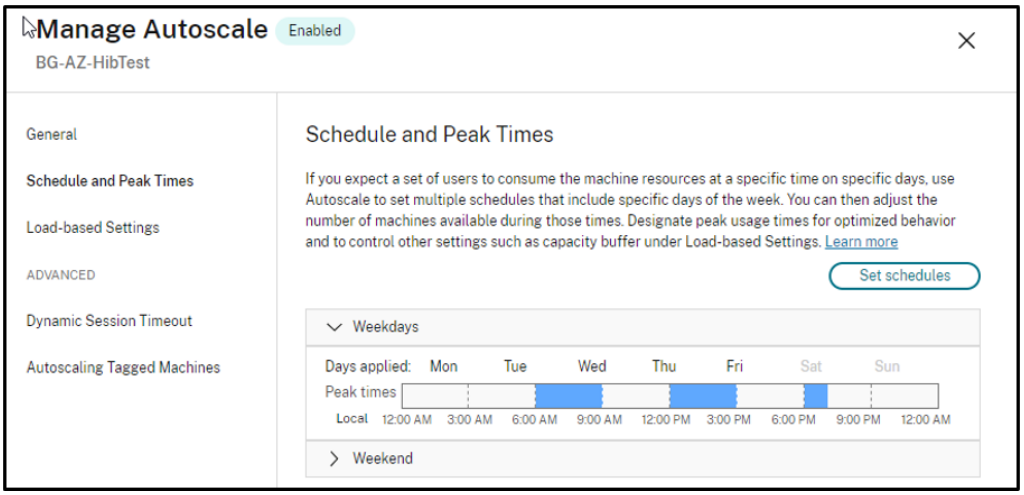
  - End users can start the VM using the Citrix Workspace menu once they click the desktop icon.



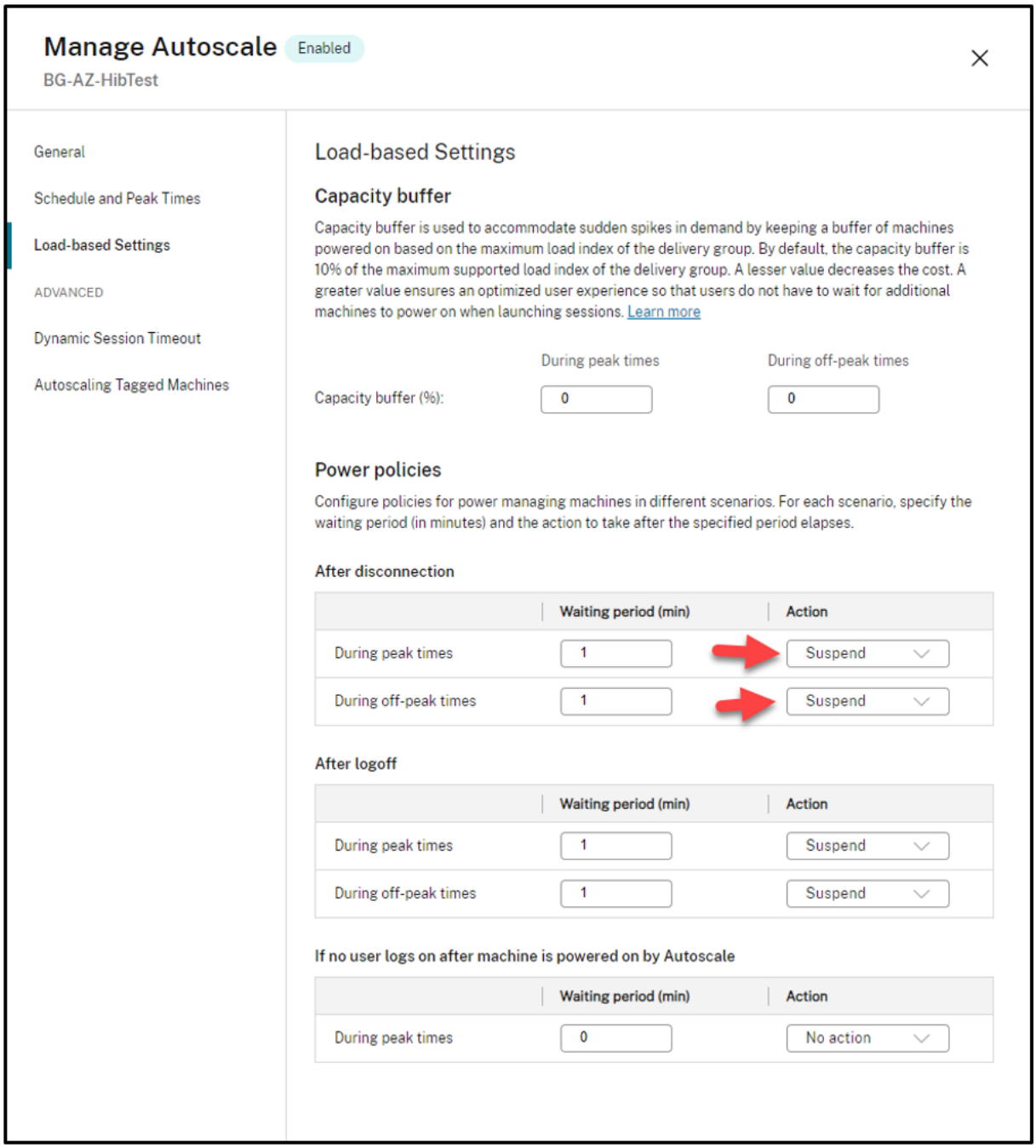
- **Automatically**:
  - Autoscale can automatically power on the hibernated machines if you configure the peak times correctly. You can set the peak times in 30-minutes intervals by clicking the time-schedule. Each blue frame represents a timeslot marked as peak time. The peak times can have consecutive and non-consecutive time slots.
    - Consecutive time slots



    - Non-consecutive time slots



> **Note:**
>
> In **Manage Autoscale > Load-based Settings**, if the **Action** is configured as **Suspend**, then make sure that all VMs within that delivery group have hibernation capability. Otherwise, VMs that can't hibernate continues to run.



More information

For more information on Citrix Azure hibernation, see the Citrix Tech Zone article.

Security policies

March 31, 2023

This article describes security features on various supported hypervisors. The security features include:

- Security group
- Secure boot
- Encryption capabilities

Security group

March 31, 2023

Security group is a group of security rules to filter network traffic between resources in a virtual network. The security rules allow or deny inbound network traffic to, or outbound network traffic from, several types of resources. Each rule specifies the following properties:

- Name: A unique name within the network security group
- Priority: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority
- Source or Destination: Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group
- Protocol: The protocols based on which you add rules for each security group
- Direction: Whether the rule applies to inbound, or outbound traffic
- Port range: You can specify an individual or range of ports
- Action: Allow or deny

See the following for more information on supported hypervisors:

- Security group in AWS
- Security group in Microsoft Azure
- Security group in Google Cloud Platform

Security group in AWS

Security groups act as virtual firewalls that control traffic for the instances in your VPC. You add rules to your security groups that allow instances in your public subnet to communicate with instances in your private subnet. You can also associate these security groups with each instance in your VPC. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.

For more information on the network setting during image preparation, see Network setting during image preparation.

When you launch an instance, you can specify one or more security groups. To configure security groups, see Configure security groups.

Security group in Microsoft Azure

Citrix DaaS supports network security groups in Azure. Network security groups are expected to associate with subnets. For more information, see Network security groups.

For more information on network security group created during image preparation, see Create a machine catalog using an Azure Resource Manager image.

Security group in Google Cloud Platform

During the preparation of a machine catalog, a machine image is prepared to serve as the master image system disk for the catalog. When this process occurs, the disk is temporarily attached to a virtual machine. This VM must run in an isolated environment that prevents all inbound and outbound network traffic. This is accomplished through a pair of deny-all firewall rules. For more information, see Firewall Rules.

Secure boot

April 12, 2024

Secure boot is designed to ensure that only trusted software is used to boot the system. The firmware has a database of trusted certificates and verifies that the image it loads is signed by one of the trusted certificates. If that image loads further images, then that image must also be verified in the same way. vTPM is a virtualized software instance of a traditional physical TPM module. The vTPM enables attestation by measuring the entire boot chain of your VM (UEFI, OS, system, and drivers).

See the following for more information on supported hypervisors:

- Secure boot in Google Cloud Platform
- Secure boot in Microsoft Azure
- Secure boot in VMware

Secure boot in Google Cloud Platform

You can provision shielded virtual machines on GCP. A shielded virtual machine is hardened using a set of security controls that provide verifiable integrity of your Compute Engine instances, using advanced platform security capabilities like secure boot, a virtual trusted platform module, UEFI firmware, and integrity monitoring.

For more information on using PowerShell to create a catalog with shielded VM, see Using PowerShell to create a catalog with shielded VM.

> **Note:**
>
> If you install Windows 11 on the master image, then you must enable vTPM during the master image creation process. Also, you must enable vTPM on the machine profile source (VM or instance template). For information on creating Windows 11 VMs on the sole-tenant node, see Create Windows 11 VMs on the sole-tenant node.

Secure boot in Microsoft Azure

In Azure environments, you can create machine catalogs enabled with Trusted launch. Azure offers trusted launch as a seamless way to improve the security of generation 2 VMs. Trusted launch protects against advanced and persistent attack techniques. At the root of trusted launch is secure boot for your VM. Trusted launch also uses the vTPM to perform remote attestation by the cloud. This is used for platform health checks and for making trust-based decisions. You can individually enable secure boot and vTPM.
For more information on creating a machine catalog with Trusted launch, see Machine catalogs with Trusted launch.

Secure boot in VMware

MCS supports creating a machine catalog with vTPM attached VMware template as a source for machine profile input. If windows 11 is installed on the master image, then it is a requirement to have vTPM enabled for the master image. Therefore, the VMware template, which is a source of machine profile, must have vTPM attached to it. For more information, see Create a machine catalog using a machine profile.

Encryption capabilities

May 15, 2024

Encryption capabilities protect the content of virtual machines from attacks by malicious guests on a shared virtual machine host and from attacks launched by the hypervisor control software that manages all the virtual machines on the host.

See the following for more information on supported hypervisors:

- Encryption capabilities in AWS
- Encryption capabilities in Google Cloud Platform
- Encryption capabilities in Microsoft Azure)

Encryption capabilities in AWS

This section describes the encryption capabilities in AWS virtualization environments.

Automatic encryption

You can turn on automatic encryption of new Amazon EBS volumes and snapshot copies created in your account. For more information, see Automatic encryption.

Encryption capabilities in Google Cloud Platform

This section describes the encryption capabilities in Google Cloud Platform (GCP) virtualization environments.

If you need more control over key operations than what Google-managed encryption keys allows, you can use customer-managed encryption keys. When using a customer-managed encryption key, an object is encrypted with the key by Cloud Storage at the time it's stored in a bucket, and the object is automatically decrypted by Cloud Storage when the object is served to requesters. For more information, see Customer-managed encryption keys.

You can use Customer Managed Encryption Keys (CMEK) for MCS catalogs. For more information, see Using Customer Managed Encryption Keys (CMEK).

Encryption capabilities in Microsoft Azure

This section describes the encryption capabilities in Azure virtualization environments.

Azure server side encryption

Most Azure managed disks are encrypted with Azure Storage encryption, which uses server-side encryption (SSE) to protect your data and to help you meet your security and compliance commitments. Citrix DaaS supports customer-managed encryption keys for Azure managed disks through Azure Key Vault. For more information, see Azure server side encryption.

Azure disk encryption at host

You can create an MCS machine catalog with encryption at host capability.

This encryption method does not encrypt the data through the Azure storage. The server hosting the VM encrypts the data and then the encrypted data flows through the Azure storage server. Hence, this method of encryption encrypts data end to end.

For more information on creating MCS machine catalog with encryption at host capability, see Azure disk encryption at host.

Azure double encryption

Double encryption is platform-side encryption (default) and customer managed encryption (CMEK). Therefore, if you are a high security sensitive customer who is concerned about the risk associated with any encryption algorithm, implementation, or a compromised key, you can opt for this double encryption. Persistent OS and data disks, snapshots, and images are all encrypted at rest with double encryption. For more information, see Double encryption on managed disk.

Azure confidential VMs

Azure confidential computing VMs ensure that your virtual desktop is encrypted in memory and protected in use.

You can use MCS to create a catalog with Azure confidential VMs. You must use the machine profile workflow to create such a catalog. You can use both VM and ARM template spec as a machine profile input.

For more information, see Azure confidential VMs.

Quick Deploy

October 25, 2023

Introduction

In Citrix DaaS, the **Manage > Quick Deploy** interface offers fast deployment of apps and desktops when you're using Microsoft Azure to host your desktops and apps. This interface offers basic configuration, without advanced features.

Use Quick Deploy to:

- Provision virtual machines and catalogs that deliver desktops and apps hosted in Microsoft Azure.
- Create Remote PC Access catalogs for existing machines.

With Quick Deploy, you can use a Citrix Managed Azure subscription, or your own Azure subscription.

(Although the names are similar, Quick Deploy is not the same as the Quick Create method of creating catalogs in the Quick Deploy interface.)

As an alternative to Quick Deploy, the **Full Configuration** interface offers advanced configuration features. For information about **Manage** tab options, see Management interfaces.

Differences between management interfaces

The following table compares the Full Configuration and Quick Deploy interfaces.

Feature	Quick Deploy	Full Configuration
Deploy using Azure	Yes	Yes *
Deploy using other cloud services	No	Yes
Deploy using on-premises hypervisors	No	Yes
Citrix prepared images available	Yes	No
Simplified user experience	Yes	No

* When using a Citrix Managed Azure subscription, you must use Quick Deploy when creating an image or catalog.

If you are familiar with using Full Configuration to create and manage catalogs, Quick Deploy has the following differences.

- Different terminology.

  - In Quick Deploy, you create a catalog.
  - In Full Configuration, you create a machine catalog. In practice, it is often referred to as simply catalog.

- Resource location and Cloud Connectors.
  - Quick Deploy automatically creates a resource location containing two Cloud Connectors when you create your first catalog.
  - In Full Configuration, creating a resource location and adding Cloud Connectors are separate steps that you must complete in Citrix Cloud before creating a catalog.

- Images used to create catalogs.
  - Quick Deploy offers several Citrix prepared images of Windows and Linux machines. You can use these images to create catalogs.

    You can also use these images to create images and then customize the new images to suit your unique deployment needs. This feature is known as the image builder. You can also import images from your own Azure subscription.
  - In Full Configuration, you customize images from the supported host you're using. Citrix prepared images are not available.

- Catalog displays:
  - Catalogs created in Quick Deploy are visible in the Quick Deploy and Full Configuration displays.
  - Catalogs created in Full Configuration are not visible in the Quick Deploy display.

- Delivery groups:
  - You do not create delivery groups in Quick Deploy. In Quick Deploy, you specify the machines, applications, desktops, and users (subscribers) in the catalog.

    Citrix automatically creates a delivery group for each Quick Deploy catalog, using the same name as the catalog. That action occurs behind the scenes. You don't need to do anything to create the delivery group. The delivery group appears only in the Full Configuration interface, not in Quick Deploy.
  - In Full Configuration, you create a delivery group and indicate which machines it contains. Optionally, you also specify applications, desktops, and users. You can also create application groups.

- Layout and user interface.
  - The Quick Deploy interface has a different layout and style from Full Configuration. Quick Deploy contains more on-screen guidance.

The interfaces are not mutually exclusive. You can use Quick Deploy to create some catalogs, and then use Full Configuration to create other catalogs.

Manage catalogs created in the Quick Deploy interface

After you create a catalog in the Quick Deploy interface, you can continue to manage that catalog in that interface. For details, see Manage catalogs in Quick Deploy. You can also use the Full Configuration interface.

When you create a catalog in Quick Deploy, that catalog (plus the delivery group and hosting connection that are created automatically behind the scenes) are assigned a scope of `Citrix managed object`. Scopes are used in delegated administration to group objects.

Catalogs, delivery groups, and connections with the `Citrix managed object` scope are prohibited from certain actions in the Full Configuration interface. (Allowing those actions in Full Configuration might adversely affect the system's ability to support both Quick Deploy and Full Configuration, so those actions are disabled.) In the Full Configuration interface:

- **Catalog:** Most of the catalog management actions are not available. You cannot delete a catalog.
- **Delivery group:** Most of the delivery group management actions are available. You cannot delete the delivery group.
- **Connection:** Most of the connection management actions are not available. You cannot delete a connection. You cannot create a connection that is based on a connection that has the `Citrix managed object` scope.

If you create a catalog in Quick Deploy using your own Azure subscription (that you added to Quick Deploy), and you want to manage the catalog (and its delivery group and connection) entirely in Full Configuration, you can *convert* the catalog.

- Converting a catalog restricts its management to only the Full Configuration interface. After a catalog is converted, you can no longer use the Quick Deploy interface to manage that catalog.
- After a catalog is converted, the actions that were previously unavailable in Full Configuration can be selected. (The `Citrix managed object` scope is removed from the converted catalog, delivery group, and hosting connection.)
- To convert a catalog:

  From the **Manage > Quick Deploy** dashboard, click anywhere in the catalog's entry. On the **Details** tab, under **Advanced settings**, select **Convert Catalog**. When prompted, confirm the conversion.

- You cannot convert a catalog that was created in Quick Deploy using a Citrix Managed Azure subscription.

Replacement of earlier Azure Quick Deploy interface

Quick Deploy replaces an earlier interface named Azure Quick Deploy. The Quick Deploy display includes all the catalogs you created using Azure Quick Deploy.

If you started creating a catalog in Azure Quick Deploy, but did not finish it, that catalog appears in the Quick Deploy catalog list. However, the only available action in Quick Deploy is to delete it.

Requirements

- Quick Deploy supports only Azure workloads. It is not available with any other cloud host types, services, or hypervisors.
- Quick Deploy is available only in Citrix DaaS for Azure, Premium, and Advanced editions, and Workspace Premium Plus.
- You must have a Citrix Cloud account and a subscription to Citrix DaaS.
- If you ordered the Citrix Managed Azure Consumption Fund, you can use a Citrix Managed Azure subscription when you create catalogs and images.

  If you did not order the Consumption Fund (or prefer to use your own Azure subscription), you must have an Azure subscription.
- You must have appropriate permission in Citrix DaaS to see the **Manage** tab. For details, see Delegated administration.

> **Important:**
>
> To ensure that you get important information about Citrix Cloud and the Citrix services you subscribe to, make sure you can receive all email notifications. For example, Citrix sends monthly informational notification emails detailing your Azure consumption (usage).
>
> In the upper right corner of the Citrix Cloud console, expand the menu to the right of the customer name and OrgID fields. Select **Account Settings**. On the **My Profile** tab, select all entries in the **Email Notifications** section.

Citrix Gateway consideration

If you use your own Citrix Gateway, it must have access to the VNet specified in the catalog creation wizard. A VPN can provide that access.

The Citrix Gateway Service works automatically with Quick Deploy catalogs.

What's next

Follow the Quick Deploy setup guidance in Get started.

After setting up your deployment using Quick Deploy, you can continue using that interface for the following management tasks.

- Manage the catalog. Catalog management includes adding or deleting machines, managing apps, and managing power management schedules.
- Manage images. Image management includes preparing or importing images, updating catalogs with a new image, renaming or deleting images, and installing or upgrading VDAs on an image.
- Add or remove users in a catalog.
- Manage resource locations.

Get started with Quick Deploy

May 9, 2023

This article summarizes the setup tasks for delivering desktops and apps using the Quick Deploy interface of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). We recommend that you review each procedure before actually doing it, so you know what to expect.

To use Quick Deploy to set up a Remote PC Access deployment, see Remote PC Access.

Setup task summary

The following sections of this article guide you through setup tasks:

1. Review and complete necessary tasks in system requirements and preparation.
2. Set up a quick proof of concept deployment or a production deployment.
3. Provide the workspace URL to your users.

System requirements and preparation

- Sign up for Citrix Cloud and Citrix DaaS.

  Also, if you plan to use Citrix Managed Azure, make sure to order the Citrix Azure Consumption Fund (in addition to Citrix DaaS), either through Citrix or Azure Marketplace.

- **Windows licensing:** Ensure that you are properly licensed for Remote Desktop Services to run either Windows Server workloads or Azure Virtual Desktop Licensing for Windows 10. For more information, see Configure a Microsoft RDS license server.
- If you plan to use a Citrix Managed Azure subscription, and want to join VDAs to a domain using Active Directory Group Policy, you must be an administrator with permission to perform that action in Active Directory. For details, see Customer responsibility.
- Configuring connections to your corporate on-premises network has extra requirements.
  - Any connection (Azure VNet peering or SD-WAN): Requirements for all connections.
  - Azure VNet peering connections: VNet peering requirements and preparation.
  - SD-WAN connections: SD-WAN connection requirements and preparation.
- If you plan to use your own Azure images when creating a catalog, those images must meet certain requirements.
- Internet connectivity requirements: System and connectivity requirements.
- Resource limits in a Citrix DaaS deployment: Limits.

Supported operating systems

When using Quick Deploy with a Citrix Managed Azure subscription:

- Windows 10 single-session
- Windows 10 multi-session
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux and Ubuntu

When using Quick Deploy with a customer-managed Azure subscription:

- Windows 10 Enterprise single-session
- Windows 10 Enterprise Virtual Desktop multi-session
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux and Ubuntu

Set up a quick proof of concept deployment

This procedure requires a Citrix Managed Azure subscription.

1. Create a catalog using quick create.
2. Add your users to the Managed Azure AD.
3. Add your users to the catalog.
4. Notify your users of the Workspace URL.

Set up a production deployment

1. If you're using your own Active Directory or Azure Active Directory to authenticate users, connect and set that method in Citrix Cloud.
2. If you're using domain-joined machines, verify that you have valid DNS server entries.
3. If you're using your own Azure subscription (instead of a Citrix Managed Azure subscription), add your Azure subscription.
4. Create or import an image. Although you can use one of the Citrix prepared images as-is in a catalog, they're intended primarily for proof of concept deployments.
5. If you're using a Citrix Managed Azure subscription, and want your users to be able to access items in your network (such as file servers), set up an Azure VNet peering or Citrix SD-WAN connection.
6. Create a catalog using custom create.
7. If you're creating a catalog of multi-session machines, add apps to the catalog, if needed.
8. If you're using the Citrix Managed Azure AD to authenticate your users, add users to the directory.
9. Add users to the catalog.
10. Notify your users of the Workspace URL.

After you set up the deployment, use the **Quick Deploy > Monitor** dashboard to see desktop usage, sessions, and machines.

Workspace URL

After you create catalogs and assign users, notify users where to find their desktops and apps: the Workspace URL. The Workspace URL is the same for all catalogs and users.

The Workspace URL is available in two locations:

- From **Manage > Quick Deploy** in Citrix DaaS, view the URL by expanding **User Access & Authentication** on the right.
- From the Citrix Cloud console, select **Workspace Configuration** from the upper left menu. The **Access tab** contains the Workspace URL.

For information about customizing the Workspace URL, see Customize the Workspace URL.

After users navigate to the Workspace URL and authenticate, they can start their desktops and apps.

Get help

- Review the Troubleshoot article.
- If you still have problems with Citrix DaaS, open a ticket by following the instructions in How to Get Help and Support.

Create catalogs using Quick Deploy

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Use the procedures in this article to create a catalog of Microsoft Azure machines using the Quick Deploy management interface.

Review the entire procedure before creating a catalog, so you know what to expect.

To create a catalog using the Full Configuration interface, see Create machine catalogs.

Machine types

A Quick Deploy catalog can contain one of the following types of machines:

- **Static:** The catalog contains single-session static machines (also known as personal, dedicated, or persistent desktops). Static means that when a user starts a desktop, that desktop "belongs" to that user. Any changes that that user makes to the desktop are retained at logoff. Later, when that user returns to Citrix Workspace and starts a desktop, it is the same desktop.
- **Random:** The catalog contains single-session random machines (also known as non-persistent desktops). Random means that when a user starts a desktop, any changes that that user makes to that desktop are discarded after logoff. Later, when that user returns to Citrix Workspace and starts a desktop, it might or might not be the same desktop.
- **Multi-session:** The catalog contains machines with apps and desktops. More than one user can access each of those machines simultaneously. Users can launch a desktop or apps from their workspace. App sessions can be shared. Session sharing is not permitted between an app and a desktop.

  - When you create a multi-session catalog, you select the work load: light (such as data entry), medium (such as office apps), heavy (such as engineering), or custom. Each option represents a specific number of machines and sessions per machine, which yields the total number of sessions that the catalog supports.
  - If you select the custom work load, you then select from available combinations of CPUs, RAM, and storage. Type the number of machines and sessions per machine, which yields the total number of sessions that the catalog supports.

When deploying desktops, the static and random machine types are sometimes called "desktop types".

Ways to create a catalog using Quick Deploy

There are several ways to create and configure a catalog:

- **Quick create** is the fastest way to get started. You provide minimal information, and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) takes care of the rest. A quick create catalog is great for a test environment or proof of concept.
- **Custom create** allows more configuration choices than quick create. It's more suited to a production environment than a quick create catalog.
- **Remote PC Access** catalogs contain existing machines (usually physical) that users access remotely. For details and instructions about these catalogs, see Remote PC Access.

Here's a comparison of quick create and custom create:

Quick create	Custom create
Less information to provide.	More information to provide.
Fewer choices for some features.	More choices for some features.
Citrix-managed Azure Active Directory user authentication.	Choice of: Citrix-managed Azure Active Directory, or your Active Directory/Azure Active Directory.
No connection to your on-premises network.	Choice of: No connection to your on-premises network, Azure VNet peering, and SD-WAN.
Uses a Citrix prepared Windows 10 image. That image contains a current desktop VDA.	Choice of: Citrix prepared images, your images that you import from Azure, or images you've built in Citrix DaaS from a Citrix prepared or imported image.
Each desktop has Azure standard disk (HDD) storage.	Several storage options are available.
Static desktops only.	Static, random, or multi-session desktops.

Quick create	Custom create
A power management schedule cannot be configured during creation. The machine hosting the desktop powers off when the session ends. (You can change this setting later.)	A power management schedule can be configured during creation. (A Quick Deploy power management schedule differs from a power management schedule you can create using the Full Configuration management interface.)
Must use a Citrix Managed Azure subscription.	Can use the Citrix Managed Azure subscription or your own Azure subscription.

For procedure details, see:

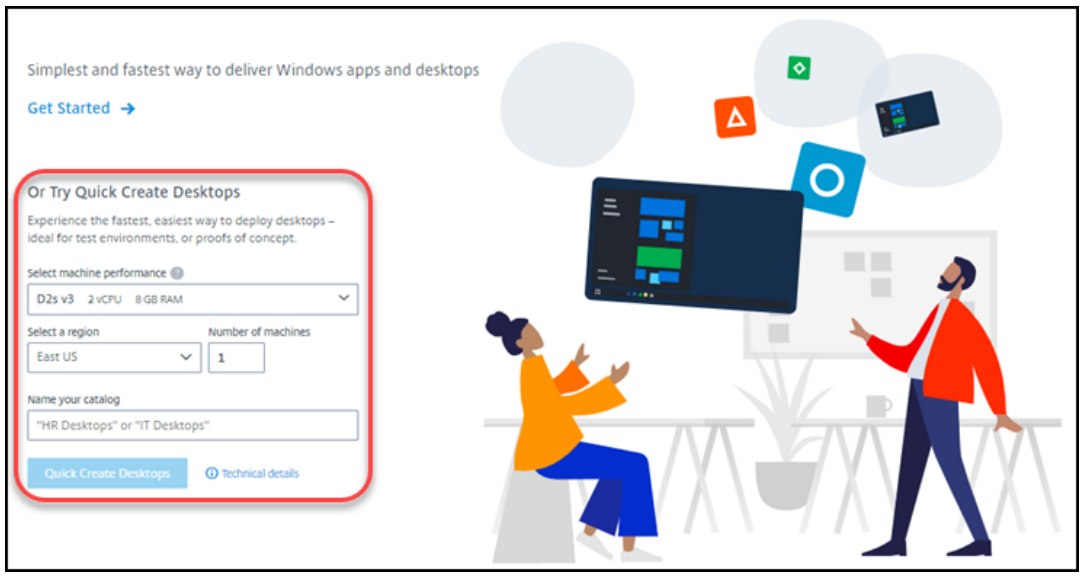
- Create a Quick Deploy catalog using quick create
- Create a Quick Deploy catalog using custom create

> **Important:**
>
> When you create a catalog (or an image) using a Citrix Managed Azure subscription for the first time, you are asked to acknowledge and consent to your responsibility for charges incurred. Reminders of that consent can also appear when creating more catalogs or images using the Citrix Managed Azure subscription.

Create a Quick Deploy catalog using quick create

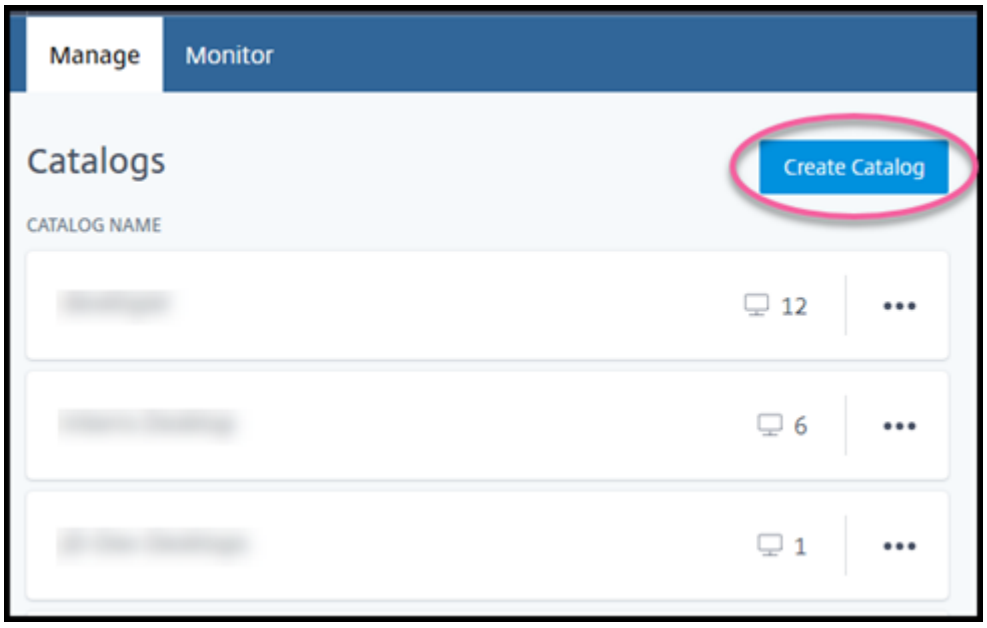
The quick create method uses a Citrix Managed Azure subscription and a Citrix prepared Windows 10 image to create a catalog containing static machines. Power management settings use the Cost Saver preset values. There is no connection to your corporate network. Users must be added using Citrix Managed Azure AD.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. Select **Manage > Quick Deploy**.
4. If a catalog has not yet been created, you're taken to the **Welcome** page. Choose one of:
    - Configure the catalog on this page. Continue with steps 6 through 10.

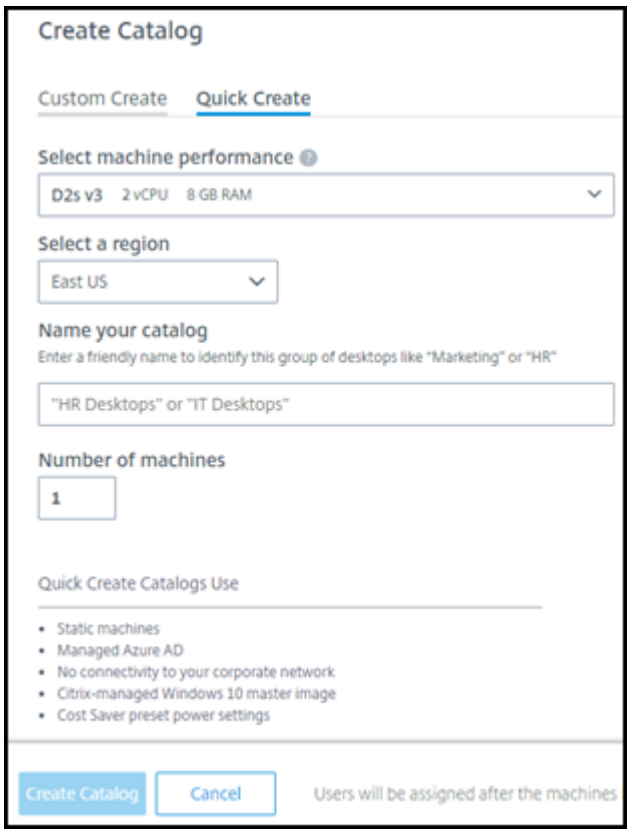


- Select **Get Started**. You're taken to the **Manage > Quick Deploy** dashboard. Select **Create Catalog**.

5. If a catalog has already been created (and you're creating another one), you're taken to the **Manage > Quick Deploy** dashboard. Select **Create Catalog**.



6. Select **Quick Create** at the top of the page, if it is not already selected.



- **Machine performance:** Select the machine type. Each choice has a unique combination of CPUs, RAM, and storage. Higher-performance machines have higher monthly costs.
- **Region:** Select a region where you want the machines created. You might select a region that's close to your users.
- **Name:** Type a name for the catalog. This field is required, and there is no default value.
- **Number of machines:** Type the number of machines you want.

7. When you're done, select **Create Catalog**. (If you're creating the first catalog from the **Welcome** page, select **Quick Create Desktops**.)
8. If this is the first catalog you're creating using a Citrix Managed Azure subscription, when prompted, acknowledge your responsibility for related charges.

While the catalog is being created, the catalog's name is added to the list of catalogs, indicating its progress through creation.

Citrix DaaS also automatically creates a resource location and adds two Citrix Cloud Connectors.

What to do next:

- You can add users to the Managed Azure AD directory while the catalog is being created.
- After the catalog is created, add users to the catalog.

Create a Quick Deploy catalog using custom create

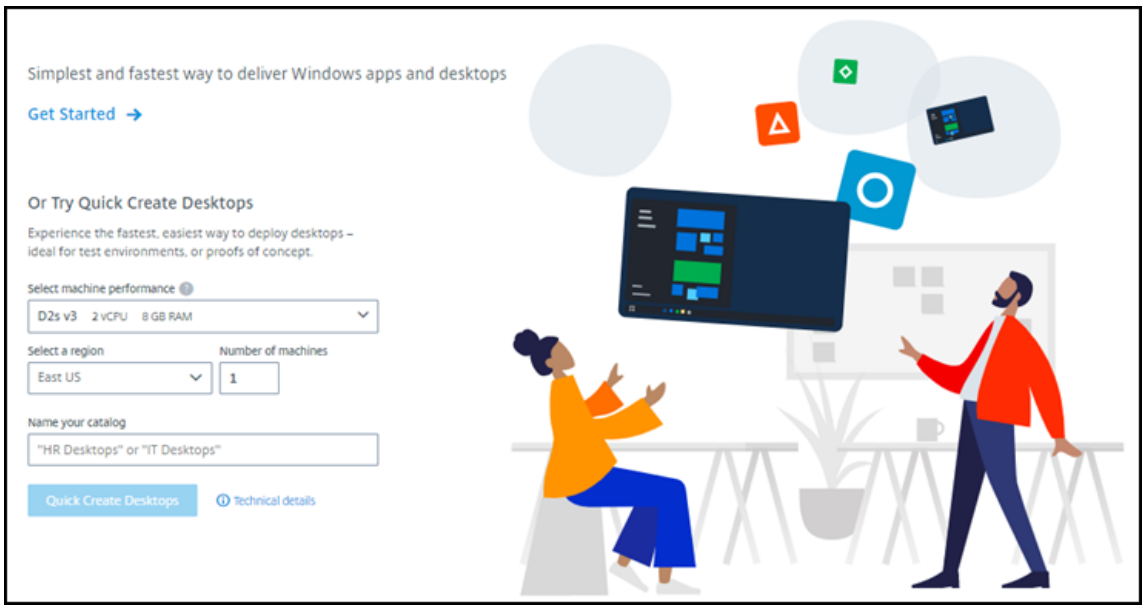
If you are using a Citrix Managed Azure subscription, and plan to use a connection to your on-premises network resources, create that network connection before creating the catalog. To allow your users access to your on-premises or other network resources, you also need Active Directory information for that location.

If you do not have a Citrix Managed Azure subscription, you can:

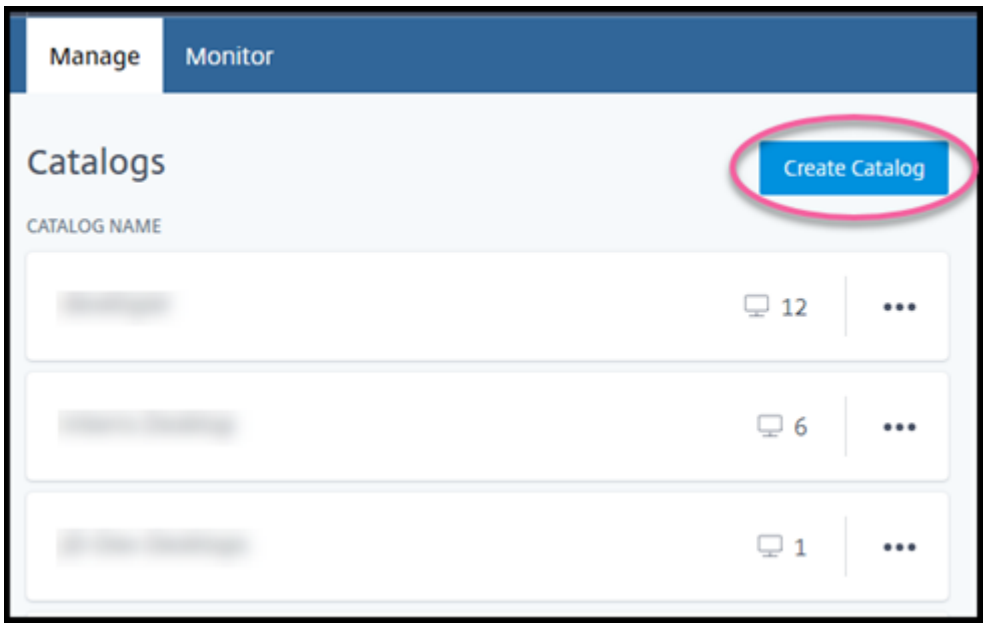
- Order the Azure Consumption Fund through Azure Marketplace, which provides you with a Citrix Managed Azure subscription.
- Import (add) one or more of your own Azure subscriptions to Citrix DaaS before creating a catalog.

To create a catalog:

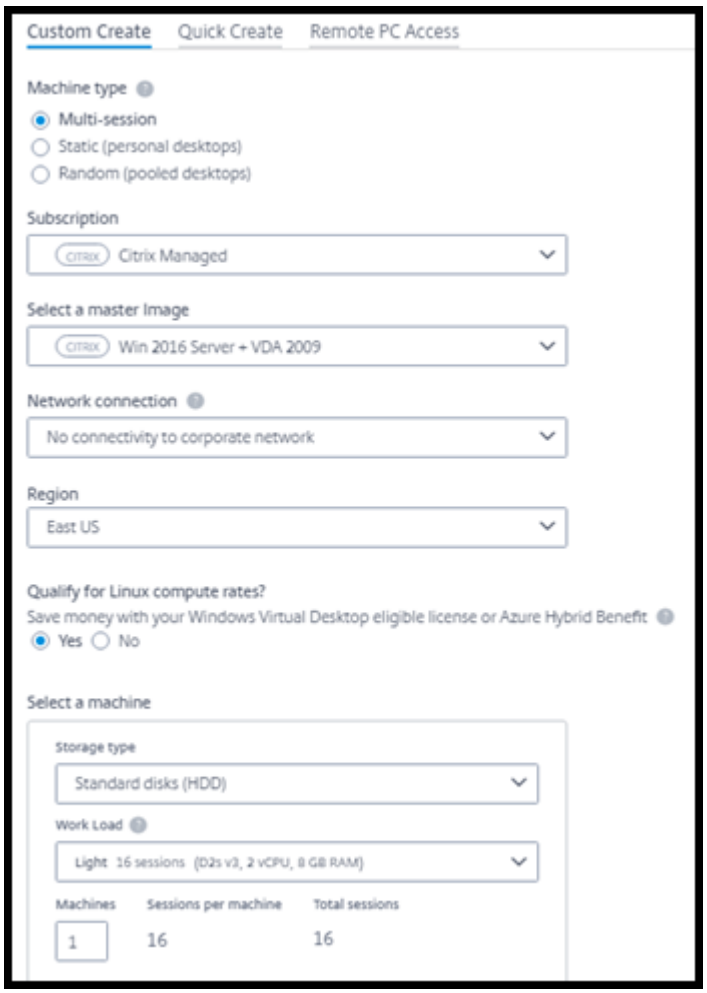
1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. Select **Manage > Quick Deploy**.
4. If a catalog has not yet been created, you're taken to the **Welcome** page. Select **Get Started**. At the end of the introduction page, you're taken to the **Manage > Quick Deploy** dashboard. Select **Create Catalog**.



If a catalog has already been created, you're taken to the **Manage > Quick Deploy** dashboard. Select **Create Catalog**.



5. Select **Custom Create** at the top of the page, if it's not already selected.



6. Complete the following fields. (Some fields are valid only for certain machine types. The field order might differ.)

   - **Machine type**. Select a machine type. For details, see Machine types.
   - **Subscription**. Select an Azure subscription.
   - **Master image:** Select an operating system image to be used for the catalog's machines.
   - **Network connection:** Select the network connection to use for accessing resources in your network.

     If you selected a Citrix Managed Azure subscription, the choices are:

     - **No Connectivity:** Users cannot access locations and resources on your on-premises corporate network.
     - *Connections:* Select a previously created connection, such as a VNet peering or SD-WAN connection.

     If you selected a customer-managed Azure subscription, select the appropriate resource group, virtual network, and subnet.
   - **Region:** (Available only if you selected **No Connectivity** in **Network connection**.) Select a region where you want the desktops created. You might select a region that's close to your users.

     If you selected a connection in **Network connection**, the catalog uses that network's region.
   - **Qualify for Linux compute rates?** (Available only if you selected a Windows image.) You can save money when you use your eligible license or Azure Hybrid Benefit.

     Windows Virtual Desktop benefit: Eligible Windows 10 or Windows 7 per user licenses for:

     - Microsoft 365 E3/ES
     - Microsoft 365 A3/AS/Student Use Benefits
     - Microsoft 365 F3
     - Microsoft 365 Business Premium
     - Windows 10 Enterprise E3/E5
     - Windows 10 Education A3/A5
     - Windows 10 VDA per user

     Per user or per device license of RDS CAL with Software Assurance for Windows Server workloads.

     Azure Hybrid benefit: Windows Server licenses with active Software Assurance or the equivalent qualifying subscription licenses. See https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Machine:**
  - **Storage type**. HDD or SSD.
  - **Machine performance** (for **Static** or **Random** machine type), or **Workload** (for multi-session machine type). Choices include only options that match the generation type (gen1 or gen2) of the image you selected.

    If you select the custom work load, type the number of machines and sessions per machine in the **Machine Performance** field.
  - **Machines**. How many machines you want in this catalog.
- **Machine naming scheme:** See Machine naming scheme.
- **Name:** Type a name for the catalog. This name appears on the **Manage** dashboard.
- **Power schedule:** By default, the **I'll configure this later** check box is selected. For details, see Power management schedules. (This power management schedule differs from power management features available in the Full Configuration management interface of Citrix DaaS.)
- **Join the local Active Directory domain:** (Available only if you selected an Azure VNet peering connection in **Network connection**.) Select **Yes** or **No**. If you select **Yes**, enter the:
  - FQDN of the domain (for example, Contoso.com).
  - Organization Unit: To use the default OU (Computers), leave this field empty.
  - Citrix Daas account name: Must be a domain or enterprise administrator in the format name@domain or domain\name.
  - Password for Citrix DaaS account name.
- **Advanced settings:** See Resource location settings when creating a catalog.

7. When you're done, select **Create Catalog**.
8. If this is the first catalog you're creating using a Citrix Managed Azure subscription, when prompted, acknowledge your responsibility for related charges.

The **Manage > Quick Deploy** dashboard indicates when your catalog is created. Citrix DaaS also automatically creates a resource location and adds two Citrix Cloud Connectors.

What to do next:

- If you haven't done it already, configure the authentication method for your users to authenticate to Citrix Workspace.
- After the catalog is created, add users to the catalog.
- If you created a multi-session catalog, add applications (before or after adding users).

Resource location settings when creating a catalog

When creating a catalog, you can optionally configure several resource location settings.

When you select **Advanced settings** in the catalog creation dialog, Citrix DaaS retrieves resource location information.

- If you already have a resource location for the domain and network connection selected for the catalog, you can save it for use by the catalog you're creating.

  If that resource location has only one Cloud Connector, another one is installed automatically. You can optionally specify advanced settings for the Cloud Connector you're adding.

- If you don't have a resource location set up for the domain and network connection selected for the catalog, you're prompted to configure one.

Configure advanced settings:

- (Required only when the resource location is already set up.) A name for the resource location.
- External connectivity type: through the Citrix Gateway service, or from within your corporate network.
- Cloud Connector settings:
  - (Available only when using a customer-managed Azure subscription) Machine performance. This selection is used for the Cloud Connectors in the resource location.
  - (Available only when using a customer-managed Azure subscription) Azure resource group. This selection is used for the Cloud Connectors in the resource location. The default is the resource group last used by the resource location (if applicable).
  - Organizational Unit (OU). The default is the OU last used by the resource location (if applicable).

When you're done with the advanced settings, select **Save** to return to the catalog creation dialog.

After you create a catalog, several resource location actions are available. For details, see Resource location actions.

Machine naming scheme

To specify a machine naming scheme when creating a catalog, select **Specify machine naming scheme**. Use from 1-4 wildcards (hash marks) to indicate where sequential numbers or letters appear in the name. Rules:

- The naming scheme must contain at least one wildcard, but not more than four wildcards. All the wildcards must be together.

- The entire name, including wildcards, must be between 2 and 15 characters.
- A name cannot include blanks (spaces), slashes, backslashes, colons, asterisks, angle brackets, pipes, commas, tildes, exclamation points, at signs, dollar signs, percent signs, carets, parentheses, braces, or underscores.
- A name cannot begin with a period.
- A name cannot contain only numbers.
- Do not use the following letters at the end of a name: `-GATEWAY`, `-GW`, and `-TAC`.

Indicate whether the sequential values are numbers (0-9) or letters (A-Z).

For example, a naming scheme of `PC-Sales-##` (with **0-9** selected) results in computer accounts named `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03`, and so on.

Leave enough room for growth.

- For example, a naming scheme with 2 wildcards and 13 other characters (for example, `MachineSales-##`) uses the maximum number of characters (15).
- Once the catalog contains 99 machines, the next machine creation fails. Citrix DaaS tries to create a machine with three digits (100), but that would create a name with 16 characters. The maximum is 15.
- So, in this example, a shorter name (for example, `PC-Sales-##`) allows scaling beyond 99 machines.

If you do not specify a machine naming scheme, Citrix DaaS uses the default naming scheme `DAS %%%%%-**-###`.

- `%%%%%` = five random alphanumeric characters matching the resource location prefix
- `**` = two random alphanumeric characters for the catalog
- `###` = three digits.

Related information

- Remote PC Access catalogs
- Create a catalog in a network that uses a proxy server
- Display catalog information
- Manage catalogs in Quick Deploy

Manage catalogs in Quick Deploy

March 31, 2022

This article describes the catalog management tasks you can use to manage catalogs that were created in Quick Deploy.

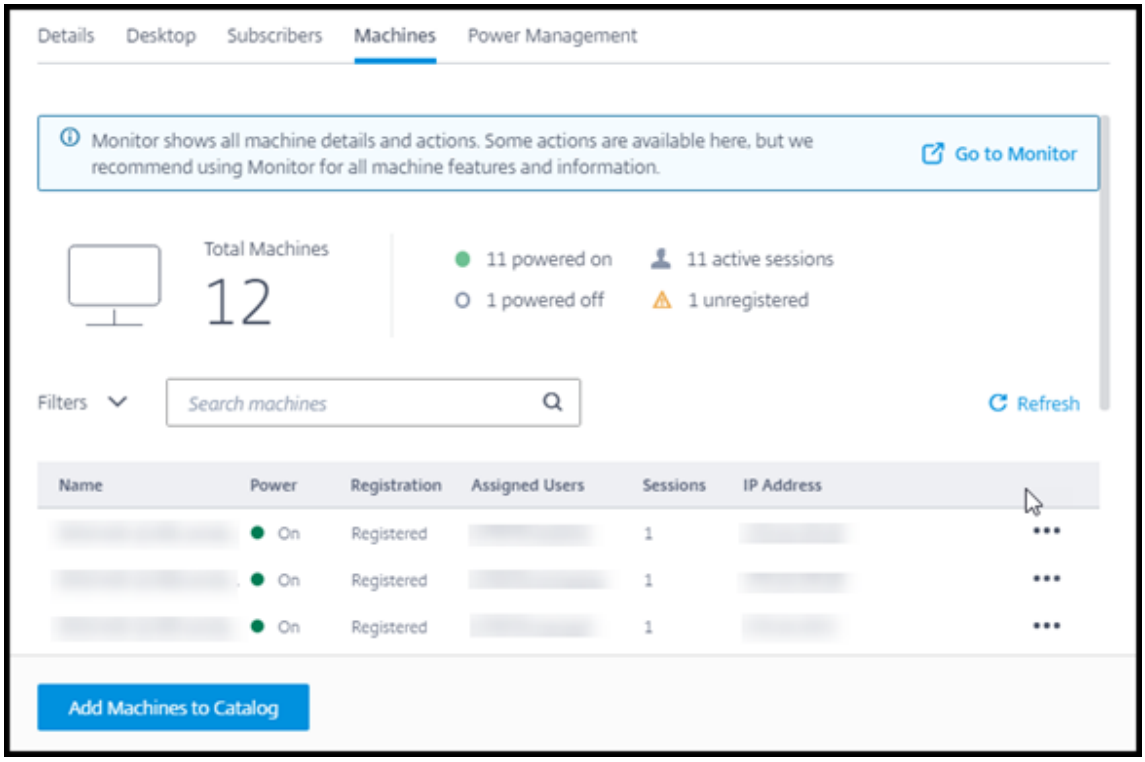
Remember: If you used Quick Deploy to create a catalog, and then use the Full Configuration interface to perform any management tasks on that catalog, you can no longer use the Quick Deploy interface for that catalog.

(For information about managing catalogs in the Full Configuration management interface, see Manage machine catalogs.)

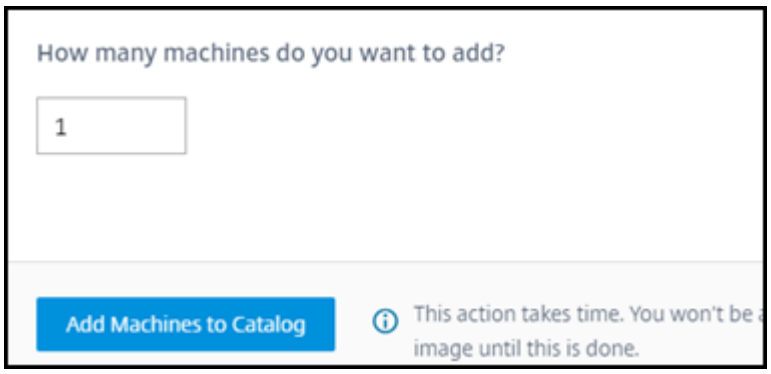
Add machines to a catalog

While machines are being added to a Quick Deploy catalog, you cannot make any other changes to that catalog.

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.
2. On the **Machines** tab, select **Add Machines to Catalog**.



3. Enter the number of machines you want to add to the catalog.



4. (Valid only if the catalog is domain-joined.) Type the user name and password for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) account.
5. Select **Add Machines to Catalog**.

You cannot reduce the machine count for a catalog. However, you can use power management schedule settings to control how many machines are powered on, or delete individual machines from the **Machines** tab. See Manage machines in a catalog for information on deleting machines from the **Machines** tab.

Change the number of sessions per machine

Changing the number of sessions per multi-session machine can affect users' experience. Increasing this value can reduce the compute resources allocated to concurrent sessions.

Recommendation: Observe your usage data to determine the appropriate balance between user experience and cost.

1. From **Manage > Quick Deploy**, select a catalog containing multi-session machines.
2. On the **Details** tab, select **Edit** next to **Sessions per Machine**.
3. Enter a new number of sessions per machine.
4. Select **Update Number of Sessions**.
5. Confirm your request.

This change does not affect current sessions. When you change the maximum number of sessions to a value that is lower than a machine's currently active sessions, the new value is implemented through the normal attrition of active sessions.

If a failure occurs before the update process begins, the catalog's **Details** display retains the correct number of sessions. If a failure occurs during the update process, the display indicates the number of sessions you wanted.

Manage machines in a catalog

> **Note:**
>
> Many of the actions that are available from **Manage > Quick Deploy** are also available from the **Monitor** tab in Quick Deploy.

To select actions from **Manage > Quick Deploy**:

1. From **Manage > Quick Deploy**, click anywhere in a catalog's entry.
2. On the **Machines** tab, find the machine you want to manage. In the ellipsis menu for that machine, select the desired action:

   - **Restart:** Restarts the selected machine.
   - **Start:** Starts the selected machine. This action is available only if the machine is powered off.
   - **Shutdown:** Shut down the selected machine. This action is available only if the machine is powered on.
   - **Turn maintenance mode on/off:** Turns maintenance mode on (if it is off) or off (if it is on) for the selected machine. By default, maintenance mode is turned off for a machine.

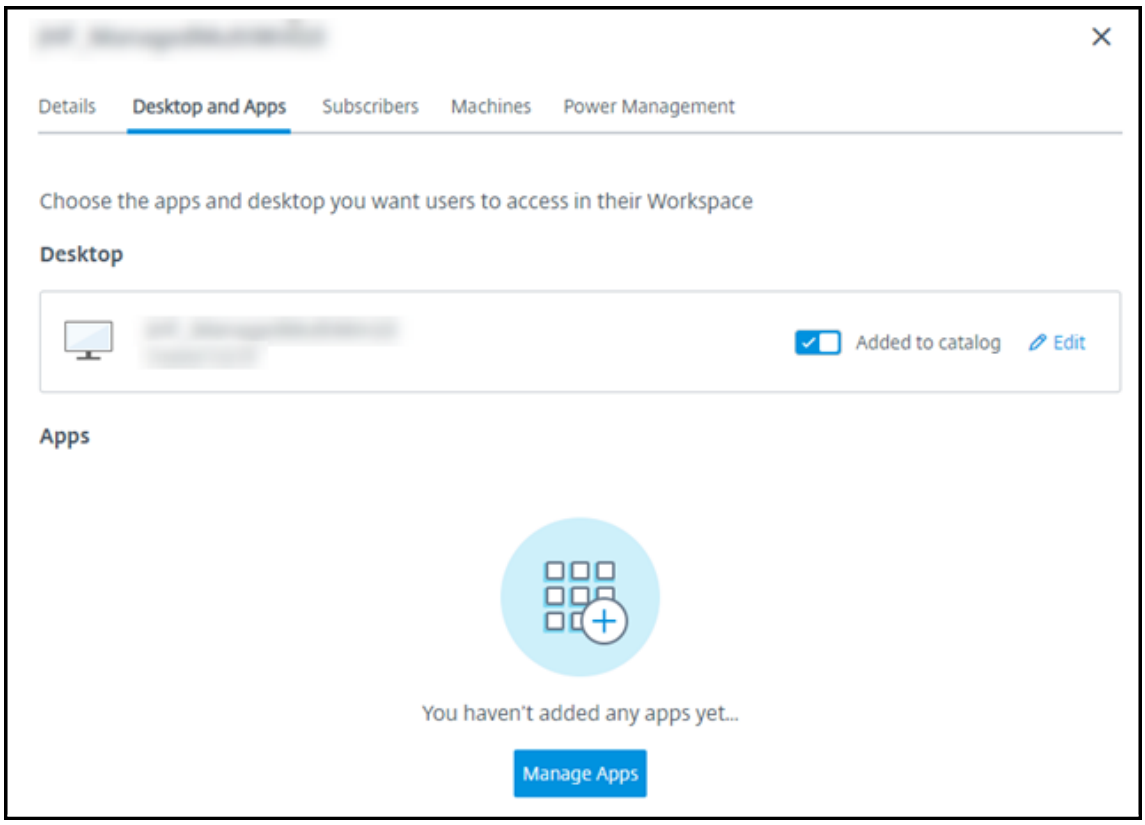
     Turning on maintenance mode prevents new connections from being made to that machine. Users can connect to existing sessions on that machine, but they cannot start new sessions on that machine.

     You might place a machine in maintenance mode before applying patches, or for troubleshooting.
   - **Delete:** Deletes the selected machine. This action is available only when the machine's session count is zero. Confirm the deletion.

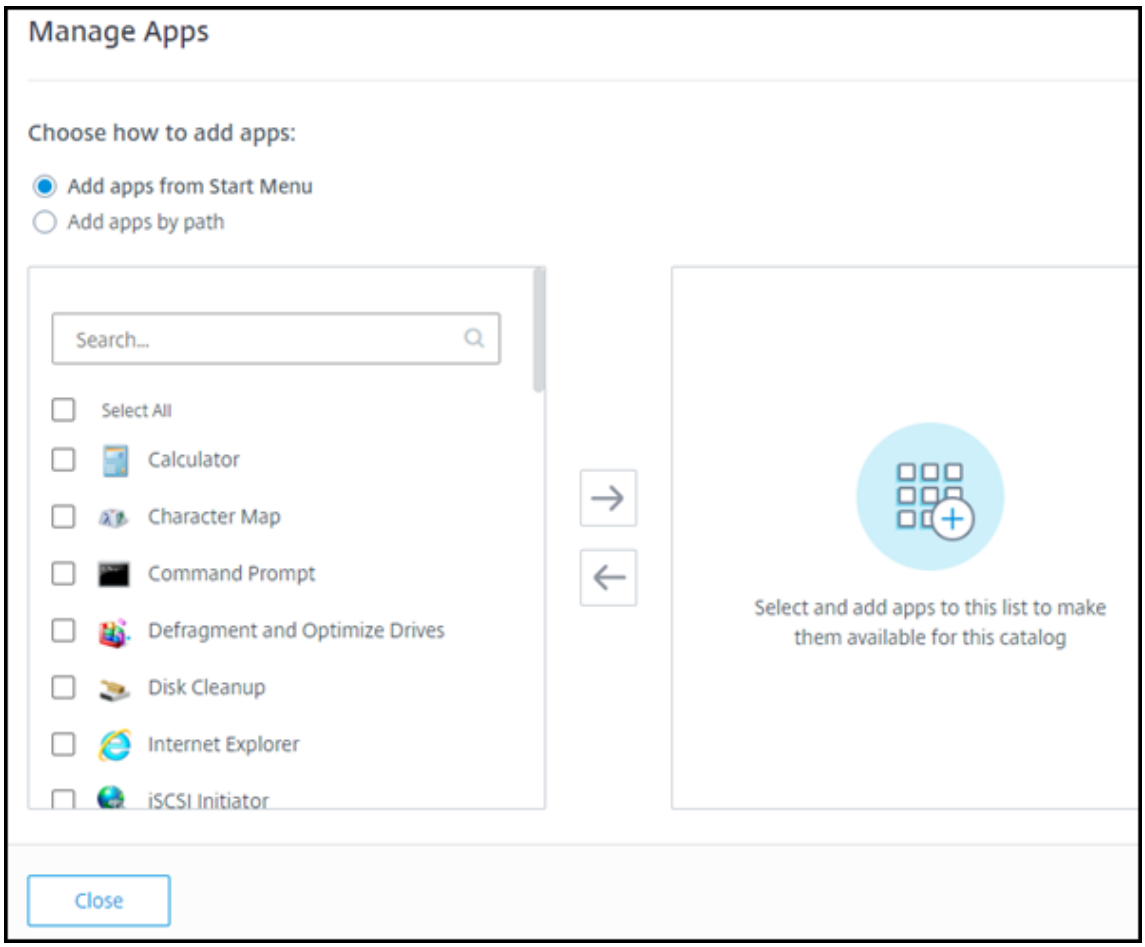
     When a machine is deleted, all data on the machine is removed.
   - **Force restart:** Forces a restart of the selected machine. Select this action only if a **Restart** action for the machine fails.

Add apps to a catalog

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.
2. On the **Desktop and Apps** tab, select **Manage Apps**.

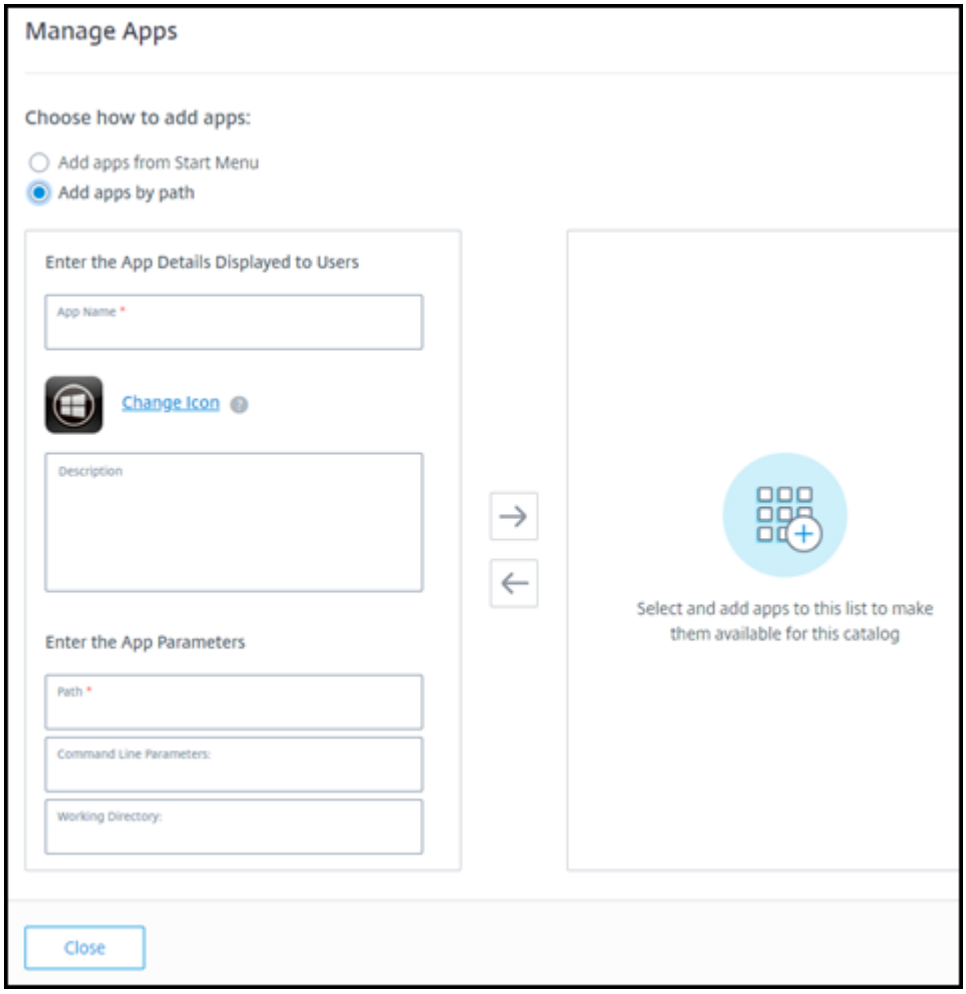


3. Select how you are adding apps: from the **Start** menu of machines in the catalog, or from a different path on the machines.
4. To add apps from the **Start** menu:



- Select available apps in the left column. (Use **Search** to tailor the apps list.) Select the right arrow between the columns. The selected apps move to the right column.
- Similarly, to remove apps, select them in the right column. Select the left arrow between columns.
- If the **Start** menu has more than one version of the same app, with the same name, you can add only one. To add another version of that app, edit that version to change its name. Then you can add that version of the app.

5. To add apps by path:



- Enter the name for the app. This is the name users see in Citrix Workspace.
- The icon shown is the icon users see in Citrix Workspace. To select another icon, select **Change icon** and navigate to the icon you want to display.
- (Optional) Enter a description of the application.
- Enter the path to the app. This field is required. Optionally, add command line parameters and the working directory. For details about command line parameters, see Pass parameters to published applications.

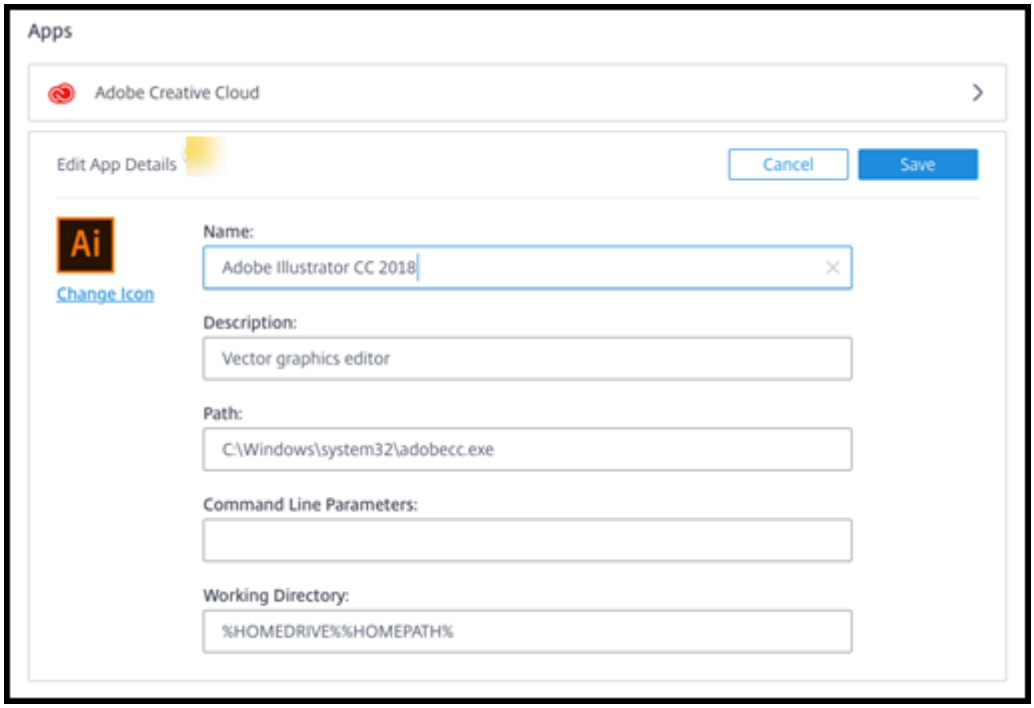
6. When you're finished, select **Close**.

On Windows Server 2019 VDAs, some application icons might not appear correctly during configuration and in the users'workspace. As a workaround, after the app is published, edit the app and use the **Change icon** feature to assign a different icon that displays correctly.

Edit an app in a catalog

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.

2. On the **Desktop and Apps** tab, click anywhere on the row containing the app you want to edit.
3. Select the pencil icon.



4. Type changes in any of the following fields:

   - **Name:** The name users see in Citrix Workspace.
   - **Description**
   - **Path:** The path to the executable.
   - **Command line parameters:** For details, see Pass parameters to published applications.
   - **Working directory**

5. To change the icon users see in their Citrix Workspace, select **Change icon** and navigate to the icon you want to display.
6. When you're done, select **Save**.

Pass parameters to published applications

When you associate a published application with file types, the percent and star symbols (enclosed in double quotation marks) are appended to the end of the command line. These symbols act as a placeholder for parameters passed to user devices.

- If a published application does not launch when expected, verify that its command line contains the correct symbols. By default, parameters supplied by user devices are validated when the symbols are appended.

For published applications that use customized parameters supplied by the user device, the symbols are appended to the command line to bypass command-line validation. If you do not see these symbols in a command line for the application, add them manually.

- If the path to the executable file includes directory names with spaces (such as "C:\Program Files"), enclose the command line for the application in double quotation marks to indicate that the space belongs in the command line. Add double quotation marks around the path, and another set of double quotation marks around the percent and star symbols. Add a space between the closing quotation mark for the path and the opening quotation mark for the percent and star symbols.

  For example, the command line for the published application Windows Media Player is: "C:\Program Files\Windows Media Player\mplayer1.exe" "%*"

Remove apps from a catalog

Removing an app from a catalog does not remove it from the machines. It just prevents it from appearing in Citrix Workspace.

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.
2. On the **Desktop and Apps** tab, select the trash icon next to the apps you want to remove.

Delete a catalog

When you delete a catalog, all the machines in the catalog are permanently destroyed. Deleting a catalog cannot be reversed.

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.
2. On the **Details** tab, select **Delete Catalog**.
3. Confirm the deletion.

To help identify residual Active Directory machine accounts that you must delete, you can download a list of machine and Cloud Connector names.

Manage power management schedules

A power management schedule affects all machines in a catalog. A schedule provides:

- Optimal user experience: Machines are available for users when they're needed.
- Security: Desktop sessions that remain idle for a specified interval are disconnected, requiring users to launch a new session in their workspace.

- Cost management and power savings: Machines with desktops that remain idle are powered-off. Machines are powered on to meet scheduled and actual demand.

You can configure a power schedule when you create a custom catalog or do it later. If no schedule is selected or configured, a machine powers off when a session ends.

You cannot select or configure a power schedule when creating a catalog with quick create. By default, quick create catalogs use the Cost Saver preset schedule. You can select or configure a different schedule later for that catalog.

Schedule management includes:

- Knowing what information a schedule contains
- Creating a schedule

Information in a schedule

The following diagram shows the schedule settings for a catalog containing multi-session machines. Settings for a catalog containing single-session (random or static) machines differ slightly.

A power management schedule contains the following information.

Preset schedules Citrix DaaS offers several preset schedules. You can also configure and save custom schedules. Although you can delete custom presets, you cannot delete Citrix-provided presets.

Time zone Used with the power-on machines setting to establish work hours and after hours, based on the selected time zone.

This setting is valid for all machine types.

Power on machines: Work hours and after hours The days of the week and start-stop hours of the day that form your work hours. This generally indicates the intervals when you want machines powered on. Any time outside of those intervals is considered after-hours. Several schedule settings allow you to enter separate values for work hours and after-hours. Other settings apply all the time.

This setting is valid for all machine types.

Disconnect desktop sessions when idle How long a desktop can remain idle (not used) before the session is disconnected. After a session is disconnected, the user must go to Workspace and start a desktop again. This is a security setting.

This setting is valid for all machine types. One setting applies all the time.

Power off idle desktops How long a machine can remain disconnected before it is powered off. After a machine is powered off, the user must go to Workspace and start a desktop again. This is a power-saving setting.

For example, let's say you want desktops to disconnect after they have been idle for 10 minutes. Then, power off the machines if they remain disconnected for another 15 minutes.

If Tom stops using his desktop and walks away for a one-hour meeting, the desktop will be disconnected after 10 minutes. After another 15 minutes, the machine will be powered off (25 minutes total).

From a user standpoint, the two idle settings (disconnect and power-off) have the same effect. If Tom stays away from his desktop for 12 minutes or an hour, he must start a desktop again from Workspace. The difference in the two timers affects the state of the virtual machine providing the desktop.

This setting is valid for single-session (static or random) machines. You can enter values for work hours and after-hours.

Log off disconnected sessions How long a machine can remain disconnected before the session is closed.

This setting is valid for multi-session machines. One setting applies all the time.

Power-off delay The minimum amount of time a machine must be powered-on before it is eligible for power-off (along with other criteria). This setting keeps machines from "flip-flopping"on and off during volatile session demands.

This setting is valid for multi-session machines, and applies all the time.

Minimum running machines How many machines must remain powered-on, regardless of how long they are idle or disconnected.

This setting is valid for random and multi-session machines. You can enter values for work hours and after-hours.

Capacity buffer A capacity buffer helps accommodate sudden spikes in demand, by keeping a buffer of machines powered-on. The buffer is specified, as a percentage of current session demand. For example, if there are 100 active sessions and the capacity buffer is 10%, Citrix DaaS provides capacity for 110 sessions. A spike in demand might occur during work hours or adding new machines to the catalog.

A lower value decreases the cost. A higher value helps ensure an optimized user experience. When launching sessions, users do not have to wait for extra machines to power on.

When there are more than enough machines to support the number of powered-on machines needed in the catalog (including the capacity buffer), extra machines are powered off. Power-off might occur because of off-peak time, session logoffs, or fewer machines in the catalog. The decision to power off a machine must meet the following criteria:

- The machine is powered on and not in maintenance mode.
- The machine is registered as available or waiting to register after power-on.
- The machine has no active sessions. Any remaining sessions have ended. (The machine was idle for the idle timeout period.)
- The machine has been powered on for at least "X"minutes, where "X"is the power-off delay specified for the catalog.

  In a static catalog, after all machines in the catalog are assigned, the capacity buffer does not play a role in powering machines on or off.

This setting is valid for all machine types. You can enter values for work hours and after-hours.

Create a power management schedule

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.
2. On the **Power Management** tab, determine whether any of the preset schedules (in the menu at the top) meet your needs. Select a preset to see the values it uses. If you want to use a preset, leave it selected.
3. If you change the values in any fields (such as days, times, or intervals), the preset selection changes to **Custom** automatically. An asterisk indicates that custom settings have not been saved.

4. Set the values you want for the custom schedule.
5. Select **Custom** at the top, and then save the current settings as a new preset. Enter a name for the new preset and select the check mark.
6. When you're done, select **Save Changes**.

Later, you can edit or delete a custom preset by using the pencil or trash icons in the **Presets** menu. You cannot edit or delete common presets.

Related information

- Update a catalog with a new image
- Add and remove users in a catalog

Azure subscriptions in Quick Deploy

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Introduction

When you create a catalog or build an image in Quick Deploy, you choose among the available Azure subscriptions. Quick Deploy supports both Citrix Managed Azure subscriptions and your own, customer-managed Azure subscriptions.

- To use your own Azure subscription, you first import (add) one or more of those subscriptions to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). That action enables Citrix DaaS to access your Azure subscriptions.
- Using a Citrix Managed Azure subscription requires no subscription configuration. However, a Citrix Managed Azure subscription is available only when you order the Citrix Azure Consumption Fund, in addition to Citrix DaaS.

Some Citrix DaaS features differ, depending on whether the catalog uses a Citrix Managed Azure subscription or in your own Azure subscription.

Citrix Managed Azure subscription	Your own Azure subscription
Supports domain-joined or non-domain-joined machines.	Supports only domain-joined machines.
Supports quick create and custom create catalogs.	Supports only custom create catalogs.
Always available when creating catalogs and images.	Must add the Azure subscription to Citrix DaaS before creating a catalog.
For user authentication, supports Citrix Managed Azure Active Directory or your own Active Directory.	Can connect your own Active Directory and Azure Active Directory.
Network connection options include **No connectivity**.	Network connection options include only your own virtual networks.
When using Azure VNet peering to connect to your resources, you must create a VNet peer connection in Citrix DaaS.	Select an existing virtual network.
When importing an image from Azure, you specify the image's URI.	When importing an image, you can select a VHD or browse storage in the Azure subscription.
Can create a bastion machine in customer's Azure subscription to troubleshoot machines.	No need to create a bastion machine because you can already access the machines in your subscription.

View Azure subscriptions

To view Azure subscription details, from **Manage > Quick Deploy**, expand **Cloud Subscriptions** on the right. Then select a subscription entry.

- The **Details** page includes the number of machines, plus the numbers and names of catalogs and images using the subscription.
- The **Resource Locations** page lists the resource locations where the subscription is used.

Add customer-managed Azure subscriptions

To use a customer-managed Azure subscription, you must add it to Citrix DaaS before creating a catalog or building an image that uses that subscription. You have two options when adding your Azure subscriptions:

- **If you are a Global Administrator for the directory and have owner permissions for the subscription:** Simply authenticate to your Azure account.

- **If you are not a Global Administrator and have owner permissions on the subscription:** Before adding the subscription to Citrix DaaS, create an Azure app in your Azure AD and then add that app as a contributor of the subscription. When you add that subscription to Citrix DaaS, you provide relevant app information.

Add customer-managed Azure subscriptions if you're a Global Administrator

This task requires Global Administrator permissions for the directory, and owner permissions for the subscription.

1. From **Manage > Quick Deploy**, expand **Cloud Subscriptions** on the right.
2. Select **Add Azure subscription**.
3. On the **Add Subscriptions** page, select **Add your Azure subscription**.
4. Select the button that allows Citrix DaaS to access your Azure subscriptions on your behalf.
5. Select **Authenticate Azure Account**. You're taken to the Azure sign-in page.
6. Enter your Azure credentials.
7. You're returned automatically to Citrix DaaS. The **Add Subscription** page lists the discovered Azure subscriptions. Use the search box to filter the list, if needed. Select one or more subscriptions. When you're done, select **Add Subscriptions**.
8. Confirm that you want to add the selected subscriptions.

The Azure subscriptions you selected are listed when you expand **Subscriptions**. The added subscriptions are available for selection when you create a catalog or image.

Add customer-managed Azure subscriptions if you're not a Global Administrator

Adding an Azure subscription when you're not a global administrator is a two-part process:

- Before you add a subscription to Citrix DaaS, create an app in Azure AD and then add that app as a contributor of the subscription.
- Add the subscription to Citrix DaaS, using information about the app you created in Azure.

Create an app in Azure AD and add it as a contributor

1. Register a new application in Azure AD:
    a) From a browser, navigate to https://portal.azure.com.
    b) In the upper left menu, select **Azure Active Directory**.
    c) In the **Manage** list, select **App registrations**.
    d) Select **+ New registration**.

e) On the **Register an application** page, provide the following information:

- **Name:** Enter the connection name
- **Application type:** Select **Web app / API**
- **Redirect URI:** leave blank

f) Select **Create**.

2. Create the application's secret access key and add the role assignment:

a) From the previous procedure, select **App Registration** to view details.

b) Make a note of the **Application ID** and **Directory ID**. You'll use this later when adding your subscription to Citrix DaaS.

c) Under **Manage**, select **Certificates & secrets**.

d) On the **Client secrets** page, select **+ New client secret**.

e) On the **Add a client secret** page, provide a description and select an expiration interval. Then select **Add**.

f) Make a note of the client secret value. You'll use this later when adding your subscription to Citrix DaaS.

g) Select the Azure subscription you want to link (add) to Citrix DaaS, and then select **Access control (IAM)**.

h) In the **Add a role assignment** box, select **Add**.

i) On the **Add role assignment** tab, select the following:

- **Role:** Contributor
- **Assign access to:** Azure AD user, group, or service principal
- **Select:** The name of the Azure app you created earlier.

j) Select **Save**.

Add your subscription to Citrix DaaS You need the application ID, directory ID, and client secret value from the app you created in Azure AD.

1. From **Manage > Quick Deploy**, expand **Cloud Subscriptions** on the right.
2. Select **Add Azure subscription**.
3. On the **Add Subscriptions** page, select **Add your Azure subscriptions**.
4. Select **I have an Azure App with contributor role to the subscription**.
5. Enter the tenant ID (directory ID), client ID (application ID), and client secret for the app you created in Azure.
6. Select **Select your subscription** and then select the subscription you want.

Later, from the subscription's **Details** page in Citrix DaaS dashboard, you can update the client secret or replace the Azure app from the ellipsis menu.

If Citrix DaaS can't access an Azure subscription after it's added, several catalog power management and individual machine actions aren't allowed. A message provides an option to add the subscription again. If the subscription was originally added using an Azure app, you can replace the Azure app.

Add Citrix Managed Azure subscriptions

A Citrix Managed Azure subscription supports a certain number of machines. (In this context, *machines* refers to VMs that have a Citrix VDA installed. These machines deliver apps and desktops to users. It does not include other machines in a resource location, such as Cloud Connectors.)

If your Citrix Managed Azure subscription is likely to reach its limit soon, and you have enough Citrix licenses, you can request another Citrix Managed Azure subscription. The dashboard contains a notification when you're close to the limit.

You can't create a catalog (or add machines to a catalog) if the total number of machines for all catalogs that use that Citrix Managed Azure subscription would exceed the limit.

For example, assume a hypothetical limit of 1,000 machines per Citrix Managed Azure subscription.

- Let's say you have two catalogs (`Cat1` and `Cat2`) that use the same Citrix Managed Azure subscription. `Cat1` currently contains 500 machines, and `Cat2` has 250.
- As you plan for future capacity needs, you add 200 machines to `Cat2`. The Citrix Managed Azure subscription now supports 950 machines (500 in `Cat 1` and 450 in `Cat 2`). The dashboard indicates that the subscription is near its limit.
- When you need 75 more machines, you can't use that subscription to create a catalog with 75 machines (or add 75 machines to an existing catalog). That would exceed the subscription limit. Instead, you request another Citrix Managed Azure subscription. Then, you can create a catalog using that subscription.

When you have more than one Citrix Managed Azure subscription:

- Nothing is shared between those subscriptions.
- Each subscription has a unique name.
- You can choose among the Citrix Managed Azure subscriptions (and any customer-managed Azure subscriptions that you've added) when:
  - Creating a catalog.
  - Building or importing an image.
  - Creating a VNet peering or SD-WAN connection.

Requirement:

- You must have enough Citrix licenses to warrant adding another Citrix Managed Azure subscription. Using the previous hypothetical example, if you have 2,000 Citrix licenses in anticipation of deploying at least 1,500 machines through Citrix Managed subscriptions, you can add another Citrix Managed Azure subscription.

To add a Citrix Managed Azure subscription:

1. Contact your Citrix representative to request another Citrix Managed Azure subscription. You are notified when you can proceed.
2. From **Manage > Quick Deploy**, expand **Cloud Subscriptions** on the right.
3. Select **Add Azure subscription**.
4. On the **Add Subscriptions** page, select **Add a Citrix Managed Azure subscription**.
5. On the **Add a Citrix Managed Subscription** page, select **Add Subscription** at the bottom of the page.

If you're notified that an error occurred during creation of a Citrix Managed Azure subscription, contact Citrix Support.

Remove Azure subscriptions

Before you can remove an Azure subscription, you must delete all catalogs and images that use it.

If you have one or more Citrix Managed Azure subscriptions, you cannot remove all of them. At least one must remain.

1. From **Manage > Quick Deploy**, expand **Cloud Subscriptions** on the right.
2. Select the subscription entry.
3. On the **Details** tab, select **Remove Subscription**.
4. Select **Authenticate Azure Account**. You're taken to the Azure sign-in page.
5. Enter your Azure credentials.
6. You're returned automatically to Citrix DaaS. Confirm the deletion and then select **Yes, Delete Subscription**.

Update expired client secrets

When the client secret of a subscription expires, you can't create machine catalogs for it and an alert appears in the subscription's entry. To resolve this issue, you have two choices:

- Update the client secret of the Azure app in use
- Switch to an Azure app with a valid expiration date

Update the client secret of the Azure app in use

To continue using the existing Azure app to access Azure resources, follow these steps:

1. In Azure, create a client secret for the Azure app in use. Note down the new secret and expiration date for future use. For more information, see Create an application secret in Azure.
2. In DaaS, provide the newly created secret information to the subscription. Detailed steps are as follows:

    a) From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right.
    b) Click the subscription that needs secret updates.
    c) On the subscription page that appears, click the ellipsis menu in the **Azure App Details** pane, and then select **Update Client Secret**.
    d) On the **Update Client Secret** page, type the new **Client Secret** and **Secret Expiration Date**.
    e) Click **Update Secret**.

Switch to an Azure app with a valid expiration date

To switch to a valid Azure app to access Azure resources, get the necessary app information and provide it to the subscription using the following steps:

1. In Azure, get a valid Azure app and note down its details. Make sure that the new Azure app is assigned *Contributor* role. For more information, see Create an app in Azure AD and add it as a contributor.
2. In DaaS, provide details of the Azure app to the subscription. Detailed steps are as follows:

    a) From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right.
    b) Click the subscription that needs secret updates.
    c) On the subscription page that appears, click the ellipsis menu in the **Azure App Details** pane, and then select **Replace Azure App.**
    d) On the **Replace Azure App** page, type the new Azure app details in the corresponding fields for **Directory (tenant) ID**, **Application (client) ID**, **Client Secret**, and **Secret Expiration Date for the service principal**.
    e) Click **Replace App**.

Images in Quick Deploy

April 12, 2024

When you create a catalog to deliver desktops or apps, an image is used (with other settings) as a template for creating the machines.

Quick Deploy provides a set of prepared images that you can choose from to build and customize an image in Quick Deploy. You can also import (add) images from your own Azure subscription.

Citrix prepared images

Quick Deploy provides several Citrix prepared images:

- Windows 11 Pro (single-session)
- Windows 11 Enterprise Virtual Desktop (multi-session)
- Windows 11 Enterprise Virtual Desktop (multi-session) with Office 365 ProPlus
- Windows 10 Pro (single-session)
- Windows 10 Enterprise Virtual Desktop (multi-session)
- Windows 10 Enterprise Virtual Desktop (multi-session) with Office 365 ProPlus
- Windows Server 2022 (multi-session)
- Windows Server 2019 (multi-session)
- Windows Server 2016 (multi-session)
- Linux Ubuntu 22.04 LTS (single-session)
- Linux Ubuntu 22.04 LTS (multi-session)

The Citrix prepared images have a current Citrix Virtual Delivery Agent (VDA) and troubleshooting tools installed. The VDA is the communication mechanism between your users' machines and the Citrix Cloud infrastructure that manages Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Images provided by Citrix have a **CITRIX** notation.

Citrix prepared images are not available in Citrix DaaS's Full Configuration interface.

You can also import and use your own image from Azure.

Ways to use images in Quick Deploy

You can:

- **Use a Citrix prepared image when creating a catalog.** This choice is recommended only for proof of concept deployments.

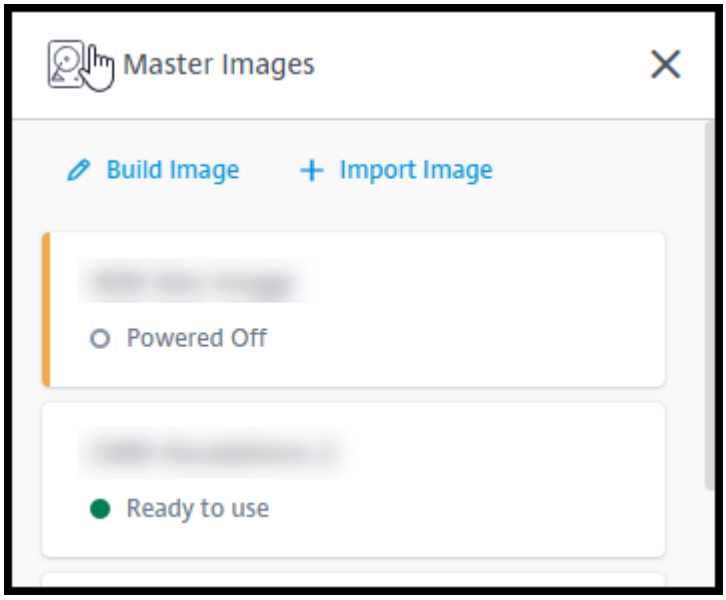
- **Use a Citrix prepared image to create another image.** After the new image created, you customize it by adding applications and other software that your users need. Then, you can use that customized image when creating a catalog.
- **Import an image from Azure.** After you import an image from Azure, you can then use that image when creating a catalog.

  Or, you can use that image to create a new image, and then customize it by adding apps. Then, you can use that customized image when creating a catalog.

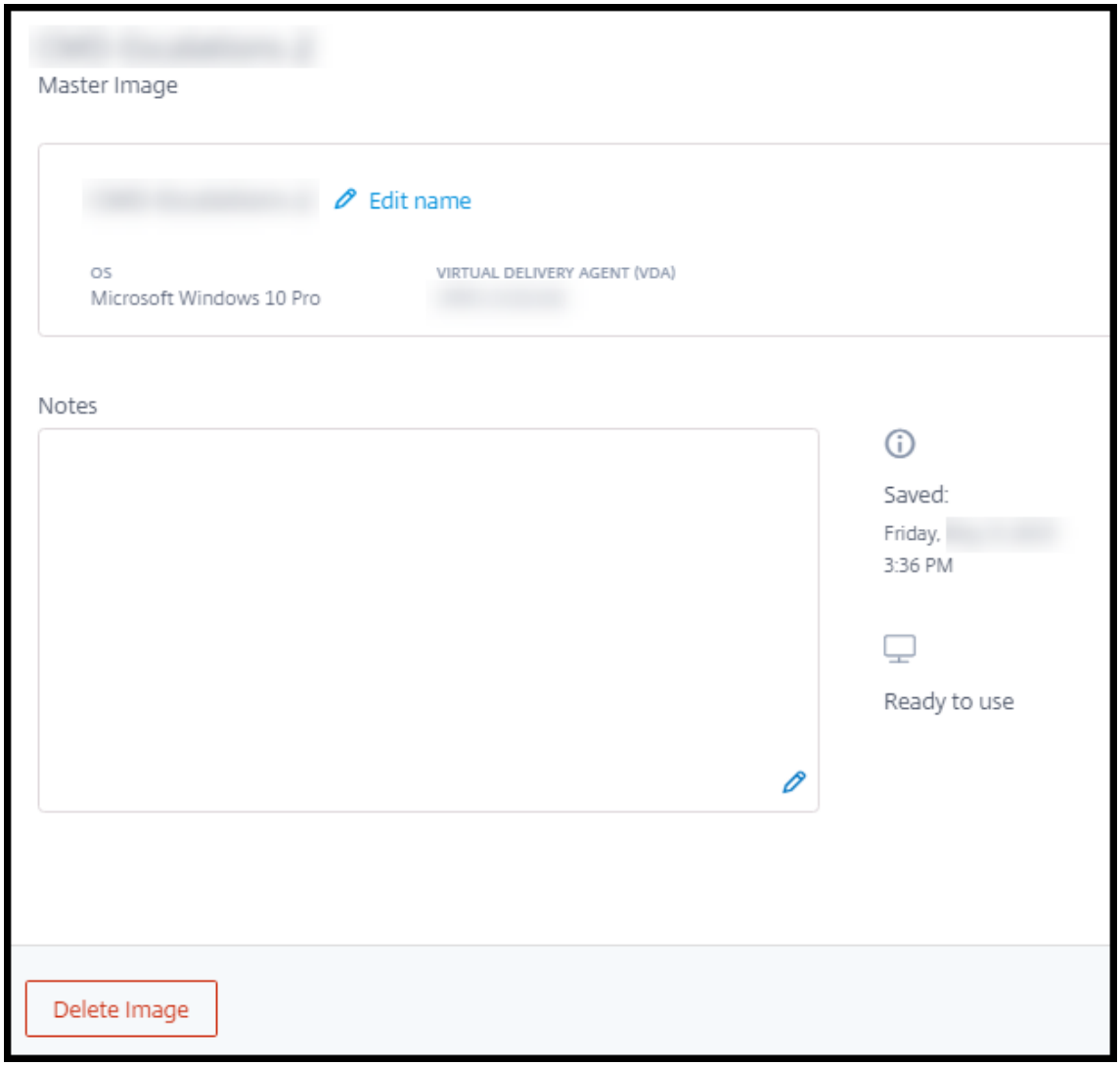
When you create a catalog, Citrix DaaS verifies that the image uses a valid operating system, and has a Citrix VDA and troubleshooting tools installed (along with other checks).

Display image information

1. From **Manage > Quick Deploy**, expand **Master Images** on the right. The display lists the Citrix prepared images, and any images you imported.



2. Select an image to display its details.



From the details card, you can:

- Change (edit) the image's name.
- Add and edit notes (available only for images you prepared or imported, not Citrix prepared images).
- Delete the image.

Prepare a new image

Preparing a new image includes creating the image and then customizing it. When you create an image, a new VM is created to load the new image.

Requirements:

- Know the performance characteristics that the machines need. For example, running CAD apps might require different CPU, RAM, and storage than other office apps.

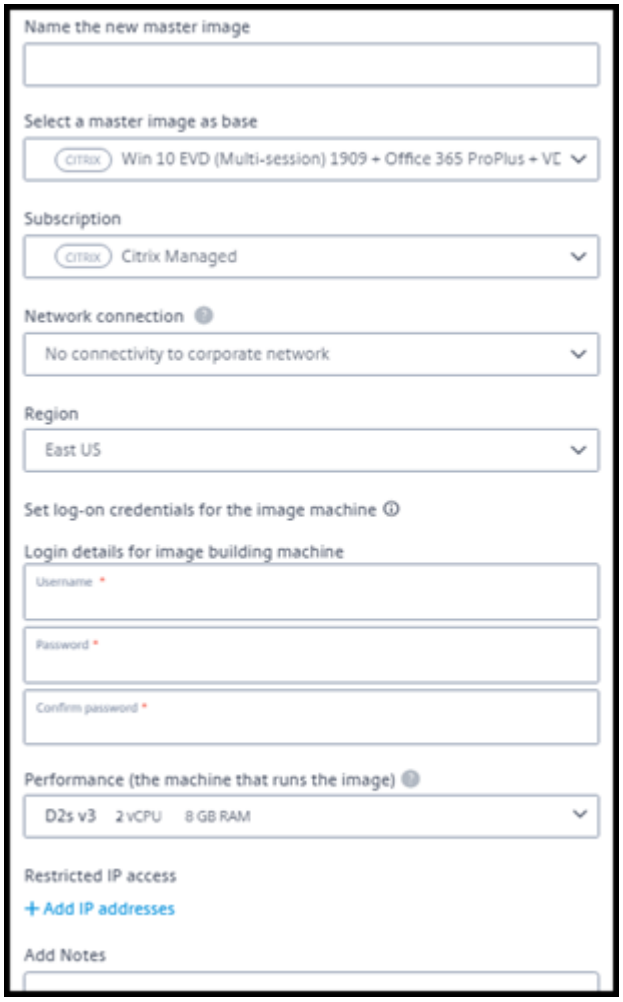
- If you plan to use a connection to your on-premises resources, set up that connection before creating the image and the catalog. For details, see Network connections.

When using a Citrix prepared Ubuntu image to build a new image, a root password is created for the new image. You can change that root password, but only during the image creation and customization process. (You cannot change the root password after the image is used in a catalog.)

- When the image is created, the administrator account that you specified (**Login details for image building machine**) is added to the `sudoers` group.
- After you RDP to the machine containing the new image, launch the terminal application and type `sudo passwd root`. When prompted, provide the password you specified when creating the image. After verification, you're prompted to enter a new password for the root user.

To create an image:

1. From **Manage > Quick Deploy**, expand **Master Images** on the right.
2. Select **Build Image**.



3. Enter values in the following fields:

- **Name:** Enter a name for the new image.
- **Master image:** Select an existing image. This is the base image that is used to create the new image.
- **Subscription:** Select an Azure subscription.
- **Network connection:**
  - If using a Citrix Managed Azure subscription, select **No connectivity** or a previously created connection.
  - If using your own customer-managed Azure subscription, select your resource group, virtual network, and subnet. Then add domain details: FQDN, OU, Citrix DaaS account name, and credentials.
- **Region:** (Available only for **No connectivity**.) Select a region where you want the machine containing the image to be created.
- **Logon credentials for image machine:** You'll use these credentials later when you connect (RDP) to the machine containing the new image, so that you can install apps and other software.
- **Machine performance:** This is CPU, RAM, and storage information for the machine that runs the image. Select a machine performance that meets your apps' requirements.
- **Restricted IP access:** If you want to restrict access to specific addresses, select **Add IP addresses** and then enter one or more addresses. After adding the addresses, select **Done** to return to the **Build image** card.
- **Notes:** Optionally add up to 1024 characters of notes. After the image is created, you can update the notes from the image's details display.
- **Local domain join:** Indicate whether you want to join the local Active Directory domain.
  - If you select **Yes**, enter the FQDN, OU, Citrix DaaS account name, and credentials.
  - If you select **No**, enter the credentials for the host machine.

4. When you're done, select **Build Image**.

An image can take up to 30 minutes to build. From **Manage > Quick Deploy**, expand **Master Images** on the right to see the current state (such as `Building image` or `Ready to customize`).

What to do next: Connect to a new image and customize it.

Connect to a new image and customize it

After a new image is created, its name is added to the images list, with a status of `Ready to customize` (or similar wording). To customize that image, you first download an RDP file. When

you use that file to connect to the image, you can then add applications and other software to the image.

1. From **Manage > Quick Deploy**, expand **Master Images** on the right. Select the image you want to connect to.
2. Select **Download RDP file**. An RDP client downloads.

   The image machine might power off if you do not RDP to it shortly after it's created. This saves costs. When that happens, select **Power On**.
3. Start the downloaded RDP client. It automatically attempts to connect to the address of the machine containing the new image. When prompted, enter the credentials you specified when creating the image.
4. After you connect to the machine, add or remove apps, install updates, and finish any other customization work.

   Do **NOT** Sysprep the image.
5. When you're done customizing the new image, return to the **Master Images** box and select **Finish build**. The new image automatically undergoes validation testing.

Later, when you create a catalog, the new image is included in the list of images you can select.

From **Manage > Quick Deploy**, the image display on the right indicates how many catalogs and machines use each image.

> **Note:**
>
> After you finalize an image, you cannot edit it. You must create a new image (optionally using the previous image as a starting point), and then update the new image.

Import an image from Azure

When you import an image from Azure that has a Citrix VDA and applications your users need, you can use it to create a catalog or replace the image in an existing catalog.

Imported image requirements

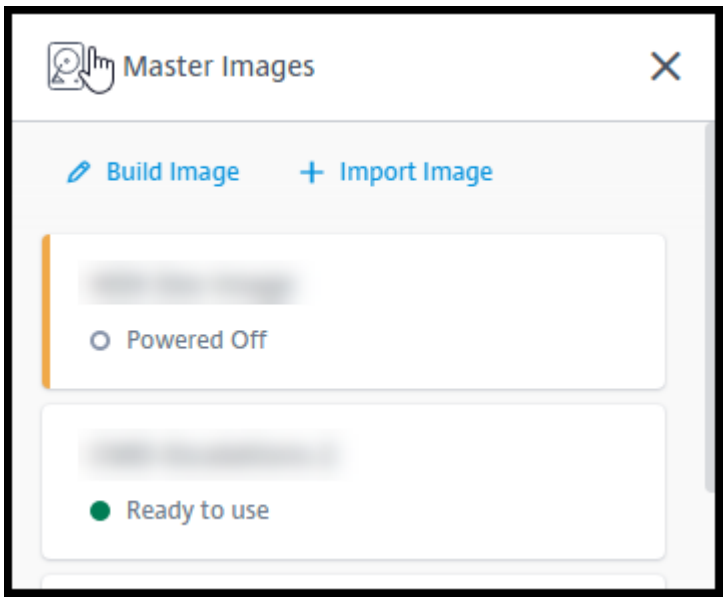
Citrix runs validation tests on the imported image. Ensure that the following requirements are met when you prepare the image that you'll import into Citrix DaaS.

- **Supported OS:** The image must be a supported OS. To check a Windows OS version, run `Get-WmiObject Win32_OperatingSystem`.

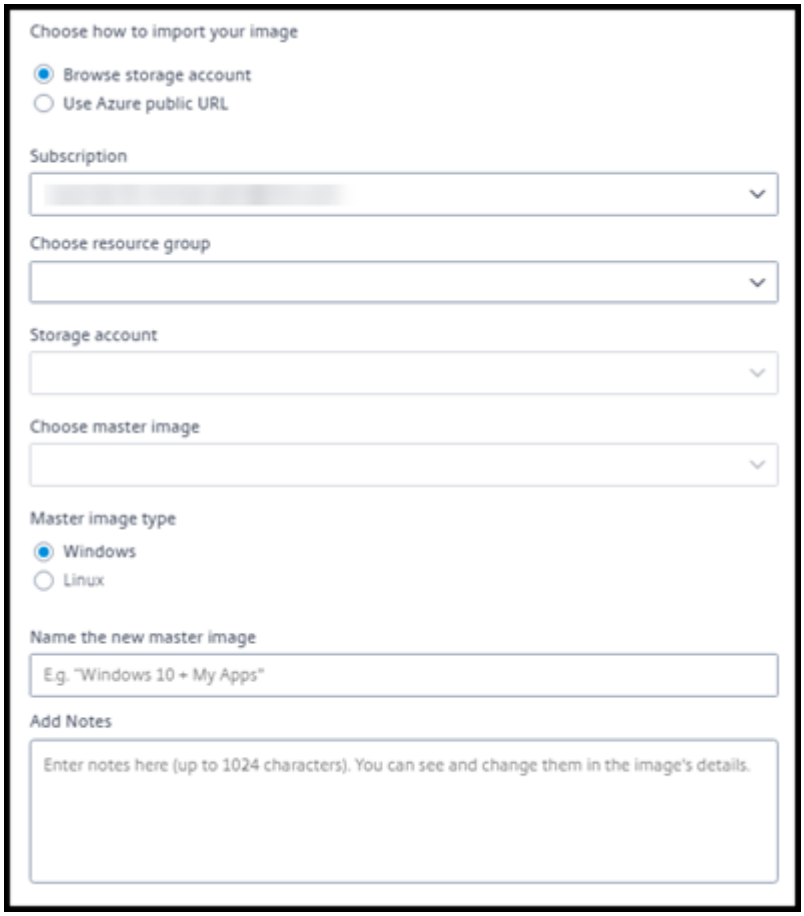
- **Supported generation:** Generation 1 virtual machines support most guest operating systems. Generation 2 virtual machines support most 64-bit versions of Windows and more current version of Linux operating systems.
- **Not generalized:** The image must not be generalized.
- **No configured Delivery Controllers:** Ensure that no Citrix Delivery Controllers are configured in the image. Ensure that the following registry keys are cleared.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Personality.ini file:** The `personality.ini` file must exist on the system drive.
- **Valid VDA:** The image must have a Citrix VDA newer than 7.11 installed.
  - Windows: To check, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. For installation guidance, see Install a Windows VDA on an image.
  - Red Hat Enterprise Linux and Ubuntu: For installation guidance, see the product documentation.
- **Azure Virtual Machine Agent:** Before importing an image, make sure that the Azure Virtual Machine Agent is installed on the image. For more information, see the Microsoft article Azure Virtual Machine Agent overview.

Import the image using Quick Deploy

1. From **Manage > Quick Deploy**, expand **Master Images** on the right.



2. Select **Import Image**.



3. Choose how to import the image.

   - For managed disks, use the export feature to generate a SAS URL. Set the expiration time

to 7200 seconds or more.
- For VHDs in a storage account, choose one of the following:
  - Generate a SAS URL for the VHD file.
  - Update the access level of a block storage container to blob or container. Then, get the file's URL.

4. If you selected **Browse storage account**:
   a) Sequentially select a subscription > resource group > storage account > image.
   b) Name the image.
5. If you selected **Azure public URL**:
   a) Enter the Azure-generated URL for the VHD. For guidance, select the link to the Microsoft document Download a Windows VHD from Azure.
   b) Select a subscription. (A Linux image can be imported only if you select a customer-managed subscription.)
   c) Name the image.
6. When you're done, select **Import Image**.

Update a Quick Deploy catalog with a new image

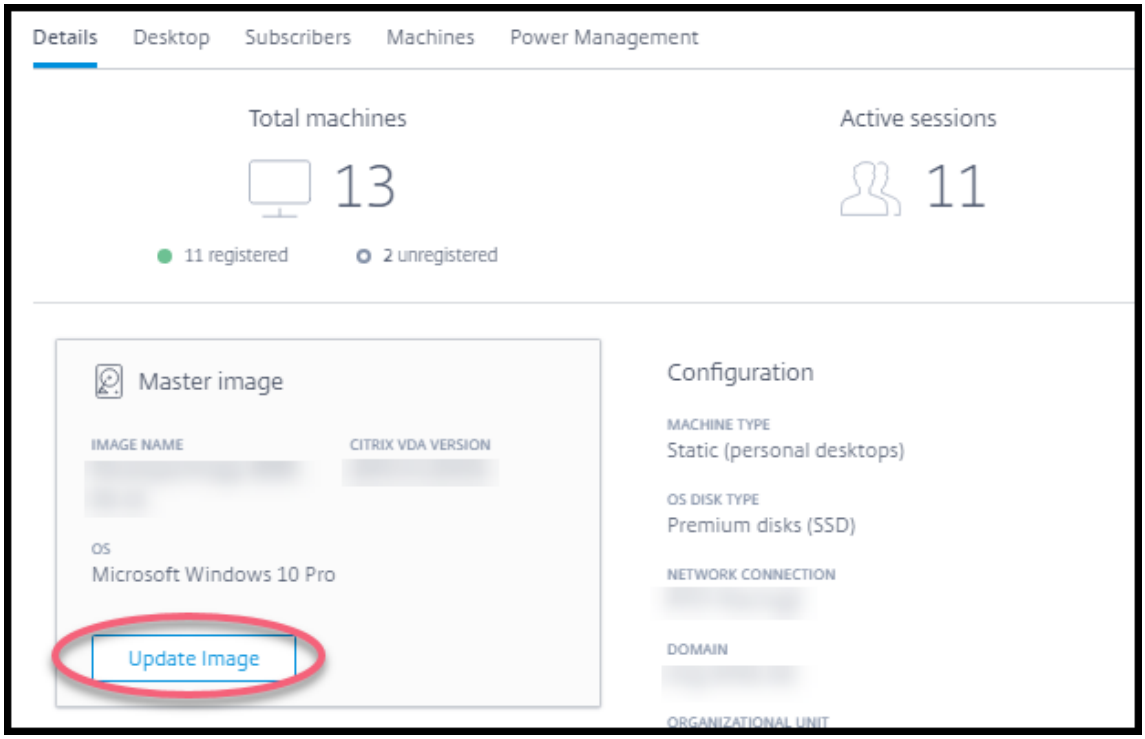
The catalog type determines which machines are updated when you update the catalog.

- For a random catalog, all the machines currently in the catalog are updated with the latest image. If you add more desktops to that catalog, they are based on the latest image.
- For a static catalog, the machines currently in the catalog are not updated with the latest image. Machines currently in the catalog continue to use the image they were created from. However, if you add more machines to that catalog, they are based on the latest image.

You can update a catalog containing machines with gen1 images with a gen2 image, if the catalog's machines support gen2. Similarly, you can update a catalog containing gen2 machines with a gen1 image, if the catalog's machines support gen1.

To update a catalog with a new image:

1. From **Manage > Quick Deploy**, click anywhere in the catalog's entry.
2. On the **Details** tab, select **Update Image**.



3. Select an image.
4. For random or multi-session catalogs: Select a logoff interval. After Citrix DaaS completes the initial image processing, subscribers receive a warning to save their work and log off from their desktops. The logoff interval indicates how long subscribers have after receiving the message until the session ends automatically.
5. Select **Update Image**.

Delete an image from Quick Deploy

1. From **Manage > Quick Deploy**, expand **Master Images** on the right.
2. Select the image you want to delete.
3. Select **Delete Image** at the bottom of the card. Confirm the deletion.

Install a Windows VDA on an image

Use the following procedure when preparing a Windows image that you plan to import into Citrix DaaS.

For Linux VDA installation guidance, see the Linux VDA product documentation.

1. In your Azure environment, connect to the image VM (if you're not already connected).

2. You can download a VDA by using the **Downloads** link on the Citrix Cloud navigation bar. Or, use a browser to navigate to Citrix DaaS download page.

   Download a VDA onto the VM. There are separate VDA download packages for a desktop (single-session) OS and a server (multi-session) OS.

3. Launch the VDA installer by double-clicking the downloaded file. The installation wizard launches.
4. On the **Environment** page, select the option to create an image using MCS, and then select **Next**.
5. On the **Core Components** page, select **Next**.
6. On the **Delivery Controller** page, select **Let Machine Creation Services do it automatically** and then select **Next**. Confirm your selection, if prompted.
7. Leave the default settings on the **Additional Components**, **Features**, and **Firewall** pages, unless Citrix instructs you otherwise. Select **Next** on each page.
8. On the **Summary** page, select **Install**. Prerequisites begin to install. When prompted to restart, agree.
9. The VDA installation resumes automatically. Prerequisite installation completes and then the components and features are installed. On the **Call Home** page, leave the default setting (unless Citrix instructs you otherwise). After you connect, select **Next**.
10. Select **Finish**. The machine restarts automatically.
11. To ensure that the configuration is correct, launch one or more of the applications you installed on the VM.
12. Shut down the VM. Do not Sysprep the image.

For more information about installing VDAs, see Install VDAs.

Network connections in Quick Deploy

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Introduction

This article provides details about how to create network connections to your corporate resources when using a Citrix Managed Azure subscription.

When using your own customer-managed Azure subscription, there is no need to create a network connection.

When creating a Quick Deploy catalog, you indicate if and how users access locations and resources on their corporate on-premises network from their Citrix desktops and apps. When using a connection, you must create the connection before creating the catalog.

When using a Citrix Managed Azure subscription, the choices are:

- No connectivity
- Azure VNet peering
- SD-WAN

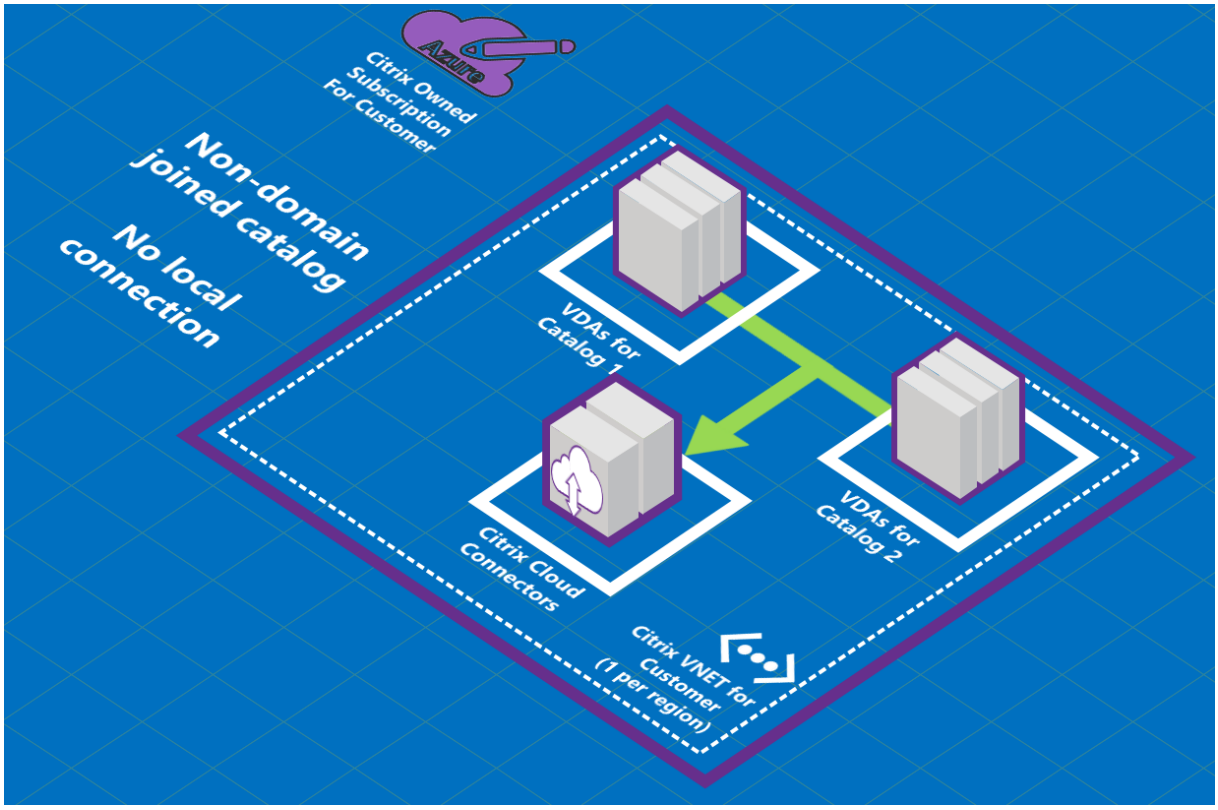
You cannot change a catalog's connection type after the catalog is created.

Requirements for all network connections

- When creating a connection, you must have valid DNS server entries.
- When using Secure DNS or a third-party DNS provider, you must add the address range that is allocated for use by Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) to the DNS provider's IP addresses on the allow list. That address range is specified when you create a connection.
- All service resources that use the connection (domain-joined machines) must be able to reach your Network Time Protocol (NTP) server, to ensure time synchronization.

No connectivity

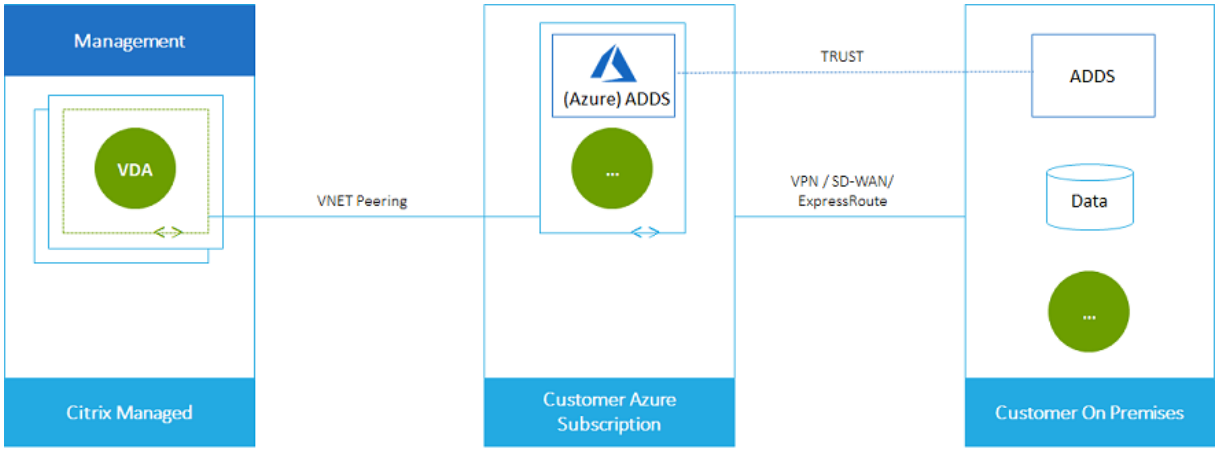
When a catalog is configured with **No connectivity**, users cannot access resources on their on-premises or other networks. This is the only choice when creating a catalog using quick create.



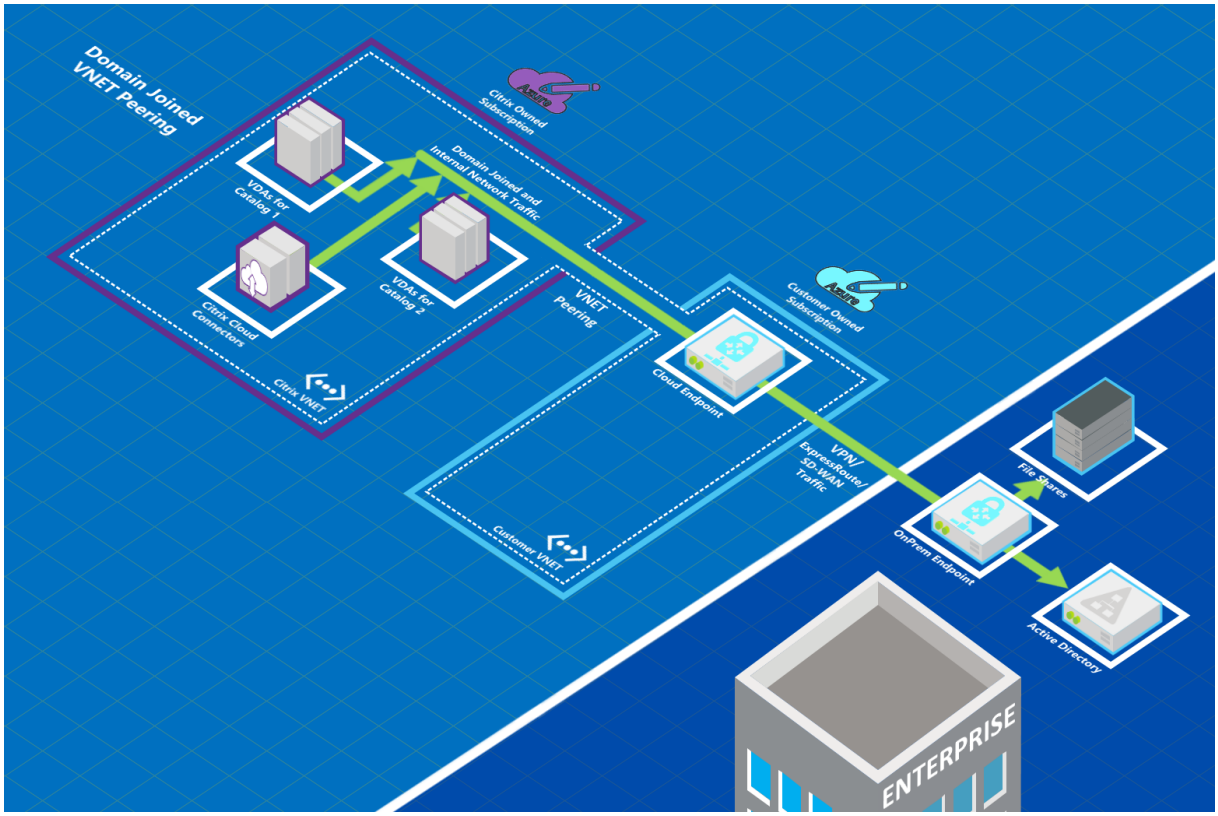
About Azure VNet peering connections

Virtual network peering seamlessly connects two Azure virtual networks (VNets): yours and Citrix DaaS VNet. Peering also helps enable users to access files and other items from your on-premises networks.

As shown in the following graphic, you create a connection using Azure VNet peering from the Citrix Managed Azure subscription to the VNet in your company's Azure subscription.



Here's another illustration of VNet peering.



Users can access their network resources (such as file servers) by joining the local domain when you create a catalog. (That is, you join the AD domain where file shares and other needed resources reside.) Your Azure subscription connects to those resources (in the graphics, using a VPN or Azure ExpressRoute). When creating the catalog, you provide the domain, OU, and account credentials.

> **Important:**
>
> - Learn about Azure VNet peering before using it in this service.
> - Create a VNet peering connection before creating a catalog that uses it.

Azure VNet peering custom routes

Custom, or user-defined, routes override Azure's default system routes for directing traffic between virtual machines in a VNet peering, on-premises networks, and the Internet. You might use custom routes if there are networks that Citrix DaaS resources are expected to access but aren't directly connected through VNet peering. For example, you might create a custom route that forces traffic through a network appliance to the Internet or to an on-premises network subnet.

To use custom routes:

- You must have an existing Azure virtual network gateway or a network appliance such as Citrix SD-WAN in your Citrix DaaS environment.

- When you add custom routes, you must update your company's route tables with Citrix DaaS's destination VNet information to ensure end-to-end connectivity.
- Custom routes are displayed in Citrix DaaS in the order in which they are entered. This display order does not affect the order in which Azure selects routes.

Before using custom routes, review the Microsoft article Virtual network traffic routing to learn about using custom routes, next hop types, and how Azure selects routes for outbound traffic.

You can add custom routes when you create an Azure VNet peering connection or to existing ones in your Citrix DaaS environment. When you're ready to use custom routes with your VNet peering, refer to the following sections in this article:

- For custom routes with new Azure VNet peerings: Create an Azure VNet peering connection
- For custom routes with existing Azure VNet peerings: Manage custom routes for existing Azure VNet peer connections

Azure VNet peering requirements and preparation

- Credentials for an Azure subscription owner. This must be an Azure Active Directory account. This service does not support other account types, such as live.com or external Azure AD accounts (in a different tenant).
- An Azure subscription, resource group, and virtual network (VNet).
- Set up the Azure network routes so that VDAs in the Citrix Managed Azure subscription can communicate with your network locations.
- Open Azure network security groups from your VNet to the specified IP range.
- **Active Directory:** For domain-joined scenarios, we recommend that you have some form of Active Directory services running in the peered VNet. This takes advantage of the low latency characteristics of the Azure VNet peering technology.

  For example, the configuration might include Azure Active Directory Domain Services (AADDS), a domain controller VM in the VNet, or Azure AD Connect to your on-premises Active Directory.

  After you enable AADDS, you cannot move your managed domain to a different VNet without deleting the managed domain. So, it's important to select the correct VNet to enable your managed domain. Before proceeding, review the Microsoft article Networking considerations for Azure AD Domain Services.
- **VNet IP range:** When creating the connection, you must provide an available CIDR address space (IP address and network prefix) that is unique among the network resources and the Azure VNets being connected. This is the IP range assigned to the VMs within Citrix DaaS's peered VNet.

Ensure that you specify an IP range that does not overlap any addresses that you use in your Azure and on-premises networks.

- For example if your Azure VNet has an address space of 10.0.0.0 /16, create the VNet peering connection in Citrix DaaS as something such as 192.168.0.0 /24.
- In this example, creating a peering connection with a 10.0.0.0 /24 IP range would be considered an overlapping address range.

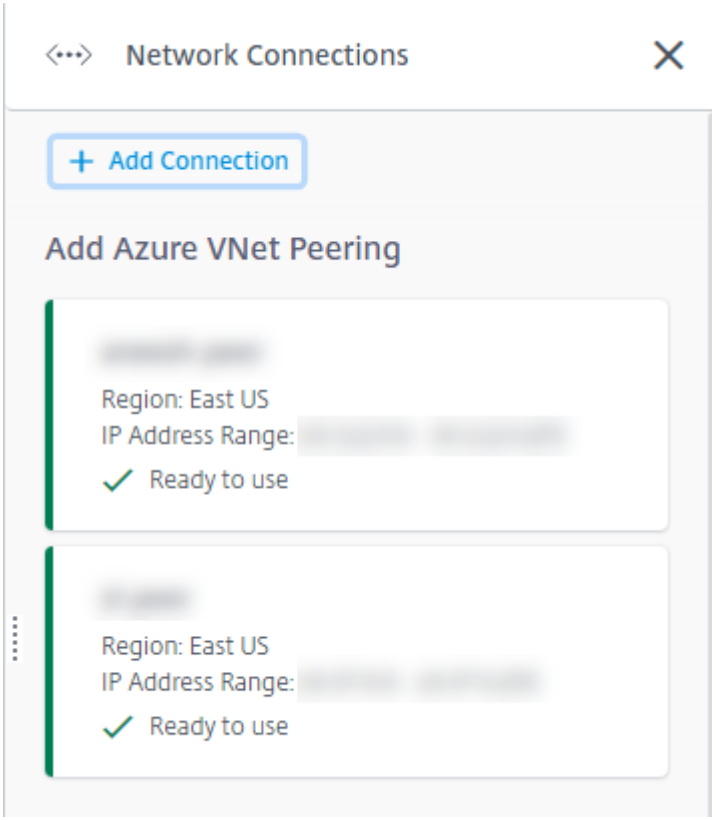
If addresses overlap, the VNet peering connection might not be created successfully. It also does not work correctly for site administration tasks.

To learn about VNet peering, see the following Microsoft articles.

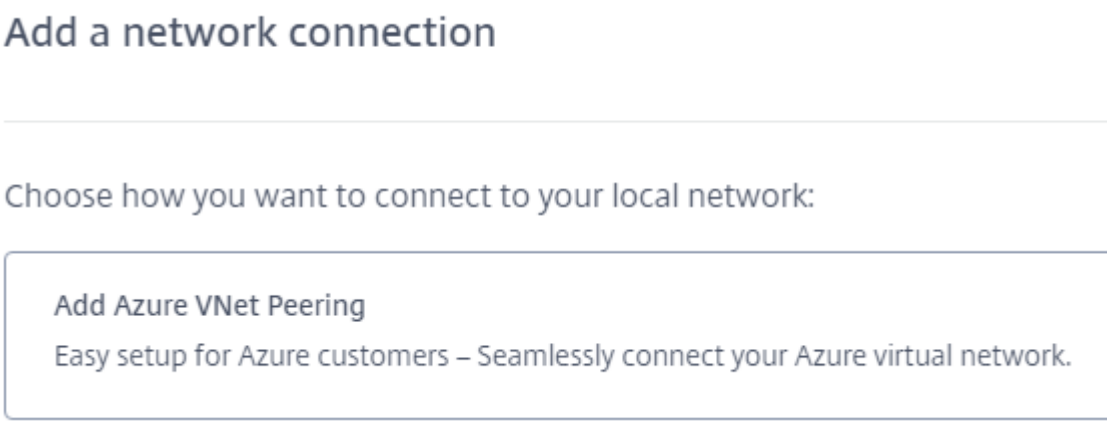
- Virtual network peering
- Azure VPN Gateway
- Create a Site-to-Site connection in the Azure portal
- VPN Gateway FAQ (search for "overlap")

Create an Azure VNet peering connection

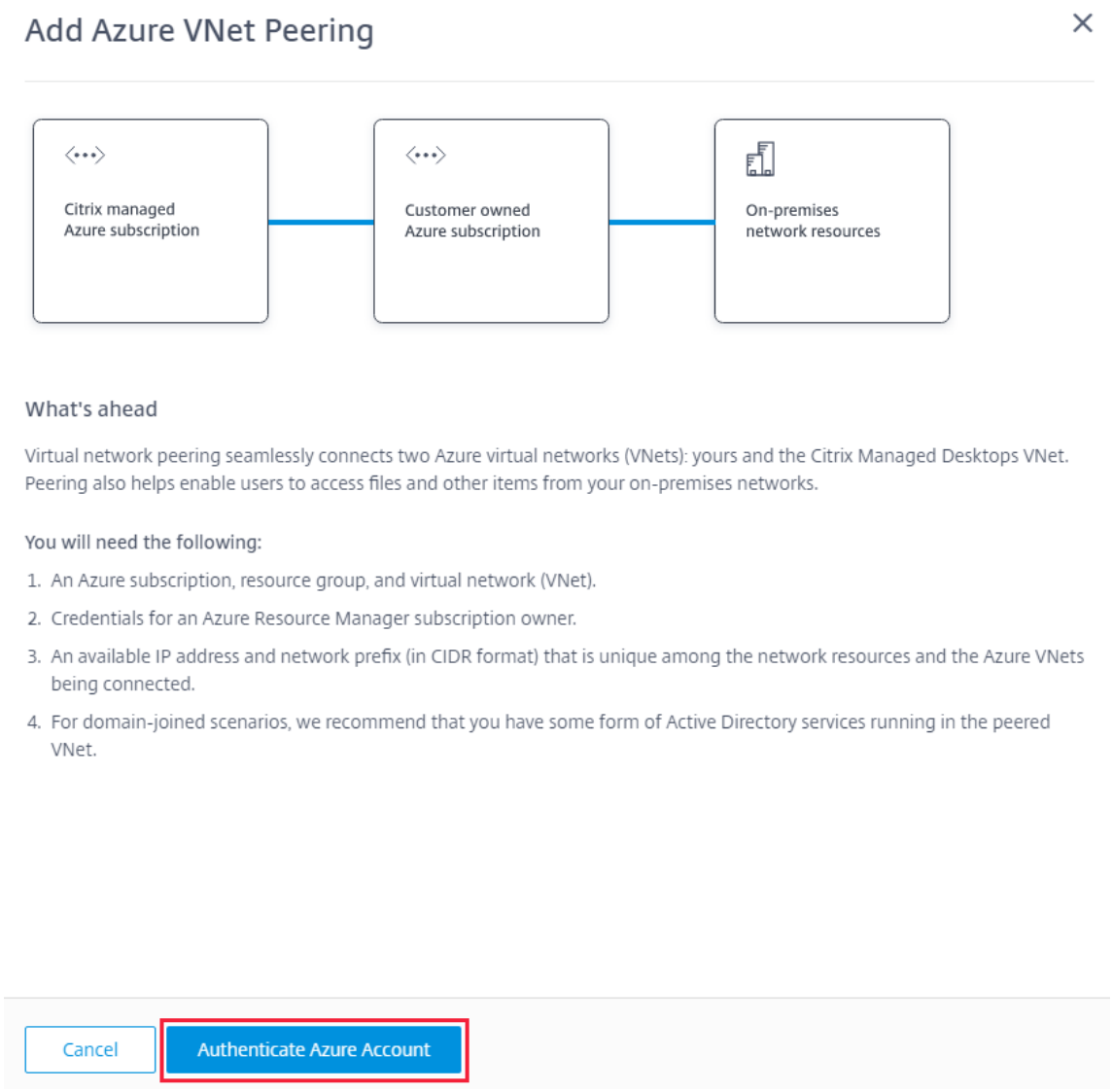
1. From **Manage > Quick Deploy**, expand **Network Connections** on the right. If you have already set up connections, they're listed.



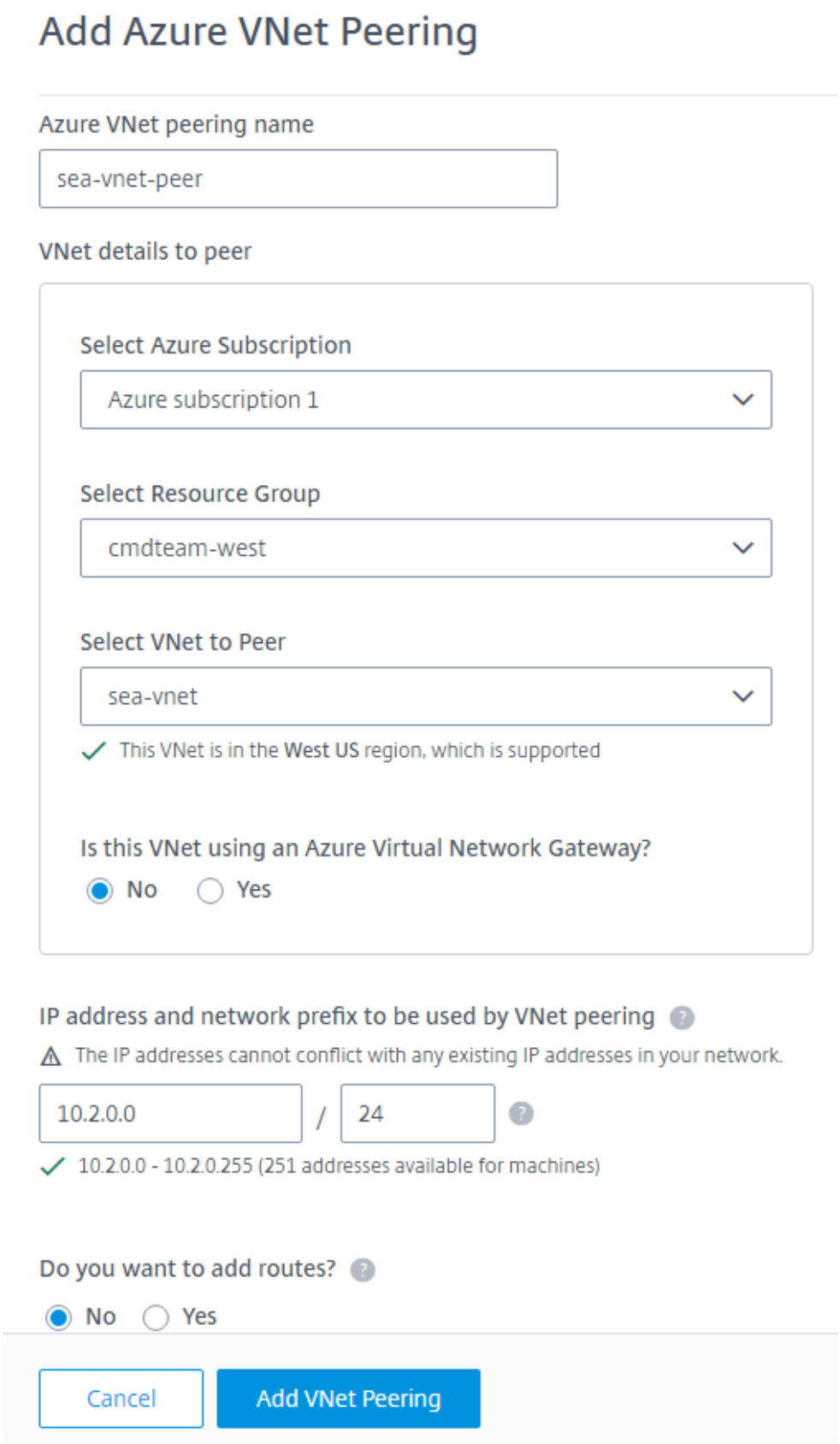
2. Select **Add Connection**.
3. Click anywhere in the **Add Azure VNet Peering** box.



4. Select **Authenticate Azure Account**.



5. Citrix DaaS automatically takes you to the Azure sign-in page to authenticate your Azure subscriptions. After you sign in to Azure (with the global administrator account credentials) and accept the terms, you are returned to the connection creation details dialog.



6. Type a name for the Azure VNet peer.
7. Select the Azure subscription, resource group, and the VNet to peer.
8. Indicate whether the selected VNet uses an Azure Virtual Network Gateway. For information, see the Microsoft article Azure VPN Gateway.
9. If you answered **Yes** in the previous step (the VNet uses an Azure virtual network gateway), indicate whether you want to enable virtual network gateway route propagation. When enabled, Azure automatically learns (adds) all routes through the gateway.

   You can change this setting later on the connection's **Details** page. However, changing it can cause route pattern changes and VDA traffic interruptions. Also, if you disable it later, you must manually add routes to the networks that VDAs will use.
10. Type an IP address and select a network mask. The address range to be used is displayed, plus how many addresses that the range supports. Ensure that the IP range does not overlap any addresses that you use in your Azure and on-premises networks.

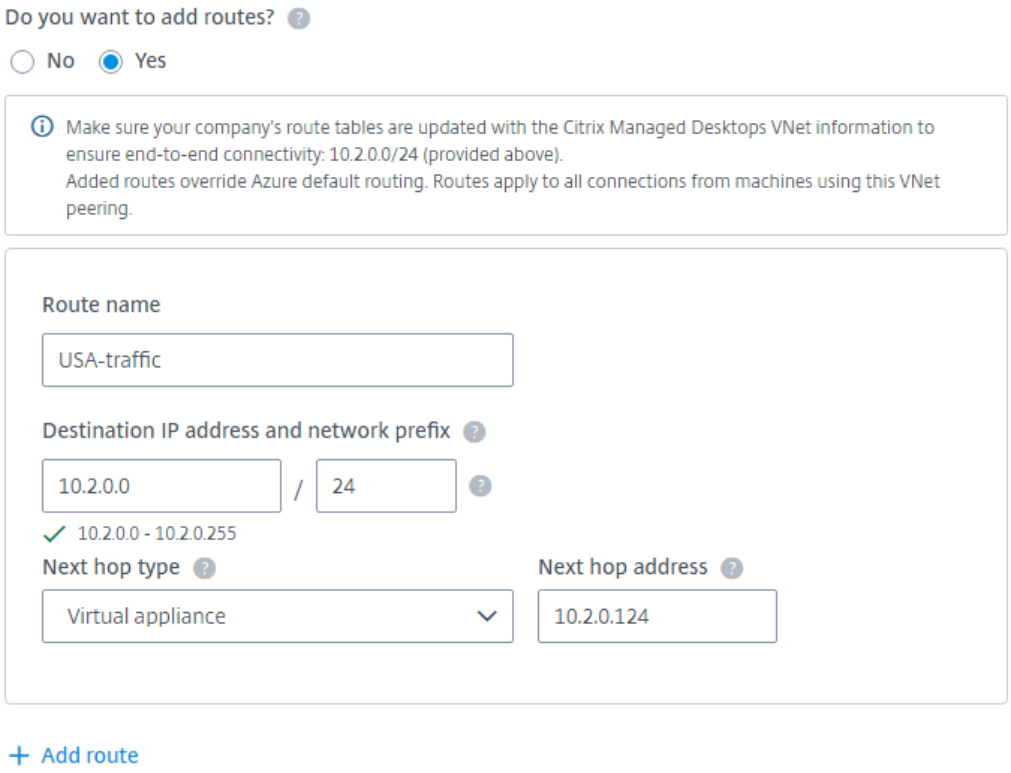
    - For example, if your Azure VNet has an address space of 10.0.0.0 /16, create the VNet peering connection in Citrix DaaS as something such as 192.168.0.0 /24.
    - In this example, creating a VNet peering connection with a 10.0.0.0 /24 IP range is considered an overlapping address range.

    If addresses overlap, the VNet peering connection might not be created successfully. It also won't work correctly for site administration tasks.
11. Indicate whether you want to add custom routes to the VNet peering connection. If you select **Yes**, enter the following information:

    a) Type a friendly name for the custom route.

    b) Enter the destination IP address and network prefix. The network prefix must be between 16 and 24.

    c) Select a next hop type for where you want traffic to be routed. If you select **Virtual appliance**, enter the internal IP address of the appliance.



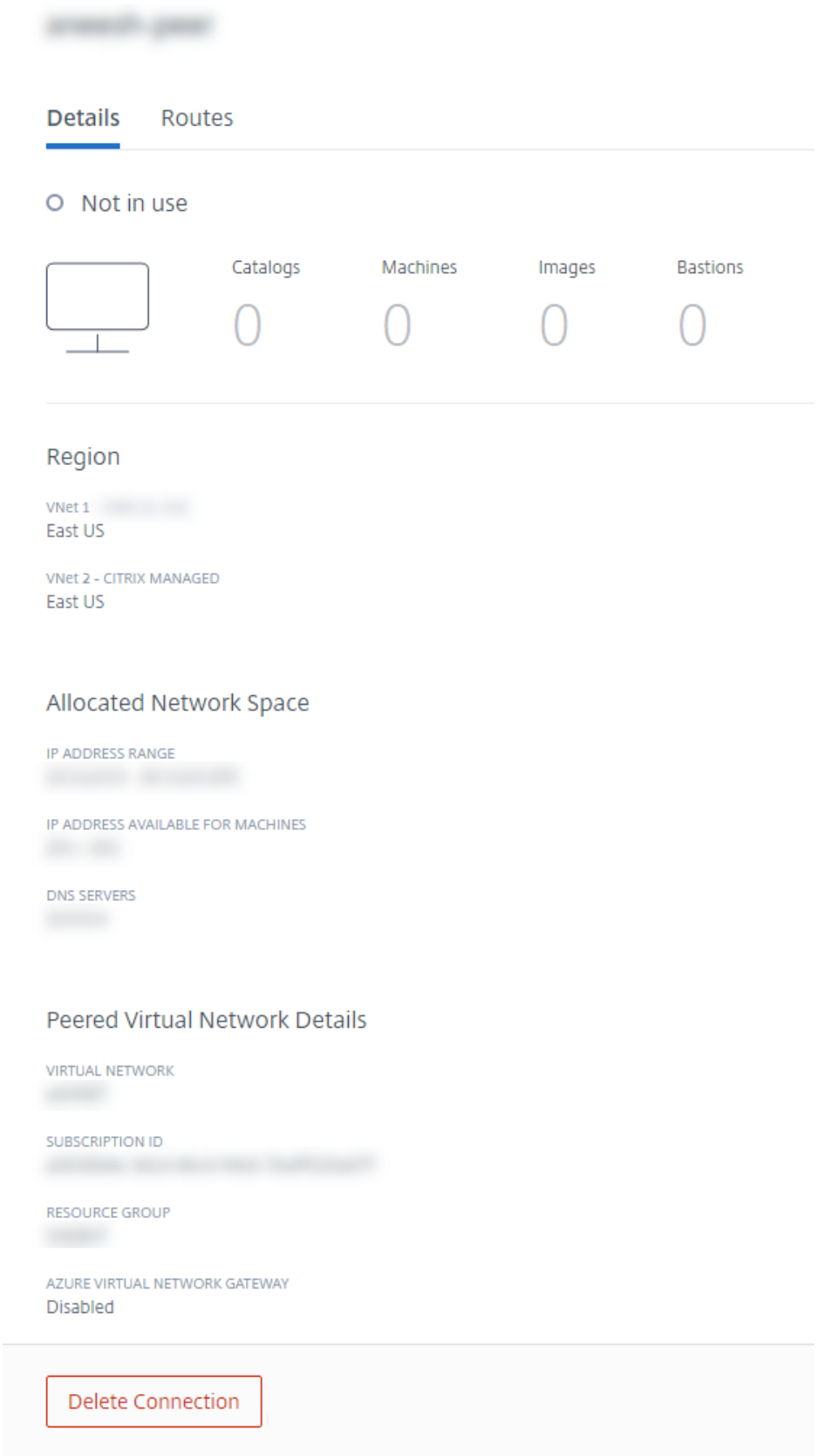
For more information about next hop types, see the Custom routes section in the Microsoft article *Virtual network traffic routing*.

d) To create another custom route for the connection, select **Add route**.

12. Select **Add VNet Peering**.

After the connection is created, it is listed under **Network Connections > Azure VNet Peers** on the right side of the **Manage > Quick Deploy** dashboard. When you create a catalog, this connection is included in the available network connections list.

View Azure VNet peering connection details



1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select the Azure VNet peering connection you want to display.

Details include:

- The number of catalogs, machines, images, and bastions that use this connection.
- The region, allocated network space, and peered VNets.
- The routes currently configured for the VNet peering connection.

Manage custom routes for existing Azure VNet peer connections

You can add new custom routes to an existing connection or modify existing custom routes, including disabling or deleting custom routes.

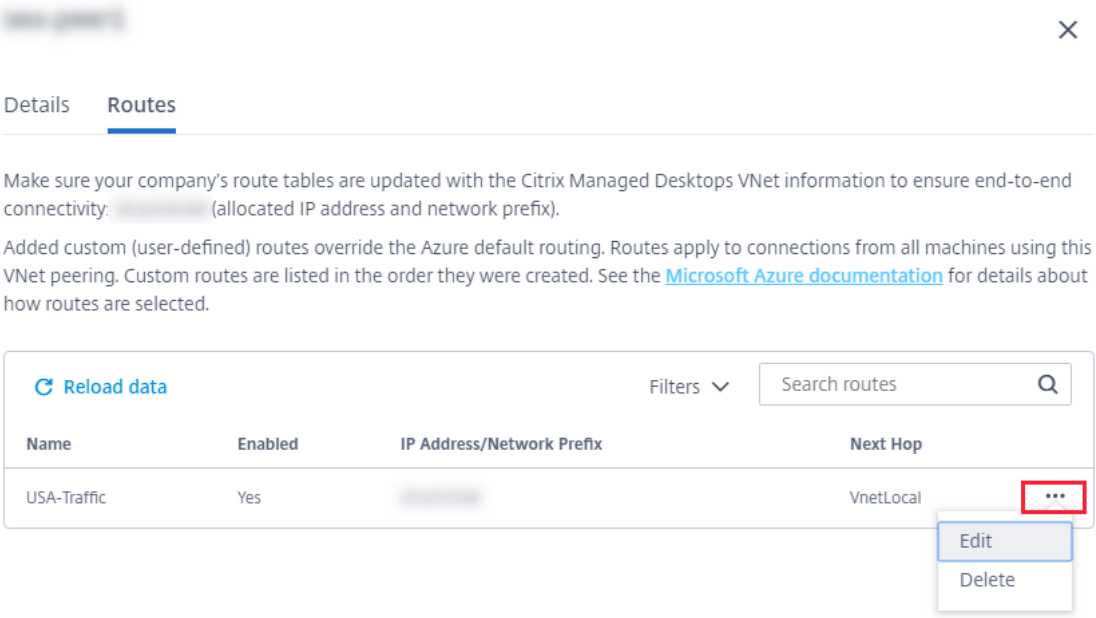
> **Important:**
>
> Modifying, disabling, or deleting custom routes changes the traffic flow of the connection and might disrupt any user sessions that might be active.

To add a custom route:

1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, select **Routes** and then select **Add Route**.
4. Enter a friendly name, the destination IP address and prefix, and the next hop type you want to use. If you select **Virtual Appliance** as the next hop type, enter the internal IP address of the appliance.
5. Indicate whether you want to enable the custom route. By default, the custom route is enabled.
6. Select **Add Route**.

To modify or disable a custom route:

1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, select **Routes** and then locate the custom route you want to manage.
4. From the ellipsis menu, select **Edit**.



5. Make any needed changes to the destination IP address and prefix or the next hop type, as needed.
6. To enable or disable a custom route, in **Enable this route?**, select **Yes** or **No**.
7. Select **Save**.

To delete a custom route:

1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, select **Routes** and then locate the custom route you want to manage.
4. From the ellipsis menu, select **Delete**.
5. Select **Deleting a route may disrupt active sessions** to acknowledge the impact of deleting the custom route.
6. Select **Delete Route**.

Delete an Azure VNet peering connection

Before you can delete an Azure VNet peering connection, remove any catalogs associated with it. See Delete a catalog.

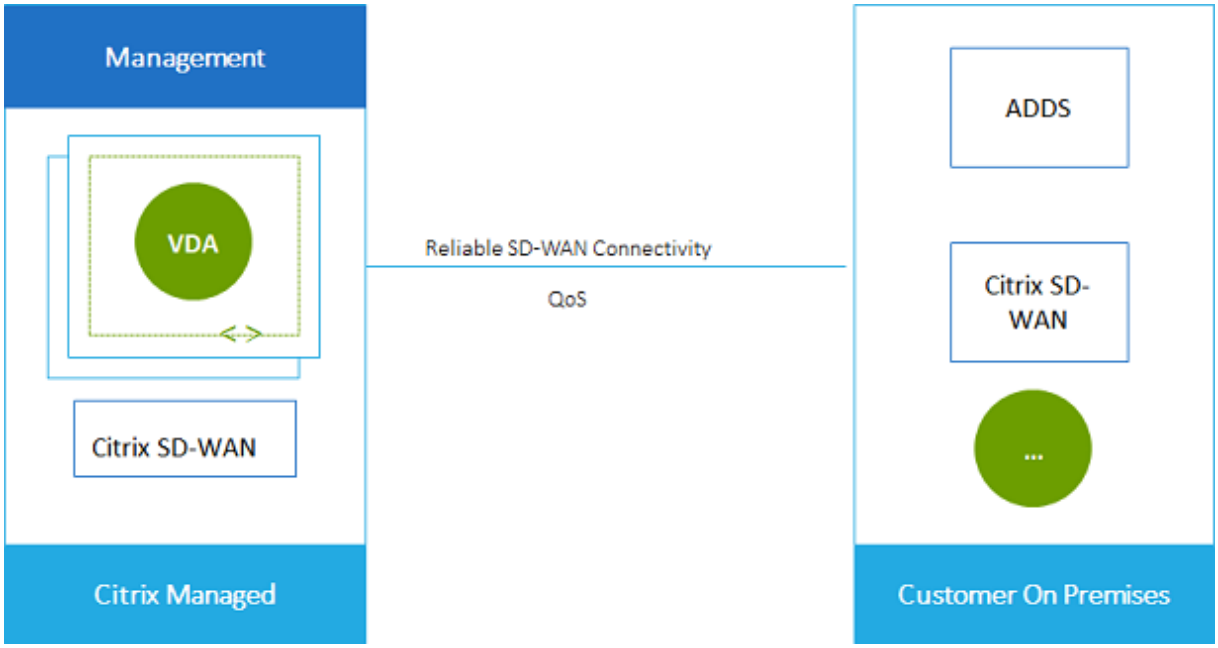
1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, select **Delete Connection**.

About SD-WAN connections

Citrix SD-WAN optimizes all the network connections needed by Citrix DaaS. Working in concert with the HDX technologies, Citrix SD-WAN provides quality-of-service and connection reliability for ICA and out-of-band Citrix DaaS traffic. Citrix SD-WAN supports the following network connections:

- Multi-stream ICA connection between users and their virtual desktops
- Internet access from the virtual desktop to websites, SaaS apps, and other cloud properties
- Access from the virtual desktop back to on-premises resources such as Active Directory, file servers, and database servers
- Real-time/interactive traffic carried over RTP from the media engine in the Workspace app to cloud-hosted Unified Communications services such as Microsoft Teams
- Client-side fetching of videos from sites like YouTube and Vimeo

As shown in the following graphic, you create an SD-WAN connection from the Citrix Managed Azure subscription to your sites. During connection creation, SD-WAN VPX appliances are created in the Citrix Managed Azure subscription. From the SD-WAN perspective, that location is treated as a branch.



SD-WAN connection requirements and preparation

- If the following requirements are not met, the SD-WAN network connection option is not available.
  - Citrix Cloud service entitlements: Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) and SD-WAN Orchestrator.

  - An installed and configured SD-WAN deployment. The deployment must include a Master Control Node (MCN), whether in the cloud or on-premises, and be managed with SD-WAN Orchestrator.

- VNet IP range: Provide an available CIDR address space (IP address and network prefix) that is unique among the network resources being connected. This is the IP range assigned to the VMs within Citrix DaaS's VNet.

  Ensure that you specify an IP range that does not overlap any addresses that you use in your cloud and on-premises networks.

  - For example, if your network has an address space of 10.0.0.0 /16, create the connection in Citrix DaaS as something such as 192.168.0.0 /24.
  - In this example, creating a connection with a 10.0.0.0 /24 IP range would be considered an overlapping address range.

  If addresses overlap, the connection might not be created successfully. It also does not work correctly for site administration tasks.

- The connection configuration process includes tasks that you (Citrix DaaS administrator) and the SD-WAN Orchestrator administrator must complete. Also, to complete your tasks, you need information provided by the SD-WAN Orchestrator administrator.

  We recommend that you both review the guidance in this document, plus the SD-WAN documentation, before actually creating a connection.

Create an SD-WAN connection

> **Important:**
>
> For details about SD-WAN configuration, see SD-WAN configuration for Citrix DaaS integration.

1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select **Add Connection**.
3. On the **Add a network connection** page, click anywhere in the SD-WAN box.
4. The next page summarizes what's ahead. When you're done reading, select **Start Configuring SD-WAN**.
5. On the **Configure SD-WAN** page, enter the information provided by your SD-WAN Orchestrator administrator.

   - **Deployment mode:** If you select **High availability**, two VPX appliances are created (recommended for production environments). If you select **Standalone**, one appliance is created. You cannot change this setting later. To change to the deployment mode, you'll have to delete and re-create the branch and all associated catalogs.

- **Name:** Type a name for the SD-WAN site.
- **Throughput and number of offices:** This information is provided by your SD-WAN Orchestrator administrator.
- **Region:** The region where the VPX appliances will be created.
- **VDA subnet and SD-WAN subnet:** This information is provided by your SD-WAN Orchestrator administrator. See SD-WAN connection requirements and preparation for information about avoiding conflicts.

6. When you're done, select **Create Branch**.
7. The next page summarizes what to look for on the **Manage > Quick Deploy** dashboard. When you're done reading, select **Got it**.
8. From **Manage > Quick Deploy**, the new SD-WAN entry under **Network Connections** shows the progress of the configuration process. When the entry turns orange with the message `Awaiting activation by SD-WAN administrator`, notify your SD-WAN Orchestrator administrator.
9. For SD-WAN Orchestrator administrator tasks, see the SD-WAN Orchestrator product documentation.
10. When the SD-WAN Orchestrator administrator finishes, the SD-WAN entry under **Network Connections** turns green, with the message `You can create catalogs using this connection`.

View SD-WAN connection details

1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select **SD-WAN** if it's not the only selection.
3. Select the connection you want to display.

The display includes:

- **Details tab:** Information you specified when configuring the connection.
- **Branch Connectivity tab:** Name, cloud connectivity, availability, bandwidth tier, role, and location for each branch and MCN.

Delete an SD-WAN connection

Before you can delete an SD-WAN connection, remove any catalogs associated with it. See Delete a catalog.

1. From **Manage > Quick Deploy**, expand **Network Connections** on the right.
2. Select SD-WAN if it's not the only selection.

3. Select the connection you want to delete, to expand its details.
4. On the **Details** tab, select **Delete Connection**.
5. Confirm the deletion.

Users and authentication in Quick Deploy

April 10, 2024

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

User authentication methods

Users must authenticate when they log in to Citrix Workspace to start their desktop or apps.

Quick Deploy supports the following user authentication methods:

- **Managed Azure AD:** Managed Azure AD is an Azure Active Directory (AAD) provided and managed by Citrix. You don't need to provide your own Active Directory structure. Just add your users to the directory.
- **Your identity provider:** You can use any available authentication method in Citrix Cloud.

> **Note:**
>
> - Remote PC Access deployments use only Active Directory. For details, see Remote PC Access.
> - If you use Azure AD Domain Services: Workspace logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.

Setting up user authentication includes the following procedures:

1. Configure the user authentication method in Citrix Cloud and Workspace Configuration.
2. If you're using Managed Azure AD for user authentication, add users to the directory.
3. Add users to a catalog.

Configure user authentication in Citrix Cloud

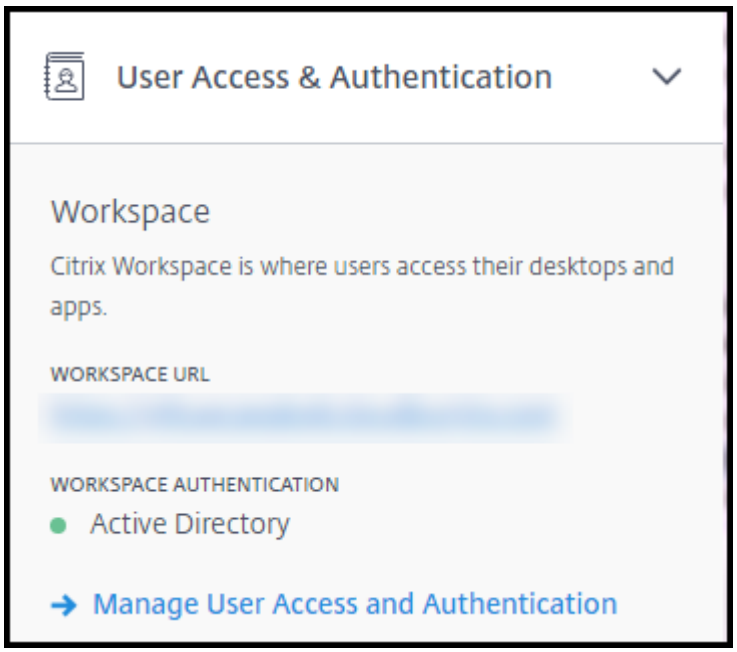
To configure user authentication in Citrix Cloud:

- Connect to the user authentication method you want to use. (In Citrix Cloud, you "connect"or "disconnect"from an authentication method.)
- In Citrix Cloud, set Workspace authentication to use the connected method.

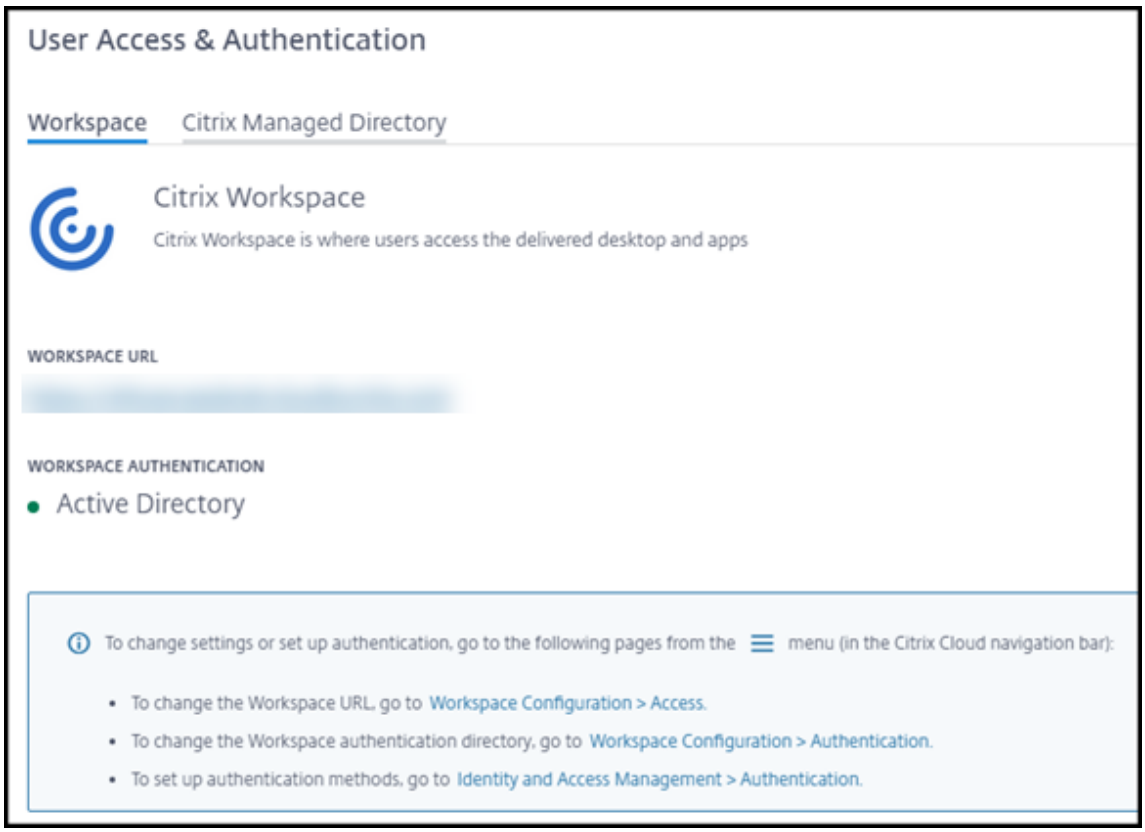
> **Note:**
>
> The Managed Azure AD authentication method is configured by default. That is, it is automatically connected in Citrix Cloud, and Workspace authentication is automatically set to use Managed Azure AD for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). If you want to use this method (and have not previously configured a different method), continue with Add and delete users in Managed Azure AD.
> If the Managed Azure AD is disconnected, the Workspace authentication will be switched to Active Directory. If you want to use a different authentication method follow the steps below.

To change the authentication method:

1. From **Manage > Quick Deploy**, select **User Access & Authentication** on the right.



2. Select **Manage User Access and Authentication**. Select the **Workspace** tab, if it isn't already selected. (The other tab indicates which user authentication method is currently configured.)



3. Follow the link **To set up authentication methods**. That link takes you to Citrix Cloud. Select **Connect** in the ellipsis menu for the method you want.
4. While still in Citrix Cloud, select **Workspace Configuration** in the upper left menu. On the **Authentication** tab, select the method you want.

What to do next:

- If you're using Managed Azure AD, add users to the directory.
- For all authentication methods, add users to the catalog.

Add and delete users in Managed Azure AD

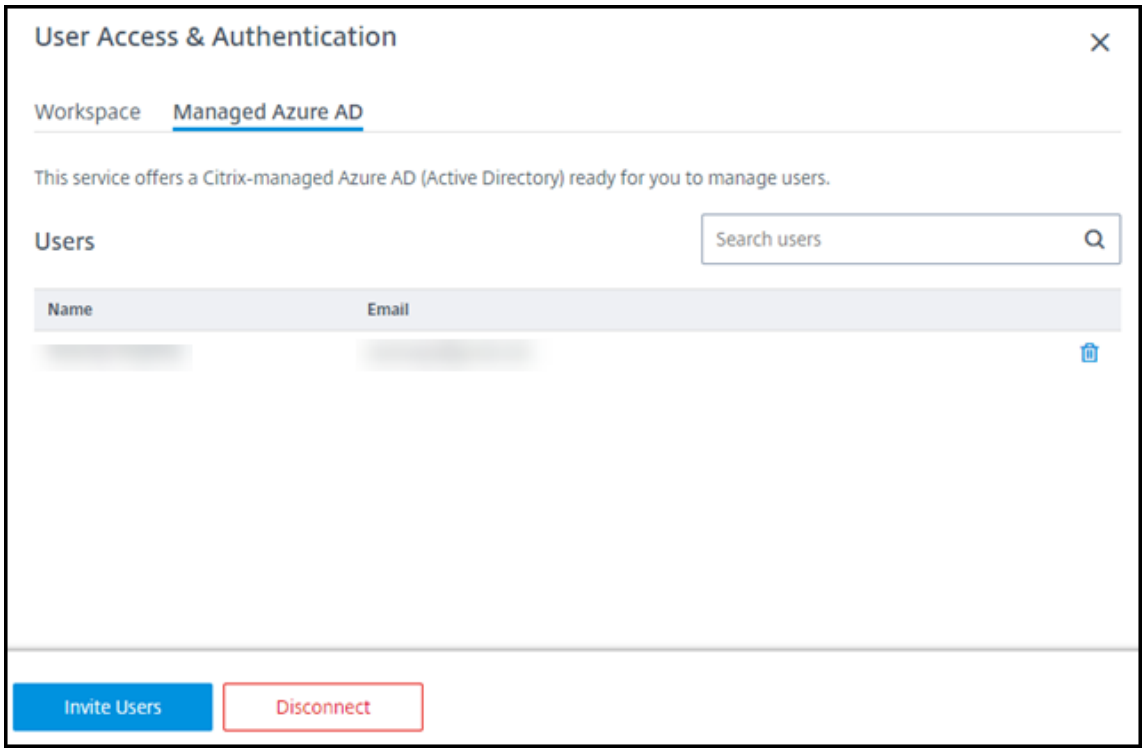
Complete this procedure only if you're using Managed Azure AD for user authentication to Citrix Workspace.

You provide your users' name and email addresses. Citrix then emails an invitation to each of them. The email instructs users to select a link that joins them to the Citrix Managed Azure AD.

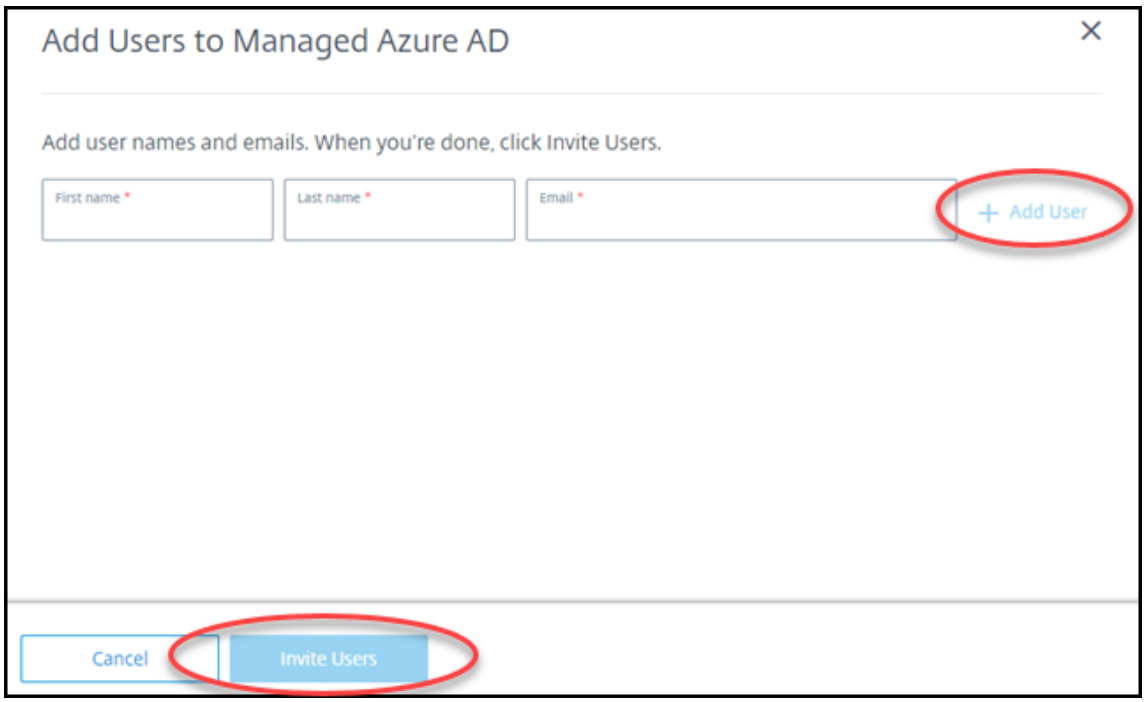
- If the user already has a Microsoft account with the email address you provided, that account is used.
- If the user does not have a Microsoft account with the email address, Microsoft creates an account.

To add and invite users to Managed Azure AD:

1. From **Manage > Quick Deploy**, expand **User Access & Authentication** on the right. Select **Manage User Access and Authentication**.
2. Select the **Managed Azure AD** tab.
3. Select **Invite Users**.



4. Type the name and email address of a user, and then select **Add User**.



5. Repeat the preceding step to add other users.
6. When you're done adding user information, select **Invite Users** at the bottom of the card.

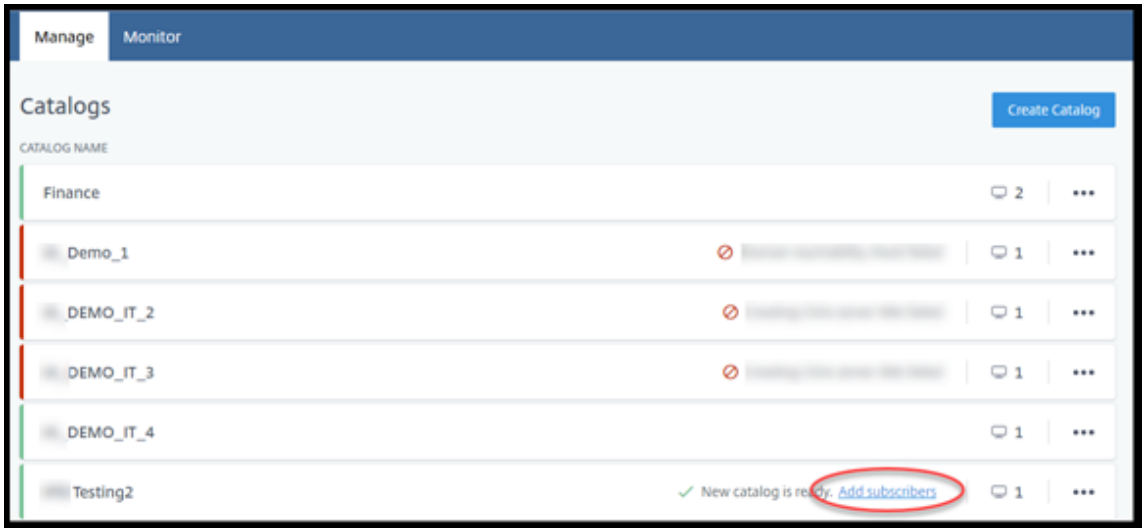
To delete a user from Managed Azure AD, select the trash icon next to the name of the user you want to delete from the directory. Confirm the deletion.

What to do next: Add users to the catalog

Add or remove users in a catalog

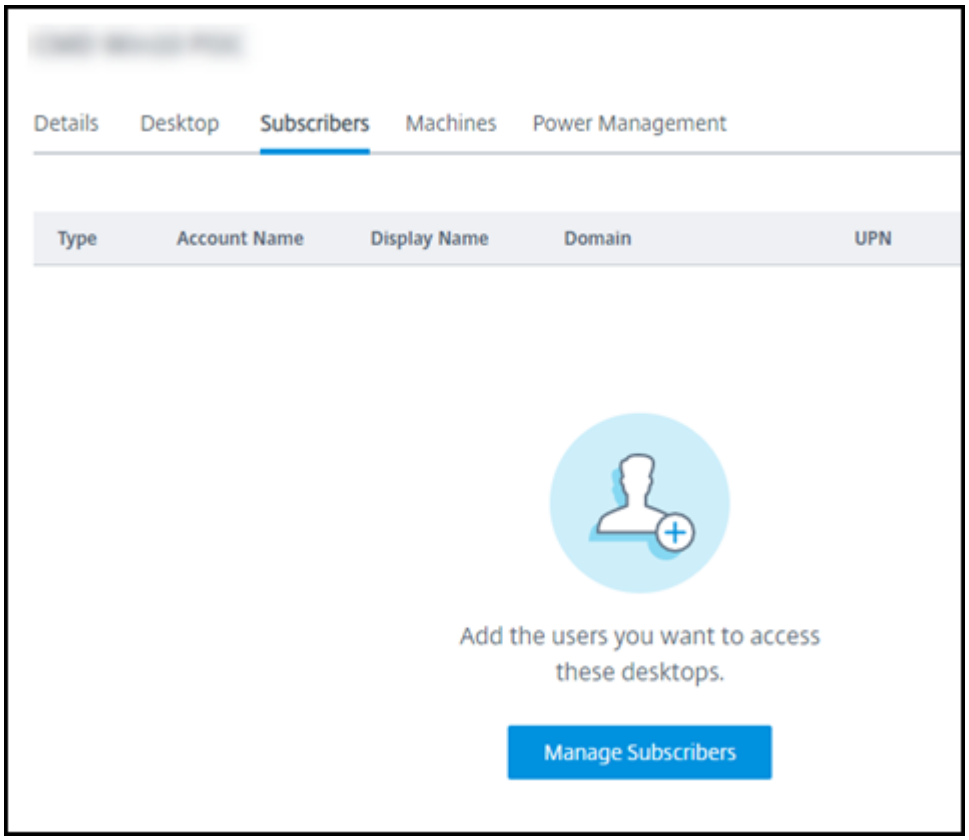
Complete this procedure regardless of which authentication method you use.

1. From **Manage > Quick Deploy**, if you haven't added any users to a catalog, select **Add subscribers**.

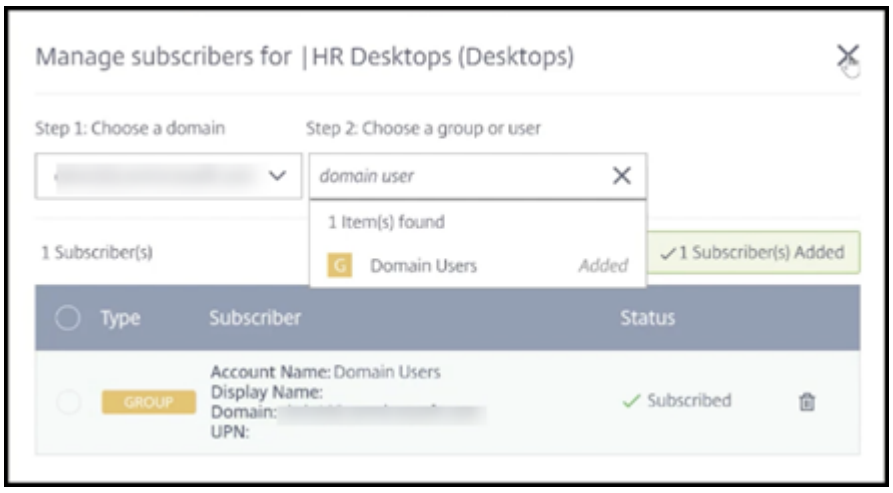


To add users to a catalog that already has users, click anywhere in the catalog's entry.

2. On the **Subscribers** tab, select **Manage Subscribers**.



3. Select a domain. (If you're using Managed Azure AD for user authentication, there's only one entry in the domain field.) Then select a user.



4. Select other users, as needed. When you're done, select the **X** in the upper right corner.

To remove users from a catalog, follow steps 1 and 2. In step 3, select the trash icon next to the name you want to delete (instead of selecting a domain and group/user). This action removes the user from the catalog, not from the source (such as Managed Azure AD or your own AD or AAD).

What to do next:

- For a catalog with multi-session machines, add applications, if you haven't already.
- For all catalogs, send the Citrix Workspace URL to your users.

More information

For more information about authentication in Citrix Cloud, see Identity and access management.

Remote PC Access in Quick Deploy

April 29, 2022

Introduction

Citrix Remote PC Access enables users to remotely use physical Windows or Linux machines located in the office. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

Remote PC Access supports domain-joined machines.

This article describes how to create a Remote PC Access deployment using the Quick Deploy interface. To create a Remote PC Access deployment using the Full Configuration interface, see Remote PC Access.

Differences from delivering virtual desktops and apps

If you're familiar with delivering virtual desktops and apps, the Remote PC Access feature has several differences:

- A Remote PC Access catalog usually contains existing physical machines. So, you don't have to prepare an image or provision machines to use Remote PC Access. Delivering desktops and apps usually uses virtual machines (VMs), and an image is used as a template to provision the VMs.
- When a machine in a Remote PC Access random pooled catalog is powered off, it is not reset to the original state of the image.
- For Remote PC Access static user assignment catalogs, the assignment occurs after a user logs in (either at the machine or via RDP). When delivering desktops and apps, a user is assigned if a machine is available.

Installation and configuration summary

Review this section before starting the tasks.

1. Before you start:
    a) Review the requirements and considerations.
    b) Complete the preparation tasks.
2. From Citrix Cloud:
    a) Set up a Citrix Cloud account and subscribe to Citrix DaaS.
    b) Set up a resource location that can access your Active Directory resources. Install at least two Cloud Connectors in the resource location. The Cloud Connectors communicate with Citrix Cloud.

    Follow the guidance for creating a resource location and installing Cloud Connectors in it. This information includes system requirements, preparation, and procedures.

    c) Connect your Active Directory to Citrix Cloud.
3. Install a Citrix Virtual Delivery Agent (VDA) on each machine that users will access remotely. VDAs communicate with Citrix Cloud through the Cloud Connectors in the resource location.
4. From **Manage > Quick Deploy**:

a) Create a Remote PC Access catalog. In this procedure, you specify the location of your resource location and select the user assignment method.
b) Add subscribers (users) to the catalog, if needed. Add users to a catalog if the catalog uses either the static autoassigned or random pooled user assignment method. You do not need to add users to a static preassigned catalog.

5. Send the workspace URL to users. From their workspace, users can log on to their machines in the office.

Requirements and considerations

References to machines in this section refer to the machines that users access remotely.

General

- The machines must be running a single-session Windows 10 or Linux (Red Hat Enterprise Linux and Ubuntu) operating system.
- The machine must be joined to an Active Directory Domain Services domain.
- If you are familiar with using Remote PC Access with Citrix Virtual Apps and Desktops, the Wake-on-LAN feature is not available in Citrix DaaS.

Network

- The machine must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.
- If using Wi-Fi:
  - Set the power settings to leave the wireless adapter turned on.
  - Configure the wireless adapter and network profile to allow automatic connection to the wireless network before the user logs on. Otherwise, the VDA does not register until the user logs on. The machine isn't available for remote access until a user logs on.
  - Ensure that the Cloud Connectors can be reached from the Wi-Fi network.

Devices and peripherals

- The following devices are not supported:
  - KVM switches or other components that can disconnect a session.
  - Hybrid PCs, including All-in-One and NVIDIA Optimus laptops and PCs.

- Connect the keyboard and mouse directly to the machine. Connecting to the monitor or other components that can be turned off or disconnected, can make these peripherals unavailable. If you must connect the input devices to components such as monitors, do not turn those components off.
- For laptop and Surface Pro devices: Ensure that the laptop is connected to a power source instead of running on the battery. Configure the laptop power options to match the options of a desktop machine. For example:
  - Disable the hibernate feature.
  - Disable the sleep feature.
  - Set the close lid action to **Do Nothing**.
  - Set the **press the power button action** to **Shut Down**.
  - Disable video card and NIC energy-saving features.

  When using a docking station, you can undock and redock laptops. When you undock the laptop, the VDA reregisters with the Cloud Connectors over Wi-Fi. However, when you redock the laptop, the VDA doesn't switch to use the wired connection unless you disconnect the wireless adapter. Some devices provide built-in functionality to disconnect the wireless adapter upon establishing a wired connection. Other devices require custom solutions or third-party utilities to disconnect the wireless adapter. Review the Wi-Fi considerations mentioned previously.

  To enable docking and undocking for Remote PC Access devices:

  - In **Start > Settings > System > Power & Sleep**, set **Sleep** to **Never**.
  - In **Device Manager > Network adapters > Ethernet adapter**, go to **Power Management** and clear **Allow the computer to turn off this device to save power**. Ensure that **Allow this device to wake the computer** is selected.

Linux VDA

- Use the Linux VDA on physical machines only in non-3D mode. Due to limitations on NVIDIA's driver, the local screen of the PC cannot be blacked out and displays the activities of the session when HDX 3D mode is enabled. Showing this screen is a security risk.
- Catalogs with Linux machines must use the static preassigned user assignment method. Catalogs with Linux machines cannot use either the static autoassigned or random pooled assignment methods.

Workspace considerations

- Multiple users with access to the same office PC see the same icon in Citrix Workspace. When a user signs in to Citrix Workspace, that machine appears as unavailable if it is already in use by

another user.

Prepare

- Decide how to install the VDA on the machines. Several methods are available:
  - Manually install the VDA on each machine.
  - Push the VDA installation using Group Policy, using a script.
  - Push the VDA installation using an Electronic Software Distribution (ESD) tool such as Microsoft System Center Configuration Manager (SCCM). For details, see Install VDAs using SCCM.
- Learn about user assignment methods and decide which method you'll use. You specify the method when creating a Remote PC Access catalog.
- Decide how the machines (actually the VDAs you install on the machines) will register with Citrix Cloud. A VDA must register to establish communications with the session broker in Citrix Cloud.

  VDAs register through the Cloud Connectors in their resource location. You can specify Cloud Connector addresses when you install a VDA, or later.

  For a VDA's first (initial) registration, Citrix recommends using policy-based GPO or LGPO. After the initial registration, Citrix recommends using auto-update, which is enabled by default. Learn more about VDA registration.

Install a VDA

Download and install a VDA on each physical machine that users will access remotely.

Download a VDA

- To download a Windows VDA:
  1. Using your Citrix Cloud account credentials, browse to the Citrix DaaS download page.
  2. Download the latest VDA. Two types of installation packages are available. The year and month values in the VDA title vary.
- To download a Linux VDA for Remote PC Access, follow the guidance in the Linux VDA documentation.

Windows VDA installation package types The Citrix download site provides two Windows VDA installation package types that can be used for Remote PC Access machines:

- Single-session core VDA installer (*release* is *yymm*): `VDAWorkstationCoreSetup_release.exe`

  The single-session core VDA installer is tailored specifically for Remote PC Access. It's lightweight and easier to deploy (than other VDA installers) over the network to all machines. It does not include components that typically aren't needed in these deployments, such as Citrix Profile Management, Machine Identity Service, and the user personalization layer.

  However, without Citrix Profile Management installed, the displays for Citrix Analytics for Performance and some Monitor details aren't available. For details about those limitations, see the blog post Monitor and troubleshoot Remote PC Access machines.

  If you want full analytics and monitoring displays, use the single-session full VDA installer.

- Single-session full VDA installer (*release* is *yymm*): `VDAWorkstationSetup_release.exe`

  Although the single-session full VDA installer is a larger package than the single-session core VDA installer, you can tailor it to install only the components you need. For example, you can install the components that support Profile Management.

Install a Windows VDA for Remote PC Access interactively

1. Double-click the VDA installation file that you downloaded.
2. On the **Environment** page, select **Enable Remote PC Access**, and then click **Next**.
3. On the **Delivery Controller** page, select one of the following:

   - If you know the addresses of your Cloud Connectors, select **Do it manually**. Enter the FQDN of a Cloud Connector and click **Add**. Repeat for the other Cloud Connectors in your resource location.
   - If you know where you installed the Cloud Connectors in your AD structure, select **Choose locations from Active Directory**, and then navigate to that location. Repeat for the other Cloud Connectors.
   - If you want to specify the Cloud Connector addresses in Citrix Group Policy, select **Do it later (Advanced)**, and then confirm that selection when prompted.

   When you're done, click **Next**.
4. If you're using the single-session full VDA installer, on the **Additional Components** page, select the components you want to install, such as Profile Management. (This page does not appear if you're using the single-session core VDA installer.)
5. On the **Features** page, click **Next**.

6. On the **Firewall** page, select **Automatically** (if it isn't already). Then click **Next**.
7. On the **Summary** page, click **Install**.
8. On the **Diagnose** page, click **Connect**. Make sure that the check box is selected. When prompted, enter your Citrix account credentials. After your credentials are validated, click **Next**.
9. On the **Finish** page, click **Finish**.

For full installation information, see Install VDAs.

Install a Windows VDA for Remote PC Access using a command line

- If you're using the single-session core VDA installer: Run `VDAWorkstationCoreSetup.exe`, and include the `/quiet`, `/enable_hdx_ports`, and `/enable_hdx_udp_ports` options. To specify Cloud Connector addresses, use the `/controllers` option.

  For example, the following command installs a single-session core VDA. Citrix Workspace app and other non-core services are not installed. The FQDNs of two Cloud Connectors are specified, and ports in the Windows Firewall Service will be opened automatically. The administrator will handle restarts.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```

- If you're using the single-session full VDA installer and want to include Profile Management (or other optional components): Run `VDAWorkstationSetup.exe` and include the `/remotepc` and `/includeadditional` options. The `/remotepc` option prevents installation of most additional components. The `/includeadditional` option specifies exactly which additional components you want to install.

  For example, the following command prevents installation of all optional additional components except Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional “Citrix User Profile Manager”,“Citrix User Profile Manager WMI Plugin” /controllers “connector.domain.com” “connector2.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

For details, see Command-line options to install a VDA.

Install a Linux VDA

Follow the guidance in the Linux documentation for installing a Linux VDA interactively or using the command line.

Create a Remote PC Access catalog

A resource location containing at least two Cloud Connectors must exist before you can successfully create a catalog.

> **Important:**
>
> A machine can belong to only one catalog at a time. This restriction is not enforced when you specify the machines to be added to a catalog. However, ignoring the restriction can cause problems later.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. If you haven't created any catalogs yet, click **Get Started** on the **Welcome** page.
4. Select **Manage > Quick Deploy**.
5. Select **Create Catalog**.
6. On the **Remote PC Access** tab, select a method for assigning users to machines.
7. Enter a name for the catalog and select the resource location you created.
8. Add machines.
9. Click **Create Catalog**.
10. On the **Your Remote PC Access catalog is being created** page, click **Done**.
11. An entry for the new catalog appears on the **Manage > Quick Deploy** dashboard.

    After the catalog is successfully created, click one of the links to add subscribers (users) to the catalog. This step applies if the catalog uses either the static autoassigned or random pool unassigned user assignment method.

After you create a catalog and add users (if needed), send the Workspace URL to your users.

User assignment methods

The user assignment method that you choose when creating a catalog indicates how users are assigned to machines.

- **Static autoassigned:** User assignment occurs when a user logs on to the machine (not using Citrix, for example, in-person or RDP), after a VDA is installed on the machine. Later, if other users log on to that machine (not using Citrix), they are also assigned. Only one user can use the machine at a time. This is a typical setup for either office workers or shift workers who share a computer.

  This method is supported for Windows machines. It cannot be used with Linux machines.

- **Static preassigned:** Users are preassigned to machines. (This is usually configured by uploading a CSV file containing machine-user mapping.) There is no need for user logon to establish assignment after the VDA is installed. There is also no need to assign users to the catalog after it's created. This is best for office workers.

  This method is supported for Windows and Linux machines.

- **Random pool unassigned:** Users are randomly assigned to an available machine. Only one user can use the machine at a time. This is ideal for computing labs in schools.

  This method is supported for Windows machines. It cannot be used with Linux machines.

Methods for adding machines to a catalog

Remember: Each machine must have a VDA installed on it.

When creating or editing a catalog, there are three ways you can add machines to a catalog:

- Select machine accounts one by one.
- Select OUs.
- Add in bulk using a CSV file. A template is available for you to use for the CSV file.

Add machine names

This method adds machine accounts one by one.

1. Select your domain.
2. Search for the machine account.
3. Click **Add**.
4. Repeat to add more machines.
5. When you finish adding machines, click **Done**.

Add OUs

This method adds machine accounts according to the Organizational Unit where they reside.
When selecting OUs, choose lower-level OUs for greater granularity. If that granularity is not required,

you can choose higher-level OUs.

For example, in the case of `Bank/Officers/Tellers`, select `Tellers` for greater granularity. Otherwise, you can select `Officers` or `Bank`, based on the requirement.

Moving or deleting OUs after they're assigned to a Remote PC Access catalog affects VDA associations and causes issues with future assignments. Ensure that your AD change plan accounts for OU assignment updates for catalogs.

To add OUs:

1. Select your domain.
2. Select the OUs that contain the machines accounts you want to add.
3. Indicate in the check box whether to include subfolders included in your selections.
4. When you finish selecting OUs, click **Done**.

Add in bulk

1. Click **Download CSV Template**.
2. In the template, add the machine account information (up to 100 entries). The CSV file can also contain the names of users assigned to each machine.
3. Save the file.
4. Either drag the file on to the **Add machines in bulk** page or browse to the file.
5. A preview of the file's content is displayed. If that's not the file you want, you can create another file and then drag or browse to it.
6. When you're finished, click **Done**.

Manage Remote PC Access catalogs

To display or change a Remote PC Access catalog's configuration information, select the catalog from the **Manage > Quick Deploy** dashboard (click anywhere in the catalog's entry).

- From the **Details** tab, you can add or remove machines.
- From the **Subscribers** tab, you can add or remove users.
- From the **Machines** tab, you can:
  - Add or remove machines: **Add or remove machines** button.
  - Change user assignments: **Remove assignment** trash icon, **Edit machine assignment** in ellipsis menu.
  - See which machines are registered, and place machines in or out of maintenance mode.

Monitor in Quick Deploy

April 29, 2022

From the **Monitor** dashboard, you can view desktop usage, sessions, and machines in your Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment. You can also control sessions, power-manage machines, end running applications, and end running processes.

To access the **Monitor** dashboard:

1. Sign in to Citrix Cloud, if you haven't already. In the upper left menu, select **My Services > DaaS**.
2. From the **Manage > Quick Deploy** dashboard, select the **Monitor** tab.

Monitor desktop usage

Displays on this page refresh every five minutes.

- **Machine and Sessions Overview:** You can tailor the display to show information about all catalogs (default) or a selected catalog. You can also tailor the time period: the last day, week, month, or three months.

  Counts at the top of the display indicate the total number of machines, plus the number of machines that are powered-on and powered-off. Hover over a value to display how many are single-session and multi-session.

  The graph below the counts shows the number of powered-on machines and peak concurrent sessions at regular points during the time period you selected. Hover on a point the graph to display the counts at that point.

- **Top 10s:** To tailor a top 10 display, select a time period: the past week (default), month, or three months. You can also tailor the display to show only information about activity involving single-session machines, multi-session machines, or applications.
  - **Top 10 Active Users:** Lists the users who started desktops most frequently during the time period. Hovering on a line displays the total launches.
  - **Top 10 Active Catalogs:** Lists the catalogs with the longest duration during the selected time period. Duration is the sum of all user sessions from that catalog.

Desktop usage report

To download a report containing information about machine launches during the last month, select **Launch Activity**. A message indicates that the request is being processed. The report downloads automatically to the default download location on the local machine.

Filter and search to monitor machines and sessions

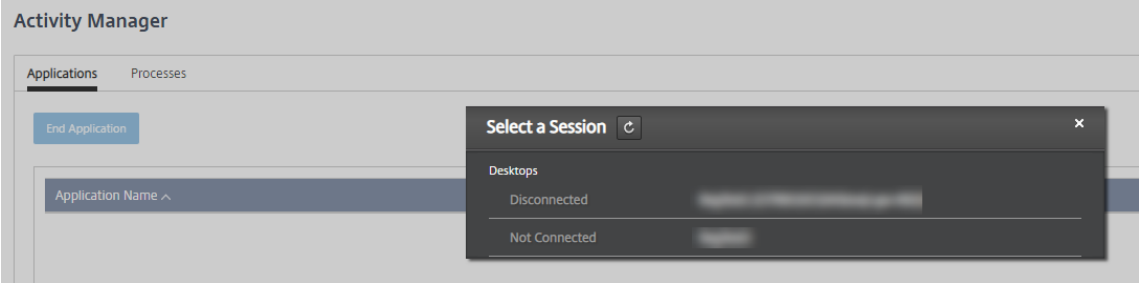
When you're monitoring session and machine information, all machines or sessions are displayed by default. You can:

- Filter the display by machines, sessions, connections, or applications.
- Refine the display of sessions or machines by choosing the criteria you want, building a filter by using expressions.
- Save the filters that you build, for reuse.

Control a user's applications

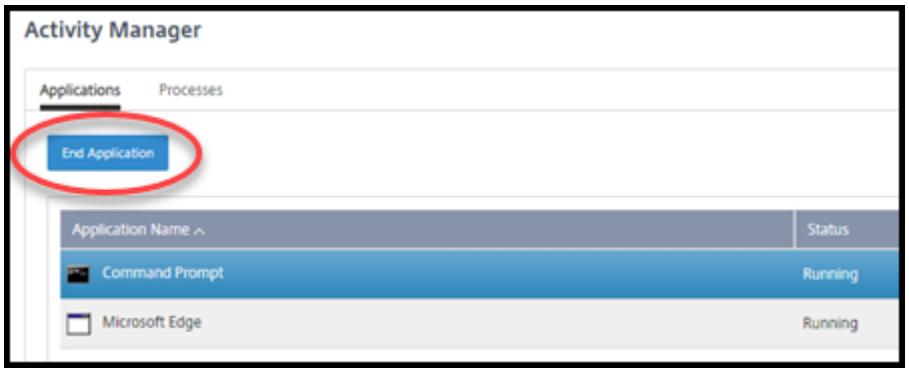
You can display and manage applications and processes for a user that has a running session or an assigned desktop.

1. From the **Monitor** dashboard in Citrix DaaS, select **Search** and enter the user name (or the beginning characters of the user name), machine, or endpoint. From the search results, select the item you're looking for. (To collapse the search box without searching, select **Search** again.)
2. Select a session.



The Activity Manager lists the applications and processes for the user's session.

3. To end an application, on the **Applications** tab in Activity Manager, select in the application's row to select that application, and then select **End Application**.



4. To end a process, on the **Processes** tab in Activity Manager, select in the process's row to select that process, and then select **End Process**.
5. To display session details, select **Details** in the upper right. To return to the applications and processes display, select Activity Manager in the upper right.
6. To control the session, select **Session Control > Log Off** or **Session Control > Disconnect**.

Shadow users

Use the shadow feature to view or work directly on a user's virtual machine or session. You can shadow Windows and Linux VDAs. The user must be connected to the machine that you want to shadow. To verify that connection, check the machine name listed in the `User` title bar.

Shadowing launches in a new browser tab. Ensure that your browser allows pop-ups from the Citrix Cloud URL.

Shadowing is supported only for users on domain-joined machines. To shadow a non-domain-joined machine, you must set up a bastion machine. For details, see Bastion access.

Shadowing must be initiated from a machine on the same virtual network as the domain-joined machines, and also meet any port requirements.

Enable shadowing

1. From **Manage > Quick Deploy > Monitor**, go to the **User Details** view.
2. Select the user session, and then select **Shadow** in the **Activity Manager** view or the **Session Details** panel.

Shadow Linux VDAs

Shadowing is available for Linux VDAs Version 7.16 or and later running the RHEL7.3 or Ubuntu Version 16.04 Linux distributions.

Monitor uses the FQDN to connect to the target Linux VDA. Ensure that the Monitor client can resolve the FQDN of the Linux VDA.

- The VDA must have the `python-websockify` and `x11vnc` packages installed.
- `noVNC` connection to the VDA uses the WebSocket protocol. By default, `ws://` WebSocket protocol is used. For security reasons, Citrix recommends that you use the secure `wss://` protocol. Install SSL certificates on each Monitor client and Linux VDA.

Follow the instructions in Session Shadowing to configure your Linux VDA for shadowing.

1. After you enable shadowing, the shadowing connection initializes and a confirmation prompt appears on the user device.
2. Instruct the user to select **Yes** to start the machine or session sharing.
3. The administrator can view only the shadowed session.

Shadow Windows VDAs

Windows VDA sessions are shadowed using Windows Remote Assistance. Enable the `Use Windows Remote Assistance` feature when installing the VDA.

1. After you enable shadowing, the shadowing connection initializes and a dialog box prompts you to open or save the `.msrc incident` file.
2. Open the incident file with the Remote Assistance Viewer, if it's not already selected by default. A confirmation prompt appears on the user device.
3. Instruct the user to select **Yes** to start the machine or session sharing.
4. For more control, ask the user to share keyboard and mouse control.

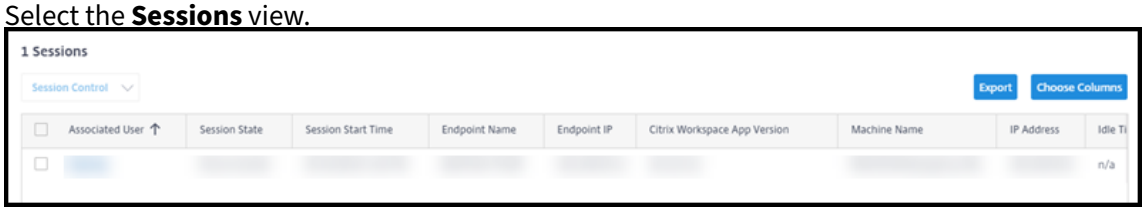
Monitor and control sessions

Session displays are updated every minute.

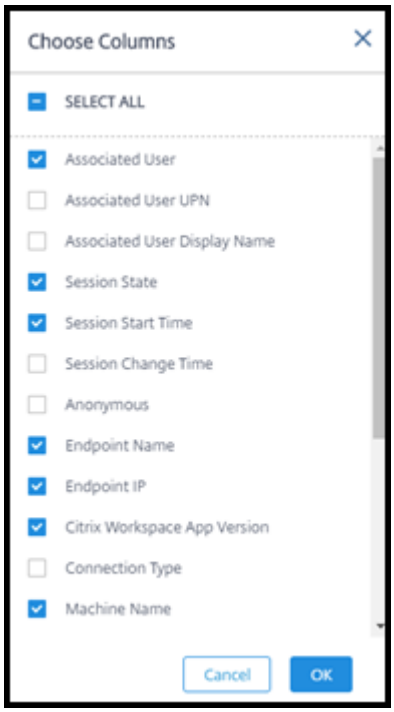
In addition to viewing sessions, you can disconnect one or more sessions or log off users from sessions.

1. From **Manage > Quick Deploy > Monitor**, select **Filters**.

2. Select the **Sessions** view.



3. To tailor the display, select **Choose Columns** and select the check boxes of items you want to appear. When you're done, select **OK**. The sessions display refreshes automatically.



4. Select the check box to the left of each session you want to control.
5. To log off or disconnect the session, elect either **Session Control > Log Off** or **Session Control > Disconnect**.

Remember that the power management schedule for the catalog can also control disconnecting sessions and logging off users from disconnected sessions.

As an alternative to the above procedure you can also **Search** for a user, select the session you want to control, and then display session details. The log off and disconnect options are available there, too.

Session information report

To download session information, select **Export** on the sessions display. A message indicates that the request is being processed. The report downloads automatically to the default download location on the local machine.

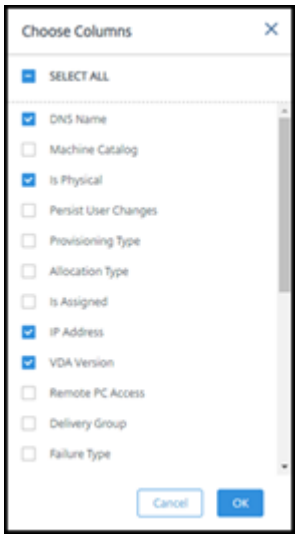
Monitor and power control machines

Machine displays are updated every minute.

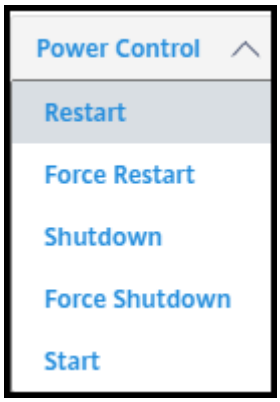
1. From **Manage > Quick Deploy > Monitor**, select **Filters**.
2. Select the **Machines** view.

   By default, the display lists single-session OS machines. Alternatively, you can display multi-session machines.

3. To tailor the display, select **Choose Columns** and select the check boxes of items you want to appear. When you're done, select **OK**. The machines display refreshes automatically.



4. To power-control machines or place them in or out of maintenance mode, select the check box to the left of each machine you want to control.
5. To power-control the selected machines, select **Power Control** and select an action.



6. To place the selected machines in or out of maintenance mode, select **Maintenance Mode > ON** or **Maintenance Mode > OFF**.

When you use the search feature to find and select a machine, you see machine details, utilization, historical utilization (from the last seven days), and average IOPS.

Machine information report

To download session information, select **Export** on the machines display. A message indicates that the request is being processed. The report downloads automatically to the default download location on the local machine.

Checking app and desktop health

Probing automates the process of checking the health of published apps and desktops. The health check results are available through the **Monitor** dashboard. For details, see:

- Application probing
- Desktop probing

Troubleshoot in Quick Deploy

March 23, 2022

Introduction

Resource locations contain the machines that deliver desktops and apps. Those machines are created in catalogs, so the catalogs are considered part of the resource location. Each resource location also contains Cloud Connectors. Cloud Connectors enable Citrix Cloud to communicate with the resource location. Usually, Citrix installs and updates the Cloud Connectors.

Optionally, you can initiate several Cloud Connector and resource location actions. See:

- Resource location actions
- Resource location settings when creating a catalog

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) has troubleshooting and supportability tools that can help resolve configuration and communication issues with the machines that deliver desktops and apps (the VDAs). For example, creating a catalog might fail, or users might be unable to start their desktop or apps.

This troubleshooting includes gaining access to your Citrix Managed Azure subscription through a bastion machine or direct RDP. After gaining access to the subscription, you can use Citrix supportability tools to locate and resolve issues. For details, see:

- VDA troubleshooting using a bastion or direct RDP
- Bastion access
- Direct RDP access

VDA troubleshooting using a bastion or direct RDP

The supportability features are for people who have experience with troubleshooting Citrix issues. This includes:

- Citrix Service Providers (CSPs) and others who have the technical knowledge and troubleshooting experience with Citrix DaaS products.
- Citrix Support personnel.

If you're not familiar or comfortable with troubleshooting Citrix components, you can request help from Citrix Support. Citrix Support representatives might ask you to set up one of the access methods described in this section. However, the Citrix representatives do the actual troubleshooting, using Citrix tools and technologies.

> **Important:**
>
> These supportability features are valid only for domain-joined machines. If the machines in your catalogs are not domain joined, you're guided to request troubleshooting help from Citrix Support.

Access methods

These access methods are valid only for the Citrix Managed Azure subscription. For more information, see Azure subscriptions.

Two supportability access methods are provided.

- Access your resources through a bastion machine in the customer's dedicated Citrix Managed Azure subscription. The bastion is a single point of entry that allows access to the machines in the subscription. It provides a secure connection to those resources by allowing remote traffic from IP addresses in a specified range.

  The steps in this method include:

  - Create the bastion machine
  - Download an RDP agent
  - RDP to the bastion machine
  - Connect from the bastion machine to the other Citrix machines in your subscription

  The bastion machine is intended for short-term use. This method is intended for issues involving the creation of catalogs or image machines.

- Direct RDP access to the machines in the customer's dedicated Citrix Managed Azure subscription. To permit RDP traffic, port 3389 must be defined in the Network Security Group.

  This method is intended for catalog issues other than creation, such as users unable to start their desktops.

Remember: As an alternative to these two access methods, contact Citrix Support for help.

Bastion access

1. From **Manage > Quick Deploy**, expand **Troubleshoot & Support** on the right.
2. Click **View troubleshooting options**.
3. On the **Troubleshoot** page, select either of the first two issue types, and then click **Use our troubleshooting machine**.
4. On the **Troubleshoot with Bastion Machine** page, select the catalog.

   - If the machines in the selected catalog are not domain joined, you're instructed to contact Citrix Support.
   - If a bastion machine has already been created with RDP access to the selected catalog's network connection, skip to step 8.

5. The RDP access range is displayed. If you want to restrict RDP access to a smaller range than allowed by the network connection, select the **Restrict RDP access to only computers in IP address range** check box and then enter the desired range.
6. Type a username and password that you'll use to log in when you RDP to the bastion machine. Password requirements.

   Do not use Unicode characters in the username.
7. Click **Create Bastion Machine**.

   When the bastion machine is successfully created, the page title changes to **Bastion** –***connection***.

   If the bastion machine creation fails (or if it fails during operation), click **Delete** at the bottom of the failure notification page. Try to create the bastion machine again.

   You can change the RDP range restriction after the bastion machine is created. Click **Edit**. Enter the new value and then click the check mark to save the change. (Click **X** to cancel the change.)
8. Click **Download RDP File**.
9. RDP to the bastion, using the credentials you specified when creating the bastion. (The bastion machine's address is embedded in the RDP file you downloaded.)
10. Connect from the bastion machine to the other Citrix machines in the subscription. You can then collect logs and run diagnostics.

Bastion machines are powered on when they are created. To save costs, machines are powered off automatically if they remain idle after startup. The machines are deleted automatically after several hours.

You can power manage or delete a bastion machine, using the buttons at the bottom of the page. If you choose to delete a bastion machine, you must acknowledge that any active sessions on the machine will end automatically. Also, any data and files that were saved on the machine will be deleted.

Direct RDP access

1. From **Manage > Quick Deploy**, expand **Troubleshoot & Support** on the right.
2. Click **View troubleshooting options**.
3. On the **Troubleshoot** page, select **Other catalog issue**.
4. On the **Troubleshoot with RDP Access** page, select the catalog.

   If RDP has already been enabled to the selected catalog's network connection, skip to step 7.

5. The RDP access range is displayed. If you want to restrict RDP access to a smaller range than permitted by the network connection, select the **Restrict RDP access to only computers in IP address range** check box and then enter the desired range.
6. Click **Enable RDP Access.**

   When RDP access is successfully enabled, the page title changes to **RDP Access** –***connection***.

   If RDP access is not successfully enabled, click **Retry Enabling RDP** at the bottom of the failure notification page.
7. Connect to machines using your Active Directory administrator credentials. You can then collect logs and run diagnostics.

Get help

If you still have problems, open a ticket by following the instructions in How to Get Help and Support.

Quick Deploy reference

July 21, 2022

Catalog tabs on the Quick Deploy dashboard

From the **Manage > Quick Deploy** dashboard in Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), click anywhere in the catalog's entry. The following tabs contain information about the catalog:

- **Details:** Lists the information specified when the catalog was created (or its most recent edit). It also contains information about the image that was used to create the catalog.

  From this tab, you can:

  - Change the image that is used in the catalog.
  - Delete the catalog.
  - Access the page containing details for the resource location used by the catalog.
- **Desktop:** Available only for catalogs containing single-session (static or random) machines. From this tab, you can change the name and description of the catalog.
- **Desktop and Apps:** The **Desktops and Apps** tab is available only for catalogs containing multi-session machines. From this tab, you can:

  - Add, edit, or remove applications that the catalog's users can access in Citrix Workspace.
  - Change the name and description of the catalog.

- **Subscribers:** Lists all users, including their type (user or group), account name, display name, plus their Active Directory domain and user principal name.

  From this tab, you can add or remove users for a catalog.

- **Machines:** Shows the total number of machines in the catalog, plus the number of registered machines, unregistered machines, and machines that have maintenance mode turned on.

  For each machine in the catalog, the display includes each machine's name, power state (on/off), registration state (registered/unregistered), assigned users, session count (0/1), and maintenance mode status (an icon indicating on or off).

  From this tab, you can:

  - Add or delete a machine
  - Start, restart, force restart, or shut down a machine
  - Turn a machine's maintenance mode on or off

  For details, see Manage catalogs. Many of the machine actions are also available from the **Monitor** tab on the Quick Deploy dashboard. See Monitor and power control machines.

- **Power Management:** Enables you to manage when machines in the catalog are powered on and off. A schedule also indicates when idle machines are disconnected.

  You can configure a power schedule when you create a custom catalog or later. If no schedule is explicitly set, a machine powers off when a session ends.

  When creating a catalog using quick create, you cannot select or configure a power schedule. By default, quick create catalogs use the Cost Saver preset schedule. However, you can edit that catalog later and change the schedule.

  For details, see Manage power management schedules.

DNS servers

This section applies to all deployments that contain domain-joined machines. You can ignore this section if you use only non-domain-joined machines.

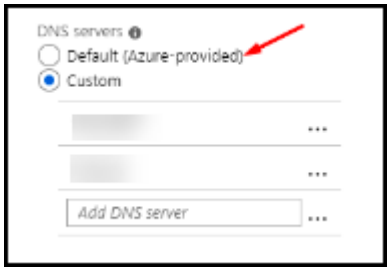
1. Before creating a domain-joined catalog (or a connection, if you're using a Citrix Managed Azure subscription), check whether you have DNS server entries that can resolve public and private domain names.

   When Citrix DaaS creates a catalog or a connection, it looks for at least one valid DNS server entry. If no valid entries are found, the creation operation fails.

Where to check:

- If you are using your own Azure subscription, check the **DNS servers** entry in your Azure.
- If you are using a Citrix Managed Azure subscription and creating an Azure VNet peering connection, check the **DNS servers** entry in the Azure VNet that you're peering.
- If you are using a Citrix Managed Azure subscription and creating an SD-WAN connection, check the DNS entries in the SD-WAN Orchestrator.

2. In Azure, the **Custom** setting must have at least one valid entry. This service cannot be used with the **Default (Azure-provided)** setting.



   - If **Default (Azure-provided)** is enabled, change the setting to **Custom**, and add at least one DNS server entry.
   - If you already have DNS server entries under **Custom**, verify that the entries you want to use with this service can resolve public and private domain IP names.
   - If you do not have any DNS servers that can resolve domain names, Citrix recommends adding an Azure-provided DNS server that has those capabilities.

3. If you change any DNS server entries, restart all machines that are connected to the virtual network. The restart assigns the new DNS server settings. (The VMs continue using their current DNS settings until the restart.)

   If you want to change DNS addresses later, after a connection is created:

- When using your own Azure subscription, you can change them in Azure (as described in the preceding steps). Or, you can change them in this service.
- When using a Citrix Managed Azure subscription, this service does not synchronize DNS address changes that you make in Azure. However, you can change DNS settings for the connection in this service.

Keep in mind that changing DNS server addresses can potentially cause connectivity issues for machines in catalogs that use that connection.

Adding DNS servers through this service

Before adding a DNS server address to a connection, make sure that the DNS server can resolve public and internal domain names. Citrix recommends that you test connectivity to a DNS server before

adding it.

1. To add, change, or remove a DNS server address when you're creating a connection, select **Edit DNS servers** on the **Add** *connection type* page. Or, if a message indicates that no DNS server addresses were found, select **Add DNS Servers**. Continue with step 3.
2. To add, change, or remove a DNS server address for an existing connection:
   a) From **Manage > Quick Deploy**, expand **Network Connections** on the right.
   b) Select the connection you want to edit.
   c) Select **Edit DNS servers**.
3. Add, change, or remove addresses.
   a) To add an address, select **Add DNS server** and then enter the IP address.
   b) To change an address, click inside the address field and change the numbers.
   c) To remove an address, select the trash icon next to the address entry. You cannot remove all DNS server addresses. The connection must have at least one.
4. When you're done, select **Confirm Changes** at the bottom of the page.
5. Restart all machines that use that connection. The restart assigns the new DNS server settings. (The VMs continue using their current DNS settings until the restart.)

Policies

Set group policies for non-domain-joined machines

1. RDP to the machine that is being used for the image.
2. Install Citrix Group Policy Management:
   a) Browse to CTX220345. Download the attachment.
   b) Double-click the downloaded file. In the `Group Policy Templates 1912 > Group Policy Management` folder, double-click `CitrixGroupPolicyManagement_x64.msi`.
3. Using the **Run** command, launch `gpedit.msc` to open the Group Policy Editor.
4. In `User Configuration Citrix Policies > Unfiltered`, select **Edit Policy**.

   If the Group Policy Management Console fails (as described in CTX225742), install the Microsoft Visual C++ 2015 Runtime (or a later version of that runtime).
5. Enable policy settings as needed. For example:
   - When working in **Computer Configuration** or **User Configuration** (depending on what you want to configure) on the **Settings** tab, in `Category > ICA / Printing`, select **Auto-create PDF Universal Printer** and set to `Enabled`.

- If you want logged-in users to be administrators of their desktop, add the **Interactive User** group to the built-in administrators group.

6. When you're done, save the image.
7. Either update the existing catalog or create a new catalog using the new image.

Set group policies for domain-joined machines

1. Ensure that the Group Policy Management feature is installed.
   - On a Windows multi-session machine, add the Group Policy Management feature, using the Windows tool for adding roles and features (such as **Add Roles and Features**).
   - On a Windows single-session machine, install the Remote Server Administration Tools for the appropriate OS. (This installation requires a domain admin account.) After that installation, the Group Policy Management console is available from the **Start** menu.
2. Download and install the Citrix Group Policy management package from the Citrix download page, and then configure policy settings as needed. Follow the procedure in Set group policies for non-domain-joined machines, step 2 through the end.

See the Policy settings reference articles to learn about what's available. All policy features are available from Citrix DaaS's Full Configuration interface.

Resource location actions

Citrix automatically creates a resource location and two Cloud Connectors when you create the first catalog for publishing desktops and apps. You can specify some information related to the resource location when you create a catalog. See Resource location settings when creating a catalog.

For Remote PC Access, you create the resource location and Cloud Connectors.

This section describes available actions after a resource location is created.

1. From **Manage > Quick Deploy**, expand **Cloud Subscriptions** on the right.
2. Select the subscription.
   - The **Details** tab shows the number and names of catalogs and images in the subscription. It also indicates the number of machines that can deliver desktops or apps. That count does not include machines used for other purposes, such as images, Cloud Connectors, or RDS license servers.
   - The **Resource Locations** tab lists each resource location. Each resource location entry includes the status and address of each Cloud Connector in the resource location.

The ellipsis menu in a resource location's entry contains the following actions.

Run Health Check

Selecting **Run Health Check** starts the connectivity check immediately. If the check fails, the Cloud Connector's state is unknown, because it is not communicating with Citrix Cloud. You might want to restart the Cloud Connector.

Restart Connectors

Citrix recommends restarting only one Cloud Connector at a time. Restarting takes the Cloud Connector offline, and disrupts user access and machine connectivity.

Select the check box for the Cloud Connector you want to restart. Select **Restart**.

Add Connectors

Adding a Cloud Connector typically takes 20 minutes to complete.

Provide the following information:

- How many Cloud Connectors to add.
- Domain service account credentials, which are used to join the Cloud Connector machines to the domain.
- Machine performance.
- Azure resource group. The default is the resource group last used by the resource location.
- Organizational Unit (OU). The default is the OU last used by the resource location.
- Whether your network requires a proxy server for internet connectivity. If you indicate **Yes**, provide the proxy server FQDN or IP address, and port number.

When you're done, select **Add Connectors**.

Delete Connectors

If a Cloud Connector cannot communicate with Citrix Cloud, and a restart does not resolve the issue, Citrix Support might recommend deleting that Cloud Connector.

Select the check box for the Cloud Connector you want to delete. Then select **Delete**. When prompted, confirm the deletion.

You can also delete an available Cloud Connector. However, if deleting that Cloud Connector would result in fewer than two available Cloud Connectors in the resource location, you're not allowed to delete the selected Cloud Connector.

Select Update Time

Citrix automatically provides software updates for the Cloud Connectors. During an update, one Cloud Connector is taken offline and updated, while other Cloud Connectors remain in service. When the first update completes, another Cloud Connector is taken offline and updated. This process continues until all Cloud Connectors in the resource location are updated. The best time to start updates is usually outside your typical business hours.

Choose the time to begin updates, or indicate that you want updates to start when an update is available. When you're done, select **Save**.

Rename

Enter the new name for the resource location. Select **Save**.

Configure Connectivity

Indicate whether users can access desktops and apps through the Citrix Gateway service, or only from within your corporate network.

Profile Management

Profile Management ensures that personal settings apply to users' virtual applications, regardless of the location of the user device.

Configuring Profile Management is optional.

You can enable Profile Management with the profile optimization service. This service provides a reliable way for managing these settings in Windows. Managing profiles ensures a consistent experience by maintaining a single profile that follows the user. It consolidates automatically and optimizes user profiles to minimize management and storage requirements. The profile optimization service requires minimal administration, support, and infrastructure. Also, profile optimization provides users with an improved logon and logoff experience.

The profile optimization service requires a file share where all the personal settings persist. You manage the file servers. We recommend setting up network connectivity to allow access to these file servers. You must specify the file share as a UNC path. The path can contain system environment variables, Active Directory user attributes, or Profile Management variables. To learn more about the format of the UNC text string, see Specify the path to the user store.

When enabling Profile Management, consider further optimizing the user's profile by configuring folder redirection to minimize the effects of the user profile size. Applying folder redirection complements the Profile Management solution. For more information, see Microsoft Folder Redirection.

Configure the Microsoft RDS License Server for Windows Server workloads

This service accesses Windows Server remote session capabilities when delivering a Windows Server workload, such as Windows 2016. This typically requires a Remote Desktop Services client access license (RDS CAL). The Windows machine where the Citrix VDA is installed must be able to contact an RDS license server to request RDS CALs.

Install and activate the license server. For more information, see the Microsoft document Activate the Remote Desktop Services License Server. For proof of concept environments, you can use the grace period provided by Microsoft.

With this method, you can have Citrix DaaS apply the license server settings. You can configure the license server and per user mode in the RDS console on the image. You can also configure the license server using Microsoft Group Policy settings. For more information, see the Microsoft document License your RDS deployment with client access licenses (CALs).

To configure the RDS license server using Group Policy settings

1. Install a Remote Desktop Services License Server on one of the available VMs. The VM must always be available. Citrix DaaS workloads must be able to reach this license server.
2. Specify the license server address and per-user license mode using Microsoft Group Policy. For details, see the Microsoft document Specify the Remote Desktop Licensing Mode for an RD Session Host Server.

Windows 10 workloads require appropriate Windows 10 license activation. We recommend that you follow Microsoft documentation to activate Windows 10 workloads.

Consumption commitment usage

> **Note:**
>
> This feature is in preview.

From **Manage > Quick Deploy**, select the **General** card. The **Consumption** value indicates how much consumption has been used in the current calendar month. That value includes monthly and term commitments.

When you select **General**, the **Notifications** tab includes:

- Total consumption used for the month (monthly and term).
- Number of units of monthly consumption commitment.
- Percentage of term consumption commitment.

The values and progress bars can alert you to potential or actual usage overages.

Actual data can take 24 hours to appear. Usage and billing data are considered final 72 hours after the end of a calendar month.

For more usage information, see Monitor licenses and active usage.

You can optionally request notifications to appear in the **Manage > Quick Deploy** dashboard when consumption usage (for monthly, term, or both commitments) reaches a specified level. By default, notifications are disabled.

1. On the **Notifications** tab, select **Edit Notification Preferences**.
2. To enable notifications, click the slider so that the check mark appears.
3. Enter a value. Repeat for the other consumption type, if needed.
4. Select **Save**.

To disable notifications, click the slider so that the check mark no longer appears, and then select **Save**.

Monitor Citrix license usage

To view your Citrix license usage information, follow the guidance in Monitor licenses and active usage. You can view:

- Licensing summary
- Usage reports
- Usage trends and license activity
- Licensed users

You can also release licenses.

Load balancing

Load balancing applies to multi-session machines, not single-session machines.

> **Important:**
>
> Changing the load balancing method affects all catalogs in your deployment. That includes all catalogs created using any supported host type, cloud-based and on-premises, regardless of interface used to create them (such as Full Configuration or Quick Deploy).
>
> Make sure you have maximum session limits configured for all catalogs before proceeding.
>
> - In Quick Deploy, that setting is located on each catalog's **Details** tab.
> - In Full Configuration, see Load balance machines.

Load balancing measures the machine load, and determines which multi-session machine to select for an incoming user session under the current conditions. This selection is based on the configured load balancing method.

You can configure one of two load balancing methods: horizontal or vertical. The method applies to all multi-session catalogs (and therefore, all multi-session machines) in your Citrix DaaS deployment.

- **Horizontal load balancing:** An incoming user session is assigned to the least-loaded powered-on machine available.

  Simple example: You have two machines configured for 10 sessions each. The first machine handles five concurrent sessions. The second machine handles five.

  Horizontal load balancing offers high user performance, but it can increase costs as more machines are kept powered-on and busy.

  This method is enabled by default.

- **Vertical load balancing:** An incoming user session is assigned to the powered-on machine with the highest load index. Citrix DaaS calculates and then assigns a load index for every multi-session machine. The calculation considers factors such as CPU, memory, and concurrency.

  This method saturates existing machines before moving on to new machines. As users disconnect and free up capacity on existing machines, new load is assigned to those machines.

  Simple example: You have two machines configured for 10 sessions each. The first machine handles the first 10 concurrent sessions. The second machine handles the eleventh session.

  With vertical load balancing, sessions maximize powered-on machine capacity, which can save machine costs.

To configure the load balancing method:

1. From **Manage > Quick Deploy**, expand **General** on the right.
2. Under **Global Settings**, select **View All**.
3. On the **Global Settings** page, under **Multi-Session Catalog Load Balancing**, choose the load balancing method.
4. Select **Confirm**.

Create a catalog in a network that uses a proxy server

Follow this procedure if your network requires a proxy server for Internet connectivity, and you are using your own Azure subscription. (Using a Citrix Managed Azure subscription with a network requiring a proxy server is not supported.)

1. From **Manage > Quick Deploy**, start the catalog creation process by providing the required information and then selecting **Create Catalog** at the bottom of the page.

2. The catalog creation fails because of the proxy requirement. However, a resource location is created. That resource location's name begins with "DAS", unless you provided a resource location name when creating the catalog. On the **manage > Quick Deploy** dashboard, expand **Cloud Subscriptions** on the right. On the **Resource Locations** tab, check whether the newly created resource location has any Cloud Connectors in it. If it does, delete them.
3. In Azure, create two VMs (see Cloud Connector system requirements). Join those machines to the domain.
4. From the Citrix Cloud console, install a Cloud Connector on each VM. Make sure that the Cloud Connectors are in the same resource location that was created earlier. Follow the guidance in:
   - Cloud Connector proxy and firewall configuration
   - System and connectivity requirements
5. From **Manage > Quick Deploy**, repeat the catalog creation process. When the catalog is created, it uses the resource location and Cloud Connectors you created in the preceding steps.

Get help

- Review Troubleshoot.
- If you need further assistance with Citrix DaaS, open a ticket by following the guidance in How to Get Help and Support.

Create delivery groups

June 14, 2024

Introduction

A delivery group is a collection of machines selected from one or more machine catalogs. The delivery group can also specify which users can use those machines, plus the applications and desktops available to those users.

Creating a delivery group is the next step in configuring your deployment after creating a machine catalog. Later, you can change the initial settings in the first delivery group and create other delivery groups. There are also features and settings you can configure only when editing a delivery group, not when creating it.

Before creating a delivery group:

- Review this section to learn about the choices you make and the information you supply.
- Ensure that you have created a connection to the hypervisor, cloud service, or other resource that hosts your machines.
- Ensure that you have created a machine catalog containing virtual or physical machines.

To launch the delivery group creation wizard:

1. Sign in to Citrix Cloud. In the upper left menu, select **My Services > DaaS**.
2. Select **Manage**.
3. If this is the first delivery group being created, the console guides you to the correct selection (such as "Set up delivery groups to be displayed as services"). The delivery group creation wizard opens and walks you through the process.
4. If you already created a delivery group and want to create another, follow these steps:

    a) From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
    b) To organize delivery groups using folders, create folders under the default **Delivery Groups** folder. For more information, see Create a group folder.
    c) Select the folder where you want to create the group, and then click **Create Delivery Group**. The group creation wizard opens.

The wizard walks you through the pages described in the following sections. The wizard pages that you see might be different, depending on the selections you make.

Step 1. Machines

To create a delivery group with single-session suspend-capable only VMs, select **Make suspend capability required for this delivery group** check box.

> **Note:**
>
> - This feature is available only for single-session VMs for now.
> - If you don't want to create a suspend-capable delivery group, select a machine catalog, and follow the rest of the delivery group creation wizard instructions.

Select a machine catalog and select the number of machines you want to use from that catalog.

Good to know:

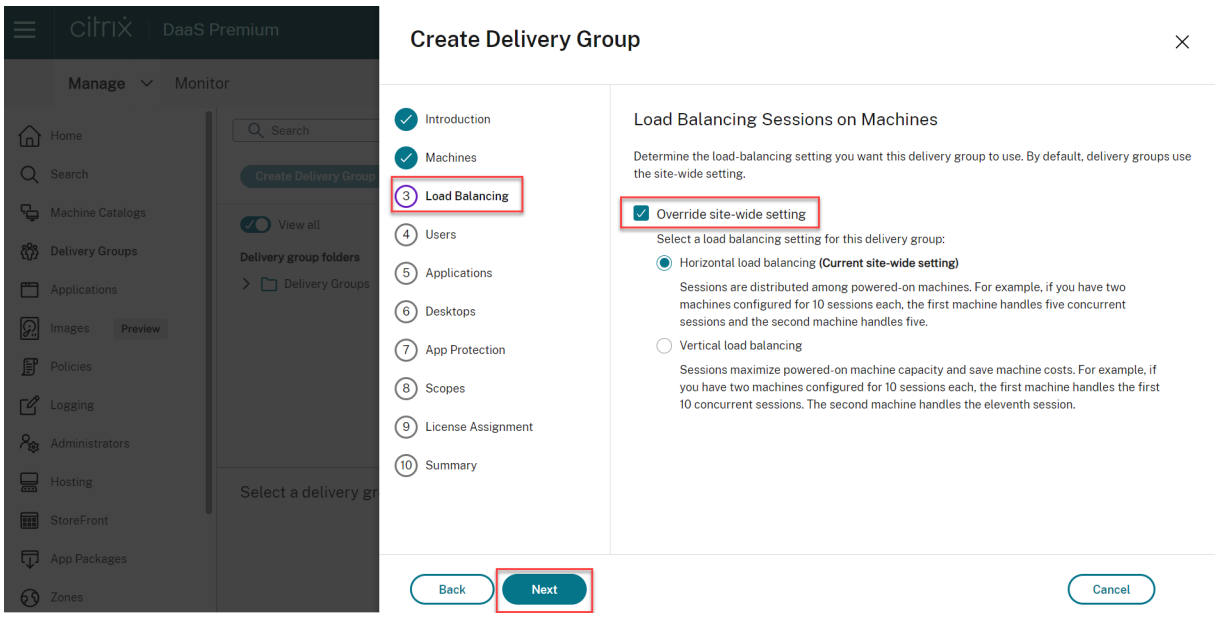
- At least one machine must remain unused in a selected catalog.
- A catalog can be specified in more than one delivery group. However, a machine can be used in only one delivery group.

- A delivery group can use machines from more than one catalog. However, those catalogs must contain the same machine types (multi-session OS, single-session OS, or Remote PC Access). In other words, you cannot mix machine types in a delivery group. Similarly, if your deployment has catalogs of Windows machines and catalogs of Linux machines, a delivery group can contain machines from either OS type, but not both.
- A MCS delivery group can only add a MCS type catalog.
- Citrix recommends that you install or upgrade all VDAs with the latest version, and then peform **Change functional level** for machine catalogs and delivery groups as needed. When creating a delivery group, if you select machines that have different VDA versions installed, the delivery group will be compatible with the earliest VDA version. For example, if one of the machines you select has VDA version 7.1 installed and other machines have a later version, all machines in the group can use only those features that were supported in VDA 7.1. This means that some features that require newer VDA versions might not be available in that delivery group.
- The following compatibility checks are performed:
  - MinimumFunctionalLevel must be compatible
  - SessionSupport must be compatible
  - AllocationType must be compatible for SingleSession
  - ProvisioningType must be compatible
  - PersistChanges must be compatible for MCS and Citrix Provisioning
  - RemotePC catalog is only compatible with RemotePC catalog
  - AppDisk related check

Step 2. Load balancing (Preview)

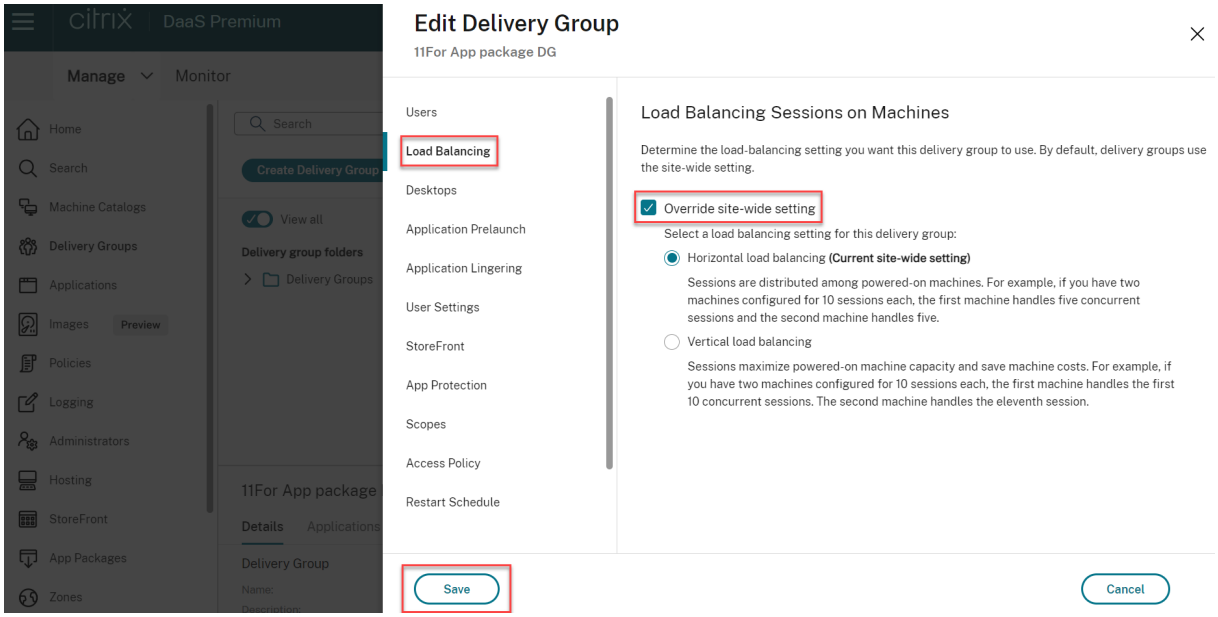
To configure the load balancing settings while creating a delivery group:

1. Log in to DaaS Premium.
2. In the left navigation, click **Delivery Groups**.
3. In the **Delivery Groups** page, click **Create Delivery Group**.
4. In the **Create Delivery Group** wizard, click **Next**. The **Machine** wizard opens.
5. In the **Machines** wizard, select a required machine catalog and click **Next**. The **Load Balancing** wizard opens.
6. In the **Load Balancing** wizard, select the **Override site-wide setting** checkbox.
7. Select the **Horizontal load balancing** or **Vertical load balancing option** as required and click **Next**.

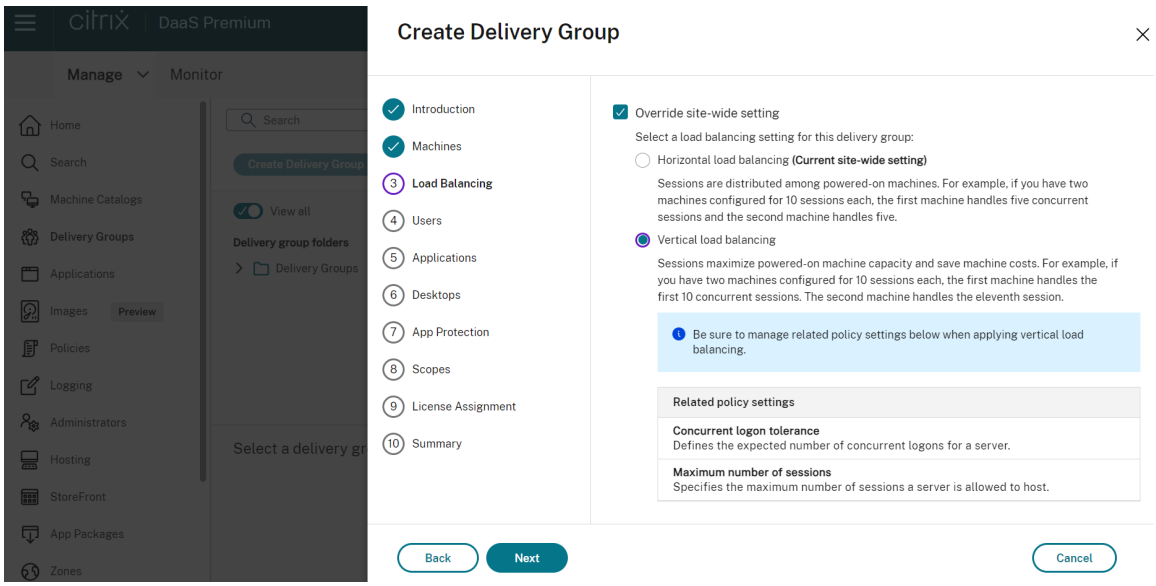


To configure the load balancing settings while editing an existing delivery group:

1. Log in to DaaS Premium.
2. In the left navigation, click **Delivery Groups**.
3. Select a **Delivery Group** from the list and click **Edit**. The **Edit Delivery Group** wizard opens.
4. In the **Edit Delivery Group** page, click **Load Balancing**.
5. Select the **Override site-wide setting** checkbox.
6. Select either **Horizontal load balancing** or **Vertical load balancing** option as required and click **Save**.



> **Note:**
>
> When Vertical load balancing setting is applied, make sure that the **Concurrent logon tolerance** and **Maximum number of sessions** polices are configured appropriately.



For more information about load balancing at site level and delivery group level, see Load balance machines.

Step 3. Delivery type

This page appears only if you chose a machine catalog containing static (assigned) single-session OS machines. Choose either **Applications** or **Desktops.** You cannot enable both.

If you selected machines from a multi-session OS or single-session OS random (pooled) catalog, the delivery type is assumed to be applications and desktops. You can deliver applications, desktops, or both.

Step 4. AppDisks

Ignore this page. Select **Next.**

Step 5. Users

Specify the users and user groups who can use the applications and desktops in the delivery group.

Where user lists are specified

User lists are specified when you create or edit the following:

- A deployment's user access list, which is not configured through this console. By default, the application entitlement policy rule includes everyone. See the PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlets for details.
- Delivery groups.
- Applications.

> **Note:**
>
> When specifying a user list, you can select user accounts from any of the following identity providers to which your Citrix Cloud account is connected: Active Directory, Azure Active Directory (Microsoft Entra ID), or Okta.

The list of users who can access an application is formed by the intersection of the above user lists.

Authenticated and unauthenticated users

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types in a delivery group.

- **Authenticated:** To access applications and desktops, the users and group members you specify by name must present credentials such as smart card or user name and password to StoreFront or Citrix Workspace app. (For delivery groups containing single-session OS machines, you can import user data (a list of users) later by editing the delivery group.)
- **Unauthenticated (anonymous):** For delivery groups containing multi-session OS machines, you can allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Workspace app. For example, at kiosks, the application might require credentials, but the Citrix access portal and tools do not. An Anonymous Users Group is created when you install the first Delivery Controller.

  To grant access to unauthenticated users, each machine in the delivery group must have a multi-session OS VDA installed. When unauthenticated users are enabled, you must have an unauthenticated StoreFront store.

  Unauthenticated user accounts are created on demand when a session is launched, and named AnonXYZ, in which XYZ is a unique three-digit value.

  Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

The following table describes your choices on the **Users** page:

Enable access for	Add/assign users and user groups?	Enable the "Give access to unauthenticated users"check box?
Only authenticated users	Yes	No
Only unauthenticated users	No	Yes
Both authenticated and unauthenticated users	Yes	Yes

Restricting user or group access

You can also restrict use of a delivery group by adding users or user groups to the **Allow list**. Only users on the **Allow list** can access apps and desktops in the delivery group. You can also add users and user groups to a block list by clicking **Add block list**, which prevents users from using apps and desktops in the selected delivery group. A block list is meaningful only when used to block users in the allow list.

Step 6. Applications

Good to know:

- You can add packaged applications to *Single-session static* and *Remote PC Access* delivery groups. The packages containing those applications are automatically mounted each time users sign in to their desktops or remote PCs.
- By default, new applications you add are placed in a folder named Applications. You can specify a different folder. For details, see the Applications article.
- You can change the properties for an application when you add it to a delivery group, or later. For details, see the Applications article.
- If you try to add an application and one with the same name already exists in that folder, you are prompted to rename the application you are adding. If you decline, the application is added with a suffix that makes it unique within that application folder.
- When you add an application to more than one delivery group, a visibility issue can occur if you do not have permission to view the application in all those delivery groups. In such cases, either consult an administrator with greater permissions or have your scope extended to include all the delivery groups to which the application was added.
- If you publish two applications with the same name to the same users, change the Application name (for user) property. Otherwise, users see duplicate names in Citrix Workspace app.

Select the **Add** menu to display the application sources.

- **From Start menu:** Applications that are discovered on a machine created from the image in the selected catalog. When you select this source, a new page launches with a list of discovered applications; select those you want to add and then select **OK**.
- **Manually:** Applications located in the deployment or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, select **OK**.
- **Existing:** Applications previously added to the deployment, perhaps in another delivery group. When you select this source, a new page launches with a list of discovered applications; select those you want to add and then select **OK**.
- **Application packages:** Applications in App-V, MSIX, MSIX app attach, or FlexApp application packages. When you select this source, the **Add Applications from Packages** page launches. Select an application package source, select the applications you want to add from the resulting display, and then select **OK**

  > **Note:**
  >
  > To publish MSIX or MSIX app attach apps, the delivery group's functional level must be 2106 or later. For FlexApp apps, the functional level must be 2206 or later. When a functional level requirement isn't met, the corresponding options in the **Application package source** dropdown list are dimmed.

- **Application group:** Application groups that exist in the deployment.

If an application source or application is not available or valid, it is either not visible or cannot be selected. For example, the **Existing** source is not available if no applications have been added to the deployment. Or, an application might not be compatible with the supported session types on machines in the selected machine catalog.

Step 7. App Protection

The following information is supplemental to the App protection article in the Citrix Virtual Apps and Desktops documentation. To use app protection in a Citrix DaaS deployment, follow the general guidance in that article, minding the following details.

- You must have a valid Citrix Cloud subscription and valid app protection entitlements. To purchase the app protection feature, you can contact your Citrix sales representative.
- App protection requires XML trust. To enable XML trust, go to **Settings > Enable XML trust**.

- Regarding anti-screen-capturing:
  - On Windows and macOS, only the window of the protected content is blank. App protection is active when a protected window is not minimized.
  - On Linux, the entire capture is blank. App protection is active whether a protected window is minimized or not.

To configure the Contextual App protection:

1. Click **Delivery Groups** in the left pane, select a **Delivery Group** and click **Edit**.
2. Click **App Protection** on the left and the following options are available:

Options	Description
Do not apply	Select this option to not apply the setting.
Apply to this delivery group	Select **Anti-keylogging** and/or **Anti key capturing** options. Hover over each of these settings to read the details in the tool tip.
Apply contextually	To apply this setting, configure the access policy in the **Access Policy settings** page. a) Click **Access Policy** in the left pane and click **Add**. b) On the **Add Policy** page, do the following • i. Enter a **Policy name** and configure the settings as required. • ii. In the **Filter** and **Value** fields, enter the details and click **Done**. The new policy is listed in the **Details App Protection** page. Enable the required settings for this policy. • iii. Click **Save**.

3. On the **Delivery Group** page, select the **Delivery Group** and click the **Details App Protection**. The new **App Protection** settings applied are displayed.

Step 8. Desktops (or Desktop Assignment Rules)

The title of this page depends on the machine catalog you chose earlier in the wizard:

- If you chose a catalog containing pooled machines, this page is titled **Desktops**.
- If you chose a catalog containing assigned machines and specified “Desktops”on the **Delivery Type** page, this page is titled **Desktop Assignment Rules**.
- If you chose a catalog containing assigned machines and specified “Applications”on the **Delivery Type** page, this page is titled **Applications**.

Select **Add**. In the dialog box:

- In the **Display name** and **Description** fields, type the information to be displayed in Citrix Workspace app.
- To add a tag restriction to a desktop, select **Restrict launches to machines with this tag** and then select the tag from the menu.
- Using the radio buttons, you can either:
  - **Allow everyone with access to this delivery group to use a desktop.** All users in the delivery group can launch a desktop (for groups with pooled machines) or be assigned a machine when they launch the desktop (for groups with assigned machines).
  - **Restrict desktop use** by adding users and user groups to the **Allow list**. Only users on the **Allow list** can access a desktop. You can also add users and user groups to a block list by clicking **Add block list,** which prevents users from using desktops in the selected delivery group. A block list is meaningful only when used to block users in the allow list.
- If the group contains assigned machines, specify the maximum number of desktops per user. This must be a value of one or greater.
- Enable or disable the desktop (for pooled machines) or desktop assignment rule (for assigned machines). Disabling a desktop stops desktop delivery. Disabling a desktop assignment rule stops desktop auto-assignment to users.
- When you are finished with the dialog box, select **OK**.

Step 9. License assignment

Determine which license you want the delivery group to use. By default, the delivery group uses the site license. For more information, see Multi-type licensing.

Step 10: Local Host Cache setting

This setting is visible only for delivery groups containing power-managed single-session pooled machines.

By default, those machines are unavailable when in Local Host Cache (LHC) mode due to data exposure risks. To change the default behavior and make them available for new user connections when in LHC mode, select **Keep resources available**.

Alternatively, you can change the default behavior using PowerShell commands. For more information, see Application and desktop support.

> **Important:**
>
> Enabling access to power-managed single-session pooled machines can cause data and changes from previous user sessions being present in subsequent sessions.

Step 11. Summary

Enter a name for the delivery group. You can also (optionally) enter a description, which appears in Workspace app and in the Full Configuration management interface.

Review the summary information and then select **Finish**. If you did not select any applications or specify any desktops to deliver, you are asked if you want to continue.

More information

- Manage delivery groups
- Applications

Manage delivery groups

June 14, 2024

Introduction

This article describes procedures for managing delivery groups from the management console. In addition to changing the settings specified when creating the group, you can configure other settings that are not available when you create a delivery group.

The procedures are organized by categories: general, users, machines, and sessions. Some tasks span more than one category. For example, "Prevent users from connecting to machines"is described in the machines category, but it also affects users. So, if you can't find a task in one category, check a related category.

Other articles also contain related information:

- Applications contains information about managing applications in delivery groups.
- Managing delivery groups requires the Delivery Group Administrator built-in role permissions. For details, see Delegated administration.

General

- View group details
- Change the delivery type
- Change StoreFront addresses

- Change the functional level
- Manage Remote PC Access delivery groups
- Change the license for a delivery group
- Organize delivery groups using folders
- Manage app protection
- Change suspend capability for a delivery group

View group details

1. Use the search function to locate a specific delivery group. Refer to Search for instances for instructions.
2. From the search results, select a group as necessary.
3. Refer to the following table for descriptions of the group columns.
4. Click a tab in the bottom details pane for more information about this group.

Column	Description
Delivery Group	The group name and the session type. Session types include Single-session OS and Multi-session OS.
Delivering	The type of resources delivered from this group. Possible values include Applications, Desktops, and Applications and Desktops. “Static machine assignment”appears if the delivery group consists of dedicated machines.
Session in Use	The number of machines that are set up and the number of machines that are in Disconnected state.
Allocated Count	The number of machines in the catalog assigned to a delivery group.
Folder	The location of the group within the **Delivery Groups** tree. It displays the name of the folder that the group is in (including the trailing backslash), or − if the group is at the root level.

Change the delivery type of a delivery group

The delivery type indicates what the group can deliver: applications, desktops, or both.

Before changing an **applications** type to the **Desktops** type, delete all applications from the group.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Delivery Type** page, select the delivery type you want.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Change StoreFront addresses

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **StoreFront** page, indicate whether you will specify a StoreFront server address later (**Manually**) or select **Add new** to specify the StoreFront servers you want to be used (**Automatically**).
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

You can also specify StoreFront server addresses by selecting **StoreFront** in the left pane of the console.

Change the functional level

Change the functional level for the delivery group after you upgrade the VDAs on its machines and the machine catalogs containing the machines used in the delivery group.

Before you start:

- If you use Citrix Provisioning (formerly Provisioning Services), upgrade the VDA version in the Citrix Provisioning console.
- Start the machines containing the upgraded VDA so that they can register with Citrix DaaS. This process tells the console about what must change in the delivery group.
- If you must continue to use earlier VDA versions, newer product features might not be available. For more information, see the upgrade documentation.

To change the functional level for a delivery group:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Change Functional Level** in the action bar. The **Change Functional Level** action appears only if upgraded VDAs are detected.

The display indicates you which, if any, machines cannot be changed to the functional level and why. You can then cancel the change action, resolve the machine issues, and then perform the change action again.

After the change completes, you can revert the machines to their previous states. Select the delivery group and then select **Undo Functional Level Change** in the action bar.

Manage Remote PC Access delivery groups

If a machine in a Remote PC Access machine catalog is not assigned to a user, the machine is temporarily assigned to a delivery group associated with that catalog. This temporary assignment enables the machine to be assigned to a user later.

The delivery group-to-machine catalog association has a priority value. Priority determines which delivery group that machine is assigned to when it registers with the system or when a user needs a machine assignment: the lower the value, the higher the priority. If a Remote PC Access machine catalog has multiple delivery group assignments, the software selects the match with the highest priority. Use the PowerShell SDK to set this priority value.

When first created, Remote PC Access machine catalogs are associated with a delivery group. This association means that machine accounts or Organizational Units added to the catalog later can be added to the delivery group. This association can be switched off or on.

To add or remove a Remote PC Access machine catalog association with a delivery group:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a Remote PC Access group.
3. In the **Details** section, select the **Machine Catalogs** tab and then select a Remote PC Access catalog.
4. To add or restore an association, select **Add Desktops**. To remove an association, select **Remove Association**.

Change the license for a delivery group

To change the license entitlement for a delivery group, follow these steps:

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **License Assignment** page, select the license you want the group to use.
4. Click **Apply** to apply any changes you made and to keep the window open. Or, click **Save** to apply changes and to close the window.

For more information about delivery group-level entitlements, see Multi-type licensing.

Organize delivery groups using folders

Create folders to organize delivery groups for easy access.

> **Tip:**
>
> You can set your preferred default view (folder or list view) for the Delivery Groups node by clicking the **Folder** icon on the top right of the action bar.

Required roles By default, you need to have the following built-in role to create and manage delivery group folders: Cloud Administrator, Full Administrator, or Delivery Group Administrator. If necessary, you can customize roles for creating and managing delivery group folders. For more information, see Required permissions.

Create a delivery group folder Before you start, plan how to organize your delivery groups. Consider the following:

- You can nest folders up to five levels (excluding the default root folder).
- A folder can contain delivery groups and subfolders.
- All nodes in **Full Configuration** (such as the **Machine Catalogs**, **Applications**, and **Delivery groups** nodes) share a folder tree in the back end. To avoid name conflicts with other nodes when renaming or moving folders, we recommend you give different names to first-level folders in different nodes.

To create a delivery group folder, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. In the folder hierarchy, select a folder and then select **Create Folder** in the **Action** bar.
3. Enter a name for the new folder, and then click **Done**.

> **Tip:**
>
> If you create a folder in an unintended location, you can drag it to the correct location.

Move a delivery group

You can move a delivery group between folders. Detailed steps are as follows:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. View groups by folder. You can also turn on **View all** above the folder hierarchy to view all groups at a time.
3. Right-click a group and then select **Move Delivery Group**.

4. Select the folder to which you want to move the group, and then click **Done**.

> **Tip:**
>
> You can drag a group to a folder.

Manage delivery group folders

You can delete, rename, and move delivery group folders.

Be aware that you can delete a folder only if it and its subfolders don't contain delivery groups.

To manage a folder, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. In the folder hierarchy, select a folder, and then select an action in the **Action** bar as needed:
   - To rename the folder, select **Rename Folder**.
   - To delete the folder, select **Delete Folder**.
   - To move the folder, select **Move Folder**.
3. Follow onscreen instructions to complete the remaining steps.

Required permissions The following table lists the permissions required to perform actions on delivery group folders.

Action	Required permissions
Create delivery group folders	Create Delivery Group Folder
Delete delivery group folders	Remove Delivery Group Folder
Move delivery group folders	Move Delivery Group Folder
Rename delivery group folders	Edit Delivery Group Folder
Move delivery groups to folders	Edit Delivery Group Folder and Edit Delivery Group Properties

Manage app protection

The following information is supplemental to the App protection article in the Citrix Virtual Apps and Desktops documentation. To use app protection in a Citrix DaaS deployment, follow the general guidance in that article, minding the following details.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **App Protection** page, you can see the following options:

Options	Description
Do not apply	Select this option to not apply the setting.
Apply to this delivery group	Select **Anti-keylogging** and/or **Anti key capturing** options. Hover over each of these settings to read the details in the tool tip.
Apply contextually	To apply this setting, configure the access policy in the **Access Policy settings** page. a) Click **Access Policy** in the left pane and click **Add**. b) On the **Add Policy** page, do the following • i. Enter a **Policy name** and configure the settings as required. • ii. In the **Filter** and **Value** fields, enter the details and click **Done**. The new policy is listed in the **App Protection** page. Enable the required settings for this policy. • iii. Click **Save**.

4. On the **Delivery Group** page, select the **Delivery Group** and click the **Details** tab at the bottom. The new **App Protection** settings applied are displayed.

- You must have a valid Citrix Cloud subscription and valid app protection entitlements. To purchase the app protection feature, you can contact your Citrix sales representative.
- App protection requires XML trust. To enable XML trust, go to **Settings > Enable XML trust**.
- Regarding anti-screen-capturing:
  - On Windows and macOS, only the window of the protected content is blank. App protection is active when a protected window is not minimized.
  - On Linux, the entire capture is blank. App protection is active whether a protected window is minimized or not.

Change suspend capability for a delivery group

Make the suspend capability required or optional for a delivery group:

- **Required**: The delivery group can only include those VMs that are suspend capable.
- **Optional**: The delivery group can include VMs that are or aren't suspend capable.

Before you begin You can only change the suspend-capability of a delivery group to `Required` if all the VMs present in the delivery group are suspend-capable.

To change the suspend-capability of a delivery group:

1. From **Manage** > **Full Configuration**, go to **Delivery Groups** in the left pane.
2. Select a group, and then click **Change Suspend Capability** in the action bar.

Users

> **Note:**
>
> The option **Leave user management to Citrix Cloud** has been removed. To manage user assignments for existing delivery groups set to **Leave user management to Citrix Cloud**, you have two options: Citrix Cloud library or Full Configuration. For more information about the Full Configuration approach, see Manage user assignments for Citrix Cloud Library-managed delivery groups.

This topic covers the following sections:

- Change user settings
- Add or remove users
- Manage user assignments for Citrix Cloud Library-managed delivery groups

Change user settings in a delivery group

The name of this page appears as either **User Settings** or **Basic Settings**.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **User Settings** page, change any of the settings in the following table.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Setting	Description
Description	The text that Citrix Workspace (or StoreFront) uses and that users see.
Enable Delivery Group	Whether the delivery group is enabled.

Setting	Description
Time zone	The time zone in which the machines of this delivery group must reside. The option lists the time zones supported by the site. **Note:** Changing the time zone on a delivery group might reboot the machines in that delivery group. To avoid this, ensure to change the time zone settings outside of production hours.
Enable Secure ICA	Secures communications to and from machines in the delivery group using SecureICA, which encrypts the ICA protocol. The default level is 128-bit. The level can be changed using the SDK. Citrix recommends using more encryption methods such as TLS encryption when traversing public networks. Also, SecureICA does not check data integrity.
Maximum desktops per user	How many desktops a user can have.

Add or remove users in a delivery group

For detailed information about users, see Users.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Users** page:
   - To add users, select **Add**, and then specify the users you want to add.
   - To remove users, select one or more users and then select **Remove**.
   - Select or clear the check box to allow access by unauthenticated users.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Manage user assignments To manage user assignments:

1. In **Manage > Full Configuration**, select **Delivery Groups**.
2. Select a group and then select **Edit** in the action bar.
3. On the **Machine Allocation** page, add or remove users. To add users, browse to them or enter a semicolon-separated list of user names.

When entering user names, consider the following:

- If the users are in Active Directory, enter the names directly. If not, enter the names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`.

Manage user assignments for Citrix Cloud Library-managed delivery groups

To manage user assignments for Citrix Cloud Library-managed delivery groups, use Citrix Cloud Library or Full Configuration.

To accomplish this task using Full Configuration, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a Citrix Cloud-managed delivery group, and then select **Edit** in the action bar.
3. To restrict the use of a desktop to certain users, follow these steps:

    a) On the **Desktops** or **Desktop Assignment Rules** page, select the desktop and click **Edit**. The **Edit Desktop** page appears with the **Restrict desktop use** option selected.
    b) Click **Add**, select one or more users as needed, and then click **Done**.
    c) Click **OK**.

4. To restrict the use of applications in this group to certain users, click **Application Assignment Rule** in the left pane, and follow the similar steps described in step 3 to add users.

Machines

- Change assignments of machines to users
- Enable Local Host Cache for single-session pooled VDAs
- Update a machine
- Add, change, or remove a tag restriction for a desktop
- Remove a machine
- Restrict access to resources
- Prevent users from connecting to a machine (maintenance mode)
- Shut down and restart machines
- Create and manage restart schedules for machines
- Load manage machines
- Manage Autoscale

In addition to the features described in this article, see Autoscale for information about proactively power managing machines.

Change assignments of machines to users in a delivery group

You can change the assignments of single-session OS machines provisioned with MCS. You cannot change assignments for multi-session OS machines or machines provisioned with Citrix Provisioning.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Machine Allocation** page, specify the new users.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Enable Local Host Cache for single-session pooled VDAs

By default, power-managed single-session pooled machines are unavailable when in Local Host Cache mode. You can override the default behavior on a per-delivery group basis. Detailed steps are as follows:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.

   In the group list, groups containing single-session pooled machines provisioned by MCS or Citrix Provisioning display a warning icon.

2. Select a group as needed, then select **Edit** in the action bar.
3. On the **Local Host Cache** page, select **Keep resources available**.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Alternatively, you can override the default behavior using PowerShell commands. For more information, see Application and desktop support.

> **Important:**
>
> Enabling access to power-managed single-session pooled machines can cause data and changes from previous user sessions being present in subsequent sessions.

Update a machine in a delivery group

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. Select a machine and then select **Update Machines** in the action bar.

To choose a different image, select **Image** and then select a snapshot.

To apply changes and notify machine users, select **Rollout notification to end-users**. Then specify:

- When to update the image: now or on the next restart
- The restart distribution time (the total time to begin updating all machines in the group)
- Whether users are notified of the restart
- The message users will receive

Add, change, or remove a tag restriction for a desktop

Adding, changing, and removing tag restrictions can have unanticipated effects on which desktops are considered for launch. Review the considerations and cautions in Tags.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the Actions bar.
3. On the **Desktops** page, select the desktop and select **Edit**.
4. To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag.
5. To change or remove a tag restriction, either:
    - Select a different tag.
    - Remove the tag restriction by clearing **Restrict launches to machines with this tag**.
6. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Remove a machine from a delivery group

Removing a machine deletes it from a delivery group. It does not delete it from the machine catalog that the delivery group uses. Therefore, that machine is available for assignment to another delivery group.

Machines must be shut down before they can be removed. To temporarily stop users from connecting to a machine while you are removing it, put the machine into maintenance mode before shutting it down.

Machines might contain personal data, so use caution before allocating the machine to another user. Consider reimaging the machine.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.

3. Ensure that the machine is shut down.
4. Select the machine and then select **Remove from Delivery Group** in the action bar.

You can also remove a machine from a delivery group through the connection the machine uses.

Restrict access to resources in a delivery group

Any changes you make to restrict access to resources in a delivery group supersede previous settings, regardless of the method you use. You can:

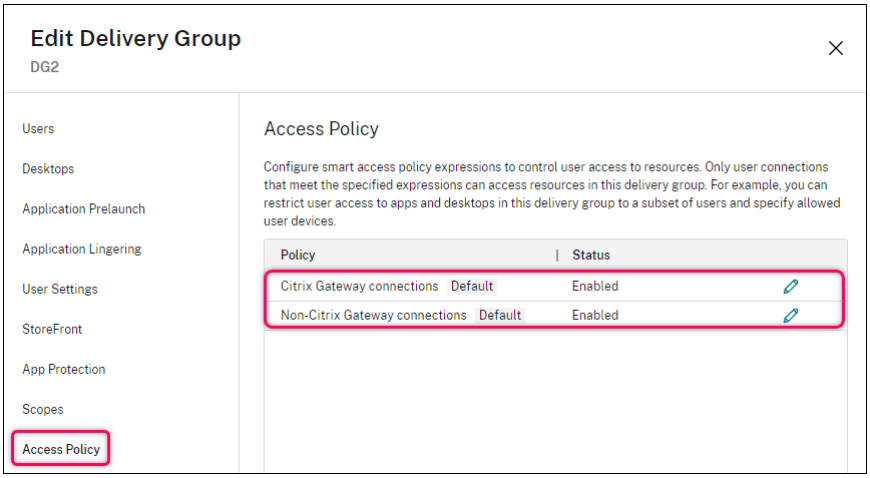
- **Restrict access for administrators using delegated administration scopes:** You can create and assign a scope that permits administrators to access all applications and another scope that provides access to only certain applications. For details, see Delegated administration.
- **Restrict access for users through smart access policy expressions:** You can configure access policy rules to control user access to a specific delivery group. Examples include:
  - Restrict access to a subset of users and specify allowed user devices.
  - Restrict access to users connected through Workspace (instead of StoreFront).
  - Restrict access to users connected through a specific Workspace URL.

This section guides you through how to restrict user access to delivery groups through access policy rules:

- About access policy rules
- Add access policy rules
- Manage access policy rules using Full Configuration
- Add and refine policy rules using PowerShell

About access policy rules You can configure multiple access policy rules for a delivery group. Apps and desktops in a delivery group appear in a user's StoreFront or Workspace when the user's connection matches any access policy rule you defined for the delivery group, irrespective of order.

Each rule can be individually enabled or disabled. A disabled rule is ignored when the access policy is evaluated.



In Full Configuration, the Access Policy list includes the following default SmartAccess policy rules. You can add more as necessary.

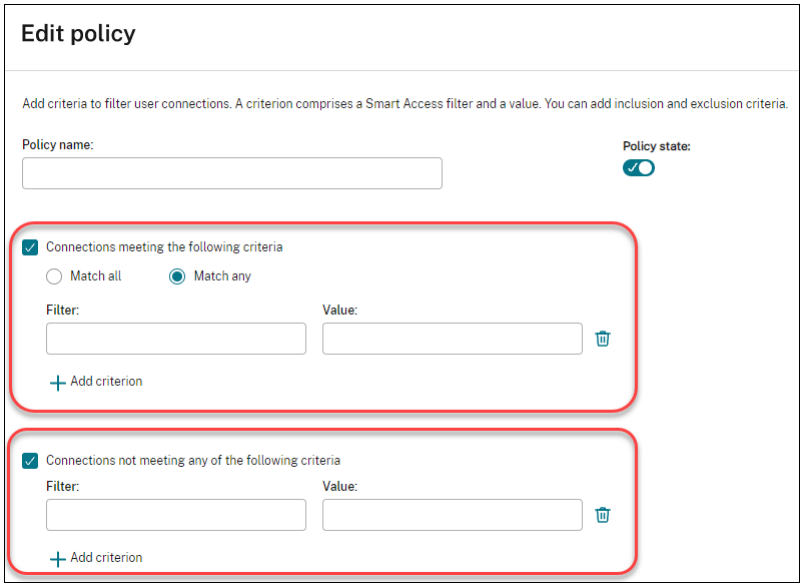
- **Citrix Gateway connections.** This policy allows only user connections made through Citrix Gateway can access resources within the delivery group. User connections made through Workspace when either the Device Posture or Network Location features are enabled are also considered connections through Citrix Gateway.
- **Non-Citrix Gateway connections.** This policy allows only user connections made not through Citrix Gateway can access resources within the delivery group.

> **Note:**
>
> - To prevent the default rules from overriding a newly configured one, you must either disable the default rules or refine them to exclude the filters used in the new policy.
> - The default policies can't be deleted but they can be disabled. To disable a policy, click the **Edit** icon and then change the **Policy state** to **Disabled**.
> - The policy list also shows rules added using PowerShell commands. Those policies can be deleted but can't be edited in Full Configuration.

Add access policy rules using Full Configuration An access policy rule comprises a set of filters. For more information about filters, see this article. When adding an access policy rule, you add multiple condition filters to the rule as needed.

To add a policy for a delivery group using Full Configuration, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Access Policy** page, click **Add**. The **Add Policy** page appears.



4. In the **Policy name** field, type a descriptive name for the policy. The name must be unique in your deployment.
5. To define the criteria for allowed user connections, follow these steps:
   a) Select **Connections meeting the following criteria**.
   b) Click **Add criterion**.
   c) In the **Filter** field, type the name of the filter that you want to use. In the **Value** field, type a desired value for the filter. For example, to allow only users connected through Workspace (instead of StoreFront) to access resources in this delivery group, type `Citrix-Via-Workspace` for **Filter** and `True` for **Value**.
   d) To add more criteria, repeat steps b-c.
   e) Select the relationship among the criteria:
      - **Match any**. Allows access only when the incoming user connection meets any of the configured filter criteria.
      - **Match all**. Allows access only when the incoming user connection meets all of the configured filter criteria.
6. To define the criteria for prohibited user connections, follow these steps:
   a) Select **Connections not meeting any of the following criteria**.
   b) Click **Add criterion**.
   c) In the **Filter** field, type the name of the filter that you want to use. In the **Value** field, type a desired value for the filter. For example, to prohibit users connected through the `example.cloud.com` Workspace URL from accessing resources in this delivery group.

Type `Citrix.Workspace.UsingDomain` for **Filter** and `example.cloud.com` for **Value**.

d) To add more criteria, repeat steps b-c.

> **Note:**
>
> User connections meeting any of the configured criteria are prohibited from resources in this delivery group.

7. Click **Done**.

   The new policy appears in the policy list.

8. Review and refine the default policy rules to avoid unintentional overlaps with connections covered by this new policy. To refine the existing policies, use the following ways:

   - Disable the default policy rules.
   - Configure the default policy rules to exclude the SmartAccess filters that you added to the inclusion criteria of the new policy. For more information, see Manage policy rules using Full Configuration and Add and manage access policy rules using PowerShell.

> **Important:**
>
> As explained in About access policy rules, when a user's connection matches one or more policy rules in a delivery group, the user gains access to its resources. Therefore, after creating a rule, you must carefully review and refine the existing rules to avoid any unintentional overlaps with connections covered by the new rule.

Manage access policy rules using Full Configuration You can use the inclusion and exclusion criteria to refine the default policies. For example, to restrict access to a subset of those connections, follow these steps:

1. Edit a default policy.
2. Select **Connections meeting any of the following criteria**.
3. Add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios.

For more information, see the Citrix Gateway documentation.

Add and manage access policy rules using PowerShell You can use the following PowerShell cmdlets to add and manage access policy rules for delivery groups:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule

- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

For more information, see the relative articles in the Citrix Developer Documentation.

Prevent users from connecting to a machine (maintenance mode) in a delivery group

When you need to temporarily stop new connections to machines, you can turn on maintenance mode for one or all machines in a delivery group. You might do this before applying patches or using management tools.

- When a multi-session OS machine is in maintenance mode, users can connect to existing sessions, but cannot start new sessions.
- When a single-session OS machine (or a PC using Remote PC Access) is in maintenance mode, users cannot connect or reconnect. Current connections remain connected until they disconnect or log off.

To turn maintenance mode on or off:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group.
3. To turn on maintenance mode for all machines in the delivery group, select **Turn On Maintenance Mode** in the action bar.

   To turn on maintenance mode for one machine, select **View Machines** in the action bar. Select a machine, and then select **Turn On Maintenance Mode** in the action bar.
4. To turn maintenance mode off for one or all machines in a delivery group, follow the previous instructions, but select **Turn Off Maintenance Mode** in the action bar.

Windows Remote Desktop Connection (RDC) settings also affect whether a multi-session OS machine is in maintenance mode. Maintenance mode is on when any of the following occur:

- Maintenance mode is set to on, as described earlier.
- RDC is set to **Don't allow connections to this computer**.
- RDC is not set to **Don't allow connections to this computer** and the Remote Host Configuration User Logon Mode setting is either **Allow reconnections, but prevent new logons** or **Allow reconnections, but prevent new logons until the server is restarted**.

You can also turn maintenance mode on or off for:

- A connection, which affects the machines using that connection.
- A machine catalog, which affects the machines in that catalog.

Shut down and restart machines in a delivery group

This procedure is not supported for Remote PC Access machines.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. Select the machine and then select one of the following actions in the action bar:

   > **Note:**
   >
   > - The following actions apply only to machines that are power managed.
   > - Some options might not be available, depending on the machine state.

   - **Force shut down:** Forcibly powers off the machine and refreshes the list of machines.
   - **Restart:** Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the machine remains in its current state.
   - **Force restart:** Forcibly shuts down the operating system and then restarts the machine.
   - **Suspend:** Pauses the machine without shutting it down, and refreshes the list of machines.
   - **Shut down:** Requests the operating system to shut down.

For non-force actions, if the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during the shutdown, there is a risk that the machine will be powered off before the updates finish.

Create and manage restart schedules for machines in a delivery group

> **Note:**
>
> - When a restart schedule is applied to a delivery group with Autoscale enabled, its machines are just powered off and left for Autoscale to power them on.
> - When restart schedules are applied to random single-session machines, those machines are powered off rather than restarted, to save costs. We recommend that you use Autoscale to power on machines.
> - Changing the time zone on a delivery group might reboot the machines in that delivery group. To avoid this, ensure to change the time zone settings outside of production hours.

A restart schedule specifies when machines in a delivery group are periodically restarted. You can create one or more schedules for a delivery group. A schedule can affect either:

- All the machines in the group.

- One or more (but not all) machines in the group. The machines are identified by a tag that you apply to the machine. This is called a tag restriction, because the tag restricts an action to only items (in this case, machines) that have the tag.

For example, let's say all of your machines are in one delivery group. You want every machine restarted once every week, and you want the machines used by the accounting team restarted daily. To accomplish this, set up one schedule for all machines, and another schedule for only the machines in accounting.

A schedule includes the day and time the restart begins, and the duration. The duration is either "start all affected machines at the same time"or an interval it will likely take to restart all affected machines.

You can enable or disable a schedule. Disabling a schedule can be helpful when testing, during special intervals, or when preparing schedules before you need them.

You cannot use schedules for automated power-on or shutdown from the management console, only to restart.

Schedule overlap Multiple schedules can overlap. In the example above, both schedules affect the accounting machines. Those machines might be restarted twice on Sunday. The scheduling code is designed to avoid restarting the same machine more often than intended, but it cannot be guaranteed.

- If the schedules coincide precisely in start and duration times, it is more likely that the machines will be restarted only once.
- The more the schedules differ in start and duration times, it's more likely that multiple restarts will occur.
- The number of machines affected by a schedule also affects the chance of an overlap. In the example, the weekly schedule that affects all machines might initiate restarts faster than the daily schedule for accounting machines, depending on the duration specified for each.

For an in-depth look at restart schedules, see Reboot schedule internals.

View restart schedules

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. Select the **Restart Schedule** page.

The **Restart Schedule** page contains the following information for each configured schedule:

- Schedule name.
- Tag restriction used, if any.

- How often the machine restarts occur.
- Whether machine users receive a notification.
- Whether the schedule is enabled. Disabling a schedule can be helpful when testing, during special intervals, or when preparing schedules before you need them.

Add (apply) tags When you configure a restart schedule that uses a tag restriction, ensure that the tag has been added (applied) to the machines that the schedule affects. In the example above, each of the machines used by the accounting team has a tag applied. For details, see Tags.

Although you can apply more than one tag to a machine, a restart schedule can specify only one tag.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select the group containing the machines to be controlled by the schedule.
3. Select **View Machines** and then select the machines you want to add a tag to.
4. Select **Manage Tags** in the action bar.
5. If the tag exists, enable the check box next to the tag name. If the tag does not exist, select **Create** and then specify the name for the tag. After the tag is created, enable the check box next to the newly created tag name.
6. Select **Save** in the **Manage Tags** dialog.

Create a restart schedule

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Restart Schedule** page, select **Add**.
4. On the **Add Restart Schedule** page:
    - To enable the schedule, select **Yes**. To disable the schedule, select **No**.
    - Type a schedule name and description.
    - For **Restrict to tag**, apply a tag restriction.
    - For **Include machines in maintenance mode**, choose whether to include machines that are in maintenance mode in this schedule. To use PowerShell instead, see Scheduled restarts for machines in maintenance mode.
    - For **Restart frequency**, select how often the restart occurs: daily, weekly, monthly, or once. If you select **Weekly** or **Monthly**, you can specify one or more specific days.
    - For **Repeats every**, specify how often you want the schedule to run.
    - For **Start date**, specify a start date for the first occurrence of the schedule.

- For **Begin restart at**, specify, in 24-hour clock format, the time of day to begin the restart.
- For **Restart duration**:
  - If you do not want to use natural restart, select **Restart all machines at the same time** or **Restart all machines within a time period**.
  - If you want to use natural restart, select **Restart all machines after draining all sessions**.

    Upon starting a restart schedule that is configured to use natural restart:

    * All idle machines belonging to the delivery group are restarted immediately
    * Each machine belonging to the delivery with one or more active sessions are restarted when all sessions are logged off.

    > **Note:**
    >
    > You can use this option for machines that are power managed and also for machines that are not power managed.

- In **Send notification to users**, choose whether to display a notification message on the applicable machines before a restart begins. By default, no message appears.
- If you choose to display a message 15 minutes before the restart begins, you can choose (in **Notification frequency**) to repeat the message every five minutes after the initial message. By default, the message does not repeat.
- Enter the notification title and text. There is no default text.

  If you want the message to include a countdown to restart, include the variable **%m%**. Unless you chose to restart all machines at the same time, the message appears on each machine at the appropriate time before the restart.

5. Click **Done** to apply the changes and to close the **Add Restart Schedule** window.
6. Click **Apply** to apply the changes you made and keep the **Edit Delivery Group** window open. Or, click **Save** to apply changes and to close the window.

Immediately run a restart schedule A restart schedule specifies when machines in a delivery group restart regularly. You can also run a restart schedule immediately to restart the machines in that schedule.

To run a restart schedule immediately, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select the applicable delivery group and then select **Edit** in the action bar

3. On the **Restart Schedule** page, select a schedule that you want to run and then select **Run schedule now**.

> **Note:**
>
> - You cannot run a schedule immediately if it is configured with the **Restart all machines after draining sessions** setting.
> - You can apply **Run schedule now** only to one schedule at a time.
> - After you edit a schedule, **Run schedule now** becomes unavailable. Select **Apply** to make it available.

Edit, remove, enable, or disable a restart schedule

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Restart Schedule** page, select the check box for a schedule.
    - To edit a schedule, select **Edit**. Update the schedule configuration, using the guidance in Create a restart schedule.
    - To enable or disable a schedule, select **Edit**. Select or clear the **Enable restart schedule** check box.
    - To remove a schedule, select **Remove**. Confirm the removal. Removing a schedule does not affect any tags applied to machines in the affected machines.

Scheduled restarts delayed due to database outage

> **Note:**
>
> This feature is available only in PowerShell.

If a site database outage occurs before a scheduled restart begins for machines (VDAs) in a delivery group, the restarts begin when the outage ends. This action can have unintended results.

For example, let's say you've scheduled a delivery group's restarts to occur during off-production hours (beginning at 3 am). A site database outage occurs one hour before a scheduled restart begins (2 am). The outage lasts six hours (until 8 am). The restart schedule begins when the connection between the Delivery Controller and the site database is restored. The VDA restarts now begin five hours after their original schedule. This action might result in VDAs restarting during production hours.

To help avoid this situation, you can use the `MaxOvertimeStartMins` parameter for the `New-BrokerRebootScheduleV2` and `Set-BrokerRebootScheduleV2` cmdlets. The value specifies the maximum number of minutes beyond the scheduled start time that a restart schedule can begin.

- If the database connection is restored within that time (scheduled time + `MaxOvertimeStartMins`), the VDA restarts begin.

- If the database connection is not restored within that time, the VDA restarts do not begin.
- If this parameter is omitted or has a zero value, the scheduled restart begins when the connection to the database is restored, regardless of the outage duration.

For more information, see the cmdlet help. This feature is available only in PowerShell.

Scheduled restarts for machines in maintenance mode To indicate whether a restart schedule affects machines that are in maintenance mode, use the `IgnoreMaintenanceMode` option with the `BrokerRebootScheduleV2` cmdlets.

For example, the following cmdlet creates a schedule that restarts both machines that are and machines that are not in maintenance mode.

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

The following cmdlet modifies an existing restart schedule.

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

For more information, see the cmdlet help.

Load manage machines in delivery groups

You can load manage multi-session OS machines only.

Load management measures the server load and determines which server to select under the current environment conditions. This selection is based on:

- **Server maintenance mode status:** A multi-session OS machine is considered for load balancing only when maintenance mode is off.
- **Server load index:** Determines how likely a server delivering multi-session OS machines is to receive connections. The index is a combination of load evaluators: the number of sessions and the settings for performance metrics such as CPU, disk, and memory use. Load evaluators are specified in load management policy settings.

  A server load index of 10000 indicates that the server is fully loaded. If no other servers are available, users might receive a message that the desktop or application is currently unavailable when they launch a session.

  You can monitor the load index in Director (Monitor), a Full Configuration management interface search, and the SDK.

In console displays, to display the **Server Load Index** column (which is hidden by default), select a machine, right-click a column header, and then select **Select Column**. In the **Machine category**, select **Load Index**.

In the SDK, use the `Get-BrokerMachine` cmdlet. For details, see CTX202150.

- **Concurrent logon tolerance policy setting:** The maximum number of concurrent requests to log on to the server. (This setting is equivalent to load throttling in XenApp 6.x versions.)

  When all servers are at or higher than the concurrent logon tolerance setting, the next logon request is assigned to the server with the lowest pending logons. If more than one server meets these criteria, the server with the lowest load index is selected.

Manage Autoscale

By default, Autoscale is disabled for delivery groups. To manage Autoscale for a delivery group (if applicable), follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Manage Autoscale** in the action bar. The **Manage Autoscale** window appears.
3. Configure settings as needed. For information about Autoscale settings, see Autoscale.
4. Select **Apply** to apply any changes you made and to keep the window open. Or, select **Save** to apply changes and to close the window.

Sessions

- Log off or disconnect a session, or send a message to users
- Configure session prelaunch and session linger
- Configure session roaming
- Control session reconnection when disconnected from machine in maintenance mode

Log off or disconnect a session, or send a message to delivery group users

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. To log a user off a session, select the session or desktop and then select **Log off** in the action bar. The session closes and the machine becomes available to other users, unless it is allocated to a specific user.
4. To disconnect a session, select the session or desktop and then select **Disconnect** in the action bar. Applications continue to run and the machine remains allocated to that user. The user can reconnect to the same machine.

5. To send a message to users, select the session, machine, or user and then select **Send message** in the action bar. Enter the message.

Configure session prelaunch and session linger in a delivery group

These features are supported only on multi-session OS machines.

The session prelaunch and session linger features help specified users access applications quickly, by:

- Starting sessions before they are requested (session prelaunch)
- Keeping application sessions active after a user closes all applications (session linger)

By default, session prelaunch and session linger are not used. A session starts (launches) when a user starts an application, and remains active until the last open application in the session closes.

Considerations:

- The delivery group must support applications, and the machines must be running a VDA for multi-session OS, minimum version 7.6.
- These features are supported only when using Citrix Workspace app for Windows, and also require more Citrix Workspace app configuration. For instructions, search for session prelaunch in the product documentation for your Citrix Workspace app for Windows version.
- Citrix Workspace app for HTML5 is not supported.
- When using session prelaunch, if a user's machine is put into suspend or hibernate mode, prelaunch does not work (regardless of session prelaunch settings). Users can lock their machines/sessions. However, if a user logs off from Citrix Workspace app, the session is ended and prelaunch no longer applies.
- When using session prelaunch, physical client machines cannot use the suspend or hibernate power management functions. Client machine users can lock their sessions but should not log off.
- Prelaunched and lingering sessions consume a concurrent license, but only when connected. If using a user/device license, the license lasts 90 days. Unused prelaunched and lingering sessions disconnect after 15 minutes by default. This value can be configured in PowerShell (`New-BrokerSessionPreLaunch` cmdlet).
- Careful planning and monitoring of your users' activity patterns are essential to tailoring these features to complement each other. Optimal configuration balances the benefits of earlier application availability for users against the cost of keeping licenses in use and resources allocated.
- You can also configure session prelaunch for a scheduled time of day in Citrix Workspace app.

How long unused prelaunched and lingering sessions remain active There are several ways to specify how long an unused session remains active if the user does not start an application: a config-

ured timeout and server load thresholds. You can configure all of them. The event that occurs first causes the unused session to end.

- **Timeout:** A configured timeout specifies the number of minutes, hours, or days an unused prelaunched or lingering session remains active. If you configure too short a timeout, prelaunched sessions end before they provide the user benefit of quicker application access. If you configure too long a timeout, incoming user connections might be denied because the server doesn't have enough resources.

  You can enable this timeout from the SDK only (`New`/`Set-BrokerSessionPreLaunch` cmdlet), not from the management console. If you disable the timeout, it does not appear in the console display for that delivery group or in the **Edit Delivery Group** pages.

- **Thresholds:** Automatically ending prelaunched and lingering sessions based on server load ensures that sessions remain open as long as possible, assuming that server resources are available. Unused prelaunched and lingering sessions do not cause denied connections because they are ended automatically when resources are needed for new user sessions.

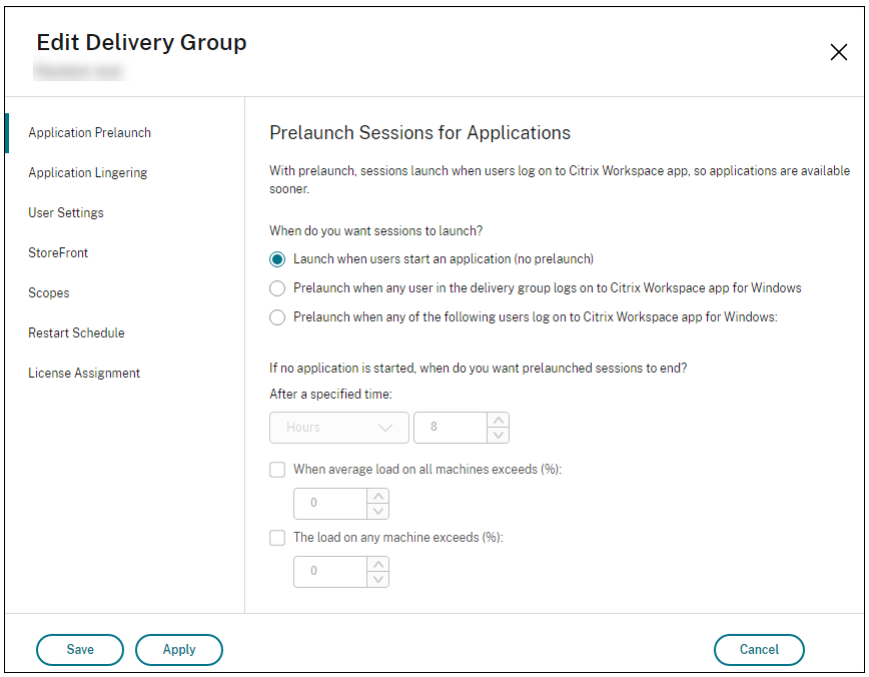
  You can configure two thresholds: the average percentage load of all servers in the delivery group, and the maximum percentage load of a single server in the group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended. Sessions are ended one-by-one at minute intervals until the load falls below the threshold. While the threshold is exceeded, no new prelaunch sessions are started.

Servers with VDAs that have not registered with a Controller and servers in maintenance mode are considered fully loaded. An unplanned outage causes prelaunch and lingering sessions to end automatically to free capacity.

To enable session prelaunch

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Application Prelaunch** page, enable session prelaunch by choosing when sessions launch:

   - When a user starts an application. This is the default setting. Session prelaunch is disabled.
   - When any user in the delivery group logs on to Citrix Workspace app for Windows.
   - When anyone in a list of users and user groups logs on to Citrix Workspace app for Windows. Be sure to also specify users or user groups if you choose this option.



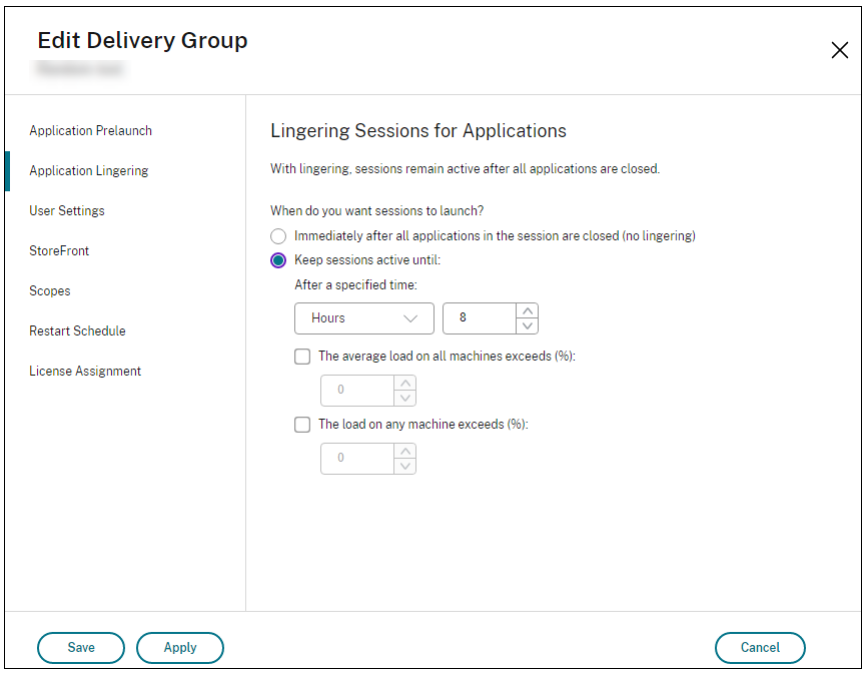
4. A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active.

   - When a specified time interval elapses. You can change the time interval (1–99 days, 1–2376 hours, or 1–142,560 minutes).
   - When the average load on all machines in the delivery group exceeds a specified percentage (1–99%).
   - When the load on any machine in the delivery group exceeds a specified percentage (1–99%).

   Recap: A prelaunched session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

To enable session linger

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Application Lingering** page, enable session linger by selecting **Keep sessions active until**.



4. Several settings affect how long a lingering session remains active if the user does not start another application.

   - When a specified time interval elapses. You can change the time interval: 1–99 days, 1–2376 hours, or 1–142,560 minutes.
   - When the average load on all machines in the delivery group exceeds a specified percentage: 1–99%.
   - When the load on any machine in the delivery group exceeds a specified percentage: 1–99%.

   Recap: A lingering session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

Configure session roaming

By default, session roaming is enabled for delivery groups. Sessions roam between client devices with the user. When the user launches a session and then moves to another device, the same session is used and applications are simultaneously available on both devices. You can view the applications on multiple devices. The applications follow, regardless of the device or whether current sessions exist. Often, printers and other resources assigned to the application also follow. Alternatively, you can also use PowerShell. For more information, see Session roaming.

Configure session roaming for applications To configure session roaming for applications, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Users** page, enable session roaming by selecting the **Sessions roam with users as they move between devices** check box.
    - When enabled, if a user launches an application session and then moves to another device, the same session is used and available on both devices. When disabled, the session no longer roams between devices.
4. Select **OK** to apply changes and close the window.

Configure session roaming for desktops To configure session roaming for a desktop, follow these steps:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Desktops** page, select the desktop and select **Edit**.
4. Enable session roaming by selecting the **Session roaming** check box.
    - When enabled, if the user launches the desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.
5. Select **OK** to apply changes and close the window.

Control session reconnection when disconnected from machine in maintenance mode

> **Note:**
>
> This feature is available only in PowerShell.

You can control whether sessions that are disconnected on machines in maintenance mode are allowed to reconnect to machines in the delivery group.

Before late May 2021, reconnection was not allowed for single-session pooled desktop sessions that had disconnected from machines in maintenance mode. Now, you can configure a delivery group to allow or prohibit reconnections (regardless of session type) after disconnection from a machine in maintenance mode.

When creating or editing a delivery group (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), use the `-AllowReconnectInMaintenanceMode` <**boolean**> parameter to allow or prohibit reconnections for machines that were disconnected from a machine in maintenance mode.

- When set to true, sessions can reconnect to machines in the group.
- When set to false, sessions cannot reconnect to machines in the group.

Default values:

- Single-session: Disabled
- Multi-session: Enabled

Applications

View applications in a delivery group and add more if needed.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.
2. Select a group. If this group contains applications, **View Applications** appears in the action bar.
3. Select **View Applications**. You are directed to the **Applications** node where all applications available in this group appear.
4. To add more applications to this group, go to the **Delivery Groups** node, select the group, and select **Add Applications** in the action bar.

Troubleshoot

- VDAs that are not registered with a Delivery Controller are not considered when launching brokered sessions. This results in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which an administrator can troubleshoot. The details display provides troubleshooting information in the catalog creation wizard, and after you add a catalog to a delivery group.

  After you create a delivery group, the details pane for a delivery group indicates the number of machines that are expected to be registered but are not. For example, one or more machines are powered on and not in maintenance mode, but are not currently registered with a Controller. When viewing a "not registered, but should be"machine, review the **Troubleshoot** tab in the details pane for possible causes and recommended corrective actions.

  For messages about functional level, see VDA versions and functional levels.

  For information about VDA registration troubleshooting, seeCTX136668.

- In the display for a delivery group, the **Installed VDA version** in the details pane might differ from the actual version installed on the machines. The machine's Windows Programs and Features display shows the actual VDA version.
- For machines with **Power State Unknown** status, see CTX131267 for guidance.

Create application groups

May 17, 2024

Introduction

Application groups let you manage collections of applications. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups. Application groups are optional. They offer an alternative to adding the same applications to multiple delivery groups. Delivery groups can be associated with more than one application group, and an application group can be associated with more than one delivery group.

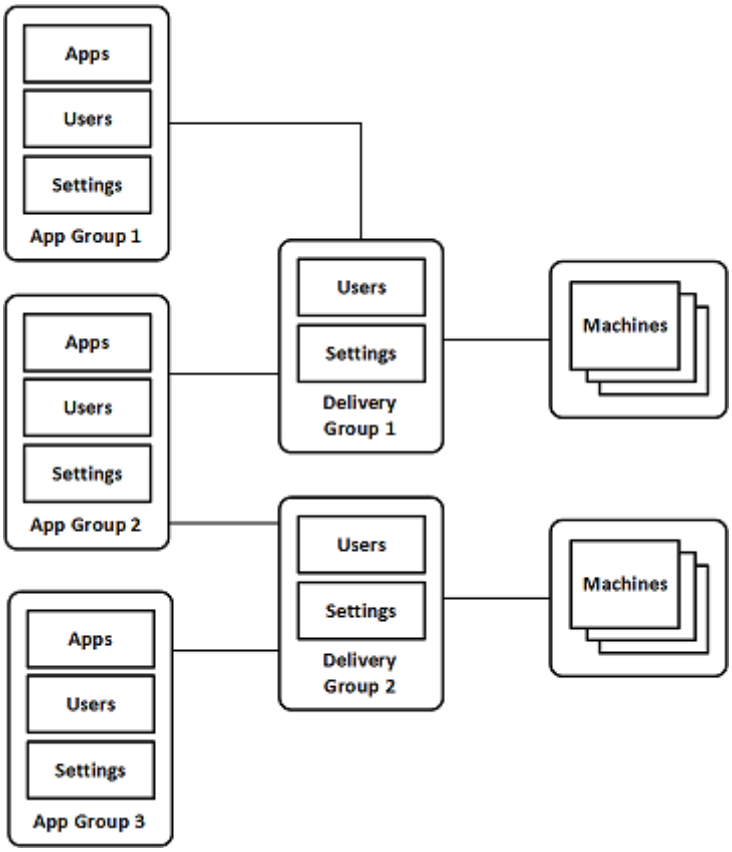
Using application groups can provide application management and resource control advantages over using more delivery groups:

- The logical grouping of applications and their settings lets you manage those applications as a single unit. For example, you don't have to add (publish) the same application to individual delivery groups one at a time.
- Session sharing between application groups can conserve resource consumption. In other cases, disabling session sharing between application groups may be beneficial.
- You can use the tag restriction feature to publish applications from an application group, considering only a subset of the machines in selected delivery groups. With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with deploying and managing additional machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a delivery group. Using an application group or desktops with a tag restriction can be helpful when isolating and troubleshooting a subset of machines in a delivery group.

Example configurations

Example 1

The following graphic shows a deployment that includes application groups:



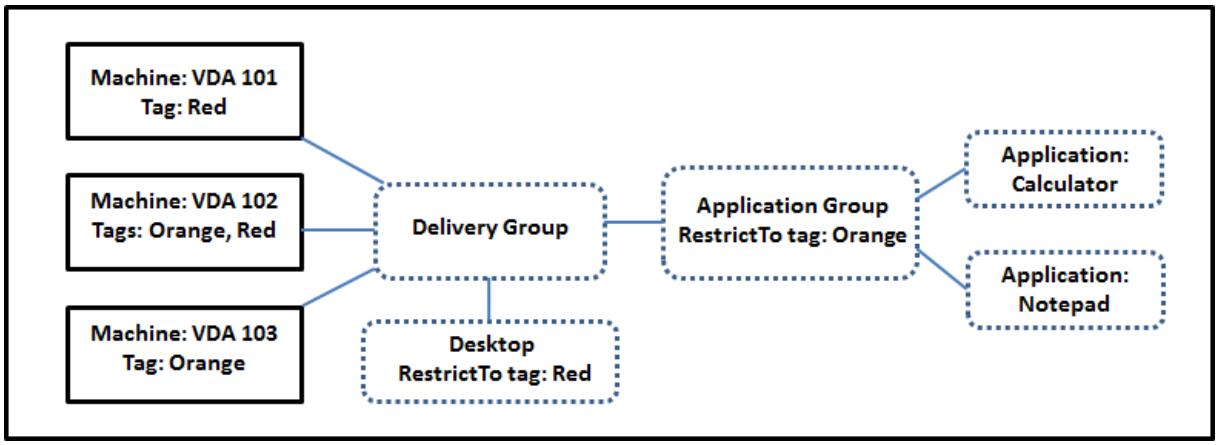
In this configuration, applications are added to the application groups, not the delivery groups. The delivery groups specify which machines will be used. (Although not shown, the machines are in machine catalogs.)

Application group 1 is associated with delivery group 1. The applications in application group 1 can be accessed by the users specified in application group 1, as long as they are also in the user list for delivery group 1. This follows the guidance that the user list for an application group should be a subset (a restriction) of the user lists for the associated delivery groups. The settings in application group 1 (such as application session sharing between application groups, associated delivery groups) apply to applications and users in that group. The settings in delivery group 1 (such as anonymous user support) apply to users in application groups 1 and 2, because those application groups have been associated with that delivery group.

Application group 2 is associated with two delivery groups: 1 and 2. Each of those delivery groups can be assigned a priority in application group 2, which indicates the order in which the delivery groups will be checked when an application is launched. delivery groups with equal priority are load balanced. The applications in application group 2 can be accessed by the users specified in application group 2, as long as they are also in the user lists for delivery group 1 and delivery group 2.

Example 2

This simple layout uses tag restrictions to limit which machines will be considered for certain desktop and application launches. The site has one shared delivery group, one published desktop, and one application group configured with two applications.



Tags have been added to each of the three machines (VDA 101-103).

The application group was created with the "Orange"tag restriction, so each of its applications (Calculator and Notepad) can be launched only on machines in that delivery group that have the tag "Orange": VDA 102 and 103.

For more comprehensive examples and guidance for using tag restrictions in application groups (and for desktops), see Tags.

Guidance and considerations

Citrix recommends adding applications to either application groups or delivery groups, but not both. Otherwise, the additional complexity of having applications in two group types can make it more difficult to manage.

By default, an application group is enabled. After you create an application group, you can edit the group to change this setting. See Manage application groups.

By default, application session sharing between application groups is enabled. See Session sharing between application groups.

Citrix recommends upgrading your delivery groups to the current version. This requires:

1. Upgrading VDAs on the machines used in the delivery group.
2. Changing to a higher function level for the machine catalogs containing those machines
3. Changing to a higher function level for the delivery group.

For details, see Manage delivery groups.

To use application groups, your core components must be minimum version 7.9.

Creating application groups requires the delegated administration permission of the Delivery Group Administrator built-in role. See Delegated administration for details.

This article refers to "associating"an application with more than one application group to differentiate that action from adding a new instance of that application from an available source. Similarly, delivery groups are associated with application groups (and vice versa), rather than being additions or components of one another.

Session sharing with application groups

When application session sharing is enabled, all applications launch in the same application session. This saves the costs associated with launching additional application sessions, and allows the use of application features that involve the clipboard, such as copy-paste operations. However, in some situations you may wish to turn off session sharing.

When you use application groups you can configure application session sharing in the following three ways which extend the standard session sharing behavior available when you are using only delivery groups:

- Session sharing enabled between application groups.
- Session sharing enabled only between applications in the same application group.
- Session sharing disabled.

Session sharing between application groups

You can enable application session sharing between application groups, or you can disable it to limit application session sharing only to applications in the same application group.

- **An example when enabling session sharing between application groups is helpful:**

  Application group 1 contains Microsoft Office applications such as Word and Excel. Application group 2 contains other applications such as Notepad and Calculator, and both application groups are attached to the same delivery group. A user who has access to both application groups starts an application session by launching Word, and then launches Notepad. If the user's existing session running Word is suitable for running Notepad then Notepad is started within the existing session. If Notepad cannot be run from the existing session—for example if the tag restriction excludes the machine that the session is running on—then a new session on a suitable machine is created rather than using session sharing.

- **An example when disabling session sharing between application groups is helpful:**

  You have a set of applications that do not interoperate well with other applications that are installed on the same machines, such as two different versions of the same software suite or two different versions of the same web browser. You prefer not to allow a user to launch both versions in the same session.

  You create an application group for each version of the software suite, and add the applications for each version of the software suite to the corresponding application group. If session sharing between groups is disabled for each of those application groups, a user specified in those groups can run applications of the same version in the same session, and can still run other applications at the same time, but not in the same session. If the user launches one of the different-versioned applications (that are in a different application group), or launches any application that is not contained in an application group, then that application is launched in a new session.

This session sharing between application groups feature is not a security sandboxing feature. It is not foolproof, and it cannot prevent users from launching applications into their sessions through other means (for example, through Windows Explorer).

If a machine is at capacity, new sessions are not started on it. New applications are started in existing sessions on the machine as needed using session sharing (providing that this complies with the session sharing restrictions described here).

You can only make prelaunched sessions available to application groups which have application session sharing allowed. (Sessions which use the session linger feature are available to all application groups.) These features must be enabled and configured in each of the delivery groups associated with the application group. You cannot configure them in the application groups.

By default, application session sharing between application groups is enabled when you create an application group. You cannot change this when you create the group. After you create an application group, you can edit the group to change this setting. See Manage application groups.

Disable session sharing within an application group

You can prevent application session sharing between applications which are in the same application group.

- **An example when disabling session sharing within application groups is helpful:**

  You want your users to access multiple simultaneous full screen sessions of an application on separate monitors.

  You create an application group and add the applications to it. If session sharing is prohibited between applications in that application group, when a user specified in it starts one applica-

tion after another they launch in separate sessions, and the user can move each to a separate monitor.

By default, application session sharing is enabled when you create an application group. You cannot change this when you create the group. After you create an application group, you can edit the group to change this setting. See Manage application groups.

Create an application group

Use the process of creating an Application Group to create Application Categories in the Citrix Workspace app. Application Categories allow to manage collections of applications in Citrix Workspace.

To create an application group:

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. To organize application groups using folders, create folders under the **Application Groups** root folder.
3. Select the folder where you want to create the group, and then click **Create Application Group**. The group creation wizard launches with an **Introduction** page. You can remove the page from future launches of this wizard.
4. Follow the wizard to configure settings on the pages described below. When you are done with each page, select **Next** until you reach the **Summary** page.

Step 1. Delivery groups

The **Delivery Groups** page lists all delivery groups, with the number of machines each group contains.

- The **Compatible Delivery Groups** list contains delivery groups you can select. Compatible delivery groups contain random (not permanently or statically assigned) server or desktop OS machines.
- The **Incompatible Delivery Groups** list contains delivery groups you cannot select. Each entry explains why it is not compatible, such as containing static assigned machines.

An application group can be associated with delivery groups containing shared (not private) machines that can deliver applications.

You can also select delivery groups containing shared machines that deliver only desktops, if both of the following conditions are met:

- The delivery group contains shared machines and was created with a XenDesktop version earlier than 7.9.

- You have Edit Delivery Group permission.

The delivery group type is automatically converted to "desktops and applications"when the group creation wizard is committed.

Although you can create an application group that has no associated delivery groups (perhaps to organize applications or to serve as storage for applications not currently used) the application group cannot be used to deliver applications until it specifies at least one delivery group. Additionally, you cannot add applications to the application group from the **From Start** menu source if there are no delivery groups specified.

The delivery groups you select specify the machines that will be used to deliver applications. Select the check boxes next to the delivery groups you want to associate with the application group.

To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the dropdown.

Step 2. Users

Specify who can use the applications in the application group. You can either allow all users and user groups in the delivery groups you selected on the previous page, or select specific users and user groups from those delivery groups. If you restrict use to users you specify, then only the users specified in the delivery group and the application group can access the applications in this application group. Essentially, the user list in the application group provides a filter on the user lists in the delivery groups.

Enabling or disabling application use by unauthenticated users is available only in delivery groups, not in application groups.

For information about where user lists are specified in a deployment, see Where user lists are specified.

Step 3. Applications

Good to know:

- By default, new applications you add are placed in a folder named **Applications**. You can specify a different folder. If you try to add an application and one with the same name already exists in that folder, you are prompted to rename the application you are adding. If you agree with the suggested unique name, the application is added with that new name. Otherwise, you must rename it yourself before it can be added. For details, see Manage application folders.
- You can change an application's properties (settings) when you add it, or later. See Change application properties. If you publish two applications with the same name to the same users,

change the **Application name (for user)** property in Full Configuration management interface. Otherwise, users will see duplicate names in the Citrix Workspace app.

- When you add an application to more than one application group, a visibility issue can occur if you do not have sufficient permission to view the application in all of those groups. In such cases, either consult an administrator with greater permissions or have your scope extended to include all the groups to which the application was added.

Select the **Add** dropdown to display the application sources.

- **From Start menu:** Applications that are discovered on a machine in the selected delivery groups. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add, and then select **OK**.

  This source cannot be selected if you selected any of the following:

  - Application groups that have no associated delivery groups.
  - Application groups with associated delivery groups that contain no machines.
  - A delivery group containing no machines.

- **Manually:** Applications located in the site or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, select **OK**.

- **Existing**: Applications previously added to the site. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add and then select **OK**. This source cannot be selected If the site has no applications.

- **Application packages:** Applications in App-V, MSIX, MSIX app attach, or FlexApp application packages. When you select this source, the **Add Applications from Packages** page launches. Select an application package source, select the applications you want to add from the resulting display, and then select **OK**

  > **Note:**
  >
  > To publish MSIX or MSIX app attach apps, the delivery group's functional level must be 2106 or later. For FlexApp apps, the functional level must be 2206 or later. When a functional level requirement isn't met, the corresponding options in the **Application package source** dropdown list are dimmed.
  >
  > **Note:**
  >
  > On VDA version 2003 and later, publishing App-V packages from HTTP URLs is not supported. You cannot select those applications from the list.

As noted, certain entries in the **Add** dropdown will not be selectable if there is no valid source of that

type. Sources that are incompatible are not listed at all (for example, you cannot add application groups to application groups, so that source is not listed when you create an application group).

Step 4. Scopes

This page appears only if you have previously created a custom scope. By default, the **All** scope is selected. For more information, see Delegated administration.

Step 5. Summary

Enter a name for the application group. You can also (optionally) enter a description.

Review the summary information and then select **Finish**.

Manage application groups

January 18, 2023

Introduction

This article describes how to manage the application groups you created.

See Applications for information about managing applications in application groups or delivery groups, including how to:

- Add or remove applications in an application group.
- Change application group associations.

Managing application groups requires the delegated administration permissions of the Delivery Group Administrator built-in role. For details, see Delegated administration.

Enable or disable an application group

When an application group is enabled, it can deliver the applications that have been added to it. Disabling an application group disables each application in that group. However, if those applications are also associated with other enabled application groups, they can be delivered from those other groups. Similarly, if the application was explicitly added to delivery groups associated with the application group (in addition to being added to the application group), disabling the application group does not affect the applications in those delivery groups.

An application group is enabled when you create it. You cannot change this when you create the group.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. On the **Settings** page, select or clear the **Enable Application Group** check box.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Enable or disable application session sharing between application groups

Session sharing between application groups is enabled when you create an application group. You cannot change this when you create the group. For more information, see Session sharing with application groups.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. On the **Settings** page, select or clear the **Enable application session sharing between Application Groups** check box.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Disable application session sharing within an application group

Session sharing between applications in the same application group is enabled by default when you create an application group. If you disable application session sharing between application groups, session sharing between applications in the same application group remains enabled.

You can use the PowerShell SDK to configure application groups with application session sharing disabled between the applications they contain. In some circumstances this can be desirable. For example, you might want users to start non-seamless applications in full-size application windows on separate monitors.

When you disable application session sharing within an application group, each application in that group launches in a new application session. If a suitable disconnected session is available which is running the same application, it is reconnected. For example, if you launch Notepad, and there is a disconnected session with Notepad running, that session is reconnected instead of creating a new one. If multiple suitable disconnected sessions are available, one of the sessions is chosen to reconnect to, in a random but deterministic manner. If the situation reoccurs in the same circumstances, the same session is chosen, but the session is not necessarily predictable otherwise.

You can use the PowerShell SDK to either disable application session sharing for all applications in an existing application group, or to create an application group with application session sharing disabled.

PowerShell cmdlet examples

To disable session sharing, use the Broker PowerShell cmdlets New-BrokerApplicationGroup or Set-BrokerApplicationGroup with the parameter SessionSharingEnabled set to False and the parameter SingleAppPerSession set to True.

- For example, to create an application group with application session sharing disabled for all applications in the group:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- For example, to disable application session sharing between all applications in an existing application group:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

Considerations

- To enable the `SingleAppPerSession` property you must set the `SessionSharingEnabled` property to False. The two properties must not be enabled at the same time. The `SessionSharingEnabled` parameter refers to sharing sessions between application groups.
- Application session sharing works only for applications that are associated with application groups but are not associated with delivery groups. All applications that are associated directly with a delivery group share sessions by default.
- If an application is assigned to multiple application groups, make sure that the groups do not have conflicting settings. For example, one group with the option set to True, and another group's option set to False results in unpredictable behavior.

Rename an application group

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Rename Application Group** in the action bar.
3. Specify the new unique name and then select **OK**.

Add, remove, or change the priority of delivery group associations with an application group

An application group can be associated with delivery groups containing shared (not private) machines that can deliver applications.

You can also select delivery groups containing shared machines that deliver only desktops, if both of the following conditions are met:

- The delivery group contains shared machines and was created with a version earlier than 7.9.
- You have Edit Delivery Group permission.

The delivery group type is automatically converted to "desktops and applications"when the **Edit Application Group** dialog is committed.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. Select the **Delivery Groups** page.
4. To add delivery groups, select **Add**. Select the check boxes of available delivery groups. (Incompatible delivery groups cannot be selected.) When you finish your selections, select **OK**.
5. To remove delivery groups, select the check boxes of the groups you want to remove and then select **Remove**. Confirm the deletion when prompted.
6. To change the priority of delivery groups, select the check box of the delivery group and then select **Edit Priority**. Enter the priority (0 = highest) and then select **OK**.
7. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Add, change, or remove a tag restriction in an application group

Adding, changing, and removing tag restrictions can have unanticipated effects on which machines are considered for application launch. Review the considerations and cautions in Tags.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. Select the **Delivery Groups** page.
4. To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the menu.
5. To change or remove a tag restriction, either select a different tag from the menu or remove the tag restriction by clearing **Restrict launches to machines with this tag**.

6. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Add or remove users in an application group

For detailed information about users, see Create application groups.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. Select the **Users** page. Indicate whether you want to allow all users in the associated delivery groups to use applications in the application group, or only specific users and groups. To add users, select **Add**, and then specify the users you want to add. To remove users, select one or more users and then select **Remove**.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Add, change, or remove an application icon in an application group

Perform the following steps to add, change, or remove an application icon.

1. In the navigation pane, select **Applications**.
2. On the **All Applications** tab, select an application and then select **Properties**.

   To make changes at an application group level, navigate to the **Application Groups** tab, select an application in a group, and then select **Properties**.
3. Select the **Delivery** page and then select **Change**. The **Select Icon** window appears.
4. In the **Select Icon** window, do either of the following:

   - To add an icon, select **Add** and then browse to the icon.
   - To remove an icon, select it and then select **Remove**.
   - To change an icon, select it for the application.

   > **Important:**
   >
   > - You cannot add an icon whose size is greater than 200 KB.
   > - You can add only .icon files.
   > - You cannot remove built-in icons.
   > - You cannot remove an icon of an application that is in use.

5. Select **OK** to apply changes and close the window.

Change scopes in an application group

You can change a scope only if you have created a scope (you cannot edit the All scope). For more information, see Delegated administration.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group in the middle pane and then select **Edit Application Group** in the action bar.
3. Select the **Scopes** page. Select or clear the check box next to the scopes you want to change.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Delete an application group

An application must be associated with at least one delivery group or application group. If deleting an application group will result in one or more applications no longer belonging to a group, you are warned that deleting that group will also delete those applications. You can then confirm or cancel the deletion.

Deleting an application does not delete it from its original source. However, if you want to make it available again, you must add it again.

1. From **Manage > Full Configuration**, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Delete Group** in the action bar.
3. Confirm the deletion when prompted.

Organize application groups using folders

You can create folders to organize application groups for easy access.

Required roles

By default, you must have one of the following built-in roles to create and manage folders for application groups:

- Cloud Administrator
- Full Administrator
- Application Group Administrator

You can delegate management actions to other users by creating custom roles. The following table lists the permissions required for each action.

Action	Required permissions
Create application group folders	Create Application Group Folder
Delete application group folders	Remove Application Group Folder
Move application groups folders	Move Application Group Folder
Rename application group folders	Edit Application Group Folder
Move application groups to folders	Edit Application Group Folder, Edit Application Group Properties

For more information, see Create and manage roles.

Create and manage folders

You can use the Actions bar or the right-click menu to create and manage application group folders. In addition, you can drag an application group or a folder to a desired location in the folder tree.

Good to know:

- You can nest folders up to five levels (excluding the default root folder).
- A folder can contain application groups and subfolders. You can delete a folder only if it and its subfolders don't contain application groups.
- All resources in Full Configuration (such as machine catalogs, delivery groups, applications, and application groups) share a folder tree in the back-end. To avoid name conflicts with other resource folders when renaming or moving folders, we recommend you give different names to first-level folders in different folder trees.

Remote PC Access

July 13, 2023

> **Note:**
>
> This article describes how to configure Remote PC Access using the Full Configuration interface.

> If you're using the Quick Deploy interface, follow the guidance in Remote PC Access in Quick Deploy.

Remote PC Access is a feature of Citrix Virtual Apps and Desktops that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Remote PC Access eliminates the need to introduce and provide other tools to accommodate teleworking. For example, virtual desktops or applications and their associated infrastructure.

Remote PC Access uses the same Citrix Virtual Apps and Desktops components that deliver virtual desktops and applications. As a result, the requirements and process of deploying and configuring Remote PC Access are the same as those required for deploying Citrix Virtual Apps and Desktops for the delivery of virtual resources. This uniformity provides a consistent and unified administrative experience. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

The feature consists of a machine catalog of type **Remote PC Access** that provides the following functionality:

- Ability to add machines by specifying OUs. This ability facilitates the addition of PCs in bulk.
- Ability to add machines by using CSV files. This ability facilitates the addition of PCs in bulk in scenarios with OU structure restrictions.
- Automatic user assignment based on the user that logs into the office Windows PC. We support single user and multiple users assignments. By default, Citrix DaaS automatically assigns multiple users to the next unassigned machine. To restrict automatic assignment to a single user, navigate to **Full Configuration > Settings** and turn off the **Enable automatic assignment of multiple users for Remote PC Access** setting.

Citrix Virtual Apps and Desktops can accommodate more use cases for physical PCs by using other types of machine catalogs. These use cases include:

- Physical Linux PCs
- Pooled physical PCs (that is, randomly assigned, not dedicated)

> **Notes:**
>
> For details on the supported OS versions, see the system requirements for the VDA for single-session OS and Linux VDA.
>
> For on-premises deployments, Remote PC Access is valid only for Citrix DaaS Advanced or Premium licenses. Sessions consume licenses in the same way as other Citrix Virtual Desktops sessions. For Citrix Cloud, Remote PC Access is valid for Citrix DaaS and Workspace Premium Plus.

Considerations

While all the technical requirements and considerations that apply to Citrix Virtual Apps and Desktops and Citrix DaaS in general also apply to Remote PC Access, some might be more relevant or exclusive to the physical PC use case.

> **Important:**
>
> Windows 11 physical systems (and some running Windows 10) include virtualization-based security features that result in the VDA software's incorrectly detecting them as virtual machines. To mitigate this issue, you have the following options:
>
> - Use the "/physicalmachine"option along with the "/remotepc"option as part of the VDA command-line installation
> - Add the following registry value after the VDA is installed if the aforementioned option was not used
>   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>   - Name: ForceEnableRemotePC
>   - Type: DWORD
>   - Data: 1

Deployment considerations

While planning the deployment of Remote PC Access, make a few general decisions.

- You can add Remote PC Access to an existing Citrix Virtual Apps and Desktops and Citrix DaaS deployment. Before choosing this option, consider the following:
  - Are the current Delivery Controllers or Cloud Connectors appropriately sized to support the additional load associated with the Remote PC Access VDAs?
  - Are the on-premises site databases and database servers appropriately sized to support the additional load associated with the Remote PC Access VDAs?
  - Will the existing VDAs and the new Remote PC Access VDAs exceed the number of maximum supported VDAs per site?
- You must deploy the VDA to office PCs through an automated process. The following are two of options available:
  - Electronic Software Distribution (ESD) tools such as SCCM: Install VDAs using SCCM.
  - Deployment scripts: Install VDAs using scripts.
- Review the Remote PC Access security considerations.

Machine catalog considerations

The type of machine catalog required depends on the use case:

- Remote PC Access machine catalog
  - Windows/Linux dedicated PCs
  - Windows/Linux dedicated multi-user PCs. This use case applies to physical office PCs that multiple users can access remotely in different shifts.
  - Pooled Windows/Linux PCs. This use case applies to physical PCs that multiple random users can access, such as computer labs.

Once you identify the type of machine catalog, consider the following:

- A machine can be assigned to only one machine catalog at a time.
- To facilitate delegated administration, consider creating machine catalogs based on geographic location, department, or any other grouping that eases delegating administration of each catalog to the appropriate administrators.
- When choosing the OUs in which the machine accounts reside, select lower-level OUs for greater granularity. If such granularity is not required, you can choose higher-level OUs. For example, in the case of Bank/Officers/Tellers, select **Tellers** for greater granularity. Otherwise, you can select **Officers** or **Bank** based on the requirement.
- Moving or deleting OUs after being assigned to a Remote PC Access machine catalog affects VDA associations and causes issues with future assignments. Therefore, make sure to plan accordingly so that OU assignment updates for machine catalogs are accounted for in the Active Directory change plan.
- You can choose OUs to add machines to the machine catalog in bulk. In some scenarios, doing that is not easy because of OU structure restrictions. Instead, you can add machines in bulk by using CSV files. That feature gives you more flexibility to bulk add machines. You can add only machines (for use with user auto-assignments) or add machines along with user assignments.
- Integrated Wake on LAN is available only with the **Remote PC Access** type machine catalog.

Linux VDA considerations

These considerations are specific to the Linux VDA:

- Physical monitor blanking for Remote PC Access VDAs is available, but not for all Linux distributions. For the unsupported Linux distributions, use the Linux VDA on physical machines only in non-3D mode. Otherwise, due to limitations on NVIDIA's driver, the local screen of the PC cannot be blacked out and displays the activities of the session when HDX 3D mode is enabled. Showing this screen is a security risk.

- We recommend you use machine catalogs of type single-session OS for physical Linux machines.

Technical requirements and considerations

This section contains the technical requirements and considerations for physical PCs.

- The following are not supported:
  - KVM switches or other components that can disconnect a session.
  - Hybrid PCs, including All-in-One and NVIDIA Optimus laptops and PCs.
  - Dual boot machines.
- Connect the keyboard and mouse directly to the PC. Connecting to the monitor or other components that can be turned off or disconnected, can make these peripherals unavailable. If you must connect the input devices to components such as monitors, do not turn those components off.
- The PCs must be joined to an Active Directory Domain Services domain.
- Secure Boot is supported on Windows 10 only.
- The PC must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.
- If using Wi-Fi, do the following:
  1. Set the power settings to leave the wireless adapter turned on.
  2. Configure the wireless adapter and network profile to allow automatic connection to the wireless network before the user logs on. Otherwise, the VDA does not register until the user logs on. The PC isn't available for remote access until a user has logged on.
  3. Ensure that the Delivery Controllers or Cloud Connectors can be reached from the Wi-Fi network.
- You can use Remote PC Access on laptop computers. Ensure that the laptop is connected to a power source instead of running on the battery. Configure the laptop power options to match the options of a desktop PC. For example:
  1. Disable the hibernate feature.
  2. Disable the sleep feature.
  3. Set the close lid action to **Do Nothing**.
  4. Set the "press the power button"action to **Shut Down**.
  5. Disable video card and NIC energy-saving features.
- Remote PC Access is supported on Surface Pro devices with Windows 10. Follow the same guidelines for laptops mentioned previously.

- If using a docking station, you can undock and redock laptops. When you undock the laptop, the VDA reregisters with the Delivery Controllers or Cloud Connectors over Wi-Fi. However, when you redock the laptop, the VDA doesn't switch to use the wired connection unless you disconnect the wireless adapter. Some devices provide built-in functionality to disconnect the wireless adapter upon establishing a wired connection. The other devices require custom solutions or third-party utilities to disconnect the wireless adapter. Review the Wi-Fi considerations mentioned previously.

  Do the following to enable docking and undocking for Remote PC Access devices:

  1. In the **Start** menu, select **Settings > System > Power & Sleep**, and set **Sleep** to **Never**.
  2. Under the **Device Manager > Network adapters > Ethernet adapter** go to **Power Management** and clear **Allow the computer to turn off this device to save power**. Ensure that **Allow this device to wake the computer** is checked.

- Multiple users with access to the same office PC see the same icon in Citrix Workspace. When a user logs on to Citrix Workspace, that resource appears as unavailable if already in use by another user.
- Install the Citrix Workspace app on each client device (for example, a home PC) that accesses the office PC.

Configuration sequence

This section contains an overview of how to configure Remote PC Access when using the **Remote PC Access** type machine catalog. For information on how to create other types of machine catalogs, see the Create machine catalogs.

1. On-premises site only - To use the integrated Wake on LAN feature, configure the prerequisites outlined in Wake on LAN.
2. If a new Citrix Virtual Apps and Desktops site was created for Remote PC Access:

   a) Select the **Remote PC Access** site type.
   b) On the **Power Management** page, choose to enable or disable power management for the default Remote PC Access machine catalog. You can change this setting later by editing the machine catalog properties. For details on configuring Wake on LAN, see Wake on LAN.
   c) Complete the information on the **Users** and **Machine Accounts** pages.

   Completing these steps creates a machine catalog named **Remote PC Access Machines** and a delivery group named **Remote PC Access Desktops**.
3. If adding to an existing Citrix Virtual Apps and Desktops site:

a) Create a machine catalog of type **Remote PC Access** (Operating System page of the wizard). For details on how to create a machine catalog, see Create machine catalogs. Make sure to assign the correct OU so that the target PCs are made available for use with Remote PC Access.
b) Create a delivery group to provide users access to the PCs in the machine catalog. For details on how to create a delivery group, see Create delivery groups. Make sure to assign the delivery group to an Active Directory group that contains the users that require access to their PCs.

4. Deploy the VDA to the office PCs.

   - We recommend using the single-session OS core VDA installer (`VDAWorkstationCoreSetup.exe`).
   - You can also use the single-session full VDA installer (`VDAWorkstationSetup.exe`) with the `/remotepc /physicalmachine` option, which achieves the same outcome as using the core VDA installer.
   - Consider enabling Windows Remote Assistance to allow help desk teams to provide remote support through Citrix Director. To do so, use the `/enable_remote_assistance` option. For details, see Install using the command line.
   - To be able to see logon duration information in Director, you must use the single-session full VDA installer and include the **Citrix User Profile Management WMI Plugin** component. Include this component by using the `/includeadditional` option. For details, see Install using the command line.
   - For information about deploying the VDA using SCCM, see Install VDAs using SCCM.
   - For information about deploying the VDA through deployment scripts, see Install VDAs using scripts.

   After you successfully complete steps 2–4, users are automatically assigned to their own machines when they log in locally on the PCs.

5. Instruct users to download and install Citrix Workspace app on each client device that they use to access the office PC remotely. Citrix Workspace app is available from the Citrix download site or the application stores for supported mobile devices.

Features managed through the registry

> **Caution:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use

> of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Sleep mode (minimum version 7.16)

To allow a Remote PC Access machine to go into a sleep state, add this registry setting on the VDA, and then restart the machine. After the restart, the operating system power saving settings are respected. The machine goes into sleep mode after the preconfigured idle timer passes. After the machine wakes up, it reregisters with the Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: DisableRemotePCSleepPreventer
- Type: DWORD
- Data: 1

Session management

By default, a remote user's session is automatically disconnected when a local user initiates a session on that machine (by pressing CTRL+ATL+DEL). To prevent this automatic action, add the following registry entry on the office PC, and then restart the machine.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: SasNotification
- Type: DWORD
- Data: 1

By default, the remote user has preference over the local user when the connection message is not acknowledged within the timeout period. To configure the behavior, use this setting:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaMode
- Type: DWORD
- Data:
  - 1 - The remote user always has preference if he or she does not respond to the messaging UI in the specified timeout period. This behavior is the default if this setting is not configured.
  - 2 - The local user has preference.

The timeout for enforcing the Remote PC Access mode is 30 seconds by default. You can configure this timeout, but do not set it lower than 30 seconds. To configure the timeout, use this registry setting:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaTimeout
- Type: DWORD
- Data: number of seconds for timeout in decimal values

When a user wants to forcibly get the console access: The local user can press Ctrl+Alt+Del twice in a gap of 10 seconds to get local control over a remote session and force a disconnect event.

After the registry change and machine restart, if a local user presses Ctrl+Alt+Del to log on to that PC while it is in use by a remote user, the remote user receives a prompt. The prompt asks whether to allow or deny the local user's connection. Allowing the connection disconnects the remote user's session.

Wake on LAN

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use to save energy costs. It also enables remote access when a machine has been turned off inadvertently.

With the Wake on LAN feature, the magic packets are sent directly from the VDA running on the PC to the subnet in which the PC resides when instructed by the delivery controller. This allows the feature to work without dependencies on additional infrastructure components or third-party solutions for delivery of magic packets.

The Wake on LAN feature differs from the legacy SCCM-based Wake on LAN feature. SCCM-integrated Wake on LAN is an alternative Wake on LAN option for Remote PC Access that is only available with on-premises Citrix Virtual Apps and Desktops. For information on the SCCM-based Wake on LAN, see Wake on LAN –SCCM-integrated.

System requirements

The following are the system requirements for using the Wake on LAN feature:

- Control plane:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 or later
- Physical PCs:
  - VDA version 2009 or later
  - Windows 10 or Windows 11. For supportability details, see the VDA system requirements.
  - Wake on LAN enabled in BIOS/UEFI
  - Wake on LAN enabled in network adapter's properties within Windows configuration

Configure Wake on LAN

To configure Wake on LAN, you can use the Full Configuration management interface or PowerShell.

Configure Wake on LAN in the Full Configuration interface To create the Wake on LAN connection:

1. Navigate to the **Hosting** node on the left.
2. Select **Add Connection and Resources**.
3. In the **Connection** page of the wizard, provide the following:
    a) Connection type: Remote PC Wake on LAN
    b) Zone name: select the zone where the Remote PC Access catalog resides
    c) Connection name: enter a name for the Wake on LAN connection
4. Finalize the remaining steps in the Add Connection and Resources wizard.

To add the Wake on LAN connection to a Remote PC Access machine catalog:

1. If you are creating a new Remote PC Access machine catalog, you can add the connection on the **Machine Type** page of the Machine Catalog Setup wizard using the drop-down list.
2. If you want to add the Wake on LAN connection to an existing machine catalog:
    a) Navigate to the **Machine Catalogs** node on the left.
    b) Select the appropriate Remote PC Access machine catalog.
    c) Right-click on the machine catalog or select the **More** menu above.
    d) Select **Edit Machine Catalog**.
    e) In the **Power Management** page, select **Yes**.
    f) Select the appropriate connection from the drop-down list.
    g) Select **Save**.

> **Note:**
>
> The configuration of Wake on LAN through the Full Configuration interface is only available with Citrix DaaS at this time.

Configure Wake on LAN through PowerShell To configure Wake on LAN through PowerShell:

1. Create the Remote PC Access machine catalog if you do not have one already.
2. Create the Wake on LAN host connection if you do not have one already.
3. Retrieve the Wake on LAN host connection's unique identifier.
4. Associate the Wake on LAN host connection with a machine catalog.

To create the Wake on LAN host connection:


```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
       $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

When the host connection is ready, run the following commands to retrieve the host connection's unique identifier:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

After you retrieve the connection's unique identifier, run the following commands to associate the connection with the Remote PC Access machine catalog:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

Design considerations

When you are planning to use Wake on LAN with Remote PC Access, consider the following:

- Multiple machine catalogs can use the same Wake on LAN host connection.
- For a PC to wake up another PC, both PCs must be in the same subnet and use the same Wake on LAN host connection. It does not matter if the PCs are in the same or different machine catalogs.
- Host connections are assigned to specific zones. If your deployment contains more than one zone, you need a Wake on LAN host connection in each zone. The same applies to machine catalogs.
- Magic packets are broadcasted using the global broadcast address 255.255.255.255. Ensure that the address is not blocked.
- There must be at least one PC turned on in the subnet - for every Wake on LAN connection - to be able to wake up machines in that subnet.

Operational considerations

The following are considerations for using the Wake on LAN feature:

- The VDA must register at least once before the PC can be woken up using the integrated Wake on LAN feature.
- Wake on LAN can only be used to wake up PCs. It does not support other power actions, such as restart or shut down.
- Magic packets are sent in one of the two ways:

    1. When a user tries to launch a session to their PC and the VDA is unregistered
    2. When an administrator manually sends a power on command from the Full Configuration interface or PowerShell

- Because the Delivery Controller is unaware of a PC's power state, the Full Configuration interface displays **Not Supported** under power state. The delivery controller uses the VDA registration state to determine whether a PC is on or off.

Troubleshoot

Monitor blanking not working

If the Windows PC's local monitor is not blank while there is an active HDX session (the local monitor displays what's happening in the session) it is likely due to issues with the GPU vendor's driver. To resolve the issue, give the Citrix Indirect Display driver (IDD) higher priority than the graphic card's vendor driver by setting the following registry value:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Name: CitrixIDD
- Type: DWORD

- Data: 3

For more details about display adapter priorities and monitor creation, see the Knowledge Center article CTX237608.

Session disconnects when you select Ctrl+Alt+Del on the machine that has session management notification enabled

The session management notification controlled by the **SasNotification** registry value only works when Remote PC Access mode is enabled on the VDA. If the physical PC has the Hyper-V role or any virtualization-based security features enabled, the PC reports as a virtual machine. If the VDA detects that it is running on a virtual machine, it automatically disables Remote PC Access mode. To enable Remote PC Access mode, add the following registry value:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Type: DWORD
- Data: 1

Restart the PC for the setting to take effect.

Diagnostic information

Diagnostic information about Remote PC Access is written to the Windows Application Event log. Informational messages are not throttled. Error messages are throttled by discarding duplicate messages.

- 3300 (informational): Machine added to catalog
- 3301 (informational): Machine added to delivery group
- 3302 (informational): Machine assigned to user
- 3303 (error): Exception

Power management

If power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method. Ensure that those settings are enabled in the advanced properties for the power management connection.

The active remote session records the local touchscreen input

When the VDA enables Remote PC Access mode, the machine ignores the local touchscreen input during an active session. If the physical PC has the Hyper-V role or any virtualization-based security features enabled, the PC reports as a virtual machine. If the VDA detects that it is running on a virtual machine, it automatically disables Remote PC Access mode. To enable Remote PC Access mode, add the following registry setting:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Type: DWORD
- Data: 1

Restart the PC for the setting to take effect.

More resources

The following are other resources for Remote PC Access:

- Solution design guidance: Remote PC Access Design Decisions.
- Examples of Remote PC Access architectures: Reference Architecture for Citrix Remote PC Access Solution.

Remove components

March 23, 2022

To remove components tht you installed (such as VDAs), Citrix recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script.

When you remove components, prerequisites are not removed, and firewall settings are not changed.

When you remove a VDA, the machine restarts automatically after the removal, by default.

Remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- To remove a VDA, select **Citrix Virtual Delivery Agent** <*version*>, then right-click and select **Uninstall**. The installer launches and you can select the components to be removed.
- To remove the Universal Print Server, select **Citrix Universal Print Server**, then right-click and select **Uninstall**.

Remove a VDA using the command line

Run the command that was used to install the VDA: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`. See Install using the command line for syntax descriptions.

- To remove only the VDA or only the Citrix Workspace app, use the `/remove` and `/components` options.
- To remove the VDA and Citrix Workspace app, use the `/removeall` option.

For example, the following command removes the VDA and Citrix Workspace app from a multi-session OS machine.

```
VDAServerSetup.exe /removeall
```

For example, the following command removes the VDA but not Citrix Workspace app for Windows (if it is installed) from a single-session OS machine.

```
VDAWorkstationSetup.exe /remove /components vda
```

You can also remove a VDA using a script provided by Citrix. See Remove VDAs using the script.

User personalization layer

February 1, 2024

The user personalization layer feature for Citrix Virtual Apps and Desktops extends the capabilities of non-persistent machine catalogs to preserve users' data and locally installed applications across sessions. Powered by underlying Citrix App Layering technology, the user personalization layer feature supports Citrix Provisioning and Machine Creation Services (MCS) in a non-persistent machine catalog.

You install the user personalization layer components alongside the Virtual Delivery Agent within the master image. A VHD file stores locally, user-installed applications. The VHD mounted on the image acts as the user's own virtual hard drive.

> **Important:**
>
> You can deploy user personalization layers in Citrix Virtual Apps and Desktops, or App Layering user layers enabled in an image template, not both. Do not install the user personalization layer feature on a layer within App Layering.

This feature replaces Personal vDisk (PvD), while also providing a persistent workspace experience for users in a non-persistent, pooled, desktop environment.

To deploy the user personalization layer feature, install and configure it using the steps detailed in the article. Until then, the feature is not available.

Application support

Aside from the following exceptions, all applications that a user installs locally on the desktop are supported in the user personalization layer.

Exceptions

The following applications are the exception and are not supported on the user personalization layer:

- Enterprise applications, such as MS Office and Visual Studio.
- Applications that modify the network stack or hardware. Example: a VPN client.
- Applications that have boot level drivers. Example: a virus scanner.
- Applications with drivers that use the driver store. Example: a printer driver.

  > **Note:**
  >
  > You can make printers available using Windows Group Policy Objects (GPOs).

Do *not* allow users to install any unsupported applications locally. Rather, install these applications directly on the master image.

Applications that require a local user or administrator account

When a user installs an application locally, the app goes into their user layer. If the user then adds or edits a local user or group, the changes do not persist beyond the session.

> **Important:**
>
> Add any required local user or group in the master image.

Requirements

The user personalization layer feature requires the following components:

- Citrix Virtual Apps and Desktops 7 1909 or later
- Virtual Delivery Agent (VDA), version 1912 or later
- Citrix Provisioning, version 1909 or later
- Windows File Share (SMB), or Azure Files with on-prem AD authentication enabled

You can deploy the User personalization layer feature on the following Windows versions when the OS is deployed as single session. Support is limited to a single user on a single session.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, version 1607 or later
- Windows 10 Multi-Session (Azure Files supported)
- Windows Server 2016 (Azure Files supported)
- Windows Server 2019 (Azure Files supported)

For Citrix Virtual Apps and Desktops 7, use of Azure Files with User personalization layers is supported on Windows Server 2019, Windows Server 2016v, and Windows 10 client.

> **Note:**
>
> If you are using a server OS, only Server VDI is supported. For deployment details, see the Server VDI article.
>
> User personalization layer supports just one user at a time per machine, and then the machine has to reboot to reset the disks. You cannot use user personalization layer with multi-session server operating systems, only with single-session server systems. User personalization layer works with non-persistent desktops only.

Uninstall the user personalization layer feature, if installed. Reboot the master image before installing the latest release.

Set up your file share

The user personalization layer feature requires Windows Server Message Block (SMB) storage. To create a Windows file share, follow the usual steps for the Windows operating system that you are on.

For more about using Azure Files with Azure-based catalogs, see Set up Azure Files storage for User personalization layers.

Recommendations

Follow the recommendations in this section for a successful user personalization layer deployment.

Microsoft System Center Configuration Manager (SCCM)

If you are using SCCM with the user personalization layer feature, follow the Microsoft guidelines for preparing your image in a VDI environment. Refer to this Microsoft TechNet article for more information.

User layer size

A user layer is a thin-provisioned disk that expands as space on the disk is used. The default size allowed for a user layer is 10 GB, the minimum we recommend.

> **Note:**
>
> During installation, if the value is set to zero (0), the default user layer size is set to 10 GB.

If you want to change the user layer size, you can enter a different value for the **User Layer Size** Studio policy. See **Step 5: Create delivery group custom policies**, under **Optional: Click Select next to User Layer Size in GB.**

Tools for overriding the User Layer Size (Optional)

You can override the User Layer Size by using a Windows tool to define a quota on the user layer file share.

Use one of the following Microsoft quota tools to set a hard quota on the user layer directory named **Users**:

- File Server Resource Manager (FSRM)
- Quota Manager

> **Note:**
>
> Increasing the quota affects new user layers and expands existing ones. Decreasing the quota only affects new user layers. Existing user layers never decrease in size.

Deploy a User personalization layer

When deploying the user personalization feature, you define the policies within Studio. You then assign the policies to the delivery group bound to the machine catalog, where the feature is deployed.

If you leave the master image with no user personalization layer configuration, the services remain idle and do not interfere with authoring activities.

If you set the policies in the master image, the services attempt to run and mount a user layer within the master image. The master image would exhibit unexpected behaviors and instability.

To deploy the user personalization layer feature, complete the following steps in this order:

- Step 1: Verify availability of a Citrix Virtual Apps and Desktops environment.
- Step 2: Prepare your master image.
- Step 3: Create a machine catalog.
- Step 4: Create a delivery group.
- Step 5: Create delivery group custom policies.

> **Note:**
>
> Logging on for the first time after upgrading Windows 10 on the image takes longer than usual. The user's layer needs to update for the new version of Windows 10, which then increases logon time.

Step 1: Verify that the Citrix Virtual Apps and Desktops environment is available

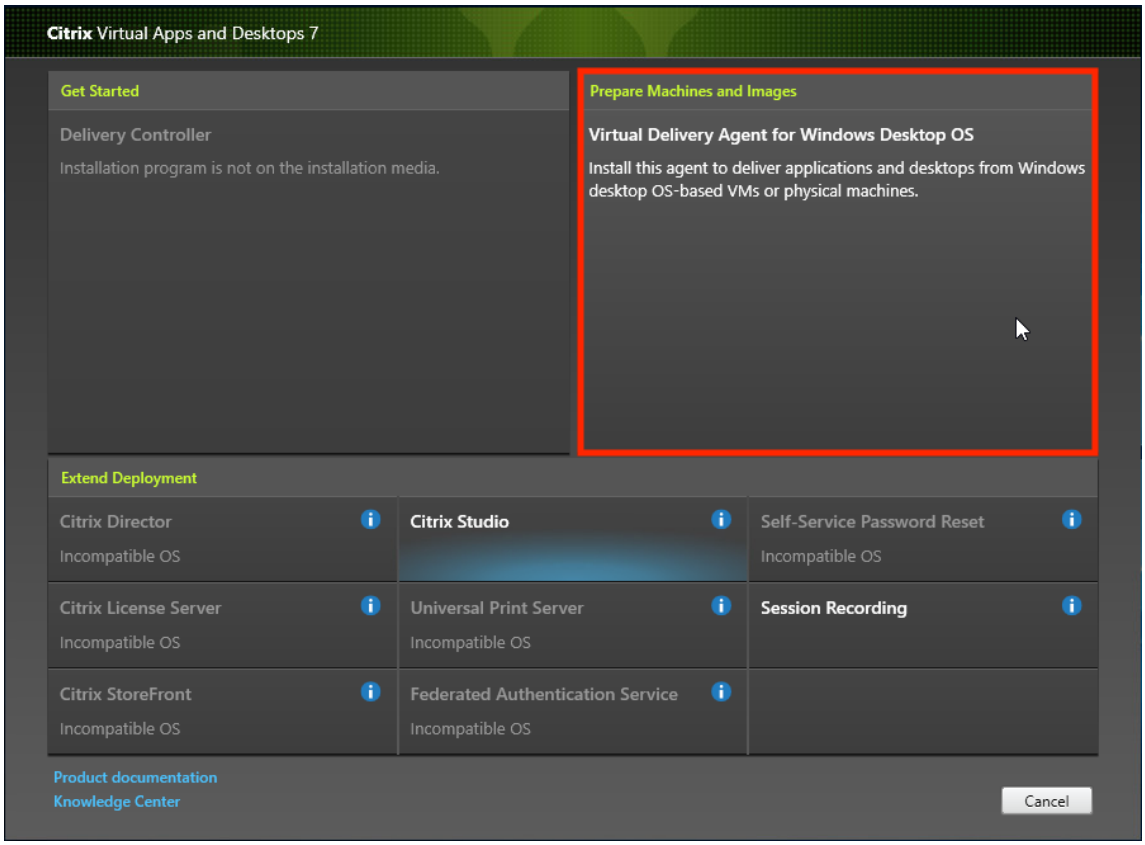
Be sure that your Citrix Virtual Apps and Desktops environment is available to use with this new feature. For setup details, see Install and configure Citrix Virtual Apps and Desktops.

Step 2: Prepare your master image

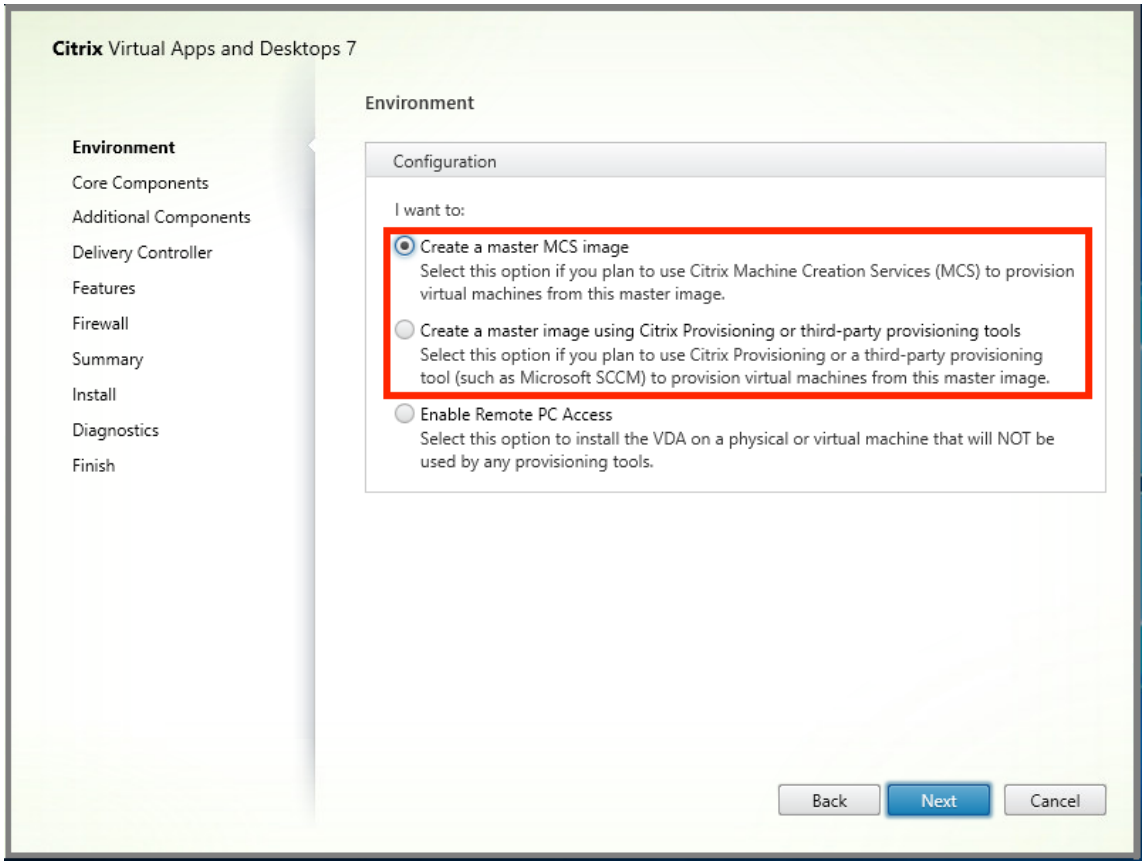
To prepare your master image:

1. Locate the master image. Install your organization's enterprise applications and any other apps your users generally find useful.
2. If you are deploying Server VDI, follow the steps in the Server VDI article. Be sure to include the optional component, the **User personalization layer**. For details, see the Command-line options for installing a VDA.
3. If you are using Windows 10, install Virtual Delivery Agent (VDA) 1912 or later. If an older version of the VDA is already installed, uninstall the old version first. When installing the new version, be sure to select and install the optional component, the **Citrix User Personalization Layer**, as follows:

a) Click the tile, **Virtual Delivery Agent for Windows Desktop OS**:

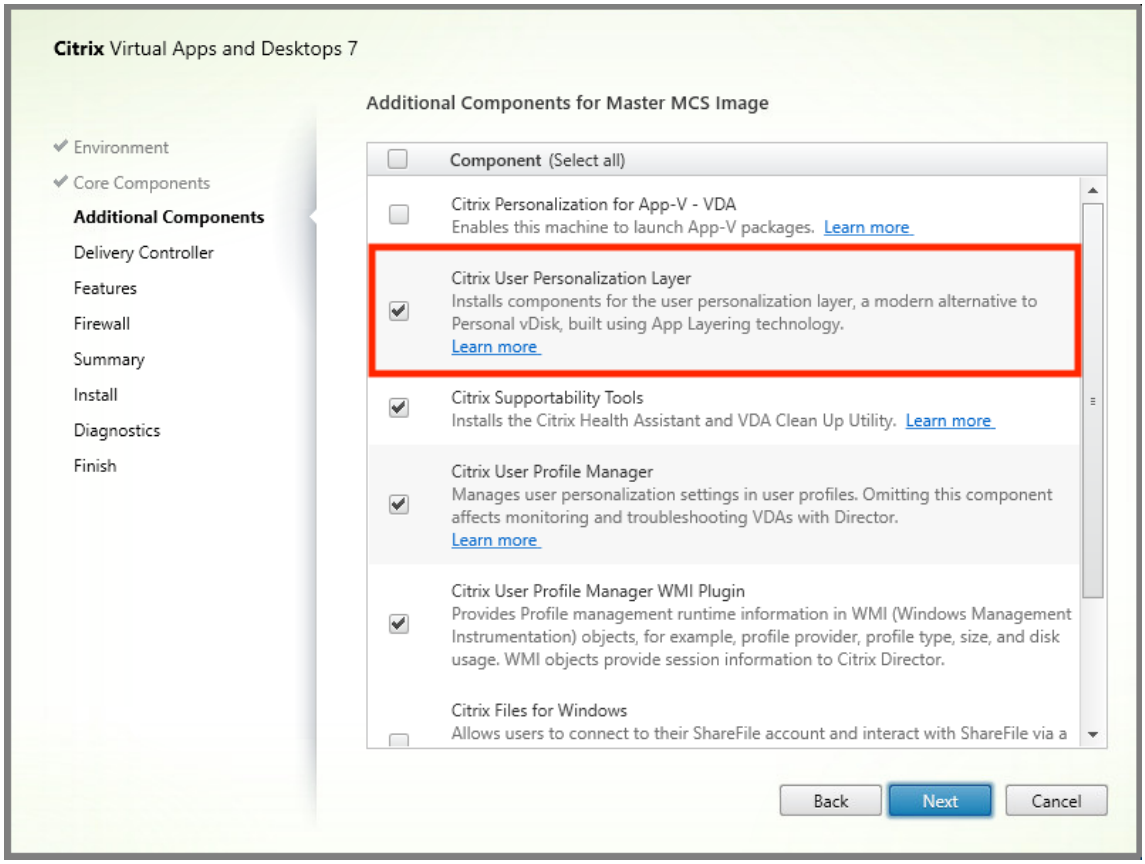


a) **Environment:** Select either **Create a master MCS image** or **Create a master image using Citrix Provisioning or third-party provisioning tools**.



a) **Core Components:** Click **Next**.

b) **Additional Components:** Check **Citrix User Personalization Layer**.



a) Click through the remaining installation screens, configuring the VDA as needed, and click **Install**. The image reboots one or more times during installation.

4. Leave **Windows updates** disabled. The user personalization layer installer disables Windows updates on the image. Leave the updates disabled.

The image is ready for you to upload into Studio.

> **Note:**
>
> If you simply wish to upgrade the user personalization layer (UPL), you can do so with a newer version of UPL and the standalone package. You do not need to upgrade the VDA.

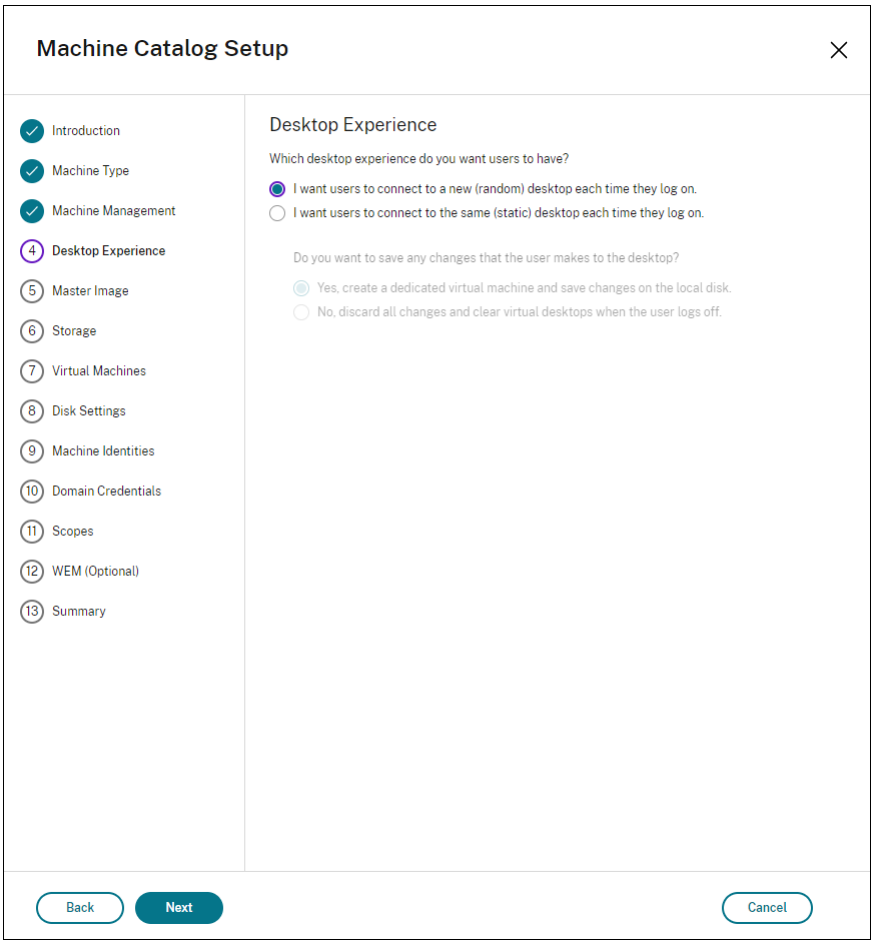
Step 3: Create a machine catalog

In Studio, follow the steps to create a machine catalog. Use the following options during catalog creation:

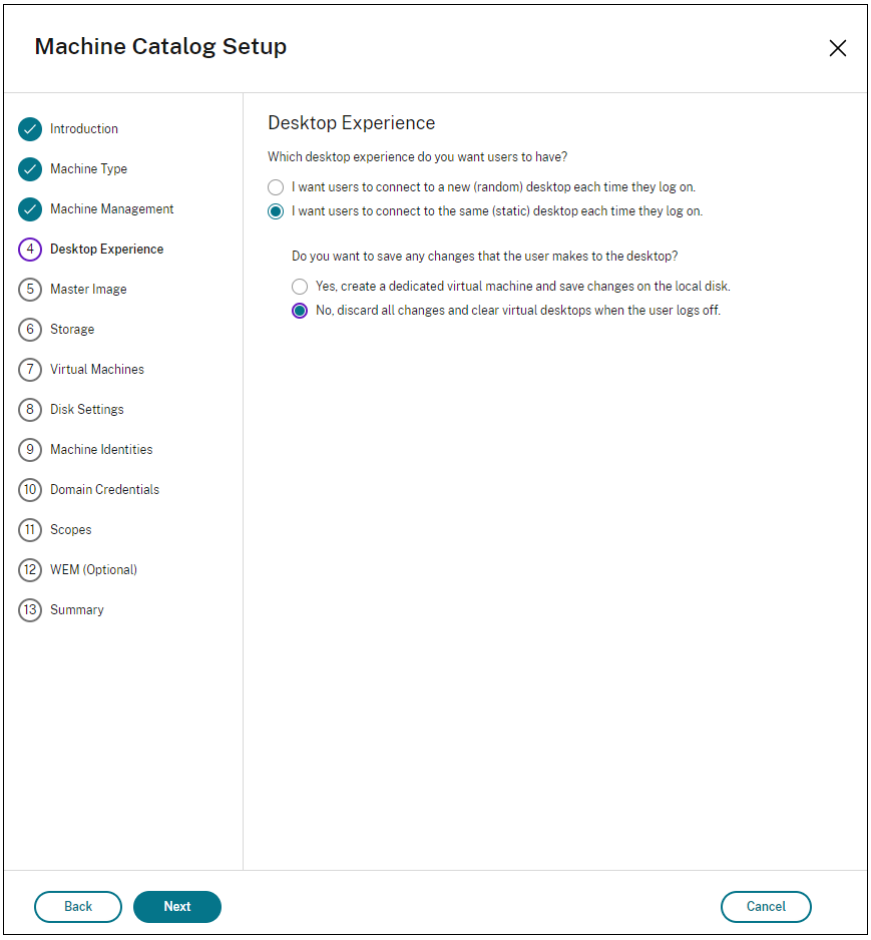
1. Select **Operating System** and set it to **Single session OS**.
2. Select **Machine Management** and set it to **Machines that are power managed**. For example, virtual machines or blade PCs.

3. Select **Desktop Experience** and set it to either **pooled-random** or **pooled-static** catalog type, as in the following examples:

   - **Pooled-random:**



   - **Pooled-static:** If you select pooled-static, configure desktops to discard all changes and clear virtual desktops when the user logs off, as shown in the following screenshot:



> **Note:**
>
> User personalization layer does not support pooled-static catalogs configured to use Citrix Personal vDisk or assigned as dedicated virtual machines.

4. If you are using MCS, select **Image** and the snapshot for the image created in the previous section.
5. Configure the remaining catalog properties as needed for your environment.

Step 4: Create a delivery group

Create and configure a **delivery group**, including machines from the machine catalog you created. For details, see the Create Delivery Groups.

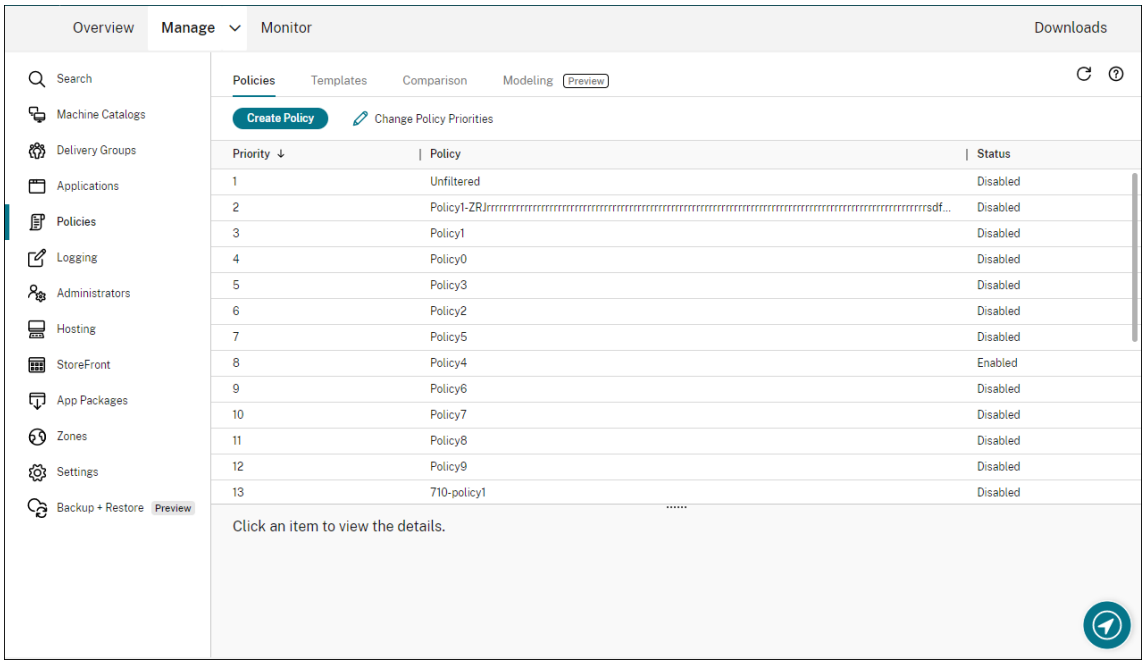
Step 5: Create delivery group custom policies

To enable mounting of user layers within the Virtual Delivery Agents, you use the configuration parameters to specify:

- Where on the network to access the user layers.
- How large to permit the user layer disks to grow.

To define the parameters as custom Citrix policies in Web Studio and assign them to your delivery group.

1. Sign in to Web Studio and select **Policies** in the left pane:



2. Select **Create Policy** in the action bar. The Create Policy window appears.
3. Type ‘user layer’into the search field. The following three policies appear in the list of available policies:

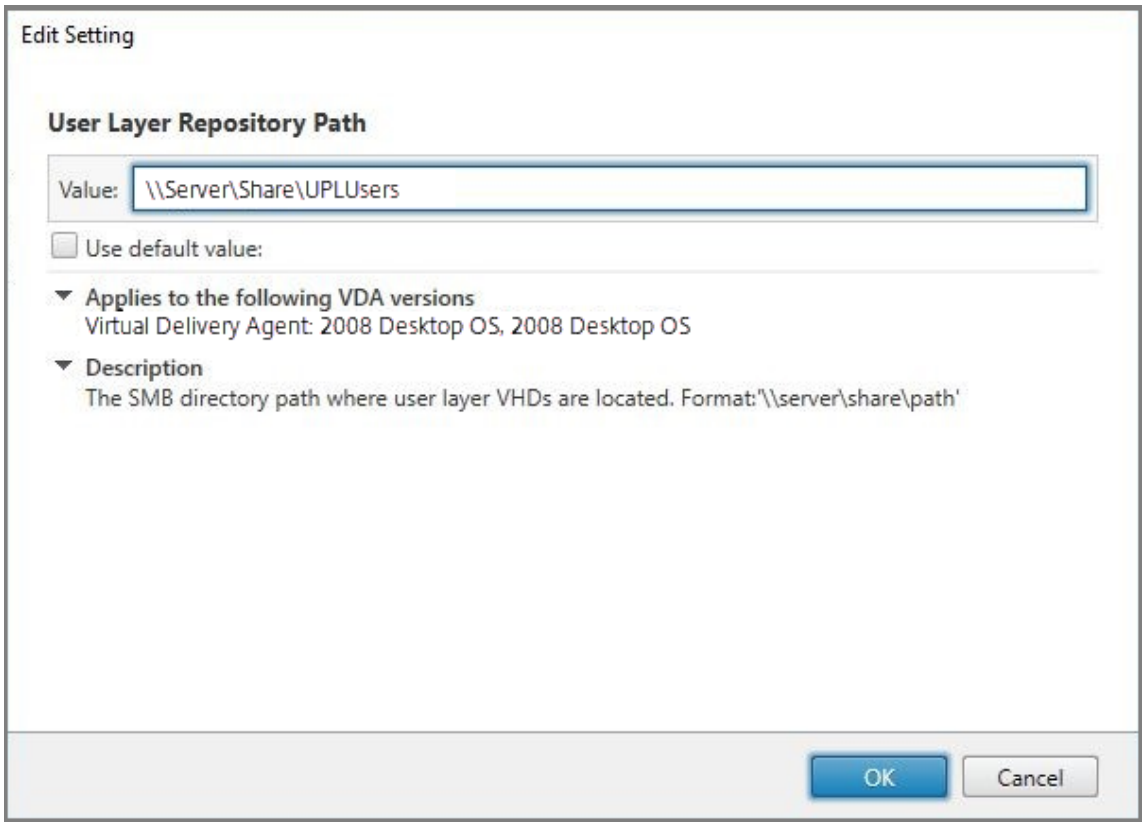
   - User Layer Exclusions
   - User Layer Repository Path
   - User Layer Size GB

   > **Note:**
   >
   > Increasing the size affects new user layers and expands existing user layers. Decreasing the size only affects new user layers. Existing user layers never decrease in size.

4. Mark the check box next to **User Layer Repository Path** and click **Edit**. The Edit Setting window appears.
5. Enter a path in the **Value** field, and click **Save**:

   - **Path format:** `\\server-name-or-address\share-name\folder`

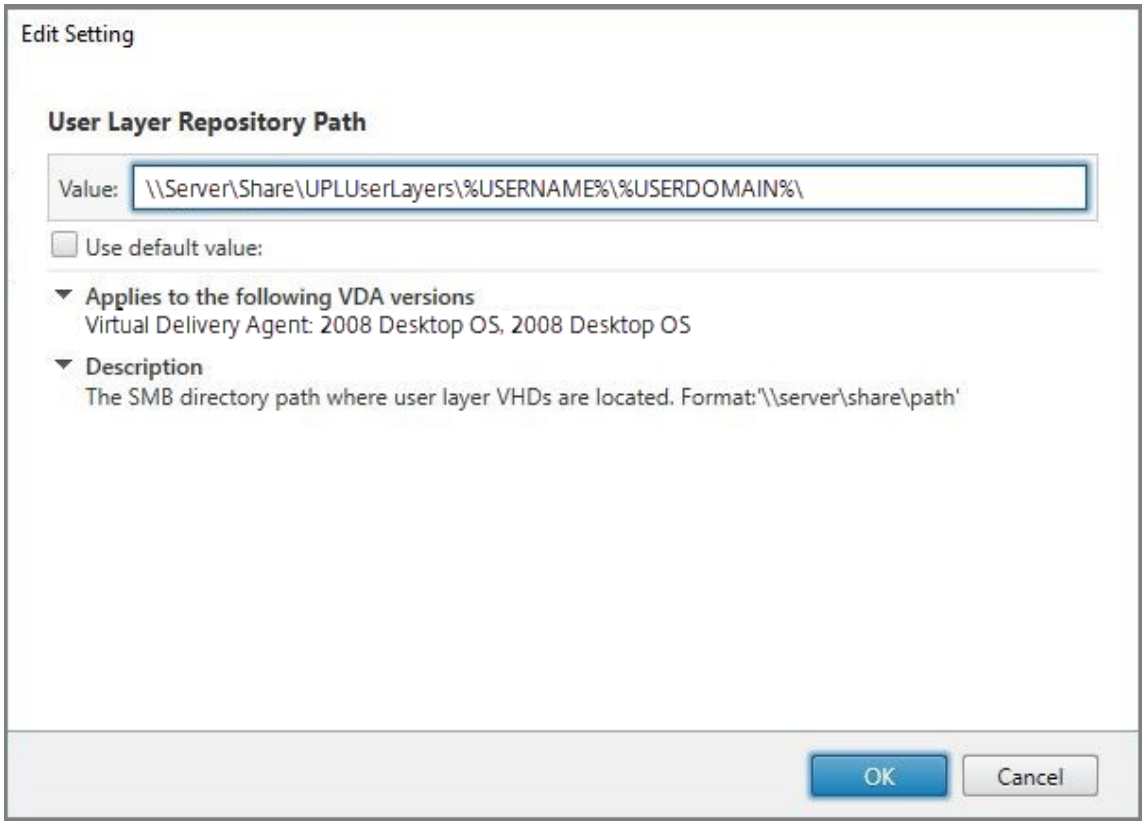
- **Path example:** \\Server\Share\UPLUsers
- **Resulting paths example:** For a user named **Alex** in **CoolCompanyDomain**, the path would be: \\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK



You can customize the path using the %USERNAME% and %USERDOMAIN% variables, machine environment variables, and Active Directory (AD) attributes. When expanded, these variables result in explicit paths.

Example of environment variables:

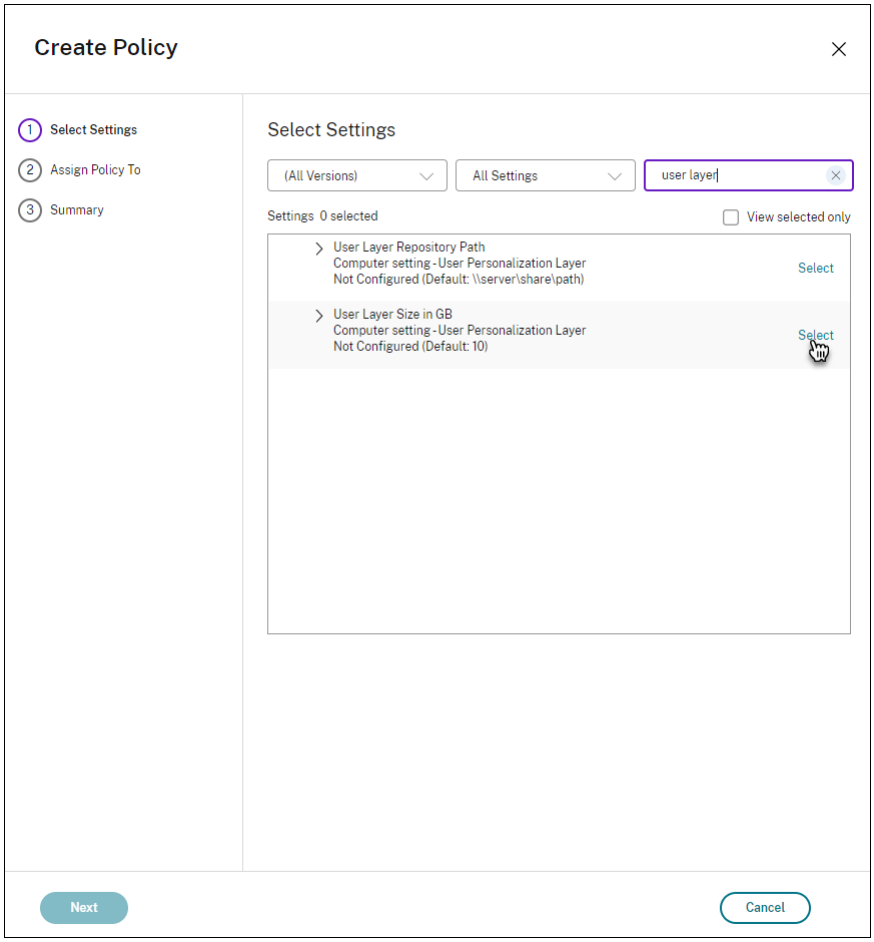
- **Path format:** \\Server-name-or-address\share-name\folder-with-environment-variables
- **Path example:** \\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%
- **Resulting paths example:** For a user named **Alex** in **CoolCompanyDomain**, the path would be: \\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK



Example of custom AD attributes:

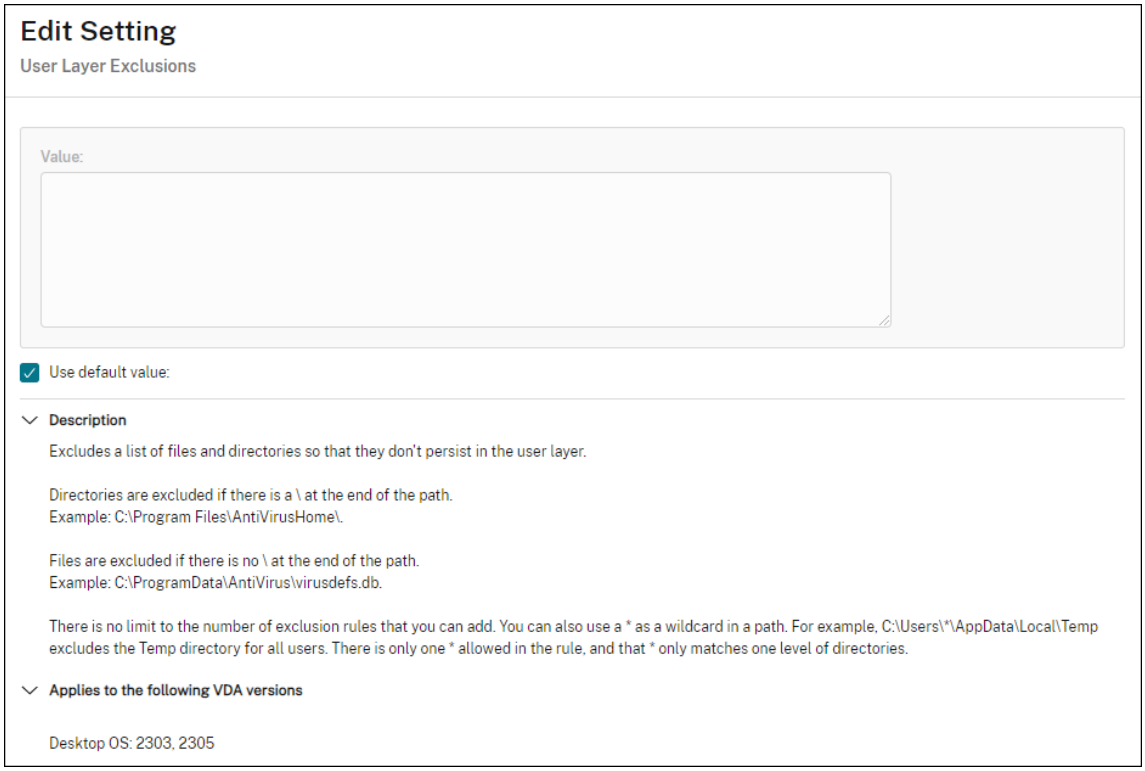
- Path format: `\\Server-name-or-address\share-name\AD-attribute`
- Path example: `\\Server\share\\#sAMAccountName#`
- Resulting paths example: `\\Server\share\JohnSmith` (if #sAMAccountName# resolves to JohnSmith for the current user)

6. Optional: Mark the check box next to **User Layer Size in GB** and click **Edit**:

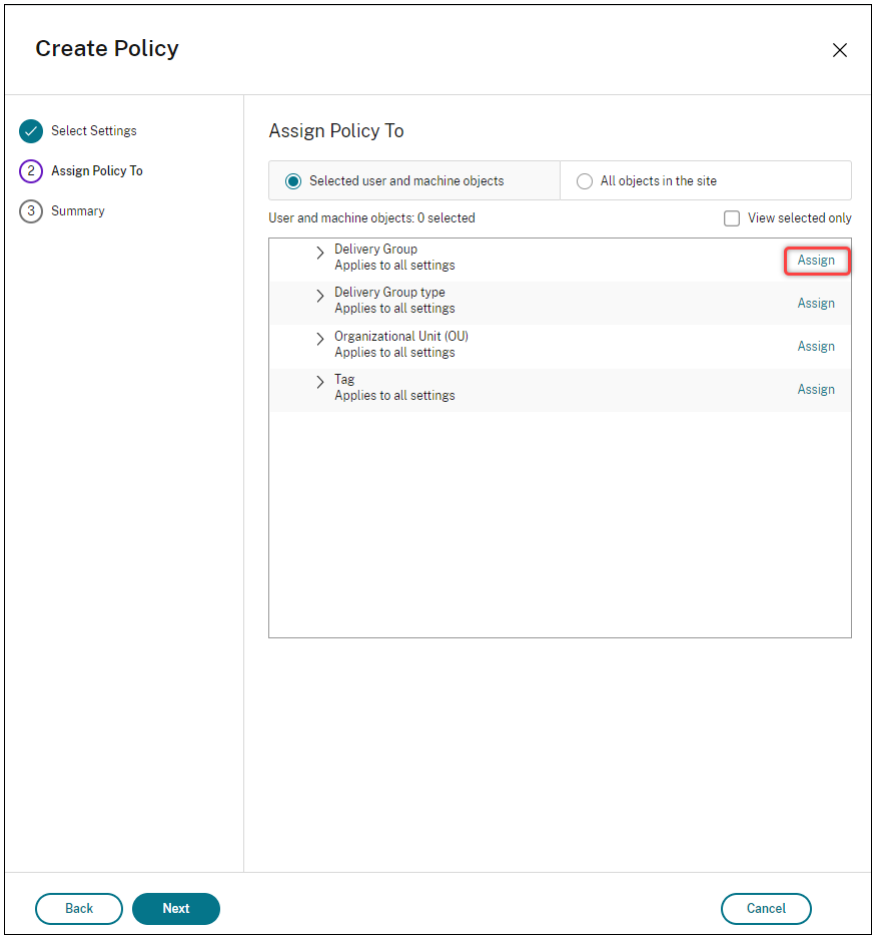


The Edit Settings window appears.

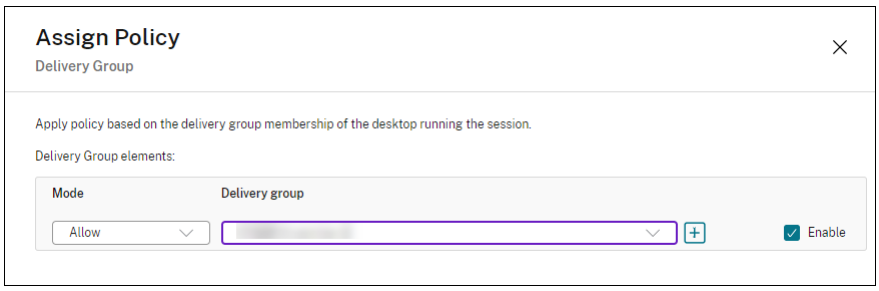
7. Optional: Change the default value of **10 GB** to the maximum size that each user layer can grow. Click **Save**.
8. Optional: Mark the check box next to **User Layer Exclusions** and click **Edit**.



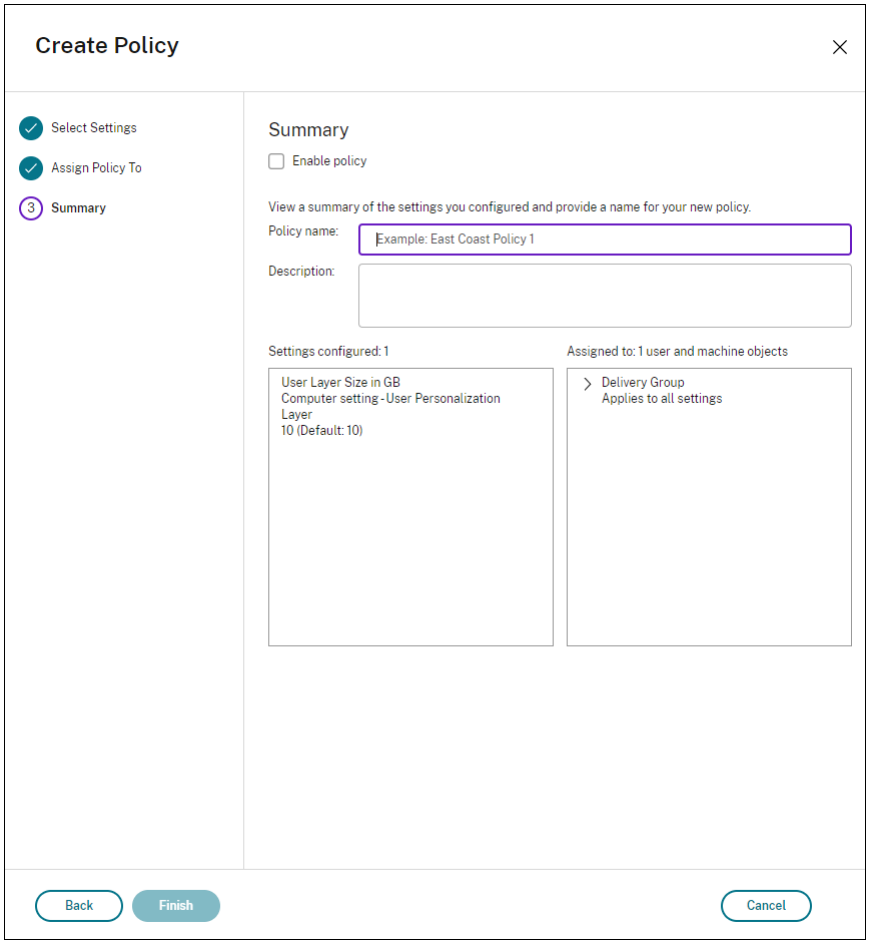
9. Optional: Specify the files and folders to exclude, then click **Save**. For more information, see the Citrix App Layering documentation.
10. Click **Next** to configure users and machines to which you want to assign. Click the **Delivery Group Assign** link highlighted in this image:



11. In the **Delivery Group** menu, select the delivery group created in the previous section. Click **OK**.



12. Enter a name for the policy. Click the check box to enable the policy, and click **Finish**.



Configure security settings on the user layer folder

As a domain administrator, you can specify more than one storage location for your user layers. Create a `\Users` subfolder For each storage location (including the default location). Secure each location using the following settings.

Setting name		Value	Apply to
Creator Owner		Modify	Subfolders and Files only
Owner Rights		Modify	Subfolders and Files only
	Users or group	Create Folder/Append Data; Traverse Folder/Execute File; List Folder/Read Data; Read Attributes	Selected Folder Only
System		Full Control	Selected Folder, Subfolders, and Files

Setting name	Value	Apply to
Domain Admins, and selected Admin group	Full Control	Selected Folder, Subfolders, and Files

User layer messages

When a user is unable to access their user layer, they receive one of these notification messages.

- **User Layer In Use**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **User Layer Unavailable**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **System not reset after user sign-out**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

Log files to use when troubleshooting

The log file, ulayersvc.log, contains the output of the user personalization layer software where changes are logged.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

Limitations

Keep the following limitations in mind when installing and using the user personalization layer feature.

- Do *not* attempt to deploy the user personalization layer software on a layer within App Layering. Either deploy user personalization layers in Citrix Virtual Apps and Desktops, or enable user layers in an App Layering image template, not both. Either process produces the user layers you need.

- Do *not* configure the user personalization layer feature with persistent machine catalogs.
- Do *not* use Session hosts.
- Do *not* update the machine catalog with an image running a new OS install (even the same version of Windows 10). Best practice is to apply updates to the OS within the same master image used when creating the machine catalog.
- Do *not* use boot-time drivers, nor any other early boot personalization.
- Do *not* migrate PvD data to the user personalization layer feature.
- Do *not* migrate existing user layers from the full App Layering product to the user personalization layer feature.
- Do *not* change the user layer SMB path to access user layers created using a different master OS image.
- When a user logs out of a session and then logs in again, the new session runs on a different machine in the pool. In a VDI environment, Microsoft Software Center lists an application as **Installed** on the first machine, but shows it as **Unavailable** on the second machine.

  To find out the true status of the application, instruct the user to select the application in the Software Center and click **Install**. SCCM then updates the status to the true value.
- Software Center occasionally stops immediately after launching within a VDA that has the user personalization layer feature enabled. To avoid this issue, follow Microsoft's recommendations for Implementing SCCM in a XenDesktop VDI environment. Also, make sure that the `ccmexec` service is running before you start the Software Center.
- In Group Polices (Computer Settings), User layer settings override settings applied to the master image. Therefore, the changes you make in Computer Settings using a GPO are not always present for the user on the next session login.

  To get around this issue, create a User Logon Script that issues the command:

  ```
  gpupdate /force
  ```

  For example, one customer set the following command to run at each user login:

  ```
  gpudate /Target:Computer /force
  ```

  For best results, apply changes to Computer Settings directly on the user layer, after the user has logged in.
- A domain user account must not be the last user to have logged in to a master image. Otherwise the machines provisioned from that image will have issues.
- Custom certificates do not persist when UPL is enabled in a pure Azure AD environment, due to an underlying issue in Windows running on Azure. If Microsoft fixes this issue in a future enhancement, we will update this article.

Upgrade VDAs

June 21, 2024

Introduction

Citrix maintains all the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) components in your deployment, except VDAs.

Before beginning a VDA upgrade:

- Review this entire article, so you know what to expect.
- Review the Lifecycle policy for Citrix DaaS.

To upgrade a VDA, download a VDA installer and run it on the machine or image. You can use the installer's graphical or command-line interface. For guidance, see:

- VDA installers
- Install VDAs using the graphical interface
- Install VDAs using the command line

If the VDA was originally installed using `VDAWorkstationCoreSetup.exe`:

- You retain that configuration if you upgrade the VDA with the latest version of the same installer.
- If you run `VDAWorkstationSetup.exe` on that machine, you can enable the features that are not supported in `VDAWorkstationCoreSetup.exe`. Keep in mind that some of those features might be enabled by default in the `VDAWorkstationSetup.exe` installer. You can also install Citrix Workspace app.

> **Note:**
>
> When upgrading a VDA to version 7.17 or a later supported version, a machine restart occurs during the upgrade process. This restart cannot be avoided. The upgrade resumes automatically after the restart (unless you specify `/noresume` on the command line).

After you upgrade VDAs, update the images and catalogs that use that VDA.

Upgrade VDAs using the Full Configuration interface

> **Important:**
>
> - As a best practice, we recommend that you test VDA upgrades thoroughly before moving into production.

> - You can switch between the CR VDA and the LTSR VDA as long as you switch from an earlier version to a later version. You cannot switch from a later version to an earlier version because that is considered a downgrade. For example, you cannot downgrade from 2212 CR to 2203 LTSR (any CU) but you can upgrade from 2112 CR to 2203 LTSR (any CU).
> - On-demand updates (such as hotfixes and patches between major releases) are not supported.
> - CVAD 2402 VDA is available through VDA Upgrade Service.

Using the Full Configuration interface, you can upgrade VDAs on a per-catalog or a per-machine basis. You can upgrade them immediately or at a scheduled time.

To learn more about the VDA Upgrade service, see Tech Brief: Citrix VDA Upgrade service. There, you will find an overview of the service, detailed information on how it works, and other useful resources.

Prerequisites

- Control plane: Citrix DaaS
- VDA type: Single-session or multi-session OS VDA. Only Windows VDA is currently supported.
- VDA version: 2109 or later, or 2203 LTSR or later

  > **Note:**
  >
  > We recommend using the latest CR VDA or the latest LTSR CU VDA.

- Provisioning type: Persistent machines (such as MCS-provisioned machines, Remote PC Access machines, Citrix HDX Plus for Windows 365). See Supported machine types.
- The VDAs must have the VDA Upgrade Agent installed and the service must be running.
- You have permissions to upgrade VDAs.
- The VDA upgrade is configured with the proper CR or LTSR track in Full Configuration.
- The VDAs are not in use. (Users must sign off from them.)

  > **Note:**
  >
  > Upgrades are skipped for any VDAs that are in use or in disconnected state. We recommend scheduling an upgrade window and requesting users to log off from the VDAs.

- The VDAs are not in maintenance mode. (A VDA can be put into maintenance mode by an administrator. A VDA can also be automatically put into maintenance mode if it has exceeded maximum allowed registration attempts.)

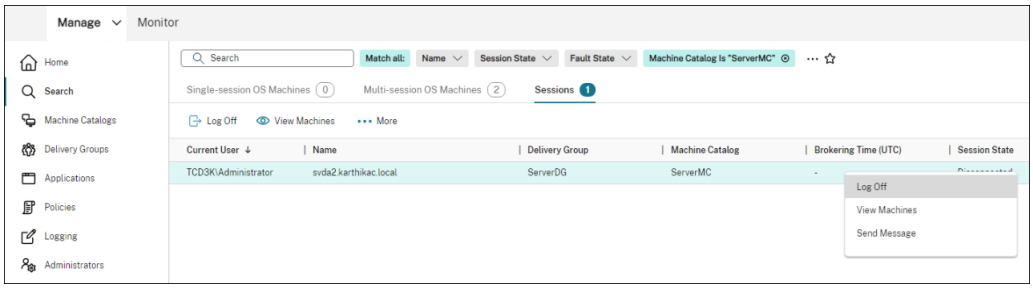
- Relevant URLs have been added to the allow list if URL filtering is in place. See VDA upgrade requirement.
- The VDAs must belong to a delivery group and be registered with DaaS.
- The functional level is set properly so that the VDA upgrade feature is available for use. See VDA versions and functional levels.
- The destination VDA supports the operating system of the current VDA.

Known issues

Issue 1: Failed to upgrade LTSR VDAs to LTSR Cumulative Update (CU) versions Attempts to upgrade LTSR VDAs to LTSR Cumulative Update (CU) versions might fail. Although the upgrade process appears to complete successfully in Full Configuration, the installed version of the VDA does not change and the status changes back to **Upgrade Available** after a minute or two. The issue occurs with VDAs that have VDA Upgrade Agent version 7.35.0.7 or earlier installed.

To work around the issue, log on to the VDA and upgrade the VDA Upgrade Agent to version 7.37.0.7 or later (using the VDA installer version 2303 or later). Starting with version 7.37.0.7, the VDA Upgrade Agent supports auto-upgrade so that agents of earlier versions running on the VDAs can automatically upgrade to the latest version. With this auto-update feature, the VDA upgrade service checks the VDA version reported by the agent and then schedules upgrades within one hour to automatically upgrade the agent to the latest version. This auto-upgrade feature reduces your maintenance effort.

For the agent on the VDA to upgrade automatically, be sure to log off sessions so that the VDA upgrade service can initiate auto-upgrades. You can log off sessions in Full Configuration.



If the agent fails to upgrade automatically, log on to the VDA and upgrade the agent manually as follows:

1. Run the following cmdlet to show the VDA Upgrade Agent in Control Panel > Uninstall or change a program.

```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
    CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
```



```
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. Install the latest VDA Upgrade Agent. To perform quiet installation, use the following cmdlet:

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

You can identify the version of the VDA Upgrade Agent by using the cmdlet or a script. See Troubleshoot.

General workflow

A general workflow to upgrade VDAs using the Full Configuration interface is as follows:

1. Enable VDA upgrade for a catalog.

   - You can enable VDA upgrade when creating a catalog.
   - You can enable VDA upgrade when editing a catalog.

2. Upgrade VDAs on a per-catalog or a per-machine basis. For more information, see Configure auto-upgrade for VDAs.

   > **Note:**
   >
   > When scheduling VDA upgrades for a catalog, be aware that all machines in the catalog will be included in the upgrade scope. Therefore, we recommend backing up those machines before initiating the upgrade.

Troubleshoot

If there are upgrade failures, you can use the following logs to troubleshoot issues on your own or provide the logs when you contact Citrix Technical Support for assistance.

- Installation logs for initial VDA installation under `%temp%/Citrix/XenDesktop Installer`
- Upgrade logs under `C:\Windows\Temp\Citrix\XenDesktop Installer`

To check VDA Upgrade Agent versions, use the following cmdlet: `Get-VusComponentVersion -ComponentType VUS`. It lists all VDAs and their VDA Upgrade Agent versions.

To get the VDA names, use the following cmdlet: `Get-BrokerMachine -UUID "<version number>"`, where `<version number>` is the VDA Upgrade Agent version that you get from the `Get-VusComponentVersion` cmdlet.

To check VDA Upgrade Agent versions at a catalog level, you can use the following script:

> **Note:**
>
> The script is intended as an example and might need to be adapted to suit your specific environment. We recommend that you test the script thoroughly before using it in a production environment.

```
Param(
    [Parameter (Mandatory=$true)]
    [string] $CatalogName
)

try
{

    $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-
       Object -Property UUID

    if($Uuids -eq $null)
    {

        throw "Cannot find CatalogName "+$CatalogName
     }

    Write-Output("Catalog Name passed is "+$CatalogName)

   foreach($Uuid in $Uuids)
    {

        $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
            -ComponentType VUS
        $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
        Write-Output("MachineName: "+$Machine.MachineName+", Machine
           UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
           Version)
     }

 }

catch
{

    Write-Output("Exception Occured")
    Write-Host $_
 }

<!--NeedCopy-->
```


Logs related to the VDA Upgrade Agent You can also collect logs related to the VDA Upgrade Agent. Logs you can collect include:

- **Citrix Diagnostic Facility (CDF) traces**. The CDF module name is `VdaUpgradeAgent`.
- **Windows event logs**. Information written to the Windows Event Log. View logs in the **Event Viewer > Applications and Services Logs > Citrix VDA Upgrade Agent Service**.

If needed, you can modify the VDA Upgrade Agent configuration file so that the logs are continuously written to a file. To enable logging to a file, follow these steps:

1. Go to the folder `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Open the file `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Change the value of `LogToFile` to 1.
4. Restart the Citrix VDA Upgrade Agent service. This creates a log file at: `C:\ProgramData\Citrix\Update Services\Logs`.

> **Note:**
>
> - Enabling logging to a file continuously writes logs, potentially consuming storage space. Remember to disable logging after the issue is resolved. To disable logging, first set `LogToFile` to `0` and then restart the Citrix VDA Upgrade Agent Service.
> - When `LogToFile=1` is set, logs are written only to the file. They will not appear in the CDF traces.

Troubleshoot VDA upgrade download failures Follow the steps below to troubleshoot and resolve download failures related to the VDA upgrade feature:

1. Make sure that relevant URLs have been added to the allow list if URL filtering is in place. See VDA upgrade requirement.
2. After adding the necessary URLs to the allow list, try rescheduling the VDA upgrade.

You can enable CDF tracing or set `LogToFile` to 1 to capture detailed logs for analysis. If the download failure issue persists, check the errors. If you see the following error message "Download Failed: This access control list is not in canonical form and therefore cannot be modified,"it indicates that the permissions on the folder `C:/ProgramData/Citrix/UpgradeServices/Downloads/VDA` are incorrect. To address the issue, do either of the following:

- **Option 1**: Reset access control lists (ACLs) on the folder using the following command. (The command reset the ACLs with default inherited ACLs for all matching files.)

  ```
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\
    VDA"/reset /T /C /L /Q
  ```


- **Option 2**: Delete the VDA folder under Downloads and then schedule the VDA upgrade.

Troubleshoot VDA upgrade validation failures Follow the steps below to troubleshoot and resolve download failures related to the VDA upgrade feature:

1. Make sure that relevant URLs have been added to the allow list if URL filtering is in place, especially the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) URLs needed for the revocation check. See VDA upgrade requirement.
2. After adding the necessary URLs to the allow list, try rescheduling the VDA upgrade.

We suggest enabling CDF tracing or setting `LogToFile` to 1 to capture detailed logs for analysis. The logs can include the following errors:

- RevocationStatusUnknown
- The revocation function was unable to check the revocation status for the certificate.
- The revocation function was unable to check revocation because the revocation server was offline.

The VDA Upgrade Agent relies on Windows system calls to validate certificates and perform revocation checks. The errors above indicate that the agent is unable to establish a connection to the CRL or OCSP URLs.

Note that the VDA Upgrade Agent does not currently support proxy settings. The outbound CRL and OCSP calls made by the CryptoAPI are not aware of proxy configurations, which can result in failures.

If your environment has a proxy setup, you can configure the system proxy on the VDA to facilitate outbound CRL calls. Follow the steps below to configure the system proxy:

```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

Upgrade VDAs using PowerShell

You can configure VDA upgrades using the Remote PowerShell SDK. For more information about the Remote PowerShell SDK, see Citrix DaaS Remote PowerShell SDK.

The following are the PowerShell cmdlets:

- **Get-VusCatalog**

Use this cmdlet to get details of a catalog such as `Name`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR), `Upgrade scheduled`, and `StateId` (status of `Upgrade scheduled`).

- **Get-VusMachine**

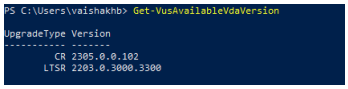
  Use this cmdlet to get details of a machine such as `MachineName`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR), and `StateId` (status of `Upgrade scheduled`).

- **Get-VusComponentVersion**

  Use this cmdlet to check if VDAs have reported the component versions. Use the `MachineId` to filter the VDAs. `MachineId` is the UUID from `Get-BrokerMachine`.

- **Get-VusAvailableVdaVersion**

  Use this cmdlet to check the latest CR/LTSR version released through the VDA Update Service.

- **Set-VusCatalogUpgradeType**

  Use this cmdlet to set the upgrade type of a catalog to CR or LTSR. The upgrade type can be set only at the machine catalog level.

- **New-VusMachineUpgrade**

  Use this cmdlet to configure VDA upgrades at the machine level.

- **New-VusCatalogSchedule**

  Use this cmdlet to schedule VDA upgrades at the machine catalog level.

Machine-level cmdlet examples

- Set the upgrade type.

  Example:
  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Use `Get-VusMachine` to check `UpgradeState` of machines in a catalog.

  Example:
  - `Get-VusMachine -CatalogName test-catalog`


```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName       : test-catalog
DNSName           : test-machine-1
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :

CatalogName       : test-catalog
DNSName           : test-machine-2
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :
```

If you see that the `UpgradeState` is `Unknown`, one possible reason is that the Citrix VDA Upgrade Agent installed on the VDA has not reported the version to the VDA Update Service. You can use the `Get-VusComponentVersion` cmdlet to check if the VDA has reported component versions.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

If no results are shown, verify the following:

- The VDA is part of a catalog and delivery group.
- The VDA Upgrade Agent is installed on the VDA and running. If necessary, try restarting the agent.

Note: If there remain no results, collect Citrix Diagnostic Facility traces while restarting the VDA Upgrade Agent and troubleshoot the issues.

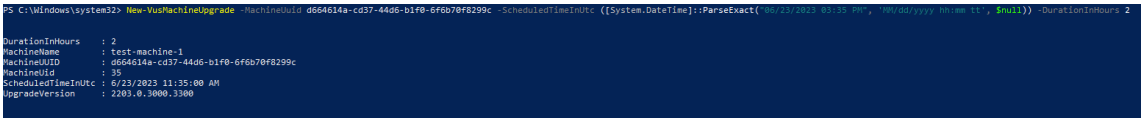
- Schedule VDA upgrades. Before you start, be aware of the following:

  - `DurationInHours`: Lets you provide the duration in hours for the upgrade process. VDAs will be put in to maintenance mode. The VDA installer will be downloaded and the upgrade will be performed. Provide longer duration if there are many VDAs to be upgraded.
  - `UpgradeNow`: Use this switch to schedule an upgrade immediately or set `ScheduledTimeInUtc` .
  - `ScheduledTimeInUtc`: Lets you schedule an upgrade for a specific date and time.

  Example:

  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  You can use `MachineUuid`, `MachineUid`, and `MachineName` to schedule the VDA upgrade.



- Check the upgrade status.

  Example:

  - `Get-VusMachine -MachineName test-machine-1`

```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 2
LastStateChange  : 6/23/2023 11:47:35 AM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 11:35:00 AM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```



```
PS C:\Users\vaishakhb> Get-VusMachine -MachineName test-machine-1

CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

Catalog-level cmdlet examples

- Set the upgrade type at the machine catalog level.

  Example:

  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Use `Get-VusCatalog` to check `UpgradeState` of the machines in a catalog:

  Example:

  - `Get-VusCatalog -Name test-catalog`

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog

CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```


If you see that the `UpgradeState` is `Unknown`, one possible reason is that the Citrix VDA Upgrade Agent installed on the VDA has not reported the version to the VDA Update Service. You can use the `Get-VusComponentVersion` cmdlet to check if the VDA has reported component versions.

```
Get-VusComponentVersion -MachineId ""
```

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

If no results are shown, verify the following:

- The VDA is part of a catalog and delivery group.
- The VDA Upgrade Agent is installed on the VDA and running. If necessary, try restarting the agent.

Note: If there remain no results, collect Citrix Diagnostic Facility traces while restarting the VDA Upgrade Agent and troubleshoot the issues.

- Schedule VDA upgrades. Before you start, be aware of the following:
  - `DurationInHours`: Lets you provide the duration in hours for the upgrade process. VDAs in the catalog will be put into maintenance mode. The VDA installer will be downloaded and the upgrade will be performed on each VDA. Provide longer duration if the catalog contains many VDAs.
  - `UpgradeNow`: Use this switch to schedule an upgrade immediately or set `ScheduledTimeInUtc` .
  - `ScheduledTimeInUtc`: Lets you schedule an upgrade for a specific date and time.

  Example:

  - ```
    New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 4
    ```

  You can use `CatalogName`, `Uid`, and `Uuid` to schedule the upgrade.

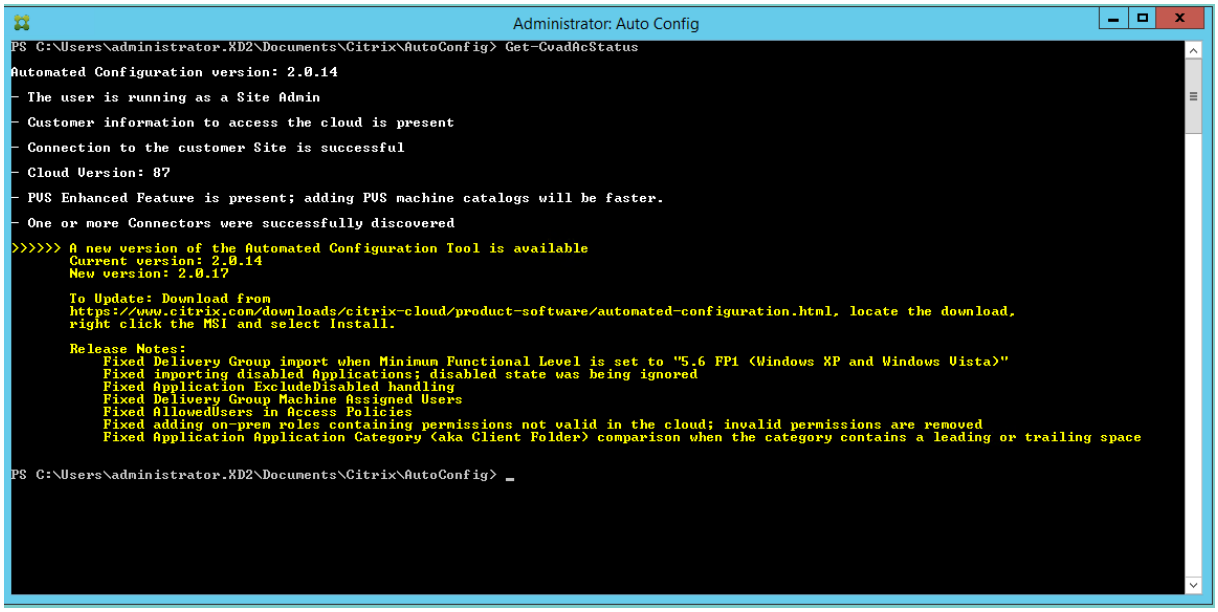
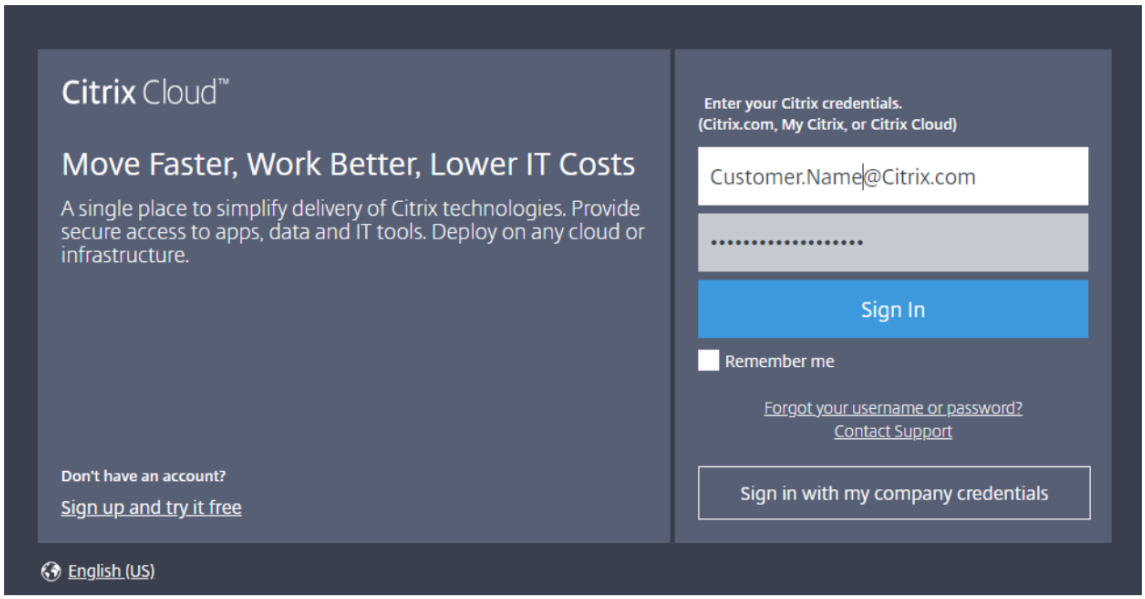
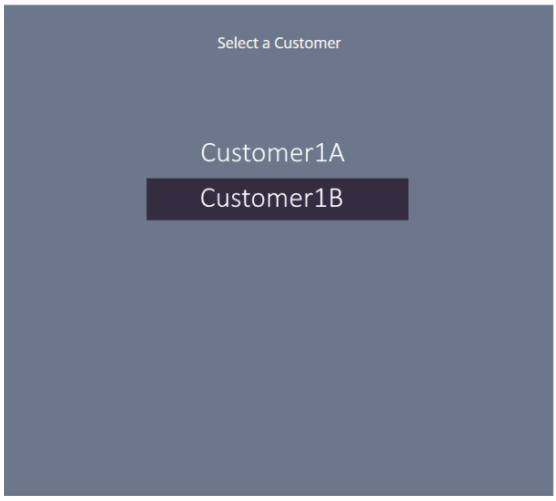
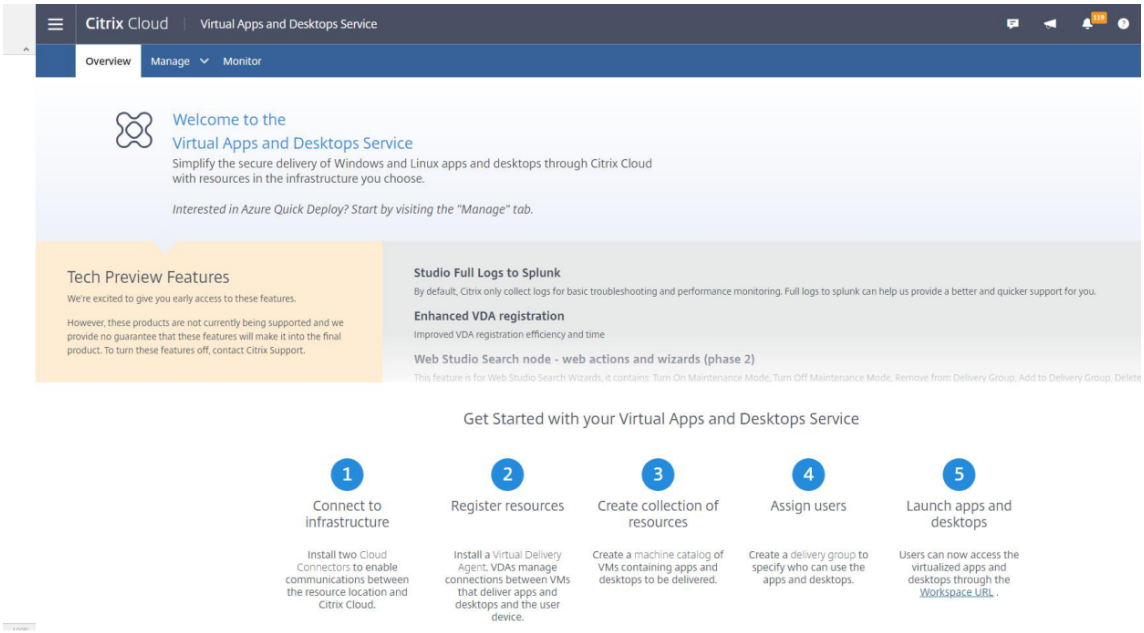
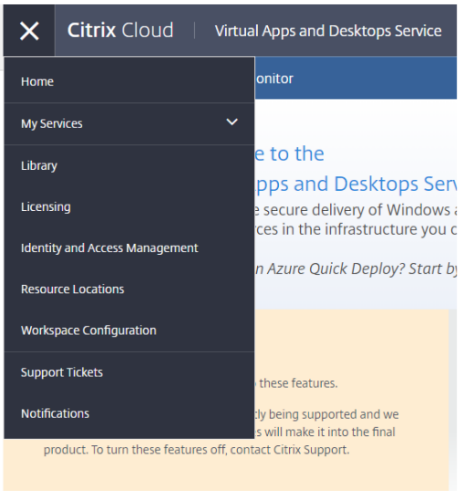
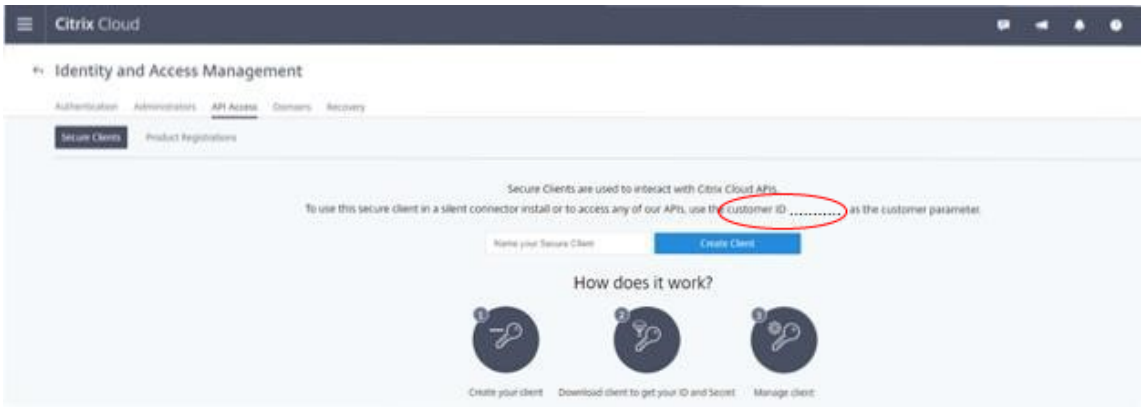
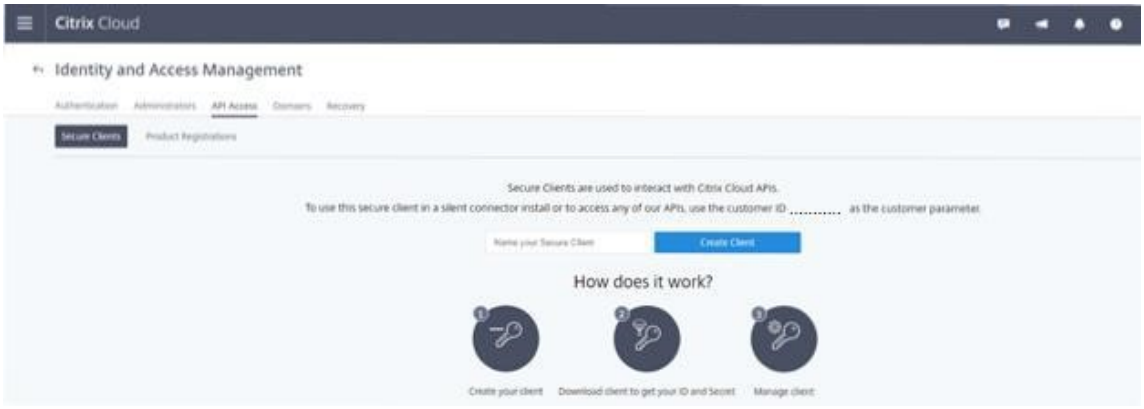
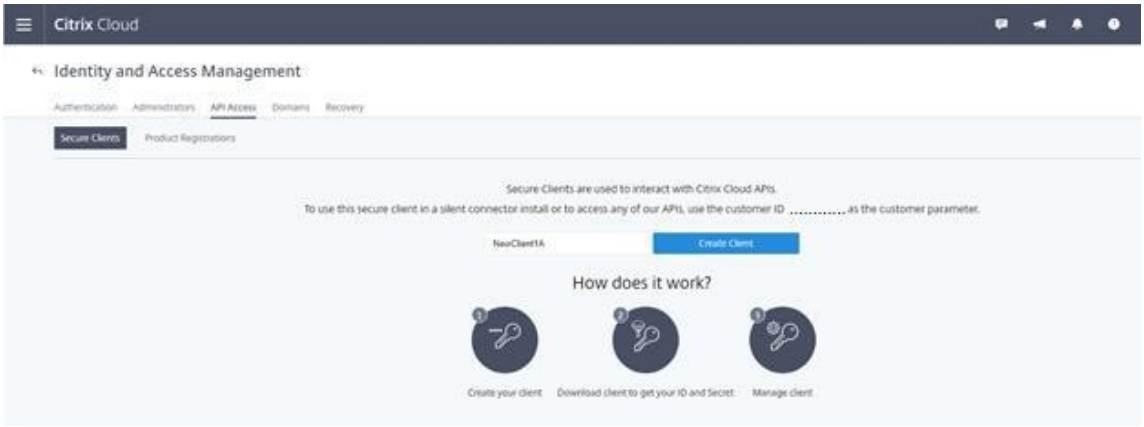
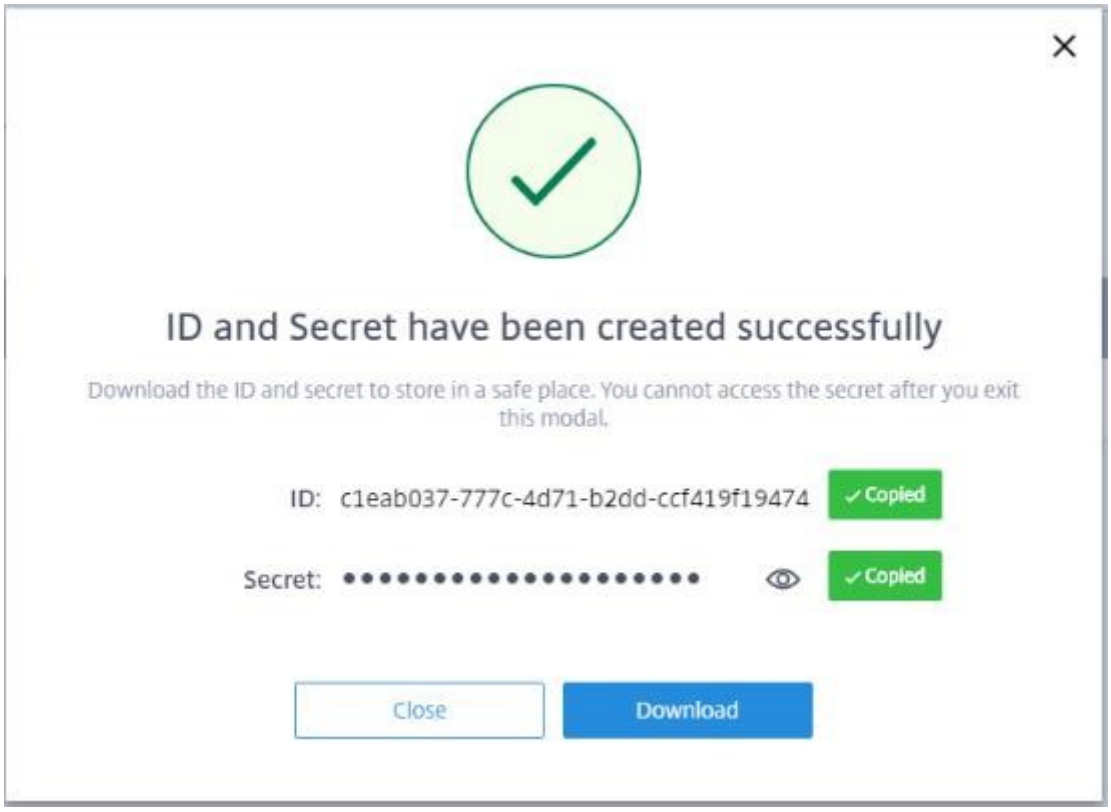
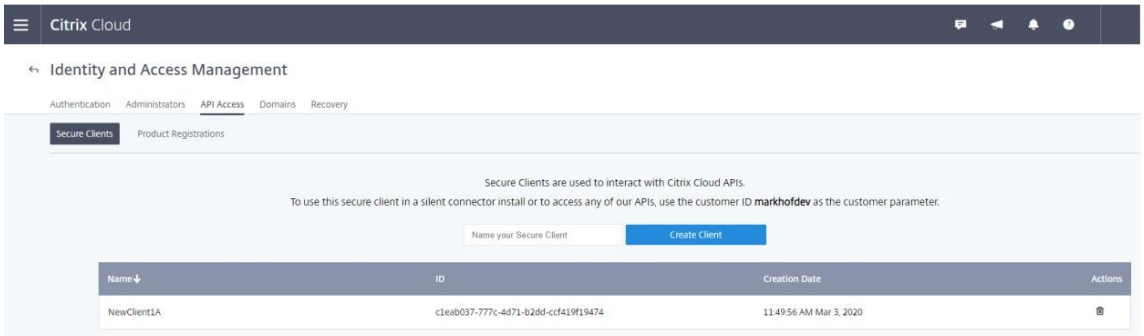
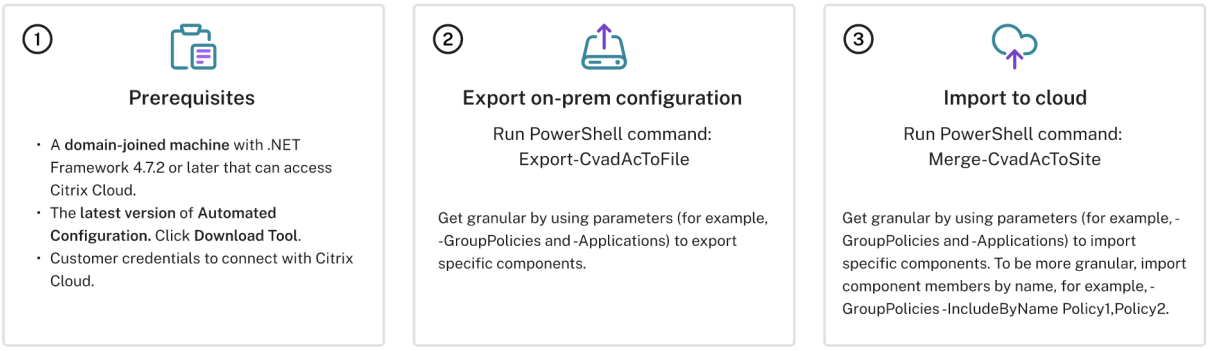
```
PS C:\Windows\system32> New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 4

CatalogName          : test-catalog
CatalogUUID          : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
CatalogUid           : 30
DurationInHours      : 4
LastStateChangeInUtc : 6/23/2023 12:08:14 PM
ScheduledTimeInUtc   : 6/23/2023 12:00:00 PM
State                : UpgradeScheduled
UpgradeVersion       : 2203.0.3000.3300
```

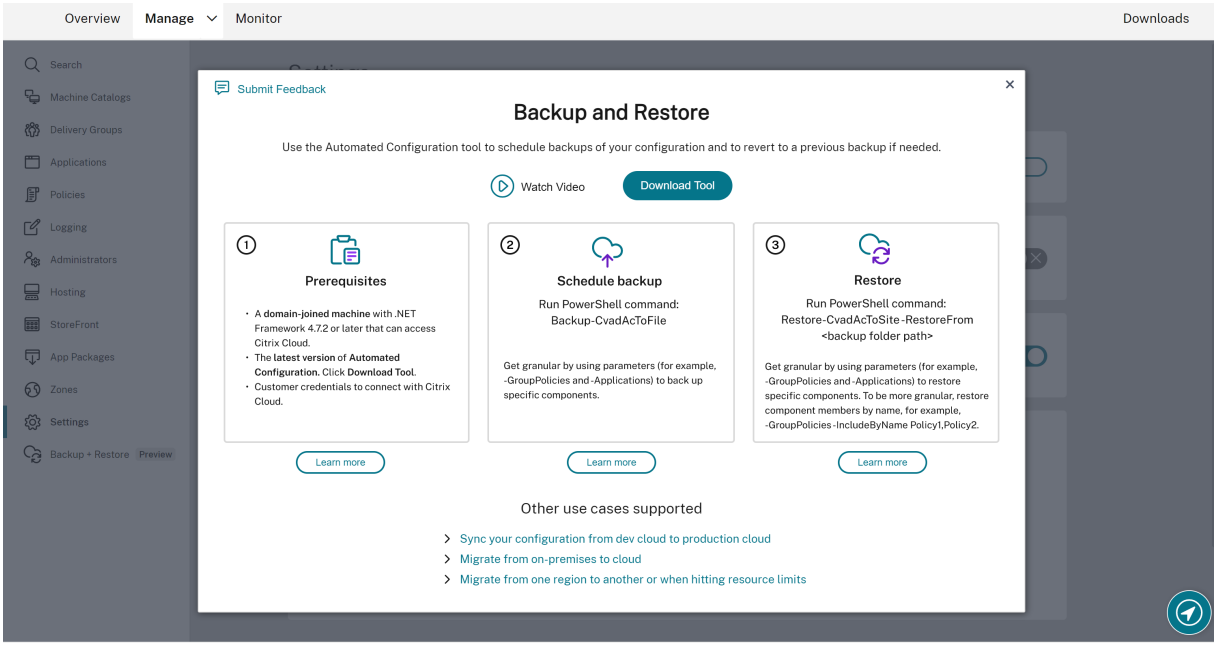
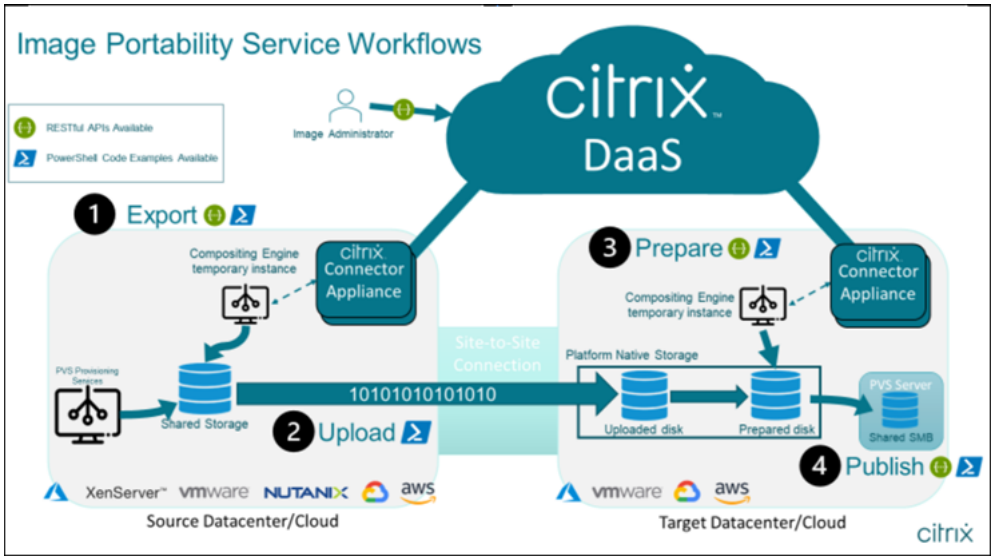
- Check the upgrade status. Use the `Get-VusCatalog` or `Get-VusMachine` cmdlet to check the VDA upgrade status periodically. Use the `MachineUuid`, `MachineUid`, and


```

`MachineName` to filter the VDAs.

Example:

- `Get-VusCatalog -Name test-catalog`

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog

CancelledUpgrades   : 0
DurationInHours   : 4
FailedUpgrades   : 0
InProgressUpgrades   : 0
LastStateChangeInUtc   : 6/23/2023 12:08:43 PM
MaxConcurrentUpgrades   : 100
Name   : test-catalog
ProvisioningType   : MCS
ScheduledTimeInUtc   : 6/23/2023 12:00:00 PM
SecurityCheckFailedUpgrades : 0
SessionSupport   : SingleSession
StateId   : UpgradeInProgress
SuccessfulUpgrades   : 0
TotalMachines   : 2
Uid   : 30
UpgradeState   : UpgradeScheduled
UpgradeType   : LTSR
UpgradeVersion   : 2203.0.3000.3300
Uuid   : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

Use `Get-VusMachine` to see the VDA upgrade status of each machine in a catalog.

```
PS C:\Users\vaishakhb> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:17:33 PM
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```


If the VDA has Personal vDisk installed

If the Personal vDisk (PvD) component was ever installed on a VDA, that VDA cannot be upgraded to version 1912 LTSR or later until you remove that component.

This instruction applies even if you never used PvD. Here's how the PvD component might have been installed in earlier versions:

- In the VDA installer's graphical interface, PvD was an option on the **Additional Components** page. The 7.15 LTSR and earlier 7.x releases enabled this option by default. So, if you accepted the defaults (or explicitly enabled the option in any release), PvD was installed.
- On the command line, the `/baseimage` option installed PvD. If you specified this option, or used a script that contained this option, PvD was installed.

What to do

If the VDA installer does not detect the PvD component in the currently installed VDA, the upgrade proceeds as usual.

If the installer detects the PvD component in the currently installed VDA:

- **Graphical interface:** The upgrade pauses. A message asks if you want the unsupported component removed automatically. When you click **OK**, the component is removed automatically and the upgrade proceeds.
- **CLI:** The command fails if the installer detects the PvD component. To avoid command failure, include the following option in the command: `/remove_pvd_ack`.

If you want to continue using PvD on your Windows 10 (1607 and earlier, without updates) machines, VDA 7.15 LTSR is the latest supported version. Be aware that the Extended Support program for XenApp and XenDesktop 7.15 LTSR doesn't apply to VDAs used with Citrix DaaS. For more information, see the Extended Support Customer Guide in the Citrix Support Knowledge Center.

Earlier operating systems

The System requirements article lists the supported Windows operating systems for current release VDAs.

- For LTSR VDAs, see the system requirements article for your LTSR version.
- For Linux VDAs, see the Linux Virtual Delivery Agent documentation.

For Windows machines with OSs that are no longer supported for installation of the latest VDA, you have the following options.

For non-WVD environments:

- Reimage the machine to a supported Windows version, and then install the new VDA.
- If reimaging the machine is not an option but you want to upgrade the OS, uninstall the VDA before upgrading the OS. Otherwise, the VDA will be in an unsupported state. After upgrading the OS, install the new VDA.
- If the machine has version 7.15 LTSR installed (and you try to install a newer version), a message informs you that you're using the latest supported version.
- If the machine has a version earlier than 7.15 LTSR installed, a message guides you to CTX139030 for information. You can download 7.15 LTSR VDAs from the Citrix website.

Migrate configuration to Citrix Cloud

March 4, 2024

Why use Automated Configuration

IT administrators in charge of large or complex environments often find migrations to be a tedious process. They frequently end up writing their own tools to accomplish this task successfully since it tends to be specific to their use cases.

Citrix wants to help ease this process by automating the migration process using the Automated Configuration tool. Administrators can easily test current configurations in Citrix Cloud and take advantage of the benefits offered by Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) while keeping their current environments *intact*. There is also no end user impact, as Automated Configuration works seamlessly in the background. Such benefits include reduced administrative overload when Citrix manages part of the back-end and control plane, automatic and customizable Citrix Cloud component updates, and others.

Citrix uses industry-standard configuration as code to provide a mechanism to help automate migration processes. Automated Configuration discovers and exports one or more on-premises sites as a collection of configuration files. These files' configuration can then be imported into Citrix DaaS.

Automated Configuration also allows administrators to merge multiple on-premises sites into a single site, while avoiding name collisions. Administrators can control whether the on-premises or cloud configuration controls resources.

Automated Configuration is not just a one time migration tool, but can also automate your day-to-day configuration in Citrix Cloud. Moving your Citrix DaaS configuration can be beneficial for many reasons:

- Syncing your site from test or stage to production

- Backing up and restoring your configuration
- Reaching resource limits
- Migrating from one region to another

The following *2-minute* video provides a quick tour of Automated Configuration.

This is an embedded video. Click the link to watch the video

For additional information on Automated Configuration, see Proof of Concept: Automated Configuration Tool on Tech Zone.

For a deeper look into moving your deployment and readying your on-premises configuration for migration, see Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud on Tech Zone.

Download Automated Configuration

Download and install the Automated Configuration tool from Citrix Downloads.

> **Important:**
>
> To prevent errors in functionality, always use the latest available version of Automated Configuration.

Upgrading Automated Configuration

When running cmdlets that access the cloud in Automated Configuration, the tool alerts you when there is a newer version available for download.



You can make sure you have the latest version by following the steps below:

1. Double-click the **Auto Config** icon. A PowerShell window appears.
2. Run the following command to check your version number.

   ```
   Get-CvadAcStatus
   ```

3. Check your tool version against the version listed in the alert or at Citrix Downloads. The latest version of the tool is located there.
4. Download and install the latest version of the tool. You do *not* need to uninstall the old version to upgrade Automated Configuration.

> **Note:**
>
> The alert appears every time you run a cmdlet that accesses the cloud. For more information on cmdlets, see Automated Configuration tool cmdlets.

Known limitations

- Machine catalogs provisioned through Machine Creation Services have special considerations. For more information on MCS, see Understanding migrating Machine Creation Services provisioned catalogs.

Supported migration objects

Automated Configuration supports moving the configuration of the following components:

- Tags
- Delegated Admin
  - Scopes
  - Roles
- Host Connections
  - A Single Resource Pool
  - Admin Scopes
- Machine Catalogs
  - Admin Scopes
  - Machines
  - Remote PC Access, Physical, Pooled, Provisioned, MCS, Assigned
- StoreFronts

- Delivery Groups
  - Access Policy
  - Admin Scope Association
  - Application Access Policy
  - Assignment Policy
  - Entitlement/Desktop Policy
  - Power Schedules
  - Session Lingering
  - Session Prelaunch
  - Reboot Schedules
  - Tags
- Application Groups
  - Admin Scope Association
  - Delivery Groups
  - Users and Groups
- Applications
  - Application Folders
  - Icons
  - Applications
  - Broker Configured FTAs
  - Tags
- Group Policies
- User Zone Preferences

Component migration order

The components and their dependencies are listed here. A component's dependencies must be in place before it can be imported or merged. If a dependency is missing, it can cause the import or merge command to fail. The **Fixups** section of the log file shows missing dependencies if an import or merge fails.

1. Tags
   - No pre-dependencies
2. Delegated Admin
   - No pre-dependencies
3. Host Connections

- Security Information in CvadAcSecurity.yml

4. Machine Catalogs
    - Machines present in Active Directory
    - Host Connections
    - Tags
5. StoreFronts
6. Delivery Groups
    - Machines present in Active Directory
    - Users present in Active Directory
    - Machine Catalogs
    - Tags
7. Application Groups
    - Delivery Groups
    - Tags
8. Applications
    - Delivery Groups
    - Application Groups
    - Tags
9. Group Policies
    - Delivery Groups
    - Tags
10. User Zone Preferences

Common prerequisites

The following are some common prerequisites that are needed for Automated Configuration to work correctly. These prerequisites are used in both on-premises to cloud and cloud to cloud migrations.

Generating the customer ID, client ID, and secret key

Before you begin your migration using Automated Configuration, you need your Citrix Cloud customer ID and you must create a client ID and a secret key to import your configuration to Citrix Cloud. All cmdlets accessing the cloud require these values.

The following steps allow you to retrieve the customer ID and create the client ID and secret key.

To retrieve the **Customer ID**:

1. Sign into your Citrix Cloud account and select the customer.





2. Click the hamburger menu, then select **Identity and Access Management** in the drop-down menu.





3. The **Customer ID** is located on the **Identity and Access Management** page.



To retrieve the **Client ID** and **Secret Key**:

1. On the **Identity and Access Management** page, click the **API Access** tab.



2. Enter a name in the box. This name is used to differentiate between multiple client IDs and secret keys. Click **Create Client** to create the client ID and the secret key.



3. The following dialog appears after you successfully create the client ID and the secret key. Be sure to copy both values to a secure location and download the .csv file containing this information. The .csv file can be used to create the CustomerInfo.yml file.



4. The client ID and the secret key are successfully created.



Place these values in a secure location and share only with trusted company members who need access to the tool or access the cloud Rest APIs. The client ID and secret key do not expire. If they are compromised, immediately remove them by using the **Trash** icon and create new ones.

> **Note:**
>
> The secret key cannot be retrieved if it is lost or forgotten; a new client ID and secret key must be created.

Populating customer info file

Using the CustomerInfo.yml file eliminates the need to provide customer information parameters with each cmdlet's execution. Any of the customer information can be overridden by using cmdlet parameters.

Create the CustomerInfo.yml file by using the `New-CvadAcCustomerInfoFile` cmdlet.

> **Important:**
>
> Do not manually edit the CustomerInfo.yml file. Doing so can cause inadvertent formatting errors.

`New-CvadAcCustomerInfoFile` has the following required parameters.

- CustomerId –customer's ID.
- ClientId –customer's client ID created on Citrix Cloud.
- Secret –customer's secret created on Citrix Cloud.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

You can also create the CustomerInfo.yml using the `SecurityCsvFileSpec` parameter that points to the downloaded security.csv file. You must also specify the CustomerId.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads/security.csv -CustomerId markhof123
```

Update the CustomerInfo.yml file by using the `Set-CvadAcCustomerInfoFile` cmdlet. This cmdlet only changes the Client ID.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

The following is a sample CustomerInfo.yml file.

```
# Created/Updated on 2020/01/29 16:46:47
CustomerId: 'markhof123'
ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
Secret: 'TwBLaaabbbaaaaaaaaaaw=='
Environment: Production
AltRootUrl: ''
StopOnError: False
AlternateFolder: ''
Locale: 'en-us'
Editor: 'C:\Program Files\Notepad++\notepad++.exe'
Confirm: True
DisplayLog: True
```


Populating zone mapping file

An on-premises zone is the equivalent of the cloud resource location. Unlike other site components, you cannot import the on-premises zone to the cloud automatically. Instead, it must be manually mapped using the ZoneMapping.yml file. Import failures can occur if the zone name is not associated with an existing resource location name.

For on-premises sites having only one zone and cloud sites only one resource location, the Automated Configuration tool makes the correct association, eliminating the need to manually manage the ZoneMapping.yml file.

For on-premises sites having multiple zones or cloud sites having multiple resource locations, the ZoneMapping.yml file must be manually updated to reflect the correct mapping of on-premises zones to cloud resource locations. This must be done before attempting any import operation to the cloud.

The ZoneMapping.yml file is located in *%HOMEPATH%\Documents\Citrix\AutoConfig*. The content of the .yml file is a dictionary with the zone name as the key and the resource location name as the value.

As an example, an on-premises Citrix Virtual Apps and Desktops site with a primary zone called "Zone-1"and a secondary zone called "Zone-2"is migrated to a Citrix DaaS deployment with two newly created cloud resource locations called "Cloud-RL-1"and "Cloud-RL-2". In this instance, the ZoneMapping.yml would be configured as follows:

```
1               Zone-1: Cloud-RL-1
2
3               Zone-2: Cloud-RL-2
```

> **Note:**
>
> A space must be between the colon and resource location name. If spaces are used in the zone or resource location name, enclose the name with quotes.

Host connections

Host connections and their associated hypervisors can be exported and imported using Automated Configuration.

Adding a hypervisor to a host connection requires security information specific to the type of hypervisor. This information cannot be exported from the on-premises site for security considerations. You must manually provide the information so that Automated Configuration can successfully import host connections and hypervisors to the cloud site.

The export process creates the CvadAcSecurity.yml file in *%HOMEPATH%\Documents\Citrix\AutoConfig* containing placeholders for each security item needed for the specific hypervisor type. You must

update the CvadAcSecurity.yml file before importing into the cloud site. Administrator updates are retained over multiple exports with new security placeholders added as needed. Security items are never removed. For more information, see Manually update the CvadAcSecurity.yml file

```
            HostConn1:
            ConnectionType: XenServer
            UserName: root
            PasswordKey: rootPassword
            HostCon2:
            ConnectionType: AWS
            ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
            SecretKey: TwBLaaaaaaaaaaaaaaaaw==
            Region: East
```

Per-hypervisor security information The following lists the security information required for each hypervisor type.

- XenServer, Hyper-V, VMware
  - User Name
  - Clear-text Password
- Microsoft Azure
  - Subscription ID
  - Application ID
  - Application Secret
- Amazon Web Services
  - Service Account ID
  - Application Secret
  - Region

Special security considerations All security information is entered as clear text. If clear text is not recommended, the host connections and associated hypervisors can be manually created using the **Manage > Full Configuration** interface. The host connections and hypervisor names must match their on-premises counterparts exactly so that machine catalogs that use the host connections can be successfully imported.

Activating sites

The delivery controller in both on-premises and cloud sites control resources such as brokering desktops, applications, and rebooting machines. Problems occur when a common set of resources is controlled by two or more sites. Such a situation can occur when migrating from an on-premises site to a

cloud site. It is possible for both the on-premises and cloud delivery controllers to manage the same set of resources. Such dual management can lead to resources becoming unavailable and unmanageable, and can be difficult to diagnose.

Site activation allows you to control where the active site is controlled.

Site activation is managed using the delivery group maintenance mode. Delivery groups are placed in maintenance mode when the site is inactive. Maintenance mode is removed from delivery groups for sites that are active.

Site activation does not affect or manage VDA registration or machine catalogs.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

All cmdlets support the `IncludeByName` and `ExcludeByName` filtering. This parameter allows you to select which delivery groups can have their maintenance mode changed. Delivery groups can be selectively changed as needed.

Import and transferring control to the cloud

The following is a high-level description on how to import and transfer control from the on-prem site to the cloud site.

1. Export and import the on-premises site to the cloud. Make sure the `–SiteActive` parameter is not present on any of the import cmdlets. The on-premises site is active and the cloud site inactive. By default, cloud site delivery groups are in maintenance mode.
2. Verify the cloud content and configuration.
3. During off hours, set the on-premises site to inactive. The `–SiteActive` parameter must be absent. All on-premises site delivery groups are in maintenance mode.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Set the cloud site to active. The `–SiteActive` parameter must be present. No cloud site delivery groups are in maintenance mode.
    - `Set-CvadAcSiteActiveStateCloud –SiteActive`
5. Verify that the cloud site is active and the on-premises site is inactive.

Transferring control back to the on-premises site

To transfer control from the cloud site to the on-premises site:

1. During off hours, set the cloud site to inactive. All cloud site delivery groups are in maintenance mode.

- `Set-CvadAcSiteActiveStateCloud`

2. Set the on-premises site to active. No on-prem site delivery groups are in maintenance mode.
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

Additional site activation information

- If no machines are power managed and there are no reboot schedules (which usually means there are no host connections either) all cloud delivery groups can be imported as active. Add `-SiteActive` to `Merge-CvadAcToSite`/`Import-CvadAcToSite` or run `Set-CvadAcSiteActiveStateCloud -SiteActive` after importing.
- If machines are power managed or there are reboot schedules, a different process is needed. For example, when switching from on-premises to cloud in this situation, set the on-premises site to inactive using `Set-CvadAcSiteActiveStateOnPrem`. Then, set the cloud site to active using `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- The `Set-CvadAcSiteActiveStateCloud` and `Set-CvadAcSiteActiveStateOnPrem` cmdlets are also used to reverse the process. For example, run `Set-CvadAcSiteActiveStateCloud` without the `-SiteActive` parameter, then run `Set-CvadAcSiteActiveStateOnPrem` with the `-SiteActive` parameter.

Understanding migrating Machine Creation Services provisioned catalogs

> **Note:**
>
> This feature is available only on versions 3.0 and later. Check your version by using `Get-CvadAcStatus` within Automated Configuration.

Machine Creation Services (MCS) catalogs create two different types of catalogs:

- When changes made to a machine are lost/reversed (Commonly Server OS, where applications are published) –this is a pooled VDI / multi-session use case
- When changes made to a machine are preserved across reboot (Commonly client OS with a dedicated user) –this is a static VDI use case

The type of catalog can be confirmed in the catalog node in Citrix Studio and looking at the "User data:"value of the catalog.

> **Note:**
>
> MCS cannot be backed up from the cloud using Automated Configuration.

Pooled VDI / multi-session catalogs

Catalogs with "User data: Discard"are pooled VDI catalogs and can only migrate the main image and configuration. Any virtual machines in these catalogs are not migrated. This is because the life cycle of the virtual machine is maintained by the site you are importing from, which means every time the machines are turned on, its state might change. This makes import impossible as the import data for the virtual machines quickly gets of out of sync.

When you are migrating these catalogs using the tool, it creates catalog metadata and initiates main image creation, but no machines are imported.

Since this process can take some time to be created based on the size of the main image, the import command within the tool only starts the MCS catalog creation and does not wait for it to finish. After the import has completed, monitor the catalog create progress using the Full Configuration management interface in the cloud deployment.

Once the main image is created, you can provision machines. Capacity considerations need to be taken into account since you would have capacity consumed from your on-premises usage.

All other objects (delivery groups/applications/policies, and so forth) that use that catalog can be imported and do not have to wait for the main image creation. When the catalog has finished creating, machines can be added to the imported catalog and then users can launch their resources.

> **Note:**
>
> Use the same commands available within the tool to migrate catalogs and all other objects.

Static VDI catalogs

> **Note:**
>
> Since this operation imports low-level details that are stored in the database, this process must be run from a machine with database access.

static VDI catalogs migrate the main image, configurations, and all virtual machines. Unlike the pooled VDI use case, no images need to be created.

The VDAs must be pointed to the connector for them to register with the cloud.

Refer to the Activating sites section to make the cloud site active, so that the reboot schedule, power management, and other items are controlled by the cloud.

Once the migration is completed, if you want to delete this catalog from your on-premises site, you must select leave VM and AD account. Otherwise, they are deleted and the cloud site would be left pointing to the deleted VM.

Update MCS tags to detect orphaned resources after migration

After you migrate from on-premises configuration to a cloud site, or from your cloud configuration to another cloud site, you must update the MCS site id tags in case of persistent VMs so that orphaned resources can be detected correctly. To do this, use the PowerShell command `Set-ProvResourceTags`. Currently, this feature is applicable to Azure.

The detailed steps are as follows:

1. Update the MCS site id tags from the new Citrix site using the PowerShell command `Set-ProvResourceTags`. For example:

```
Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <
   String>] [-VMBatchSize XX] [-ResourceType XX]
<!--NeedCopy-->
```

   Or,

```
Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <
   String>] [-VMBatchSize XX] [-ResourceType XX]
<!--NeedCopy-->
```

The parameter details are as follows:

- `ProvisioningSchemeUid` or `ProvisioningSchemeName` is a mandatory parameter.
- `VMName` is an optional parameter. If no `VMName` is specified, tags of all the VMs of this machine catalog are updated.
- `VMBatchSize` is an optional parameter to divide all VMs into batches. If no `VMBatchSize` is specified, the default value (10) is applied. The range is from 1-60.
- `ResourceType` can be one of the following:
  - `MachineCatalog`: For updating tags of machine catalog resources.
  - `VirtualMachine`: For updating tags of VM related resources.
  - `All`: (default ResourceType): For updating tags of both machine catalog and VM related resources.

Migrating from on-premises to cloud

June 6, 2024

Automated Configuration allows you to automate moving your on-premises configuration to a cloud site.

The following image is a high-level view of what Automated Configuration can do to migrate your configuration to the cloud.



Prerequisites for migrating your configuration

For *exporting* your configuration from Citrix Virtual Apps and Desktops, you need:

- Citrix Virtual Apps and Desktops: current release and its immediate predecessor or Citrix Virtual Apps and Desktops, XenApp and XenDesktop LTSRs: all versions
- A domain-joined machine with .NET Framework 4.7.2 or later and the Citrix PowerShell SDK. This is automatically installed on the Delivery Controller. (To run on machine other than the on-premises Delivery Controller, Citrix Studio must be installed, as Studio installs the correct PowerShell snap-ins. The Studio installer can be found on the Citrix Virtual Apps and Desktops installation media.)

For *importing* your configuration into Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), you need:

- A machine with access to Citrix Cloud. This does not have to be a Delivery Controller or a domain-joined machine.
- Citrix DaaS provisioned.
- An active resource location with Connector installed and domain-joined to the same domain as the on-premises setup.
- Connectivity to sites accessing Citrix Cloud must be allowed and available. For more information, see System and Connectivity Requirements.

> **Note:**
>
> Automated Configuration cannot be installed on a Cloud Connector system.

Exporting your Citrix Virtual Apps and Desktops on-premises configuration

> **Important:**
>
> - You must have your CustomerInfo.yml file with your customer ID, client ID, and the secret key information included. For more information on how to retrieve your customer ID, client ID and secret key, see Generating the customer ID, client ID, and secret key. For information on how to add this information to the CustomerInfo.yml file, see Populating customer info file.
> - The ZoneMapping.yml file must include information that maps your on-premises zone to Resource Locations in the cloud. For more information on how to map your zones, see Populating zone mapping file.
> - If you have host connections, you must input the corresponding info in the CvadAcSecurity.yml file.

1. Install Automated Configuration.
2. Double-click the **Auto Config** icon. A PowerShell window appears.
3. Run the following command to export all components. Exporting your on-premises configuration does *not* change it in any way.

   ```
   Export-CvadAcToFile
   ```

After you run any cmdlet for the first time, an export folder with the .yml configuration files and logs is created. The folder is at *%HOMEPATH%\Documents\Citrix\AutoConfig*. Each successive export creates a subfolder. The parent folder *%HOMEPATH%\Documents\Citrix\AutoConfig* always contains the exported files from the most recent export.

> **Note:**
>
> If Automated Configuration is not installed on the Delivery Controller, run `import-module Citrix.AutoConfig.Commands` before using the tool through PowerShell. This step is not needed if you open Automated Configuration using the **Auto Config** icon.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

Importing your configuration to Citrix DaaS

> **Important:**
>
> - You must have your CustomerInfo.yml file with your customer ID, client ID, and the secret key information included. For more information on how to retrieve your customer ID, client ID and secret key, see Generating the customer ID, client ID, and secret key. For information on how to add this information to the CustomerInfo.yml file, see Populating customer info file.

- The ZoneMapping.yml file must include information that maps your on-premises zone to resource locations in the cloud. For more information on how to map your zones, see Populating zone mapping file.
- If you have host connections, you must input the corresponding info in the CvadAcSecurity.yml file.
- When migrating an on-premises deployment to cloud, make sure that the domain and OU GPOs that contain the Citrix settings are migrated to cloud. Citrix Web Studio does not support GPMC and hence, the domain and OU GPOs are not visible in the Web Studio. The Citrix policy engine enforces the domain and OU GPOs on VDAs and users that are in the domains and OUs. Post log in to a VDA, a user might see that the policies from the domain and OU GPOs are applied to their session. However, administrators cannot see these policies and settings which might lead to confusions.

Running an import

1. Double-click the **Auto Config** icon. A PowerShell window appears.
2. Run the following command to import all components.

   ```
   Merge-CvadAcToSite
   ```

Verify the expected state with the new current state. Various import options control whether the import results are identical or a subset of the on-premises site.

After you run the cmdlet, an export folder with the .yml configuration files and logs is created. The folder is at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

> **Note:**
>
> If Automated Configuration is not installed on the Delivery Controller, run `import-module Citrix.AutoConfig.Commands` before using the tool through PowerShell. This step is not needed if you open Automated Configuration using the **Auto Config** icon.

To revert to your original Citrix DaaS configuration, see Backing up your Citrix DaaS configuration.

Import operation in detail

The import process is designed to accurately perform updates, only perform needed updates and verify that all updates have been correctly made. The steps followed in all import operations follow.

1. Read the exported .yml file (expected state).
2. Read the cloud (current state).

3. Back up the pre-import cloud state to .yml files (pre-backup can be restored if necessary).
4. Evaluate the differences between the expected and current state. This determines which updates to make.
5. Make the updates.
6. Reread the cloud (new current state).
7. Back up the post-import cloud state to .yml files (post-backup can be restored if necessary).
8. Compare the new current state with the expected state.
9. Report the results of the comparison.

Granular migration

> **Important:**
>
> For more information on component migration order, see Component migration order.

You can selectively migrate components only or even component names only.

- Component parameters supported include `MachineCatalogs`, `Tags` and more.
- Component name parameters supported include `IncludeByName` and `ExcludeByName` parameters, and others.

For more information on parameters and how to use them, see Granular migration parameters.

Activating sites

Site activation allows you to control which site is active and controls your resources. For more information, see Activating sites.

Merging multiple sites into a single site

March 4, 2024

Multi-site support for Automated Configuration provides a method to merge multiple on-premises sites into a single cloud site.

Multi-site support adds unique prefixes and suffixes to component names on a per on-premises-site basis, ensuring name uniqueness after multiple on-premises sites are merged to a single cloud site.

Prefixes and suffixes can be assigned for each of the following components on a per-on-premises-site basis.

- `AdminScope`

- AdminRole
- ApplicationAdmin
- ApplicationFolder
- ApplicationGroup
- ApplicationUser
- DeliveryGroup
- GroupPolicy
- HostConnection
- MachineCatalog
- StoreFront
- Tag

Application folders support prefixing, suffixing, and rerooting. Rerooting adds an extra top level folder to an application's existing folder structure.

Prefixing and suffixing rules

1. Prefixes and suffixes cannot contain any of the following special characters: `\ , / ; : # . * ? = < > | ( )"' { } [ ]`
2. Prefixes and suffixes can contain trailing spaces but not leading spaces.
3. Prefixes and suffixes must be double quoted to contain trailing spaces.
4. Prefixes and suffixes are applied at the time of import, merge, and add. The source .yml files are never modified.
5. The prefix and suffix process automatically prefixes or suffixes dependent component names when applicable. For example, if machine catalog names are prefixed with "East,"delivery groups referencing them are also prefixed with "East."
6. If a component name already begins with the prefix or suffix, no prefix or suffix is added. Component names cannot contain double identical prefixes or suffixes.
7. Prefixes and suffixes can be individually used or used in combination.
8. Use of a prefix or a suffix on a component is optional.

> **Note:**
>
> The Full Configuration interface displays components in alphabetical order.

Group by site

Use prefixing to visually group components from a single site. Each site is listed in its own group with prefixing alphabetically controlling the ordering of different site groups.

Group by name

Use suffixing to visually group like-named components from multiple sites. Like-named components from different sites visually alternate.

SitePrefixes.yml file

Site prefixing begins with the SiteMerging.yml file that contains the site prefix and suffix mapping for one or more on-premises sites. You can manage the SiteMerging.yml file manually, or by using the available cmdlets listed at the Merging multiple on-premises sites cmdlets section.

Exporting, importing, merging, and adding

Merging cannot begin until you have exported an on-premises site. To export an on-premises site, see Migrating from on-premises to cloud.

Central export target folder

The methods described in this section place multiple site exports into a central file share location. The SiteMerging.yml file, CustomerInfo.yml file, and all export files reside in that file share location, allowing you to do the import from one location independent of the on-premises sites.

Cloud accessing operations never reference the on-premises sites or Active Directory, therefore allowing you to do cloud-accessing operations from anywhere.

Direct file share

The export, import, merge, and new/add operations provide a parameter to target or source a folder other than the default folder, *%HOMEPATH%\Documents\Citrix\AutoConfig*. The following examples use a central file share located at `\\share.central.net` that the admin already has access to, having provided credentials as needed.

To target the export to a site-specific folder, use the `–TargetFolder` parameter:

From the East DDC:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteEast
```

From the West DDC:


```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteWest
```

After the exports are complete, create the CustomerInfo.yml and SiteMerging.yml files and place them in `\\share.central.net\AutoConfig`.

> **Note:**
>
> Do not use the `SiteRootFolder` parameter when creating the SitePrefixes.yml when using this direct file share reference method.

To import, merge, or add from the direct file share, you must decide from which machine you want to do the cloud accessing operation. Options include:

- One of the on-premises DDCs where the tool is already installed.
- The machine hosting the file share.
- A different machine.

Automated Configuration must be installed on the machine accessing the cloud. Neither the on-premises PowerShell SDK, DDC, nor Active Directory are used, so the cloud accessing execution requirements are simpler than the export requirements.

To merge the East DDC to the cloud:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \\share.central.
net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

To merge the West DDC to the cloud:

```
Merge-CvadAcToSite –SiteName West –SourceFolder \\share.central.
net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

The following is a sample SitePrefixes.yml file used in the previous example.

```
1     East:
2       SiteRootFolder: "" # Important: leave this empty
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
            is used instead
7       ApplicationFolderRoot: "East"
8       ApplicationGroupPrefix: "East_"
9       ApplicationUserPrefix: "East_"
10      DeliveryGroupPrefix: "East_"
11      GroupPolicyPrefix: "East_"
```



```
        HostConnectionPrefix: "East_"
        MachineCatalogPrefix: "East_"
        StoreFrontPrefix: "East_"
        TagPrefix: "East_"
        AdminScopeSuffix: "_east"
        AdminRoleSuffix: "_east"
        ApplicationAdminSuffix: "_east"
        ApplicationFolderSuffix: "_east"
        ApplicationGroupSuffix: "_east"
        ApplicationUserSuffix: "_east"
        DeliveryGroupSuffix: "_east"
        GroupPolicySuffix: "_east"
        HostConnectionSuffix: "_east"
        MachineCatalogSuffix: "_east"
        StoreFrontSuffix: "_east"
        TagSuffix: "_east"
      West:
        SiteRootFolder: "" # Important: leave this empty
        AdminScopePrefix: "Western "
        AdminRolePrefix: "Western "
        ApplicationAdminPrefix: "Western "
        ApplicationFolderPrefix: "" # Note that a new parent root folder
            is used instead
        ApplicationFolderRoot: "Western"
        ApplicationGroupPrefix: "Western "
        ApplicationUserPrefix: "Western "
        DeliveryGroupPrefix: "Western "
        GroupPolicyPrefix: "Western "
        HostConnectionPrefix: "Western "
        MachineCatalogPrefix: "Western "
        StoreFrontPrefix: "Western "
        TagPrefix: "Western "
        AdminScopeSuffix: ""
        AdminRoleSuffix: ""
        ApplicationAdminSuffix: ""
        ApplicationFolderSuffix: ""
        ApplicationGroupSuffix: ""
        ApplicationUserSuffix: ""
        DeliveryGroupSuffix: ""
        GroupPolicySuffix: ""
        HostConnectionSuffix: ""
        MachineCatalogSuffix: ""
        StoreFrontSuffix: ""
        TagSuffix: ""
```

File share reference using SiteMerging.yml

This method uses the `SiteRootFolder` member of the site's prefixes set. While more involved than the direct file share method, this method reduces the odds of targeting the wrong folder when exporting, importing, merging, or adding.

First, set the `SiteRootFolder` for each site in the SiteMerging.yml file. You must do this on the shared location.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder \\share.central.net\AutoConfig
```

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -SitePrefixesFolder \\share.central.net\AutoConfig
```

In this example, East is a fully qualified folder specification and West is a relative folder specification.

To target the export to a site-specific folder using the SiteMerging.yml file:

From the East DDC:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \\share.central.net\AutoConfig\CustomerInfo.yml
```

From the West DDC:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.central.net\AutoConfig\CustomerInfo.yml
```

The export cmdlet uses the CustomerInfo.yml folder location to locate the SiteMerging.yml file. In the case of East, the `SiteRootFolder` is fully qualified. It is used as-is. In the case of West, the `SiteRootFolder` is not fully qualified. It is combined with the CustomerInfo.yml folder location to retrieve a fully qualified folder location for West.

To merge the East DDC to the cloud:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \\share.central.net\AutoConfig\CustomerInfo.yml
```

To merge the West DDC to the cloud:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \\share.central.net\AutoConfig\CustomerInfo.yml
```

The following is a sample SitePrefixes.yml file used in the previous example.

```
1       East:
2       SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
```



```
      ApplicationFolderRoot: "East"
      ApplicationGroupPrefix: "East_"
      ApplicationUserPrefix: "East_"
      DeliveryGroupPrefix: "East_"
      GroupPolicyPrefix: "East_"
      HostConnectionPrefix: "East_"
      MachineCatalogPrefix: "East_"
      StoreFrontPrefix: "East_"
      TagPrefix: "East_"
      AdminScopeSuffix: "_east"
      AdminRoleSuffix: "_east"
      ApplicationAdminSuffix: "_east"
      ApplicationFolderSuffix: "_east"
      ApplicationGroupSuffix: "_east"
      ApplicationUserSuffix: "_east"
      DeliveryGroupSuffix: "_east"
      GroupPolicySuffix: "_east"
      HostConnectionSuffix: "_east"
      MachineCatalogSuffix: "_east"
      StoreFrontSuffix: "_east"
      TagSuffix: "_east"
    West:
      SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
      AdminScopePrefix: "Western "
      AdminRolePrefix: "Western "
      ApplicationAdminPrefix: "Western "
      ApplicationFolderPrefix: "" # Note that a new parent root folder
          is used instead
      ApplicationFolderRoot: "Western"
      ApplicationGroupPrefix: "Western "
      ApplicationUserPrefix: "Western "
      DeliveryGroupPrefix: "Western "
      GroupPolicyPrefix: "Western "
      HostConnectionPrefix: "Western "
      MachineCatalogPrefix: "Western "
      StoreFrontPrefix: "Western "
      TagPrefix: "Western "
      AdminScopeSuffix: ""
      AdminRoleSuffix: ""
      ApplicationAdminSuffix: ""
      ApplicationFolderSuffix: ""
      ApplicationGroupSuffix: ""
      ApplicationUserSuffix: ""
      DeliveryGroupSuffix: ""
      GroupPolicySuffix: ""
      HostConnectionSuffix: ""
      MachineCatalogSuffix: ""
      StoreFrontSuffix: ""
      TagSuffix: ""
```

If a central file share method is not used and the import, merge, or add is done from the individual DDCs, then create and replicate the SiteMerging.yml file on each DDC being migrated into the cloud. The default location is *%HOMEPATH%\Documents\Citrix\AutoConfig*. You must specify the –

`SiteName` parameter to select the correct site prefixes.

Merging the sites

Citrix recommends performing the cloud operations in steps and to do a complete review of each result before doing the next cloud operation. For example, if merging three sites to a single cloud site:

1. Merge the initial site to the cloud using the appropriate `SiteName` value.
2. Review the results in the Full Configuration management interface.
3. If the results are incorrect, determine the issue and its cause, correct it, and then rerun the merge. If necessary, remove the cloud components and start from scratch by using `Remove -CvadAcFromSite` for the selected component and members. If the results are correct, continue.
4. If the initial merge is correct, merge the second site to the single cloud site.
5. Repeat steps 2 and 3.
6. If the second merge is correct, merge the third site to the single cloud site.
7. Repeat steps 2 and 3.
8. Review the resources from the user's perspective and verify that the view is in the desired state.

Remove a component using the site prefix

You can selectively remove single site components by using the prefix on the `–IncludeByName` parameter of the `Remove-CvadAcFromSite` cmdlet. In the following example, the West DDC delivery groups are not correct. To remove the delivery groups for just the West site:

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName "Western *"
```

To remove all West components, run the following cmdlets in order.

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName "Western *"
Remove-CvadAcFromSite –Applications –IncludeByName "Western *"
Remove-CvadAcFromSite – ApplicationGroups –IncludeByName "Western *"
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName "Western *"
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName "Western *"
Remove-CvadAcFromSite –HostConnections –IncludeByName "Western *"
Remove-CvadAcFromSite –Tags –IncludeByName "Western *"
```

To remove group policies of the East components, use the suffix:

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName "*_east"
```


Migrating from cloud to cloud

June 6, 2024

Automated Configuration allows you to automate moving your cloud configuration to another cloud site or allowing you to restore your own cloud site.

Using Automated Configuration can solve many use cases:

- Syncing your site from test or stage to production
- Backing up and restoring your configuration
- Reaching resource limits
- Migrating from one region to another

In Full Configuration on Citrix Cloud, see the Backup and Restore node for information about Automated Configuration and how it can be used to migrate your configuration from cloud to cloud.



Prerequisites for migrating your configuration

For backing up and restoring your configuration, you need:

- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) provisioned.
- An active resource location with Connector installed.
- Connectivity to sites accessing Citrix Cloud must be allowed and available. For more information, see System and Connectivity Requirements.

> **Note:**
>
> MCS cannot be backed up from the cloud using Automated Configuration.

Backing up your Citrix DaaS configuration

> **Important:**
>
> - You must have your CustomerInfo.yml file with your customer ID, client ID, and the secret key information included. For more information on how to retrieve your customer ID, client ID and secret key, see Generating the customer ID, client ID, and secret key. For information on how to add this information to the CustomerInfo.yml file, see Populating customer info file.
> - When you run the backup commands, the CustomerInfo.yml must have the details of the source site customer from where you are taking the backup.
> - When you run the restore commands, the CustomerInfo.yml must have the details of the destination site customer to where you are restoring the configurations.
> - The ZoneMapping.yml file must include information that maps your resource locations in the cloud. For more information on how to map your zones, see Populating zone mapping file.
> - If you have host connections, you must input the corresponding info in the CvadAcSecurity.yml file.

1. Install Automated Configuration.

   > **Note:**
   >
   > For cloud-to-cloud migration, Automated Configuration can be installed on a machine having access to the internet that the administrator has direct access to.

2. Double-click the **Auto Config** icon. A PowerShell window appears.
3. Run the following command to do a backup.

   ```
   Backup-CvadAcToFile
   ```

After you run any cmdlet for the first time, an export folder with the .yml configuration files and logs is created. The folder is at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

Restoring your configuration to Citrix DaaS

1. Double-click the **Auto Config** icon. A PowerShell window appears.

2. Run the following command to do a restore.

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

Verify the expected state with the new current state.

After you run the cmdlet, an export folder with the .yml configuration files and logs is created. The folder is at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

The backup and restore process protects you from unintentional cloud site configuration changes or corruption. While Automated Configuration makes backups each time a change is made, this backup reflects the state of the cloud site configuration before the changes. Protecting yourself requires that you periodically back up your cloud site configuration and saving it in a safe place. If an undesirable change or corruption takes place, the backup can be used to fix the change or corruption at either a granular or full site configuration level.

Granular migration

> **Important:**
>
> For more information on component migration orders, see Component migration order.

Restoring entire components

Restoring one component involves selecting one or more component parameters.

To restore the entire delivery group and machine catalog components, follow this example:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Restoring component members

Restoring one or more component members makes use of the `IncludeByName` feature. The `Restore` cmdlet is invoked with the `RestoreFolder` parameter along with the selected single component and the inclusion list.

To restore two group policies from a backup, follow this example:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
-GroupPolicies -IncludeByName Policy1,Policy2
```



```
-DeliveryGroups -MachineCatalogs
```

Restoring the entire cloud site configuration

Restoring the full cloud site configuration means selecting all components to restore.

To restore the entire cloud site configuration, follow this example:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Activating sites

Site activation allows you to control which site is active and controls your resources. For more information, see Activating sites.

Migrate Cloud configurations to on-premises

June 27, 2024

This article describes backing up and migrating your Cloud configurations to on-premises sites.

Prerequisites for migrating your configuration

- Citrix Virtual Apps and Desktops on-premises environment with at least one registered VDA.
- Citrix Virtual Apps and Desktops on-premises environment running on one of the following versions:
  - The most recent Long-Term Service Release (LTSR) version - 2402.
  - Any of the Current Releases (CR) versions - 2308, 2311.
- Run the Automated Configuration tool (ACT) commands on a domain-joined machine with .Net 4.7.2 version or higher.
- A machine with the Citrix PowerShell SDK. PowerShell SDK is available within the Citrix Delivery Controller installable.

> **Note:**
>
> - If you are running the ACT on a different machine, it must be domain-joined and Full Configuration console must have the correct PowerShell snap-ins installed. To get the installer, go to Citrix Virtual Apps and Desktopsdownloads website.

> - In the on-prem site, we recommend ACT be installed on the DDC. ACT can be started via the desktop icon.
> - If ACT is intended to be used from the standard Powershell window then the following command must be executed:
> `Import-Module Citrix.AutoConfig.Commands`

ACT is not part of the system PowerShell path so must be explicitly imported

Procedure

Follow the instructions to complete the migration of your Cloud configurations to on-premises:

1. Backup Cloud configuration
2. Modify YML files
3. Import configurations to on-premises

Backup Cloud configuration

1. Install the **Automated Configuration**.
2. Double-click the **Auto Config** icon. A PowerShell window appears.
3. Run `New-CvadAcCustomerInfoFile` to create a **CustomerInfo.yml** file. For more information, see Populating customer info file.
4. Run the command `Backup-CvadAcToFile` to take a backup of your Cloud configurations.

> **Note:**
>
> - After you run any cmdlet for the first time, an export folder with the .yml configuration files and logs is created. The folder is at `%HOMEPATH%\Documents\Citrix\AutoConfig`.
> - If you encounter any errors or exceptions, see the **Fixups** section in the log file.
> - Backup-CvadToFile does not support the parameters `IncludeByName` or `ExcludeByName`.

> **Important:**
>
> Citrix recommends backing up all the components together.

Modify YML files

Modify the .yml files located at ‘ %HOMEPATH%\Documents\Citrix\AutoConfig ‘ to include the on-prem details as described in the following table:

YML File	Parameter	Description	Examples
CustomerInfo.yml	Environment	Change Environment to OnPrem. The environment parameter value is case-sensitive.	
ZoneMapping.yml	DaaS:CVAD	Map your Cloud resource locations to your on-premises zones.	It has to be old:new zones
CvadAcSecurity.yml	Hypervisor: ConnectionType: “Username: ‘’ Password: “	Add the hypervisor username and passwords.	If the hypervisor is XenServer,XenServer: ConnectionType: ‘XenServer’Username: ‘root’Password: “

Import configurations to on-premises

1. Run either of the following commands in your on-prem site based on your requirements:
    a) `Merge-CvadAcToSite` - if there is an on-premises site running and you want to merge the Cloud configurations to it.
    b) `Import-CvadAcToSite -Environment OnPrem` - If on-premises configurations are not available and you are importing the Cloud configurations to create one.

> **Important:**
>
> Citrix recommends importing one component at a time to avoid conflicts.

Automated configuration tool cmdlets

March 4, 2024

This page lists all the cmdlets and parameters supported by the tool.

All cmdlets take parameters having one of the following types.

- String
- List of strings

- Boolean: `$true` or `$false`
- SwitchParameter: presence of the parameter means `$true`; absence of the parameter means `$false`

> **Note:**
>
> SwitchParameter is the preferred method for true or false selections but booleans are still used in the tool due to legacy issues.

The following table is a summary of all cmdlets. See each individual section to find what parameters each cmdlet supports.

Category	Cmdlet	Description
On-premises to cloud migration	`Export-CvadAcToFile`	Export on-premises files to YAML files.
		`Import-CvadAcToSite`
		`Merge-CvadAcToSite`
		`New-CvadAcToSite`
		`Sync-CvadAcToSite`
		Granular migration For components, use parameters with commands above. Examples: `MachineCatalogs`, `Tags`. For component names, use parameters with commands above. Examples: `IncludeByName`, `ExcludeByName`.
Cloud to cloud cmdlets	`Backup-CvadAcToFile`	Backs up all the configuration from your cloud site.
		`Restore-CvadAcToSite`
		`Remove-CvadAcFromSite`

Category	Cmdlet	Description
		Granular migration For components, use parameters with commands above. Examples: `MachineCatalogs`, `Tags`. For component names, use parameters with commands above. Examples: `IncludeByName`, `ExcludeByName`.
Other basic cmdlets	`Compare-CvadAcToSite`	Compares the on-premises .yml files with the cloud configuration.
Prerequisites-related cmdlets	`New-CvadAcCustomerInfoFile`	Create a customer info file.
		`Set-CvadAcCustomerInfoFile`
Support and troubleshooting cmdlets	`New-CvadAcZipInfoForSupport`	Zips all log and .yml files in a single zip file to send to Citrix for support.
		`Get-CvadAcStatus`
		`Test-CvadAcConnectionWithSite`
		`Find-CvadAcConnector`
		`Get-CvadAcCustomerSites`
		`New-CvadAcTemplateToFile`
		`Show-CvadAcDocument`
		`Find-CvadAcInFile`

Category	Cmdlet	Description
Site activation cmdlets	`Set-CvadAcSiteActiveStateOnPrem`	Sets the on-premises site state to either active or inactive. `Set-CvadAcSiteActiveStateCloud`

Merging multiple on-premises sites cmdlets	`New-CvadAcSiteMergingInfo`	Creates a site merging prefix/suffix info set.
		
		`Set-CvadAcSiteMergingInfo`
		
		`Remove-CvadAcSiteMergingInfo`

For more information on parameters and how to use them, see Granular migration parameters.

Basic cmdlets

On-premises to cloud cmdlets

- `Export-CvadAcToFile` - Export on-premises files to YAML files.

  Exports configuration from your on-premises setup. This is the default export operation for Automated configuration. No modifications are made to the on-premises site configuration. Exported files are placed in the directory *%HOMEPATH%\Documents\Citrix\AutoConfig* in a uniquely named **Export** subfolder. The folder *%HOMEPATH%\Documents\Citrix\AutoConfig* always contains the latest exported on-premises site configuration.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components		SwitchParameters
Filtering by object names	See Filtering by object names		List of strings
`TargetFolder`	Specifies the export destination folder.		String

Name	Description	Required?	Type
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`AdminAddress`	Specifies the Delivery Controller's DNS or IP address when the export is not being run on the Delivery Controller.		String
`CheckUserAndMachines`	Verifies if users and machines are in Active Directory. Users and machines that are not in Active Directory might result in import failures.		`$true` or `$false`
`ZipResults`	Zips backup up YAML files into a single zip file. The file is in the same folder as the backed up YAML files and has the same name as the folder.		SwitchParameter

Returns:

- See Cmdlet return values

There are three ways of importing data into the cloud. Running specific cmdlets can result in one of the three combinations of actions on the cloud site:

- Add, Update, and Delete
- Add and Update only
- Add only

Cmdlet	Add	Update	Delete
Import	X	X	X
Merge	X	X	
New	X		

- `Import-CvadAcToSite` - Import YAML files to the cloud. Supports create, update and delete operations.

  Imports all the on-premises files to the cloud. This command ensures that the cloud end state is identical to the on-premises state. This option deletes any changes that exist in the cloud. Imported site configuration files are sourced from *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Use with caution.*

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		SwitchParameter
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

- `Merge-CvadAcToSite` - Import YAML files to the cloud. Supports create and update opera-

tions.

Merges the on-premises files to the cloud, but does *not* delete any components in the cloud or the on-premises site. This preserves changes already made in the cloud. If a component exists in Citrix Cloud with the same name, this command can modify that component. This is the default import operation for Automated configuration. Merged site configuration files are sourced from *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`

Name	Description	Required?	Type
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		SwitchParameter
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

- `New-CvadAcToSite` - Import YAML files to the cloud. Supports create and update operations.

  Imports on-premises site configuration to the cloud but only adds new components. Existing cloud site components are neither updated nor deleted. Use this command if your existing cloud site components must remain unchanged.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`OnErrorAction`	See OnErrorAction parameter.		String

Name	Description	Required?	Type

Returns:

- See Cmdlet return values

- `Sync-CvadAcToSite` - Export and import in one step.

  Sync performs both an export and import in one step. Use the `SourceTargetFolder` parameter to specify the export/import destination folder.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components		SwitchParameters
Filtering by object names	See Filtering by object names		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SourceTargetFolder`	Specifies the export/import destination folder.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`AdminAddress`	Specifies the delivery controller's DNS or IP address when the export is not being executed on the delivery controller.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`

Name	Description	Required?	Type
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		SwitchParameter

Returns:

- See Cmdlet return values

Cloud to cloud cmdlets

- `Backup-CvadAcToFile` - Backs up all the configuration from your cloud site.

  Exports your cloud configuration to .yml files. This backup can be used in a backup and restore process to restore lost components.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components		SwitchParameters
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`TargetFolder`	Specifies the export destination folder.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`ZipResults`	Zips backup up YAML files into a single zip file. The file is in the same folder as the backed up YAML files and has the same name as the folder.		SwitchParameter

Returns:

- See Cmdlet return values

- `Restore-CvadAcToSite` - Restores backup YAML files to the cloud site. This cloud site can be the same or different than the source cloud site.

  Restores the cloud site to the previous configuration. Imported files are sourced from the folder specified using the `-RestoreFolder` parameter, which identifies the folder containing the .yml files to restore to the cloud site. This must be a fully qualified folder specification. This cmdlet can be used for reverting to your previous configuration or for backing up and restoring your cloud site. This command can add, delete, and update your cloud site.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`RestoreFolder`	Identifies the folder containing the .yml files to restore to the cloud site. This must be a fully qualified folder specification.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`

Name	Description	Required?	Type
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		SwitchParameter
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

- `Remove-CvadAcFromSite` –Remove component members from cloud.

  Can reset the entire site or remove member items from a component (For example, removing one machine catalog from the list of catalogs). This can be used when coupled with the `IncludeByName` parameter to selectively remove specific members.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components		SwitchParameters
Filtering by object names	See Filtering by object names		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`

Returns:

- See Cmdlet return values

Other basic cmdlets

- `Compare-CvadAcToSite` - Compares the on-premises .yml files with the cloud configuration, producing a report of changes that are made by an `Import`, `Merge`, or `Restore` cmdlet.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`OnErrorAction`	See OnErrorAction parameter.		String

  Returns:

  - See Cmdlet return values

Granular migration parameters

Migrate by components

The following components can be specified with cmdlets supporting them. The `All` option is automatically selected when no component parameters are specified. To avoid errors, we recommend that you migrate components in the following order:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

Filtering by object names

Migrate by component names The `IncludeByName` and `ExcludeByName` parameters enable including and excluding component members in cmdlets by name. Only one component (for example, delivery groups) can be chosen at a time in any of the supported cmdlets. If a component member is in both areas, exclude overrides any other parameter and an entry is made in the log fixup list identifying the component and member name that was excluded.

`IncludeByName` and `ExcludeByName` take a list of component member names. Any name can contain one or more wildcards. Two types of wildcards are supported. The list of component member names must be enclosed in single-quotes when any member name contains special characters.

- * Matches any number of characters
- ? Matches a single character

`IncludeByName` and `ExcludeByName` can also take a file containing a list of members where each member can be explicit or contain wildcards. Each line in the file can contain one member. Leading and trailing spaces are trimmed from the member name. The file name must be preceded by the @ sign and be surrounded by single quotes (a PowerShell requirement so the @ is not reinterpreted). Multiple files can be listed in addition to being mixed with member names.

One example of merging all delivery groups whose names begin with `DgSite1` and contain `Home2` would be written:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

By Delivery Group Name `ByDeliveryGroupName` filters by the delivery group name for applications and application groups. This parameter is always an inclusion list identifying members to include based on their delivery group association.

`ByDeliveryGroupName` takes a list of delivery group names. Any name can contain one or more wildcards. Two types of wildcards are supported.

- * matches any number of characters
- ? matches a single character

The following example merges all applications that reference all delivery group names beginning with `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

Exclude Disabled `ExcludeDisabled` filters out from import operations all applications and application groups that are disabled. `ExcludeDisabled` defaults to **`false`**, meaning all applications and application groups are imported regardless of their enabled state.

By Machine Name `ByMachineName` filters by the machine name for machine catalogs and delivery groups. This parameter is always an inclusion list identifying members to include based on their machine name association.

`ByMachineName` takes a list of machine names where any name can contain one or more wildcards. Two types of wildcards are supported.

- * matches any number of characters
- ? matches a single character

When exporting or importing and using `ByMachineName` and a machine name filter results in no machines in the machine catalog or delivery group, the machine catalog or delivery group is excluded from the export or import.

> **Note:**
>
> Use of `ByMachineName` in any import type cmdlet results in `MergeMachines` being set to `$true`.

Merge Machines `MergeMachines`, when set to `$true`, instructs the import operation to add machines only to the machine catalog or delivery group. Machines are not removed, allowing for incremental additive operations.

`MergeMachines` defaults to false meaning machines are removed if they are not present in the machine catalog or delivery group .yml file. `MergeMachines` is set to `$true` when `ByMachineName` is used but can be overridden by setting `MergeMachines` to false.

Prerequisites-related cmdlets

- `New-CvadAcCustomerInfoFile` - Create a customer info file. By default, the customer info file is located at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parameters:

Name	Description	Required?	Type
`CustomerId`	Customer's ID.	x	String
`ClientId`	Customer's client ID created on Citrix Cloud. The CustomerId and Secret must be specified when using this parameter.	Conditionally	String
`Secret`	Customer's secret key created on Citrix Cloud. The CustomerId and ClientId must be specified when using this parameter.	Conditionally	String
`Environment`	Production, ProductionGov, or ProductionJP environment.		Enumeration
`LogFileName`	Change the log file prefix from CitrixLog to something else.		String
`AltRootUrl`	Use only under the direction of Citrix.		String
`StopOnError`	Stops the operation upon first error.		`$true` or `$false`
`TargetFolder`	Use the specified folder as the root folder instead of *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Use the specified local instead of the locale derived from the system the tool is run on.		String

Name	Description	Required?	Type
`Editor`	Use the specified editor to display the log at the completion of each cmdlet. Notepad.exe is the default editor. This parameter must include the fully qualified file specification to the editor and the editor must take the log file spec as its only parameter.		String
`SecurityCsvFileSpec`	The fully qualified file specification pointing to the SecurityClient.csv file downloaded from Citrix Identity and Access Management. The CustomerId must be specified when using this parameter.		String

Returns:

- See Cmdlet return values

- `Set-CvadAcCustomerInfoFile` - Update an existing customer info file. Only cmdlet specified parameters are changed. All unspecified parameter values in the CustomerInfo.yml file are unchanged.

  Parameters:

Name	Description	Required?	Type
`CustomerId`	Customer's ID.		String
`ClientId`	Customer's client ID created on Citrix Cloud.		String
`Secret`	Customer's secret key created on Citrix Cloud.		String
`Environment`	Production, ProductionGov, or ProductionJP environment.		Enumeration
`LogFileName`	Change the log file prefix from CitrixLog to something else.		String
`StopOnError`	Stops the operation upon first error.		`$true` or `$false`
`TargetFolder`	Use the specified folder as the root folder instead of *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Use the specified local instead of the locale derived from the system the tool is run on.		String

Name	Description	Required?	Type
`Editor`	Use the specified editor to display the log at the completion of each cmdlet. Notepad.exe is the default editor. This parameter must include the fully qualified file specification to the editor and the editor must take the log file spec as its only parameter.		String
`SecurityCsvFileSpec`	The fully qualified file specification pointing to the SecurityClient.csv file downloaded from Citrix Identity and Access Management. The CustomerId must be specified when using this parameter.		String

Returns:

- See Cmdlet return values

Prerequisites-related parameters

Along with the cloud accessing parameters, the following parameters can be used with the prerequisites-related cmdlets:

- `Environment` –Production or ProductionGov environment.
- `LogFileName` –Change the log file prefix from CitrixLog to something else.
- `StopOnError` –Stops the operation upon first error.
- `AlternateRootFolder` –Use the specified folder as the root folder instead of *%HOMEPATH%\Documents\Citrix\AutoConfig*.
- `Locale` –use the specified local instead of the locale derived from the system the tool is run on.
- `Editor` –use the specified editor to display the log at the completion of each cmdlet. Notepad.exe is the default editor. This parameter must include the fully qualified file specification to the editor and the editor must take the log file spec as its only parameter.

Support and troubleshooting cmdlets

- `New-CvadAcZipInfoForSupport` - Zips all log and .yml files in a single zip file to send to Citrix for support. Customer sensitive information (CustomerInfo.yml and CvadAcSecurity.yml) is not included in the zip. The Icon.yml file is also excluded due to its size. The

zip file is placed in *%HOMEPATH%\Documents\Citrix\AutoConfig* and named *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, based on the date and timestamp. This zip file can also act as a backup.

Parameters:

Name	Description	Required?	Type
`TargetFolder`	Specifies a target folder to create and save the zip file.		String
`Quiet`	Suppress logging to the console.		SwitchParameter

Returns:

- Zip file with zip file name and location is displayed on the command prompt.

- `Get-CvadAcStatus` - Use to test connectivity and to ensure all prerequisites are met. Returns information about the tool like version number and connectivity with the cloud and connector status.

  Parameters:

Name	Description	Required?	Type
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SiteId`	Identifies the site to connect to.		String
`AdminAddress`	This is the DNS or IP address of the on-premises Delivery Controller used to verify the admins access level. This is required if the tool is not being run on a Delivery Controller.		String

  Returns:

  - Displays the results for each item.

- `Test-CvadAcConnectionWithSite` –Test the connection with the cloud site to verify that the communication connection is working. This cmdlet uses the cloud accessing parameters or the CustomerInfo.yml file to specify the customer connection information.

  Parameters:

Name	Description	Required?	Type
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter

Returns:

- Test results are displayed on the command line.

- `Find-CvadAcConnector` - Locates existing connectors and determines their running state. This cmdlet uses information from the CustomerInfo.yml file or the customer ID parameter to locate the customer's connectors.

  Parameters:

Name	Description	Required?	Type
`CustomerInfoFileSpec`	The file specification pointing to a customer information file to override the default location and name. This parameter is ignored when the `CustomerId` parameter is provided.		String
`CustomerId`	The customer's ID. This parameter overrides the same value in the CustomerInfo.yml file.		String

  Returns:

  - Results are shown on the command line.

- `Get-CvadAcCustomerSites` - Returns the list of all the customer sites. This cmdlet uses the cloud accessing parameters or the CustomerInfo.yml file to specify the customer connection information.

  Parameters:

  - See Cloud-accessing parameters

  Returns:

  - Displays a list of found customer site IDs.

- `New-CvadAcTemplateToFile` –Creates a template file for selected components, allowing you to manually create an import file.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components		SwitchParameters
`TargetFolder`	Specifies the export destination folder.		String

Returns:

- See Cmdlet return values

- `Show-CvadAcDocument` - Displays this documentation in the default browser.

  Parameters:

  - None.

  Returns:

  - Display this webpage in the default web browser.

- `Find-CvadAcInFile` - Find in file searches component YAML files looking for members matching a one or more names that may contain wildcards. The result is a report of found members. Find in file can only search one component at a time. Find in file searches all YAML files in the current folder and all subfolders. Use `FindSourceFolder` to limit the number of files to search.

  Parameters:

Name	Description	Required?	Type
Migrate by components	See Migrate by components. Note: The `-All` value is not valid.		SwitchParameters
`IncludeByName`	A list specifying the names of delivery groups to include when setting the site active state to active. The '*'and '?'wildcards are supported in names.		List of strings
`Unique`	Report only unique-found members.		SwitchParameter
`IncludeYaml`	Include the member specific YAML.		SwitchParameter
`FindSourceFolder`	The folder find begins searching in.		String

Name	Description	Required?	Type
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		SwitchParameter
`Quiet`	Suppress logging to the console.		SwitchParameter

Return:

- Creates a report containing found members for the specified component.

Site activation cmdlets

For more information on activating sites and the usage of these cmdlets, see Activating sites.

- `Set-CvadAcSiteActiveStateOnPrem` - Sets the on-premises site state to either active or inactive.

  Parameters:

Name	Description	Required?	Type
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SiteActive`	When present, sets the on-premises site to active removing the maintenance mode from all delivery groups. When this parameter is not present, maintenance mode is set on all delivery groups.		SwitchParameter
`IncludeByName`	A list specifying the names of delivery groups to include when setting the site active state to active. The '*'and '?'wildcards are supported in names.		List of strings
`ExcludeByName`	A list specifying the names of delivery groups to exclude when setting the site active state to active. The '*'and '?'wildcards are supported in names.		List of strings
`Quiet`	Suppress logging to the console.		SwitchParameter

Name	Description	Required?	Type
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true or $false`

Returns:

- See Cmdlet return values

- `Set-CvadAcSiteActiveStateCloud` - Sets the cloud site state to either active or inactive.

Parameters:

Name	Description	Required?	Type
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SiteActive`	When present, sets the cloud site to active removing the maintenance mode from all delivery groups. When this parameter is not present, maintenance mode is set on all delivery groups.		SwitchParameter
`IncludeByName`	A list specifying the names of delivery groups to include when setting the site active state to active. The '*'and '?'wildcards are supported in names.		List of strings
`ExcludeByName`	A list specifying the names of delivery groups to exclude when setting the site active state to active. The '*'and '?'wildcards are supported in names.		List of strings
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true or $false`

Returns:

- See Cmdlet return values

Merging multiple on-premises sites cmdlets

For more information on site merging and usage of these cmdlets, see Merge multiple sites into a single site.

- `New-CvadAcSiteMergingInfo` - Creates a site merging prefix/suffix info set. It is not necessary to know all prefixes or suffixes at the beginning. They can be updated with `Set-CvadAcSiteMergingInfo` or by manually editing the SiteMerging.yml file.
  Parameters:

Name	Description	Required?	Type
`SiteName`	The name used to identify the set of prefixes/suffixes for a specific site. It can match the name of the actual site but does not need to.	x	String
Site merging parameters	See Site merging parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter

  Returns:

  - None

- `Set-CvadAcSiteMergingInfo` - Updates an existing site merging prefix/suffix info set.

  Parameters:

Name	Description	Required?	Type
`SiteName`	The name used to identify the set of prefixes/suffixes for a specific site. It can match the name of the actual site but does not need to.	x	String
Site merging parameters	See Site merging parameters		SwitchParameters

Name	Description	Required?	Type
Quiet	Suppress logging to the console.		SwitchParameter

Returns:

- None

- Remove-CvadAcSiteMergingInfo - Removes an existing site merging prefix/suffix info set.

  Parameters:

  - SiteName –identifies the set of site prefixes and suffixes. This is a string and is required.

  Returns:

  - None

Site merging parameters

The following parameters can be used when running the site merging cmdlets. All listed parameters are strings.

- SiteName –the name used to identify the set of prefixes/suffixes for a specific site. It can match the name of the actual site but does not need to. SiteName is a required parameter.
- AdminScopedPrefix –the prefix to apply to administrator scopes.
- ApplicationPrefix - the prefix to apply to applications.
- ApplicationFolderPrefix –the prefix to apply to application folders; ApplicationFolderPrefi can be combined with ApplicationFolderRoot.
- ApplicationFolderRoot –the new root folder to application folders. This creates an extra folder hierarchy. ApplicationFolderRoot can be combined with ApplicationFolderPrefix.
- ApplicationGroupPrefix –the prefix for application groups.
- ApplicationUserPrefix –the prefix to apply to the application name the user sees.
- ApplicationAdminPrefix –the prefix to apply to the application name the administrator sees.
- DeliveryGroupPrefix –the prefix to apply to delivery groups.
- GroupPolicyPrefix –the prefix to apply to policy names.
- HostConnectionPrefix –the prefix to apply to host connections.
- MachineCatalogPrefix –the prefix to apply to machine catalogs.
- StoreFrontPrefix –the prefix to apply to StoreFront names.

- `TagPrefix` –the prefix to apply to tags.
- `AdminScopedSuffix` –the suffix to apply to administrator scopes.
- `ApplicationSuffix` - the suffix to apply to applications.
- `ApplicationFolderSuffix` –the suffix to apply to application folders; `ApplicationFolderSuffi` can be combined with `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` –the suffix for application groups.
- `ApplicationUserSuffix` –the suffix to apply to the application name the user sees.
- `ApplicationAdminSuffix` –the suffix to apply to the application name the administrator sees.
- `DeliveryGroupSuffix` –the suffix to apply to delivery groups.
- `GroupPolicySuffix` –the suffix to apply to policy names.
- `HostConnectionSuffix` –the suffix to apply to host connections.
- `MachineCatalogSuffix` –the suffix to apply to machine catalogs.
- `StoreFrontSuffix` –the suffix to apply to StoreFront names.
- `TagSuffix` –the suffix to apply to tags.
- `SiteRootFolder` –the fully qualified folder name to use for exports and imports; this can be a local folder or a file share.

Generic parameters

Cloud accessing parameters

All cmdlets accessing the cloud support the following extra parameters.

> **Note:**
>
> The CustomerId, ClientId, and Secret can be placed in the CustomerInfo.yml file or specified with the cmdlet using the following parameters. When they are specified in both places, the cmdlet parameters take precedence.

- `CustomerId` –The customer ID used in the Rest APIs and is required to access all Rest APIs. Your customer ID is found in Citrix Cloud.
- `ClientId` –The clientID created on the Citrix Cloud Identity and Access Management website. This is required to obtain the bearer token needed for authentication for all Rest APIs.
- `Secret` –The secret key created on the Citrix Cloud Identity and Access Management website. This is required to obtain the bearer token needed for authentication for all Rest APIs.
- `CustomerInfoFileSpec` –The file specification pointing to a customer information file to override the default location and name.

Migration mode parameters

Cmdlets modifying the cloud site configuration (`Import`, `Restore`, `Merge`, `New`, and `Sync`) support the following extra parameters to provide further flexibility.

- `CheckMode` –Performs the import operation but makes *no* changes. All expected changes are reported before the import completes. You can use this command to test your import before it occurs.
- `BackupFirst` –Backs up the cloud contents to .yml files before modifying the cloud configuration. This is enabled by default.
- `Confirm` –When true, prompts users to confirm that they want to make changes to the cloud site configuration. The `Remove` cmdlet shows a prompt due to its destructive nature. Set to false if no prompt is desired, such as running inside automated scripts. `Confirm` defaults to true.
- `SecurityFileFolder` –This is the fully qualified folder containing the CustomerInfo.yml file which might point to a local folder or a network share folder that may be under authentication control. The tool will not prompt for credentials; access to the controlled resource must be obtained before running the tool.
- `SiteName` –Specifies the site merging prefix and suffix set to use when importing.
- `SiteActive` –Specifies whether the imported site is active or inactive. By default, this parameter is set to `$false` meaning the imported site is inactive.

Log display parameters

The `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare`, and `Remove` cmdlets display the log file when the operation completes. You can suppress the display by setting the `-DisplayLog` parameter to `$false`. Notepad.exe is used by default to display the log file. You can specify a different editor in the CustomerInfo.yml file.

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

Cmdlet return values

ActionResult

All cmdlets return the following value.

```
1            public class ActionResult
2            {
3
4                public bool                          Overall_Success;
5                public Dictionary<string, string>   Individual_Success;
```



```
6                   public object                           CustomResult;
7               }
```

`Overall_Success` returns a single boolean showing the overall success of the cmdlet across all selected components: true meaning successful and false meaning unsuccessful.

`Individual_Success` returns one or three values for each main component. A component's result can be Success, Failure, or Skipped. Skipped indicates that the component was not selected for execution by the cmdlet.

`CustomResult` is cmdlet specific.

CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File`, and `Remove` return the following custom result information to a single instance of `EvaluationResultData`.

> **Note:**
>
> `Export` and `Template` cmdlets do not return a custom result.

```
1               public class EvaluationResultData
2               {
3
4                   public Dictionary<string, Dictionary<string,
                       ActionResultValues >> EvaluationResults;
5                   public int                  Added;
6                   public int                  Updated;
7                   public int                  Deleted;
8                   public int                  NoChange;
9                   public int                  TotalChanged;
10                  public EvaluationResults     OverallResult;
11                  public string               CloudBackupFolder;
12                  public string               SourceBackupFolder;
13               }
14
15              Where:
16              public enum ActionResultValues
17              {
18
19                  Add,
20                  Update,
21                  Delete,
22                  Identical,
23                  DoNothing
24               }
25
26              public enum EvaluationResults
27              {
28
```



```
29                      Success,
30                      Failure,
31                      Skipped
32                  }
```

`EvaluationResults` displays a list with one entry per selected component. The key is the component name and the value is a list of each component member and the action taken on that component member. Actions can be any one of the `ActionResultValues` values.

`Added`, `Updated`, `Deleted`, and `NoChange` indicate that the total number of component members added, updated, deleted, or no action taken, in that order.

`TotalChanged` is the sum of `Added`, `Updated`, and `Deleted`.

`OverallResult` is a single boolean indicating the result of the cmdlet. True indicates total success across all components and false indicates failure in processing one or more components.

`CloudBackupFolder` is the fully qualified file specification of the cloud site configuration backup before the cmdlet performing any cloud-modifying actions.

`SourceBackupFolder` is the fully qualified file specification of the source file backup made after completion of the cmdlet. By default, these files are at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

PowerShell help

PowerShell help is available for each cmdlet. All parameters are documented with each cmdlet along with a brief explanation of the cmdlet. To access help for any cmdlet, type `Get-Help` in front of the cmdlet.

```
Get-Help Import-CvadAcToSite
```

Troubleshoot Automated configuration and additional information

March 4, 2024

> **Important:**
>
> For commonly occurring error messages for Automated configuration and corresponding solutions, see the *troubleshooting FAQ* at Knowledge Center article CTX277730.

Automated configuration tool errors

Automated configuration tool operations can sometimes produce errors. When this happens failures can occur when processing components like Machine Catalogs, Delivery Groups, or Group Policies,

for example. Using `OnErrorAction` and continuation parameters allows you to catch errors mid-processing, resolve them, and pick up where you left off.

The default `OnErrorAction` value is `StopCompEnd`. When an error occurs, the tool finishes processing the current component. No additional components are processed, and errors do not carry forward to downstream, dependent components. After you resolve any errors, you can rerun your cmdlets with any continuation parameter applied.

OnErrorAction parameter

You can define `OnErrorAction` parameter values on migration commands to control how the tool responds to errors that it finds when processing components.

This table shows parameter values and their descriptions:

Value	Description
`Continue`	Attempts to process as many of all components as possible.
`Pause`	Pauses at the end of processing and prompts you to continue or stop.
`StopCompEnd`	Attempts to process as much of the component as possible. Stops after the component is finished. (Default)
`StopImmediately`	Processing stops when an error is found.

Migration cmdlets

You can apply the `OnErrorAction` parameter to the following migration commands:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Example: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

Resume parameters

These parameters define how the tool resumes after an operation pauses or stops because of an error.

You can apply resume parameters to migration cmdlets that include one of the following `OnErrorAction` parameter values:

- `Pause`
- `StopCompEnd`
- `StopImmediately`

This table shows parameter values and their descriptions:

Value	Description
`-AllRemaining`	Requires a starting component. Processing begins at the starting component and processes all remaining components. Multiple components are processed.
`-Resume`	Uses the component from `CurrentComponent.txt` as the starting point. All remaining is set to true. Multiple components are processed.
`-Repeat`	Uses the component from `CurrentComponent.txt` as the starting point. All remaining is set to false. Only one component is processed.

The last component processed is stored in the `CurrentComponent.txt` file in the AutoConfig folder. Editing this file is not recommended.
If you specify `-Resume` or `-Repeat`, and `CurrentComponent.txt` is missing or invalid, processing stops, and you are prompted to select a component.

Setting the OnErrorAction in the CustomerInfo.yml file

You can also set `OnErrorAction` values in the `CustomerInfo.yml` file. Set the values using the following cmdlets:

- For a new file: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

- For an existing file: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

Logs

Running any cmdlet results in a log file creation and an entry in the main history log file. All operation log files are placed in a backup folder. All log file names begin with `CitrixLog`, then show the auto-config operation and the date and timestamp of the cmdlet execution. Logs do not auto-delete.

The main history log is located in `*%HOMEPATH%\Documents\Citrix\AutoConfig*`, in the file named **History.Log**. Each cmdlet execution results in a main log entry containing the date, operation, result, backup, and log file locations of the execution.

You can also use the `New-CvadAcZipInfoForSupport` cmdlet to collect logs to send to Citrix for support. This cmdlet zips all log and .yml files in a single zip file. Customer sensitive information (CustomerInfo.yml and CvadAcSecurity.yml) is not included in the zip. The Icon.yml file is also excluded due to its size. The zip file is placed in *%HOMEPATH%\Documents\Citrix\AutoConfig* and named *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, based on the date and timestamp. This zip file can also act as a backup.

Each log file includes the following:

- The name of the operation and whether the check mode is enabled
- The start and end date and time
- Multiple entries for each component's actions and success/failure notifications
- Summary of actions taken including various counts of created objects
- Suggested fixes where applicable
- Backup folder location where applicable
- Main log location
- Duration

Diagnostic files

Diagnostic files assist you in determining and resolving problems. The following files are created when their operation is run. They are located in the action-specific subfolder under *%HOMEPATH%\Documents\Citrix\AutoConfig*. Include these files when providing information for problem resolution support.

Export

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

This file counts all Broker PowerShell SDK calls made to export the site configuration to files.

Import, Merge, Restore, Sync, Backup, Compare

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

This file documents each Rest API call and related information.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

This file contains the all `Add`, `Update`, and `Delete` Rest API content.

Problems resulting from dependencies

Imports and merges might fail due to missing dependencies. Some common problems are:

1. Group Policies are missing delivery group filters. The usual causes are delivery groups that have not been imported.
2. Applications fail to import or merge. The usual cause is missing delivery groups or application groups that have not been imported.
3. Application groups are missing a RestrictToTag. The usual causes are tags that have not been imported.
4. Host connections fail. The usual cause is missing security information in the CvadAcSecurity.yml file.
5. Machine catalogs fail. The usual cause is host connections that were not imported.
6. Machines missing from machine catalogs and delivery groups. The usual cause is machines that were not found in Active Directory.
7. Users missing from delivery groups. The usual cause is users that were not found in Active Directory.

Recommendations

- Do not run more than one instance of Automated configuration at a time. Running multiple concurrent instances produces unpredictable results in the cloud site. If this occurs, rerun one instance of Automated configuration to bring the site to the expected state.
- Do not work or change data in the Manage tab in Full Configuration while running Automated configuration.
- Always visually verify the merge or import or restore results in Full Configuration to ensure that the cloud site meets expectations.

Folders

Default folder root location

All Automated configuration tool operations occur in the root folder or in subfolders inside it. The root folder is located in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Export

All exported files are placed in two folder locations, providing ease-of-use and a history of exports. Exports are always placed in the root folder. Copies are placed in a subfolder named **Export** with the date and time of the export.

The root folder always contains the most recent exported on-premises site configuration. Each **Export** subfolder contains the export done on the indicated date and time, which maintains a history of exports. You can use any **Export** subfolder to configure the cloud site. Automated configuration does not delete or modify existing export subfolders.

Import/Merge/Sync/Compare

`Import`, `Merge`, and `Compare` operations always sourced from files located in the root folder. Each operation results in the creation of a subfolder to which files in the root folder are copied, providing a history of cloud site changing source files.

Restore

The `Restore` operation uses an existing subfolder to configure the cloud site. The source folder is specified on the required `-RestoreFolder` parameter. Unlike with other commands, no new subfolder is created because the `Restore` operation uses an existing subfolder. The restore folder can be the root folder but still must be specified on the `-RestoreFolder` parameter.

Backups

Automated Configuration initializes, updates, and backs up a cloud site configuration. When used over time, many different configurations can change on the cloud site. To facilitate long-term use and preserve history changes, Automated Configuration uses a preservation scheme to save this history of changes and provide a method to restore earlier states.

Cloud site configuration backups are always made to a subfolder named **Backup** with the data and time of the backup. Automated Configuration does not delete or modify existing export subfolders.

You can use the backups to restore specific components or your entire configuration. To restore the entire delivery group and machine catalog components, use the cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Note:**
>
> The backup file information in the preceding cmdlet is based on your own backups.

To restore the entire cloud site configuration, use the cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

> **Note:**
>
> The backup file information in the preceding cmdlet is based on your own backups.

Changing the default root folder

The `Export`, `Import`, `Merge`, `Sync`, and `Compare` operations can change the default root folder by using the `–AlternateFolder` parameter. The creation and management of per-operation subfolders remains the same as previously described.

Files copied to subfolders

All files having an ".yml"extension are copied to operation subfolders except for the following:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

Automated fail-safe cloud site backups

A backup of the current cloud site configuration is made before running operations that change the configuration. This includes `Import`, `Merge`, `Sync`, and `Restore` parameters. The backup is always in a subfolder beneath the operational subfolder.

In the case of `Restore`, the backup folder is a subfolder of the folder specified on the `–RestoreFolder` parameter.

Automation

Automated configuration tool cmdlets can be run in automation scripts without administrator intervention by suppressing prompts and the display of the log results at cmdlet completion. You can also set parameters to do the same by using the CustomerInfo.yml file.

Add the following parameter to cloud modifying cmdlets to suppress the display of prompts.

```
-Confirm $false
```

Add the following parameter to cmdlets to suppress the display of log at the completion of the cmdlet.

```
-DisplayLog $false
```

Add the following parameter to cmdlets to suppress logging to the PowerShell command window.

```
-Quiet
```

As another method, the following parameters can be placed in the CustomerInfo.yml file.

```
Confirm: False
```

```
DisplayLog: False
```

Exporting from PCs other than the Delivery Controller

The Automated configuration tool uses multiple Citrix PowerShell SDKs to export the on-premises site configuration to files. These SDKs are automatically installed on the Delivery Controller, enabling the tool to run on the Delivery Controller without extra actions. When running on non-Delivery Controller machines, it is necessary to install the set of Citrix PowerShell SDKs needed by the tool. This SDK set is part of Citrix Studio which can be installed from the Citrix Virtual Apps and Desktops installation media.

> **Note:**
>
> Automated configuration cannot be run on the Cloud Connector.

Moving to Citrix Cloud Government and Japan Control Plane

The Citrix Cloud Government and Japan Control Plane environments use different access points to authenticate and allocate access tokens. This unique requirement applies to any Automated configuration tool accessing the cloud. Perform the following steps to use Automated configuration in these environments.

1. In the *%HOMEPATH%\Documents\Citrix\AutoConfig* folder, edit CustomerInfo.yml.

2. Add one of the following lines, depending on the environment you want to connect to, to CustomerInfo.yml (or change it, if already present.)

   ```
   Environment: 'ProductionGov'
   ```

   or

   ```
   Environment: 'ProductionJP'
   ```

Automated Configuration is now able to be used on these environments.

Citrix Cloud data collection

For information on what information Citrix Cloud collects, see Citrix Cloud Services Customer Content and Log Handling.

Additional resources

Discussion forum

Visit the Citrix Discussion forum for Automated Configuration.

Video

Watch Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops on YouTube.

Training

The Cloud Learning Center contains step-by-step video guides to building a service deployment, including the tasks described in this article. See Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

Migrate workloads between Resource Locations using Image Portability Service

May 6, 2024

Image Portability Service simplifies the management of images across platforms. The Citrix Virtual Apps and Desktops REST APIs can be used to automate the administration of resources within a Citrix Virtual Apps and Desktops site.

The Image Portability workflow begins when you use Citrix Cloud to start the migration of an image between two Resource Locations. After exporting your image, Image Portability Service helps you transfer and prepare the image to run on the target hypervisor or public cloud. Finally, Citrix Provisioning or Machine Creation Services provisions the image in the target environment.

Components

Image Portability Service components include:

- Citrix Cloud services
- Citrix Credential Wallet
- Citrix Connector Appliance
- Compositing Engine VM
- PowerShell Example Scripts

Citrix Cloud services

The Citrix Cloud Services API is a REST API service that interacts with the Image Portability Service. Using the REST API service, you can create and monitor Image Portability jobs. For example, you make an API call to start an Image Portability job, such as to export a disk, and then make calls to get the status of the job.

Citrix Credentials Wallet

The Citrix Credentials Wallet service securely manages system credentials, allowing the Image Portability Service to interact with your assets. For example, when exporting a disk from vSphere to an SMB share, Image Portability Service requires credentials to open a connection to the SMB share to write the disk. If the credentials are stored in the Credential Wallet, then the Image Portability Service can retrieve and use those credentials.

This service gives you the ability to fully manage your credentials. The Cloud Services API acts as an access point, giving you the ability to create, update, and delete credentials.

Compositing Engine

The Compositing Engine is the workhorse of the Image Portability Service. The Compositing Engine (CE) is a single VM created at the start of an Image Portability export or prepare job. These VMs are

created in the same environment where the job is taking place. For example, when exporting a disk from vSphere, the CE is created on the vSphere server. Likewise, when running a prepare job in Azure, AWS, or Google Cloud, the CE is created in Azure, AWS, or Google Cloud respectively. The CE mounts your disk to itself, and then does the necessary manipulations to the disk. Upon completion of the prepare or export job, the CE VM and all of its components are deleted.

Connector Appliance

The Connector Appliance, running provider software to manage IPS resources, runs in your environment (both on-premises and in your Azure, AWS, or Google Cloud subscription) and acts as a controller for individual jobs. It receives job instructions from the cloud service, and creates and manages the Compositing Engine VMs. The Connector Appliance VM acts as a single, secure point of communication between the Cloud Services and your environments. Deploy one or more Connector Appliances in each of your Resource Locations (on-premises, Azure, AWS, or Google Cloud). A Connector Appliance is deployed to each Resource Location for security. By co-locating the Connector Appliance and the Compositing Engine, the deployment's security posture increases greatly, as all components and communications are kept within your Resource Location.

PowerShell modules

We provide a collection of PowerShell modules for use within scripts as a starting point to develop your own custom automation. The supplied modules are supported as is, but you can modify them if necessary for your deployment.

The PowerShell automation uses supplied configuration parameters to compose a REST call to the Citrix Cloud API service to start the job and then provide you with periodic updates as the job progresses.

If you want to develop your own automation solution, you can make calls to the cloud service directly using your preferred programming language. See the API portal for detailed information about configuring and using the Image Portability Service REST endpoints and PowerShell modules.

Workflows

The Image Portability Service uses a multi-phase workflow to prepare a master catalog image from an on-premises resource location for your public cloud subscription. The service exports the image from the on-premises hypervisor platform and you upload it to your public cloud subscription (our provided PowerShell upload utility can help automate this). Then, Image Portability prepares the image to be compatible with your public cloud platform. Finally, the image is published and ready to be deployed as a new machine catalog within your cloud resource location.



These high-level workflows are based on the image's source and target provisioning configuration (Machine Creation or Citrix Provisioning). The chosen workflow determines which Image Portability Job Steps are required.

Refer to the following table to understand which jobs are required for each of the supported IPS workflows.

Workflow (Source to Target)	Export	Upload	Prepare	Publish
MCS to MCS	Y	Y	Y	N
PVS to MCS*	N	Y	Y	N
PVS to PVS	N/A	Y	Y	Y
MCS to PVS	Y	Y	Y	Y

*Assumes you have the original image as a Citrix Provisioning vDisk and do not need to export it directly out of the source platform hypervisor.

Requirements

To get started with Image Portability, you must meet the following requirements.

A Citrix Machine Catalog image

IPS requires using images that have one of the following tested configurations:

- Windows Server 2016, 2019, and 2022H2
- Windows 10 or 11
- Provisioned using Machine Creation Services or Citrix Provisioning
- Citrix Virtual Delivery Agent:
  - Most recent two cumulative updates for 1912 and 2203 LTSR
  - Most recent two current releases
- Remote Desktop Services enabled for console access in Azure

Image portability service supports the following hypervisors and cloud platforms:

Source platforms:

- VMware vSphere 7.0 and 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (Prism Element only)
- Microsoft Azure
- Google Cloud Platform

Destination platforms:

- VMware vSphere 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (Prism Element only)
- Microsoft Azure
- AWS
- Google Cloud Platform

A Citrix Connector Appliance

You need a Citrix Connector Appliance installed and configured in each Resource Location where you plan to use Image Portability. For example, if you use image portability to move an image from vSphere to Azure, AWS, and Google Cloud, you need at least four Citrix Connector Appliances:

See Deploy Connector Appliances for detailed instructions.

An SMB (Windows) file share

You need a Windows **SMB file share** for storage of the output of export jobs. The share must be accessible to the Compositing Engine VM which will be created in the Resource Location where you're using the Image Portability Service. Make sure that the available free space on the share is at least twice the configured size of your image's file system.

A machine for running PowerShell scripts

Make sure your machine running the PowerShell scripts has the following:

- PowerShell version 5.1.
- A fast network connection to the SMB file share. It can be the same machine that is hosting the file share.
- A fast network connection to the public cloud platforms where you plan to use the Image Portability feature. For example, Azure, AWS, or Google Cloud.

  See the section Prepare a machine for PowerShell for details about how to download and configure the Image Portability modules from the PowerShell Gallery.

Your Citrix Cloud Customer ID

Make sure you have a valid Citrix DaaS subscription.

To continue, you need access to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). If you don't have access, contact your Citrix representative.

Refer to the API Getting Started documentation for instructions to create and configure an API client to use with image portability.

Azure required permissions and configuration

For the Image Portability Service to perform actions on your Azure resource, you need to grant permissions to certain Azure capabilities to the Azure service principal used by the Image Portability Service. For the detailed list, see Microsoft Azure required permissions.

You can assign the **Contributor** role to the service principal in the associated resource. Or, to assign the minimum permissions required, you can create custom roles with the required permissions, and assign them to the service principal scoped to the appropriate resources.

See the Azure documentation for configuring security roles for your Azure service principal and for creating custom roles.

Google Cloud required permissions and configuration

For the Image Portability Service to perform actions in your Google Cloud project, you grant permissions to certain capabilities to the Google Cloud service principal used by the Image Portability Service.

For the detailed list, see Google Cloud required permissions.

You can assign these permissions using the following roles:

- Cloud Build Editor
- Compute Admin
- Storage Admin
- Service Account User

See the Google Cloud documentation for more information on configuring service account permissions.

Amazon Web Services required permissions and configuration

To perform image portability service workflows with an Amazon Web Services (AWS) account, the respective Identity and Access Management (IAM) identity must have the correct permissions.

For the detailed list, see AWS required permissions.

Set up the Image Portability Service

To set up the Image Portability Service you:

- Deploy connector appliances
- Prepare a machine for PowerShell
- Add credentials to Credential Wallet

Deploy Connector Appliances

Image Portability requires Citrix Connector Appliances to create Image Portability jobs. Connector Appliances help secure interactions with your on-premises and public cloud environments. The Connector Appliances communicate back to the Image Portability Service to report on job status and overall service health.

To deploy and configure Connector Appliance in your environment, follow the steps in Connector Appliance for Cloud Services.

Note the required hardware configuration and network port access for the appliance when planning your deployment.

When your appliance is deployed and registered, the components needed to enable Image Portability are automatically installed.

Prepare a machine for PowerShell

To assist you in getting up and running with Image Portability, we have created PowerShell modules you can customize and use with the service.

The following sections describe how to prepare a machine to run the PowerShell scripts. These scripts are just a few examples. Modify or enhance them to suit your needs.

> **Note:**
>
> After the initial installation, use **Update-Module** to update the PowerShell module.

PowerShell requirements To use the PowerShell scripts, you need the following:

- A Windows machine to run the PowerShell scripts that drive image portability jobs. The machine:
  - Has the latest version of PowerShell.
  - Has a 10-Gbs or better network connection to the on-premises SMB file share and a fast connection to your public cloud (Azure, AWS, or Google Cloud, for example).
  - Can be the same machine hosting the file share.
  - Is a machine running Windows 10, Windows Server 2019, or Windows Server 2022, with the latest Microsoft patches.
  - Can connect to the Microsoft PowerShell Gallery to download the required PowerShell libraries.

Depending on your version of Windows, you might need to disable TLS 1.0/1.1 support. Refer to Microsoft PowerShell Gallery TLS support documentation for more information.

By default, PowerShell does not automatically authenticate through a proxy server. Make sure you've configured your PowerShell session to use your proxy server, per Microsoft, and your proxy vendor best practices.

If you see errors when running the PowerShell scripts relating to a missing or old version of PowerShellGet, you need to install the latest version as follows:


```
Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
    AllowClobber
<!--NeedCopy-->
```

Install libraries and modules Image Portability Service draws on libraries from the Microsoft PowerShell Gallery to drive portability operations.

> **Important:**
>
> After the initial installation, use **Update-Module** to install new versions.

1. Run the following PowerShell command to download the latest modules:

   ```
   Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
       Uploader" -Scope CurrentUser
   <!--NeedCopy-->
   ```

   - To change the PATH Environment Variable:

     Press **Y** and **Enter** to accept.

   - To install the NuGet provider:

     Press **Y** and **Enter** to accept.

   - If informed about an untrusted repository:

     Press **A** (Yes to All) and **Enter** to continue.

2. Confirm that all necessary modules were downloaded by running the command:

   ```
   Get-InstalledModule -Name Citrix.*
   <!--NeedCopy-->
   ```

   This command returns an output similar to the following:

Name	Repository	Description
Citrix.Image.Uploader	PSGallery	Commands to Upload a VHD(x) to an Azure Storage Account, AWS, or GCP and Get information about a VHD(x)
Citrix.Workloads.Portability	PSGallery	Standalone Cmdlet for the Image Job of Citrix Image Portability Service

Update modules to the latest version Run the following command to update the script to the latest version.

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

Install the Citrix Virtual Apps and Desktops Remote PowerShell SDK Image Portability Service requires the Citrix Virtual Apps and Desktops Remote PowerShell SDK to create and manage portability jobs within the Citrix Cloud.

Download and install the Remote PowerShell SDK on your machine.

Install platform-specific third-party components The Image Portability Service PowerShell module does not install third-party dependencies. Hence, you can limit installation to only the platforms you're targeting. If you're using one of the following platforms, follow the relevant instructions for the installation of platform dependencies:

VMware If you're creating Image Portability jobs that communicate with your VMware environment, run the following command to install the required VMware PowerShell modules.

```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

Amazon Web Services If you're creating Image Portability jobs in AWS, download and install the AWS Command Line Interface, then run these commands to install the required AWS PowerShell modules:

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```

Azure If you're creating Image Portability jobs in Azure, download and install the Azure command-line utilities, then run these commands to install the required Azure PowerShell modules:

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```


Google Cloud If you're creating Image Portability jobs in Google Cloud, download and install the Google Cloud SDK on your machine.

Uninstall scripts and modules Run the following commands to uninstall modules used by the Image Portability software.

> **Note:**
>
> Third-party scripts and components aren't automatically removed when uninstalling IPS modules.

To uninstall modules:

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images.Uploader" | Uninstall-Module
<!--NeedCopy-->
```

Add credentials to Credential Wallet

For end-to-end automation scenarios, you can configure the Image Portability Service to authenticate non-interactively with Citrix Cloud, your public cloud, and on-premises resources. Also, the Image Portability Service uses credentials stored in the Citrix Credential Wallet anytime our APIs are directly authenticated with your on-premises and public cloud resources. Setting credentials as described in this section is a required step for running export, prepare, and publish jobs.

When running jobs, the Image Portability Service requires access to resources you can control. For example, for the Image Portability Service to export a disk from a vSphere server to an SMB share, the service needs login access to both systems. To secure this account information, the Image Portability Service uses the Citrix Credential Wallet service. This service stores your credentials in the wallet with a user-defined name. When you want to run a job, provide the name of the credential to use. Also, these credentials can be updated or deleted from the wallet at any time.

Credentials are often stored for these platforms:

- Microsoft Azure
- AWS
- Google Cloud
- SMB Share
- VMware vSphere
- Nutanix AHV
- XenServer

To manage credentials, refer to the Image Portability Service APIs and Credentials Management section of the Developer API Portal.

Use the Image Portability Service

Preparing images in your on-premises Resource Locations to your public cloud subscription requires creating Image Portability jobs within Citrix Cloud. You can create a job to make direct API calls to the service within your script or program, or by using the example PowerShell modules we've developed to automate API calls. Refer to the Image Portability Service Developer API Portal for information about using REST APIs and PowerShell modules to create IPS jobs.

Publish machine catalogs using Citrix Provisioning

The Image Portability Service (IPS) is used with Machine Creation Services (MCS) in Azure, AWS, Google Cloud, Nutanix, vSphere, and XenServer, or with Citrix Provisioning (PVS) in Azure, Google Cloud, vSphere, and XenServer. You can combine the PowerShell and REST solutions described in this guide with your platform's tools, your platform's APIs, or Citrix DaaS SDKs to create a seamless and automated end-to-end workflow for creating a machine catalog based on the prepared image. Depending on your chosen cloud platform, there can be intermediate steps required between the completion of an IPS prepare job and the creation of a catalog or assignment to a PVS target.

AWS IPS prepare jobs on AWS produce a volume. Machine Creation Services require an Amazon Machine Image (AMI) during catalog creation. To generate an AMI from your migrated image, you first need to create an image snapshot from the resulting volume, and then create an AMI based on that snapshot. This can be done with the AWS command line interface (CLI):

```
> aws ec2 create-snapshot --volume-id <VolumeId>
> aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
 SnapshotId=<SnapshotID> }
 '
<!--NeedCopy-->
```

The <VolumeId> is the output from the IPS prepare job. The resulting AMI can be used as an MCS master image.

A PowerShell example script for automating this portion of the workflow is provided in the Citrix.Workloads.Portability module as a script named New-IpsAwsImage.ps1.

Azure On Azure, IPS produces managed disks that are directly usable as MCS master images. To assign the resulting image to PVS targets, IPS provides a 'publish'operation for copying the managed disk into a VHD(x) file in your PVS store.

Google Cloud IPS prepare jobs on Google Cloud produce a disk. MCS requires a Google Cloud instance template. The process for creating an MCS instance template from a disk is covered in detail in Prepare a master VM instance and a persistent disk.

For PVS targets on Google Cloud, IPS provides a 'publish'operation for copying the disk into a VHD(x) file in your PVS store.

Automate VDA configuration

When preparing a Citrix-managed image that originated on-premises, you can reconfigure the VDA within the image to support the target environment for which the image is being prepared. Image Portability Service can apply VDA configuration changes on the fly during the preparation phase of the workflow. The following configuration parameters define how the VDA operates in the migrated image: **InstallMisa**, **XdReconfigure**, and **InstallMcsio**. See Image Portability Service PowerShell examples to define these parameters when creating IPS jobs.

Configurations

- Configuring **InstallMisa** to `true` enables the Image Portability Service to install any missing VDA components that is required to provision the image using MCS.
- Configuring **InstallMisa** to `true` or **InstallMcsio** to `true` also requires configuring **CloudProvisioningType** to `Mcs`.
- Set **InstallPvs** to the version of the PVS server where the image is being deployed. When **InstallPvs** is set, the Image Portability Service (IPS) automatically installs the specified version of the PVS target device software in the image during prepare jobs. IPS supports the latest two builds (base release or cumulative updates) for the latest two Long-Term Service Releases (LTSR) and Current Releases (CR).

For both **InstallMisa** and **InstallMcsio**, note the following:

- These features are only supported for recent LTSR and CR releases of the VDA.
- If the necessary components are already present for the installed VDA, no changes are made, even if the parameters are configured.
- For supported versions of the VDA, Image Portability installs the appropriate version of the required components, even if the necessary VDA components aren't present.
- For unsupported versions of the VDA, reconfiguration fails and a message is logged if the necessary VDA components aren't present. The preparation job is completed even if the VDA reconfiguration does not.

XdReconfigure requires one of the following values: `controllers` or `site_guid`. Here are example configuration parameters using each value:

Using **controllers**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'controllers'
        ParameterValue = 'comma-separated-list-of-your-cloud-connectors
           -fqdns'
     }

)
<!--NeedCopy-->
```

where the **ParameterValue** is the list of FQDNs of the new DDCs where you want to point the VDA. Multiple DDCs can be specified in a comma-separated format.

Using **site_guid**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'site_guid'
        ParameterValue = 'active-directory-site-guid'
     }

)
<!--NeedCopy-->
```

XdReconfigure also accepts values that are supported when running the VDA command-line installer with the **/reconfigure** install switch, for example, **XenDesktopVdaSetup.exe /reconfigure**. Some examples of these values include **wem_agent_port**, **wem_cached_data_sync_port**, **wem_cloud_connectors**, or **wem_server**. For a complete list of VDA reconfigure command-line options, refer to the Citrix DaaS VDA documentation.

Configuring **InstallMcsio** to **`true`** automatically installs MCSIO on the image. To disable automatic MCSIO installation on the image, configure **InstallMcsio** to **`false`**.

> **Note:**
>
> You can use `-DryRun` while running your commands to validate your configuration and your connector appliance's network settings.

Reference

This section details technical reference information, based on your needs.

Permissions required by the Image Portability Services

This section details the permissions required by the Image Portability Service on each of the supported on-premises and Cloud platforms.

Connector Appliance required permissions The Connector Appliance needs access to the following URLs to prepare images in the Image Portability Service:

```
api-ap-s.cloud.com
api-eu.cloud.com
api-us.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

VMware vCenter required permissions The following vCenter permissions are necessary to run the IPS export disk job in a VMware environment. These permissions can be found under **Roles** in the **Access Control** section of the vCenter administration panel.

```
- Cryptographic operations
    - Direct Access

- Datastore
    - Allocate space
    - Browse datastore
    - Low level file operations
    - Remove file

- Folder
    - Create folder
    - Delete folder

- Network
    - Assign network

- Resource
    - Assign virtual machine to resource pool

- Virtual machine
    - Change Configuration
        - Add existing disk
        - Add new disk
        - Remove disk

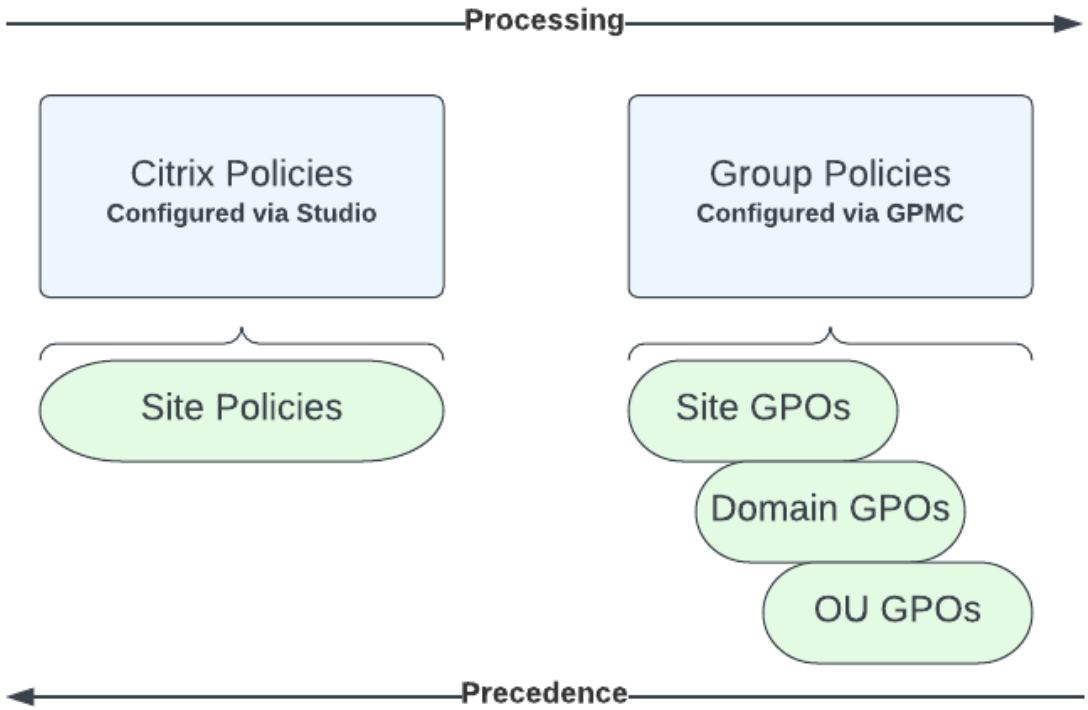
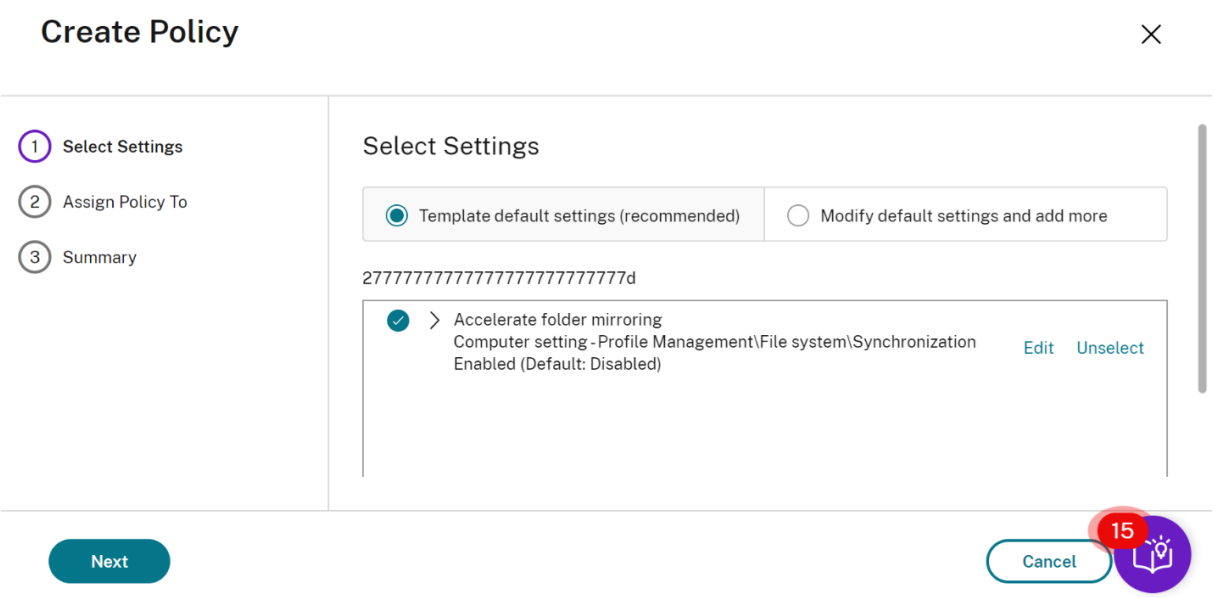
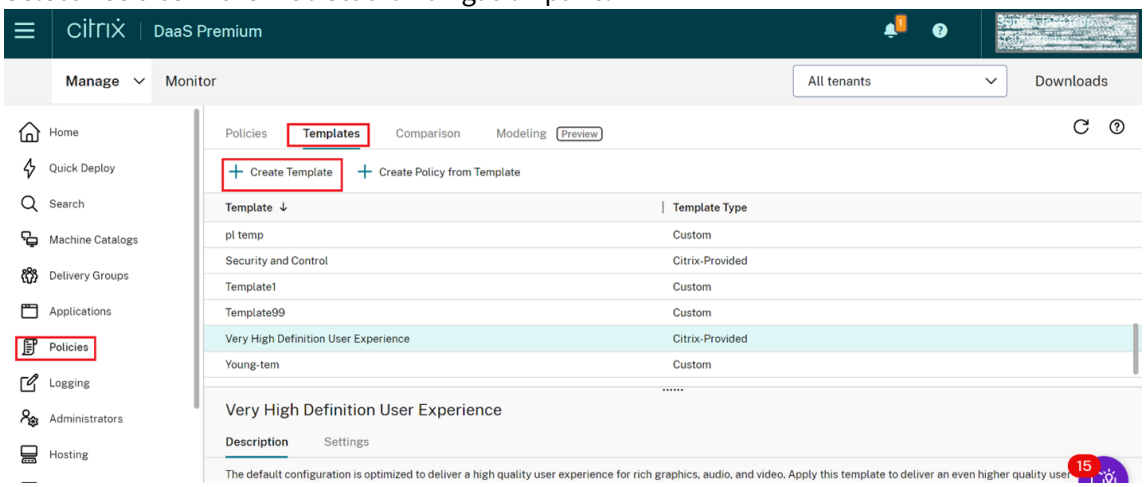
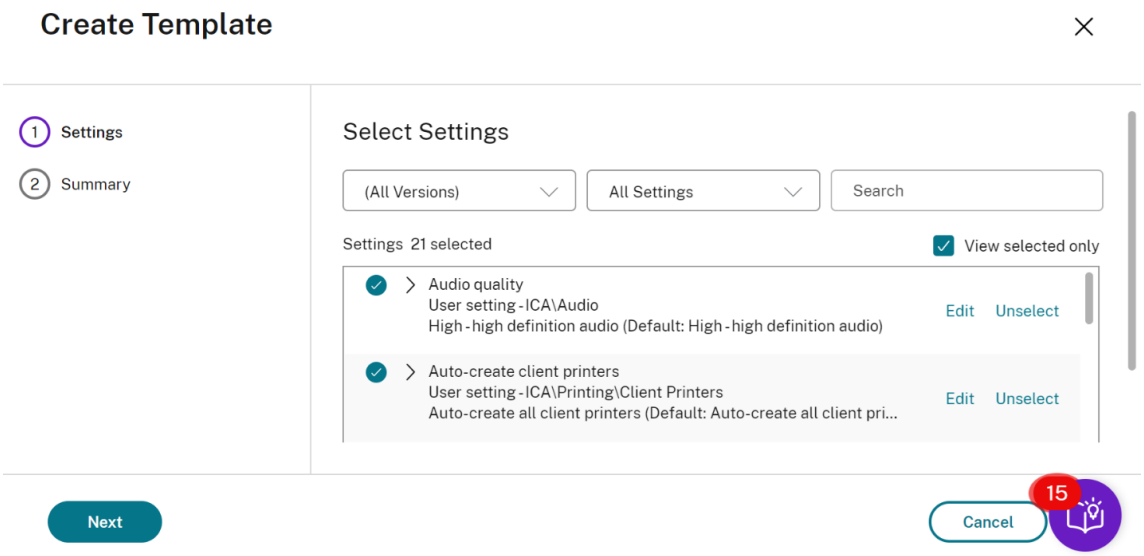
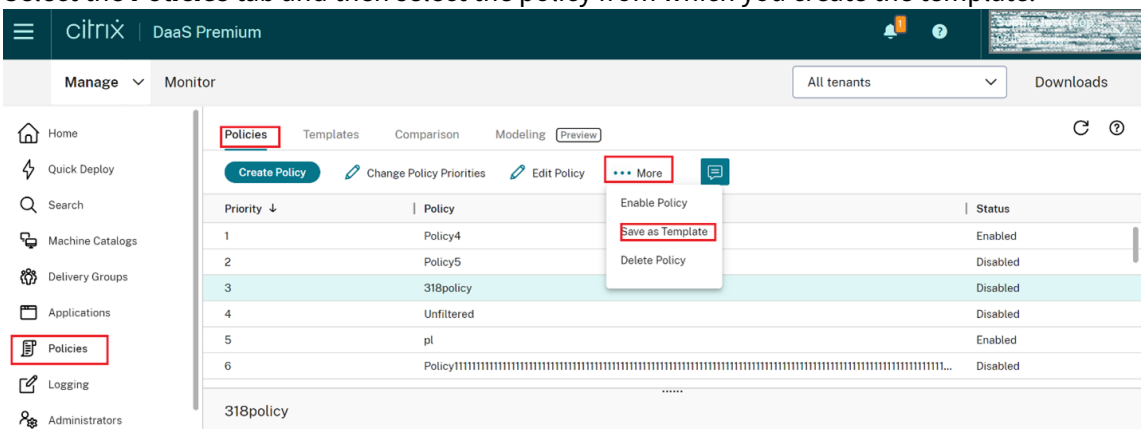
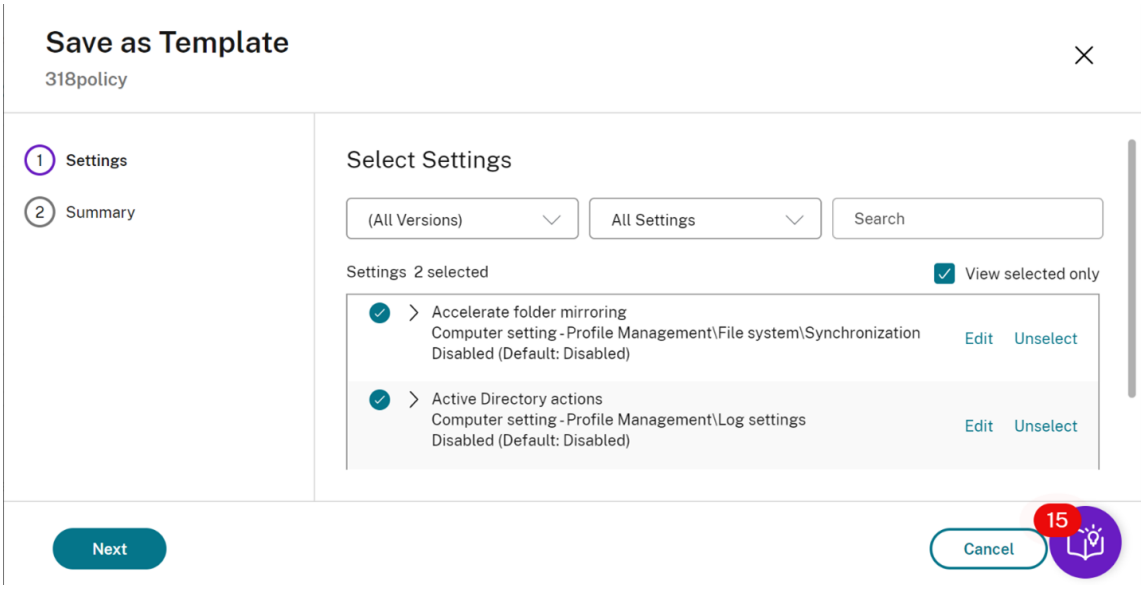
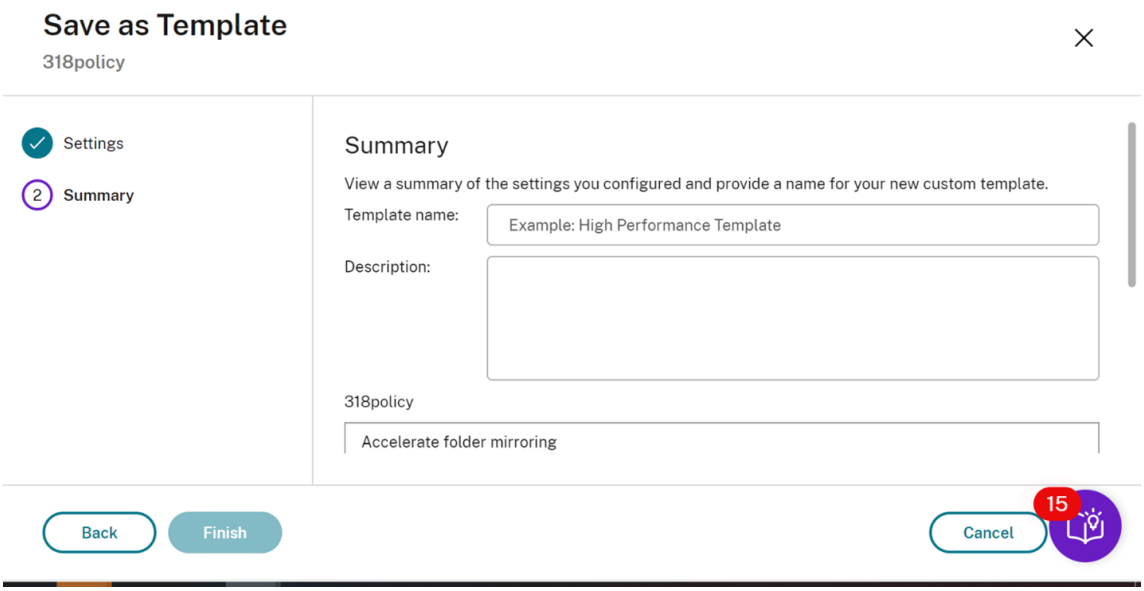
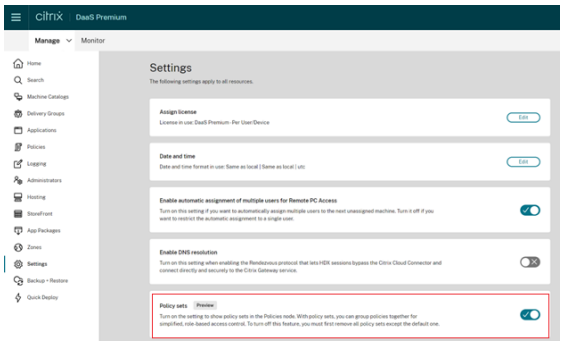
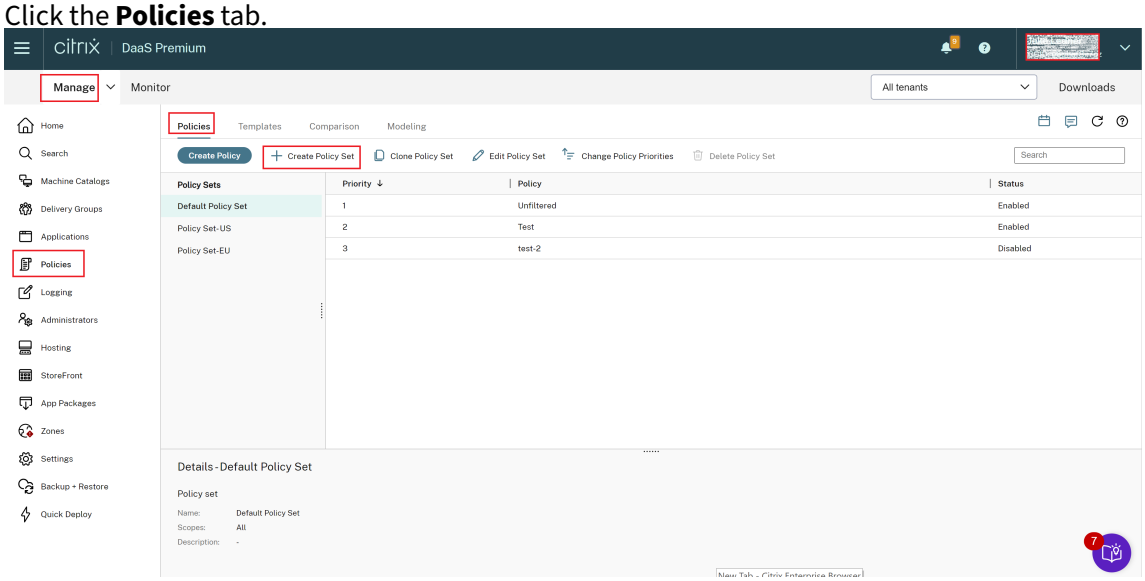
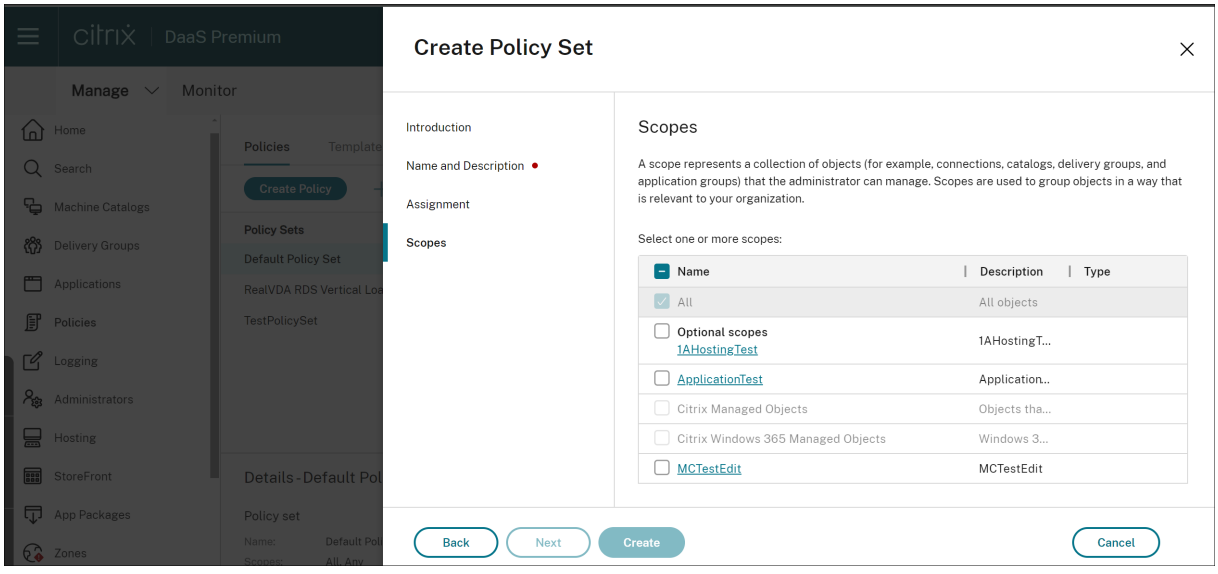
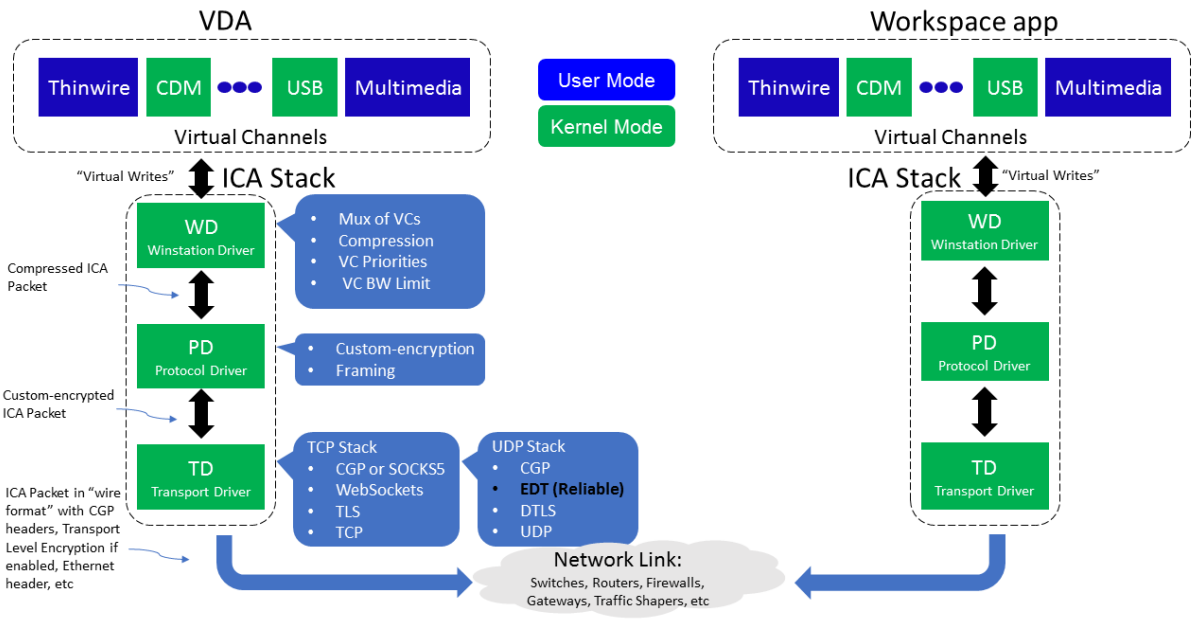
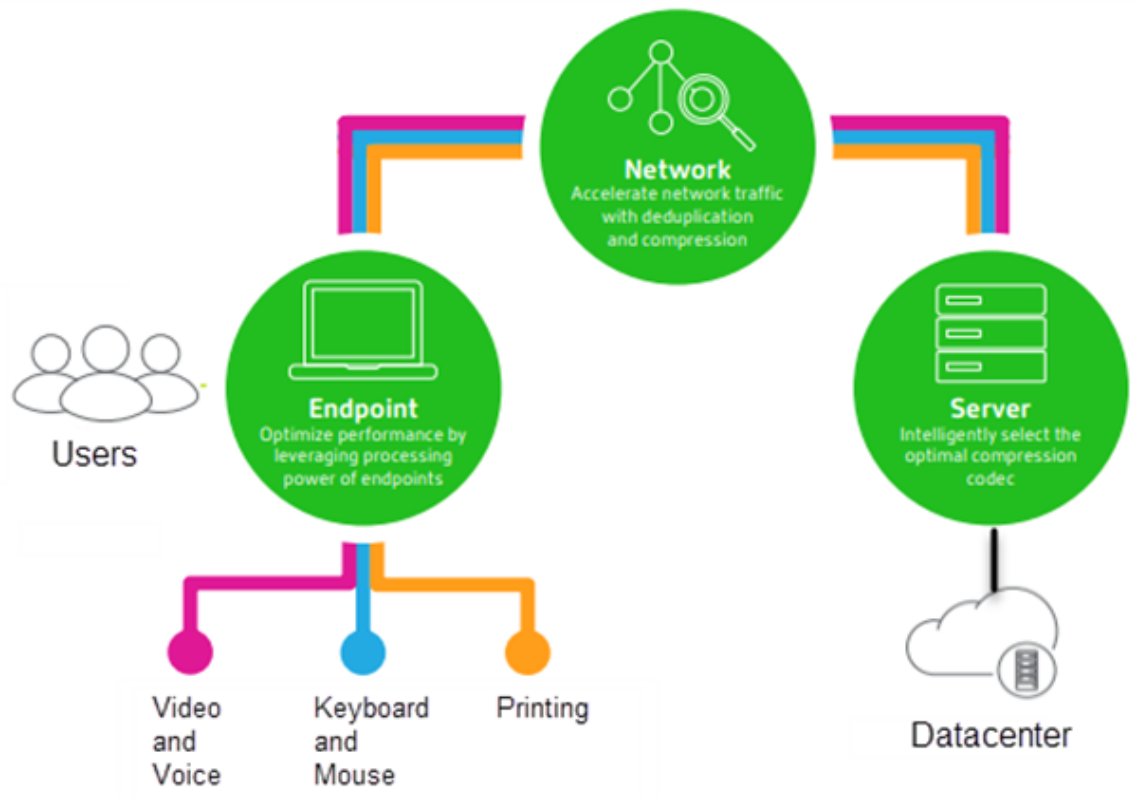
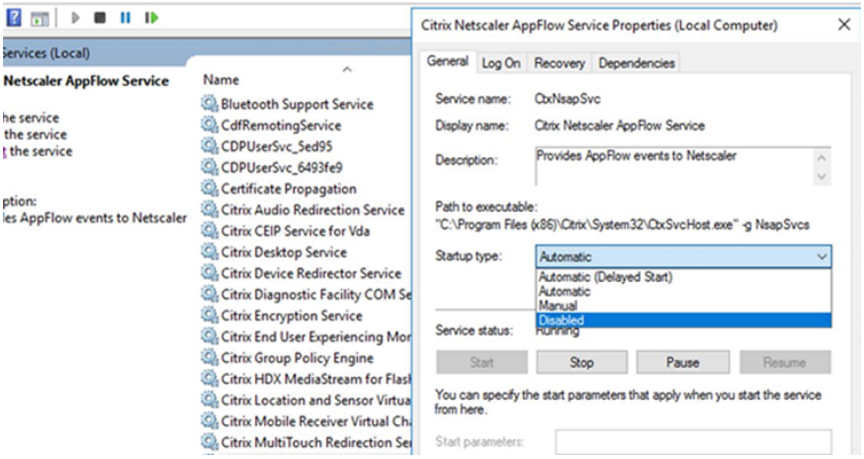
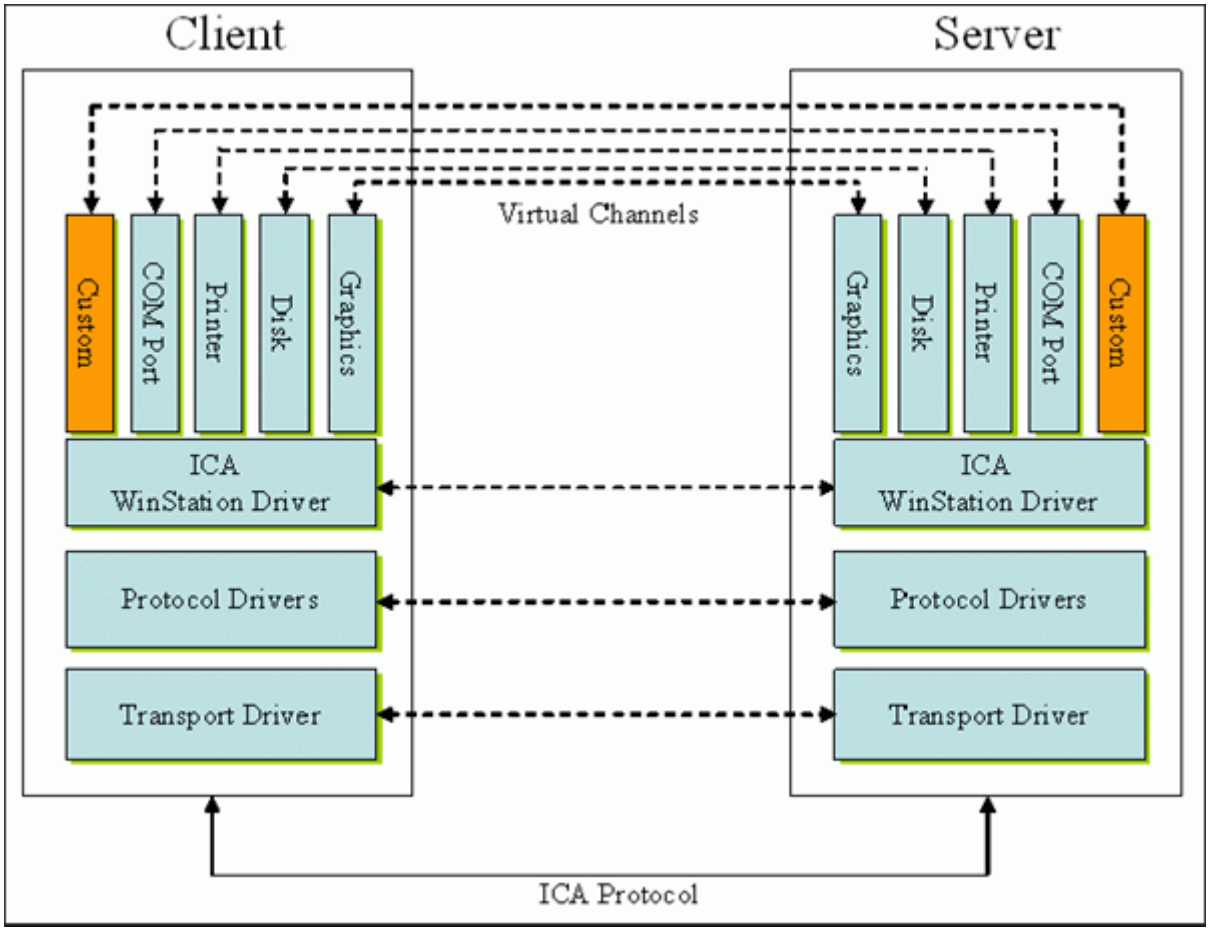
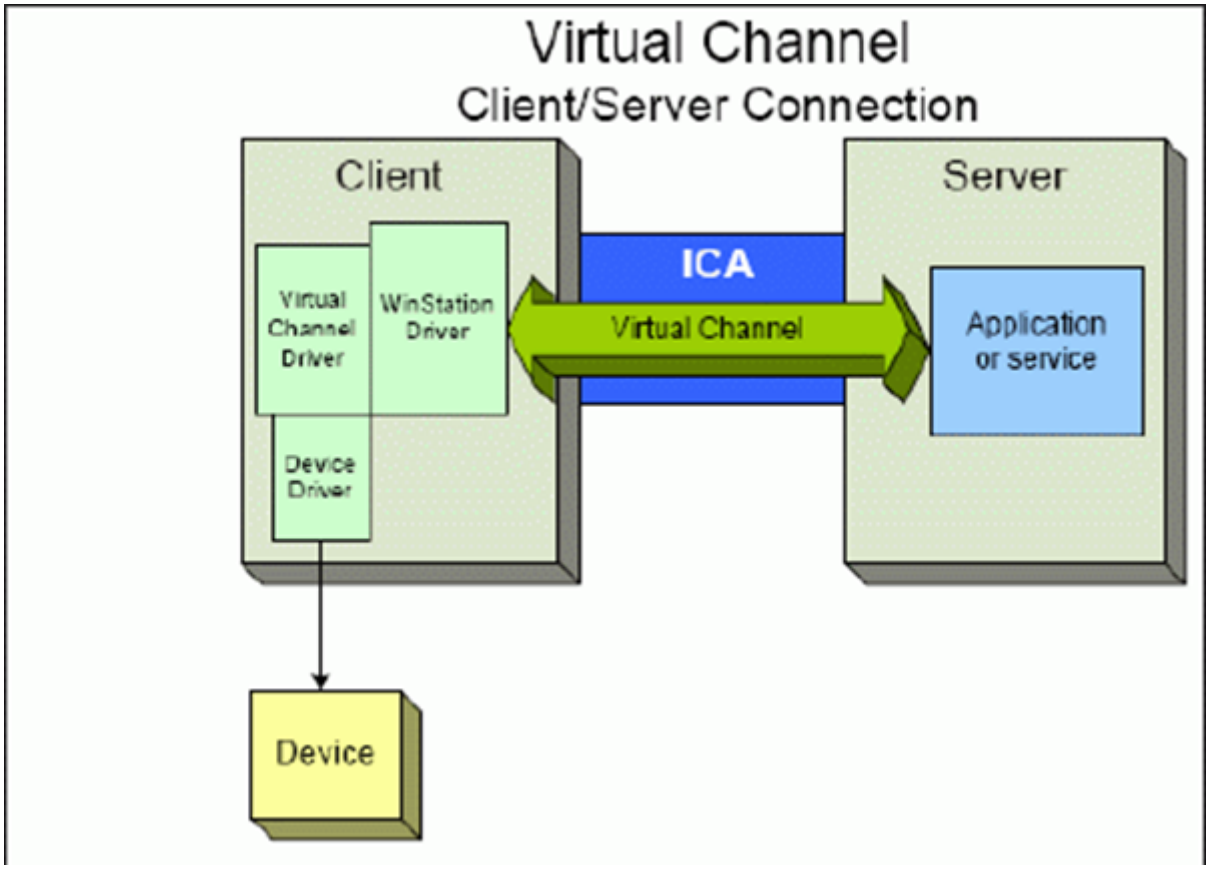
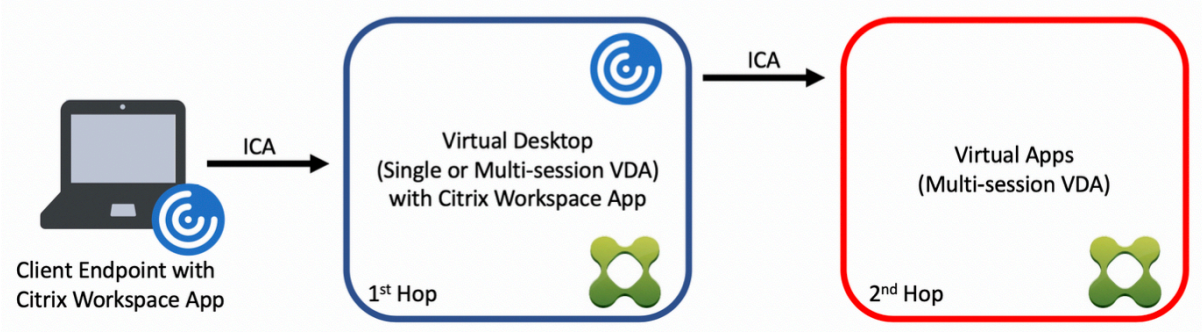
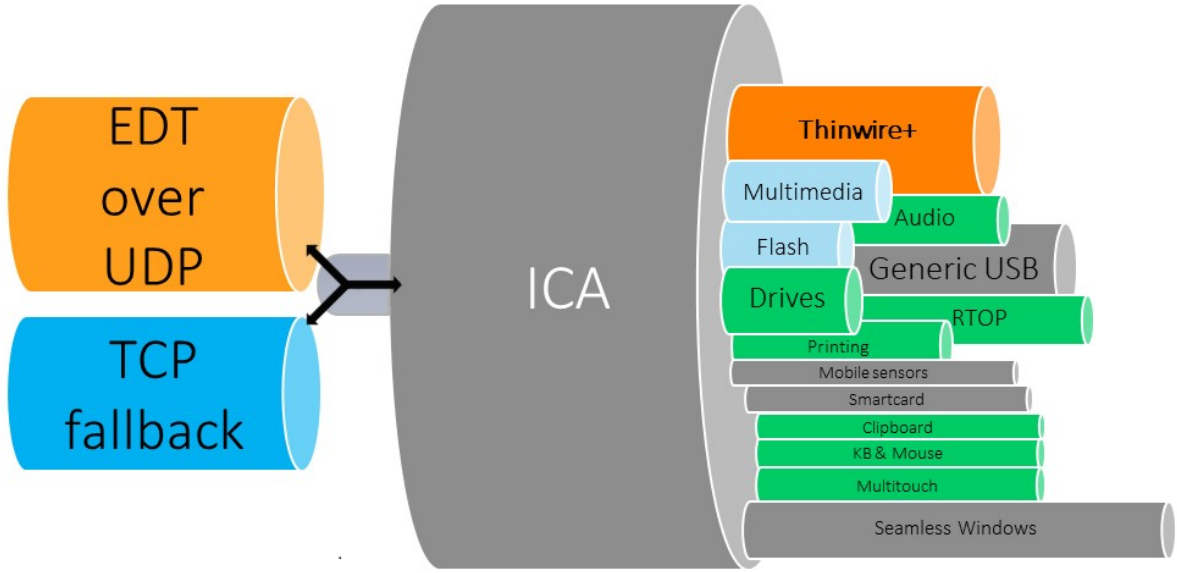
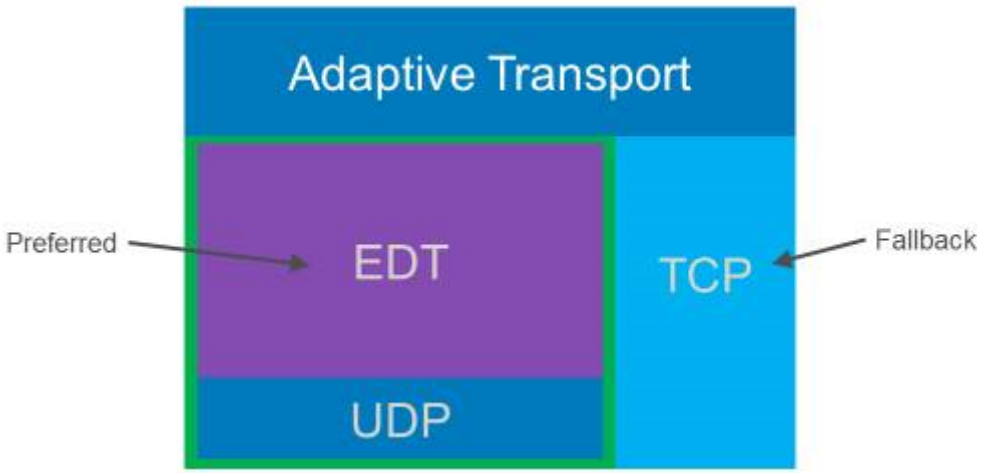
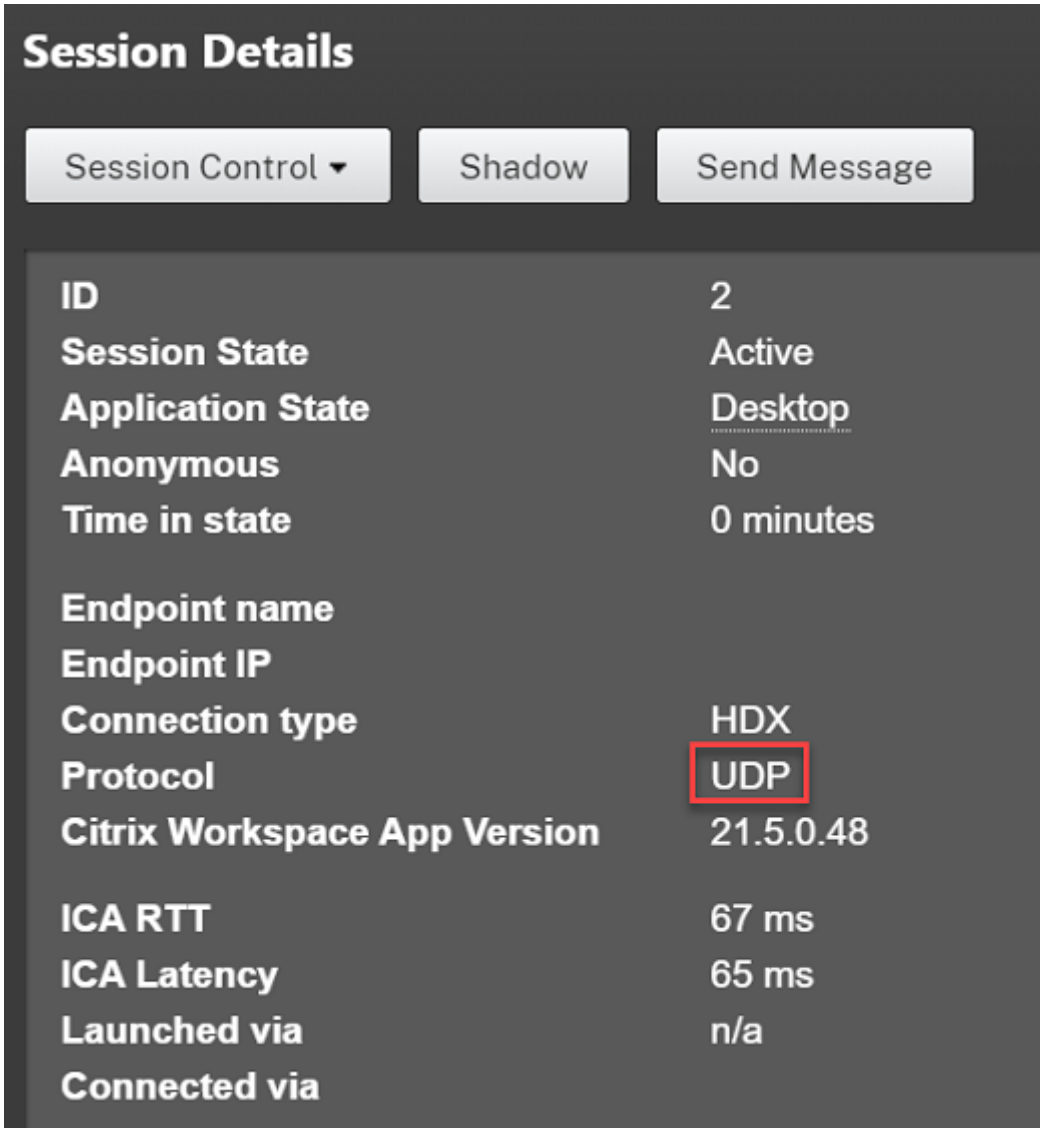
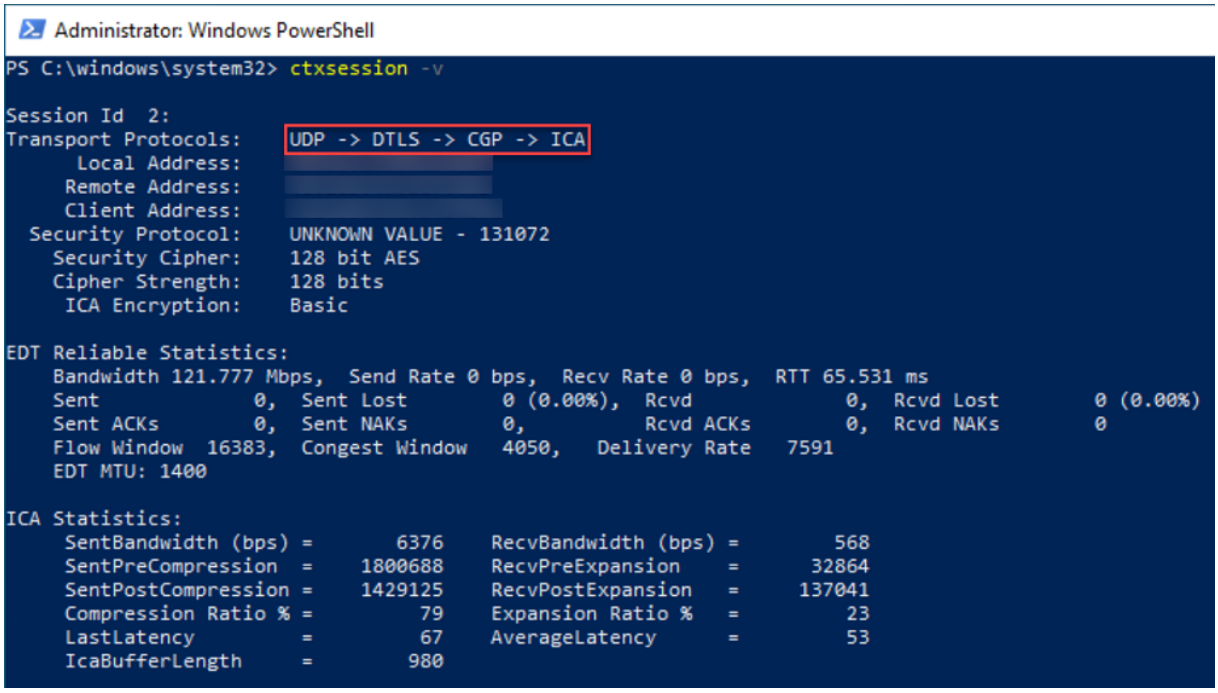
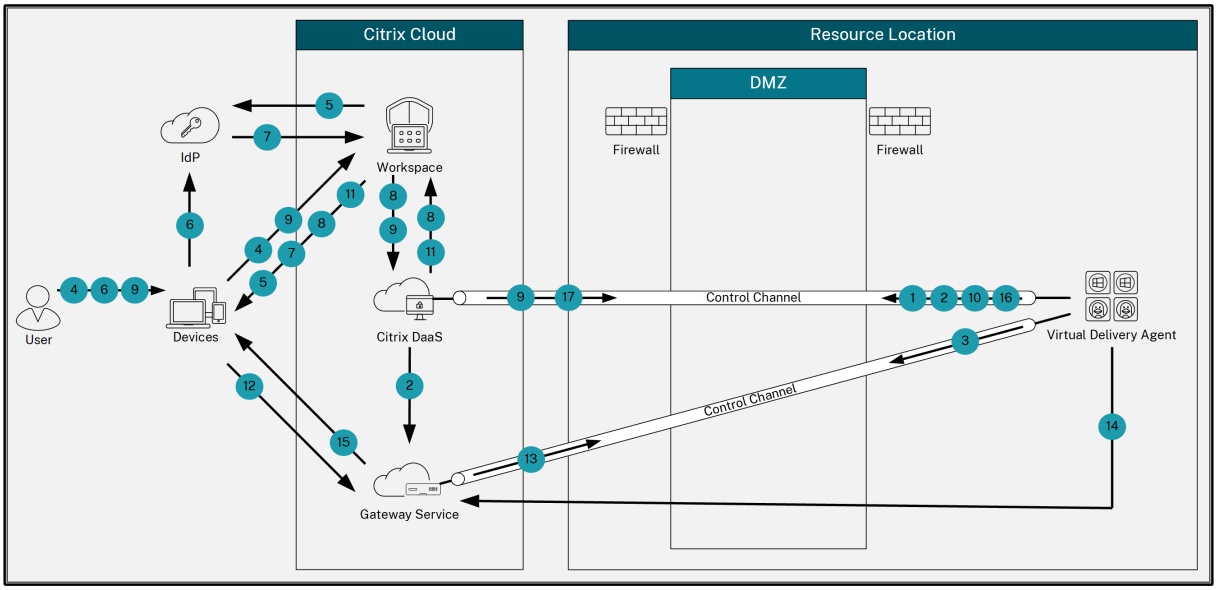
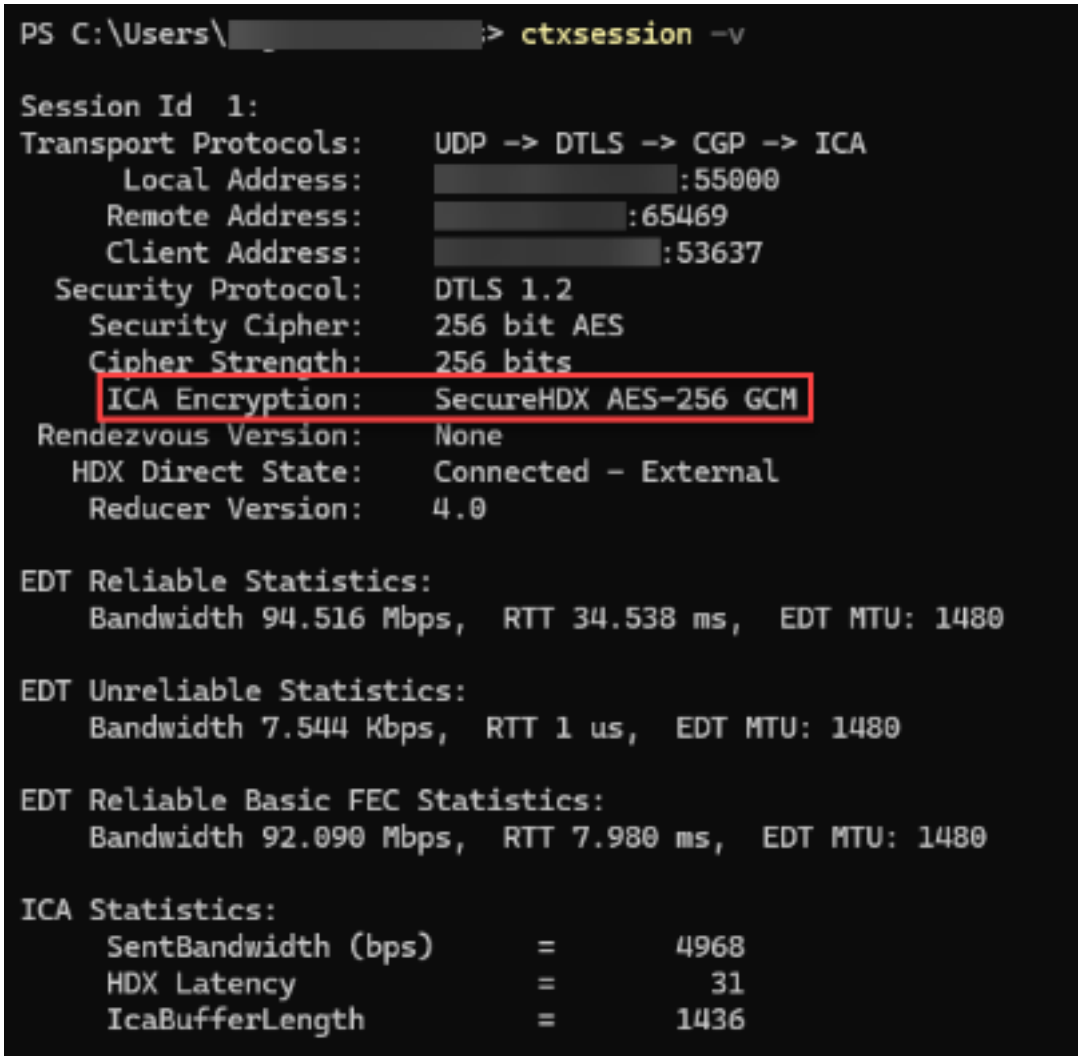
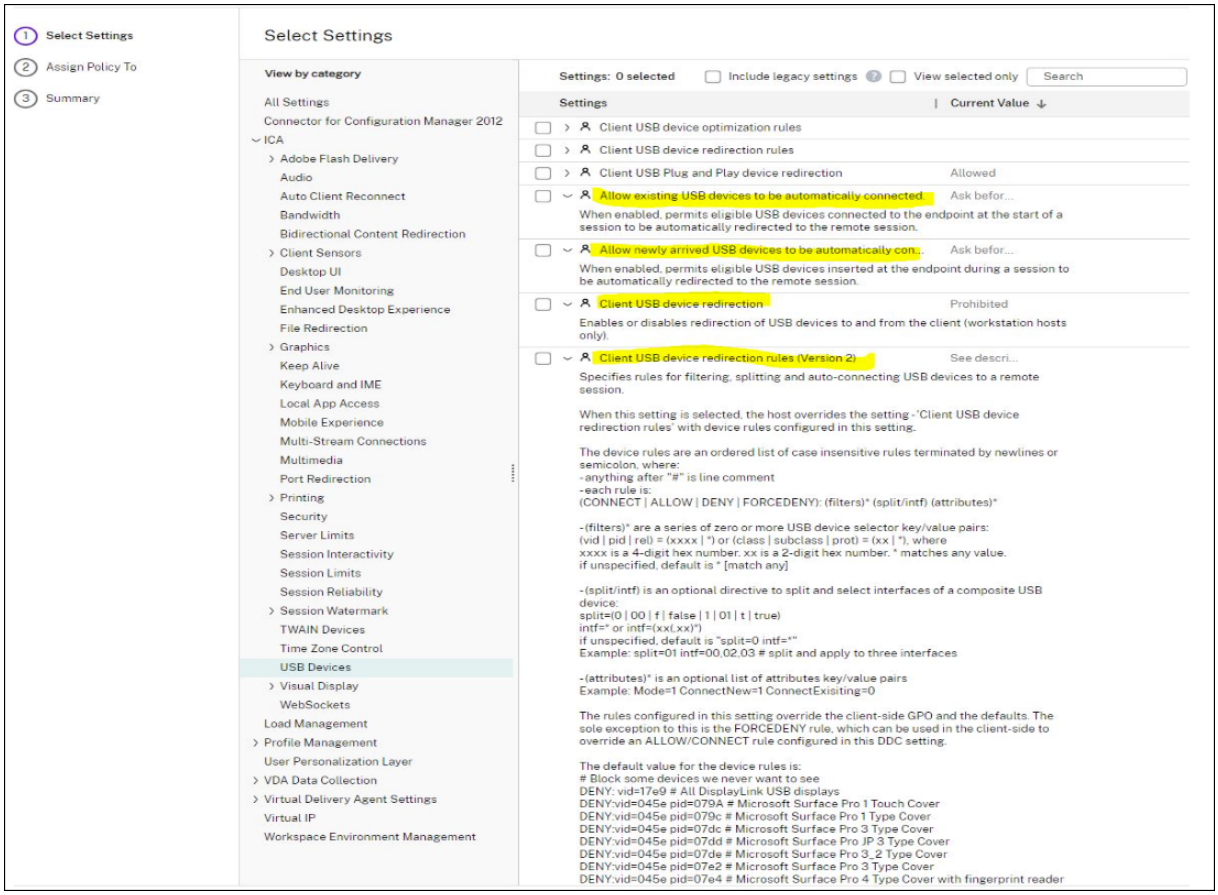
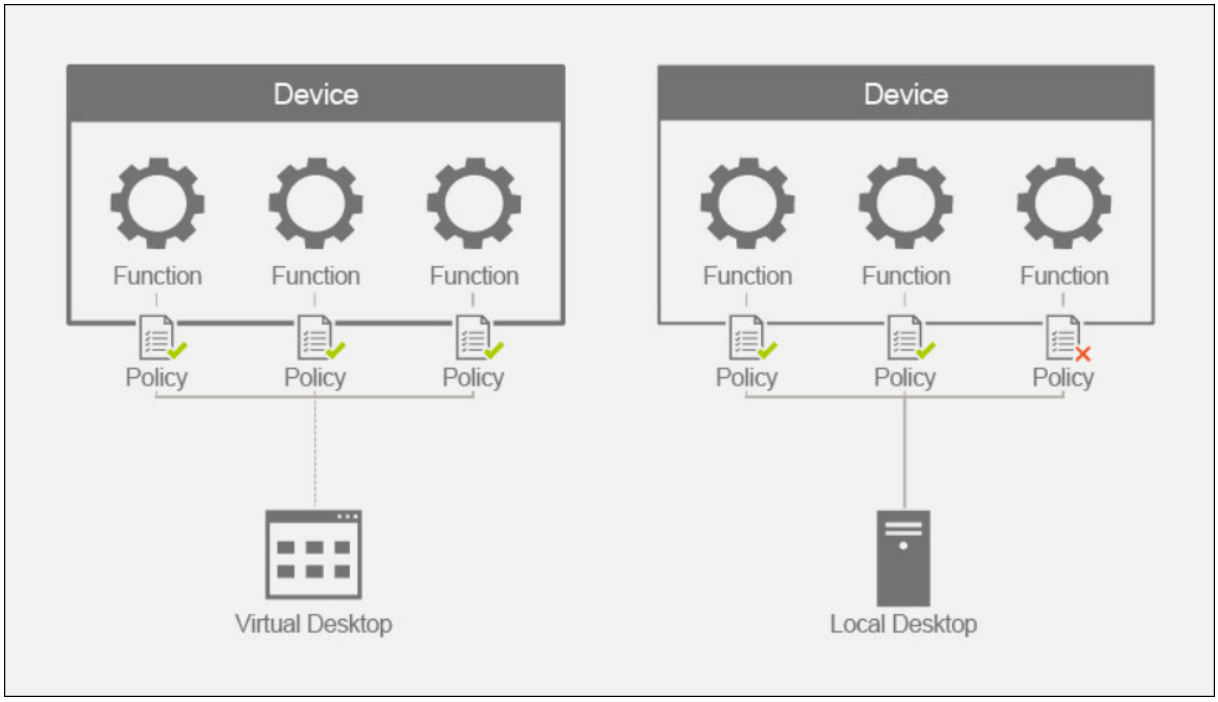
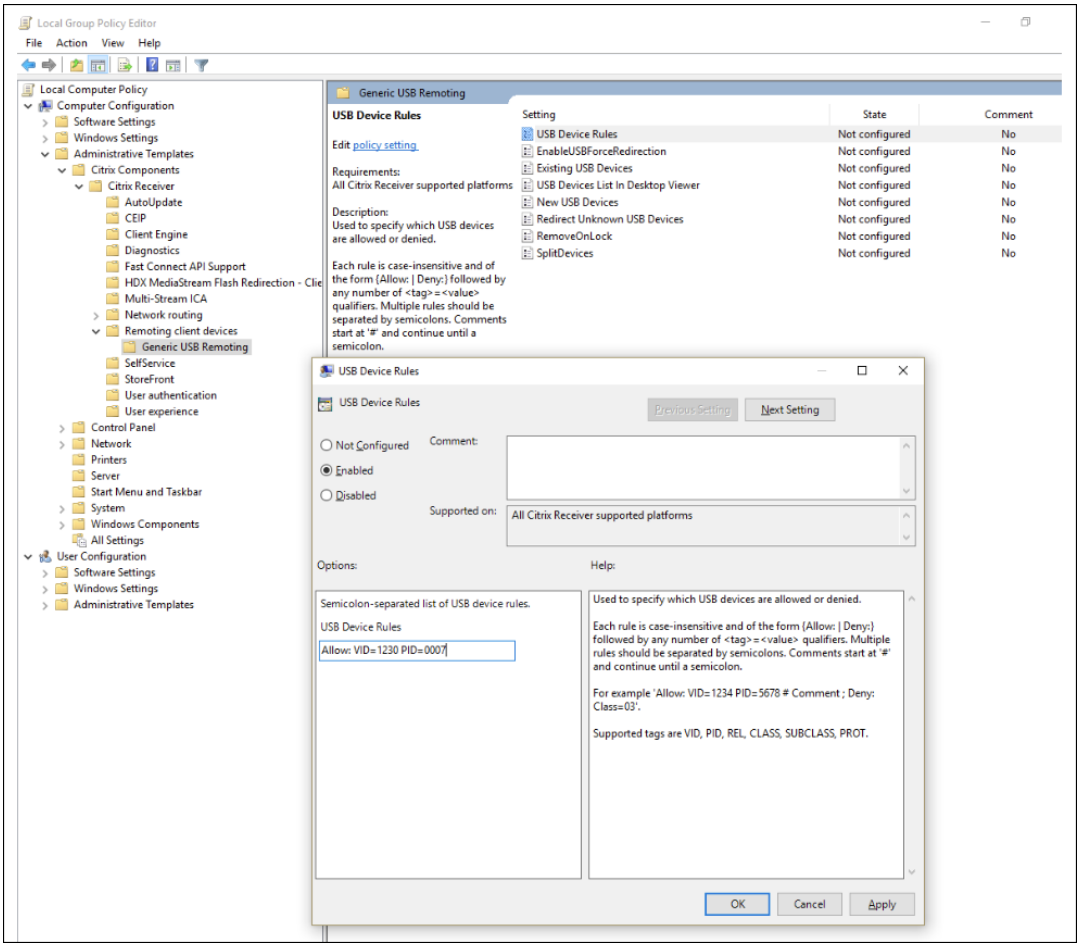
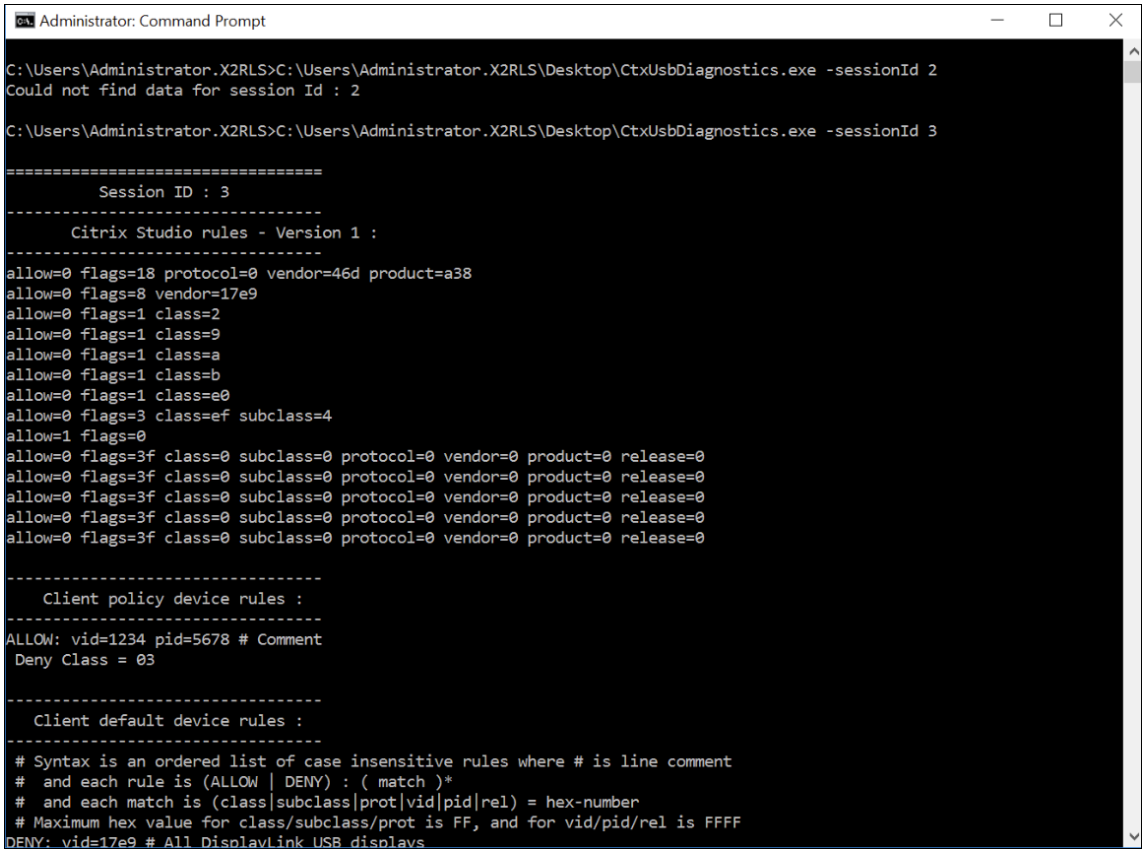
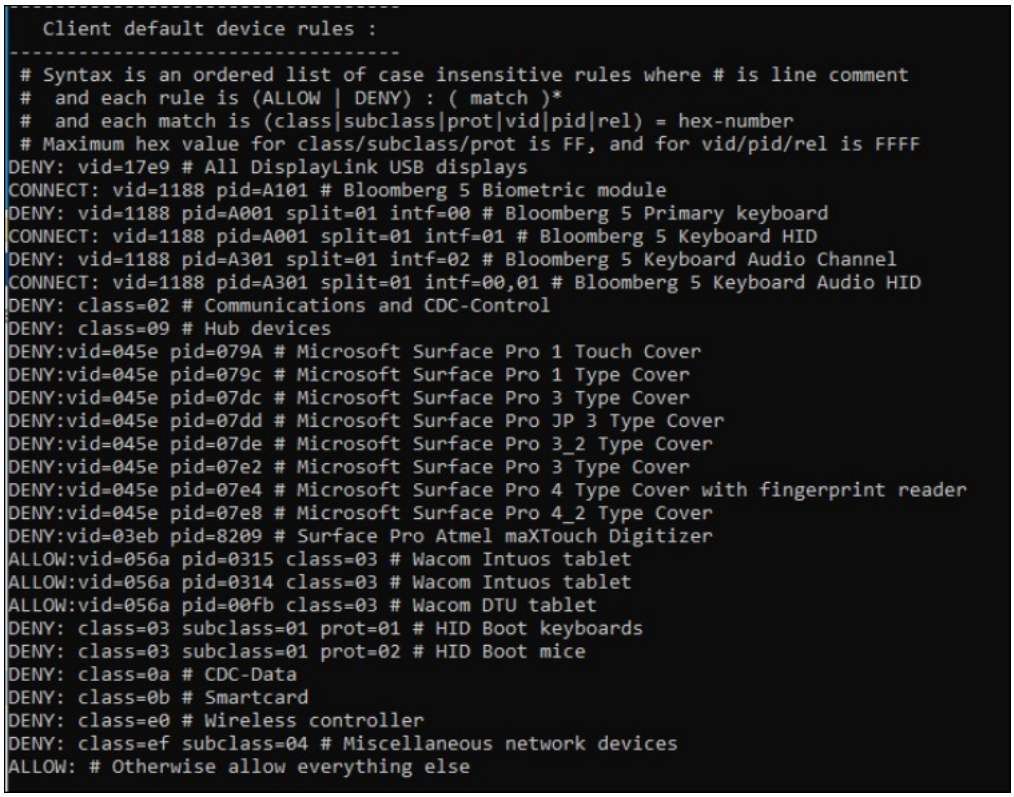
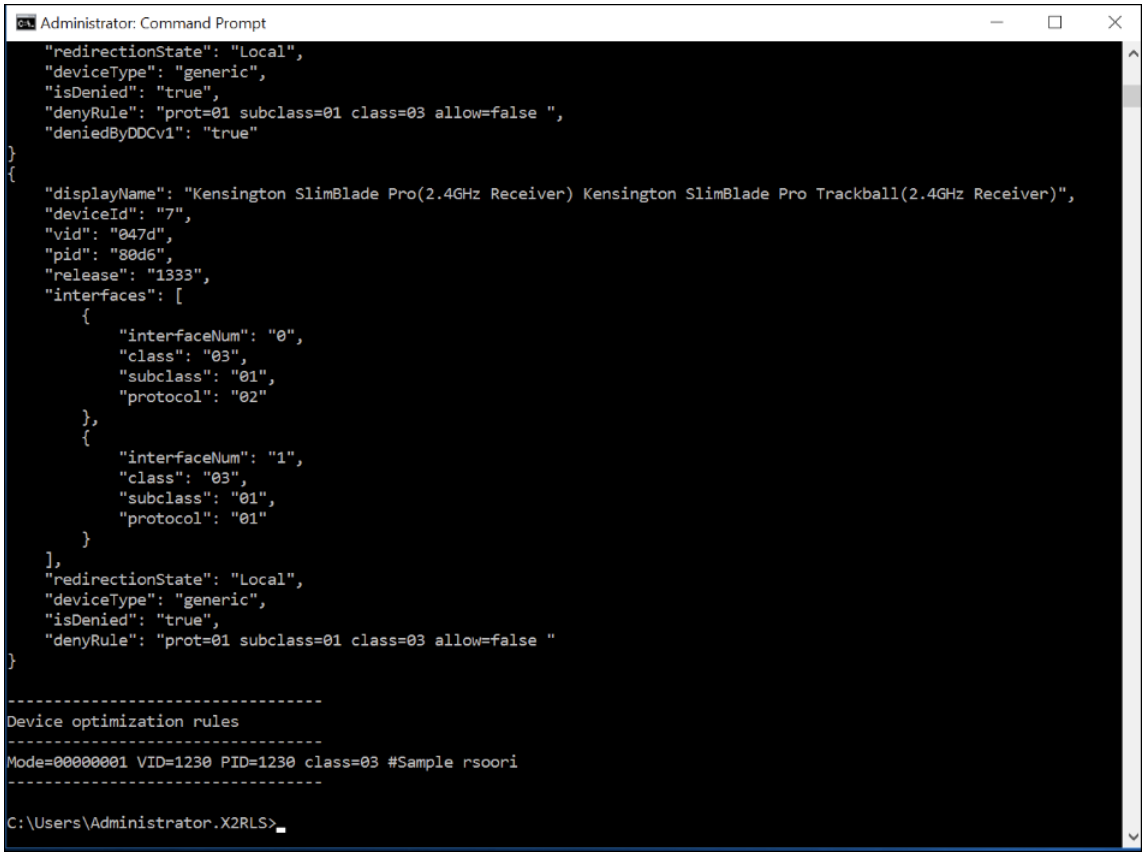
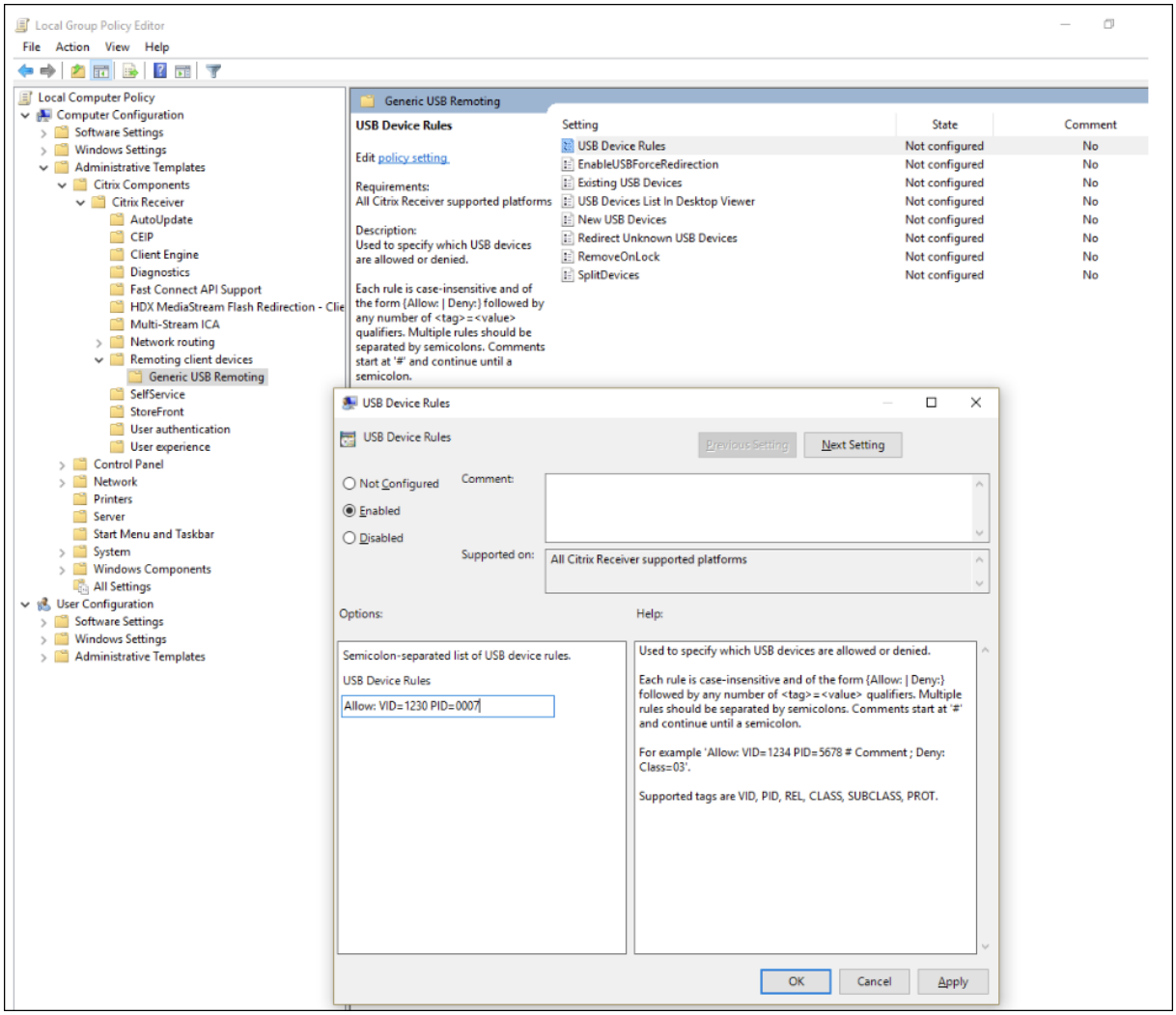
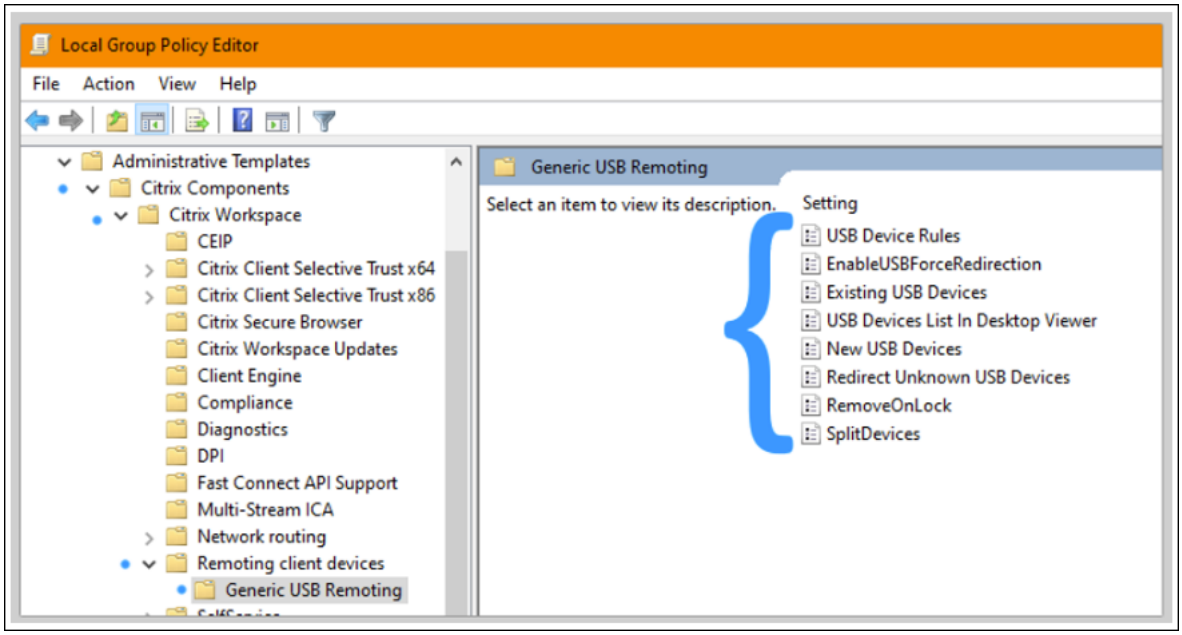
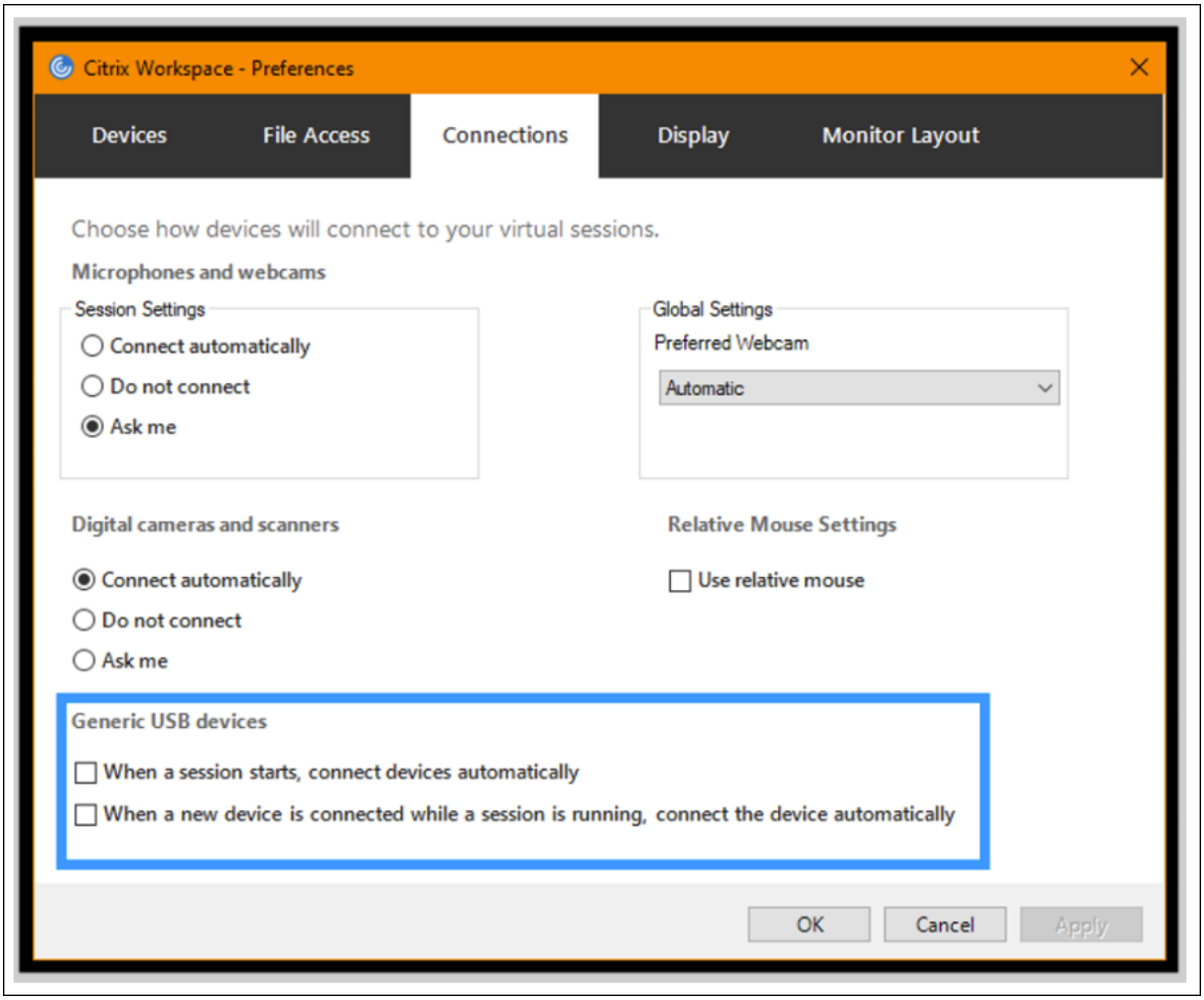
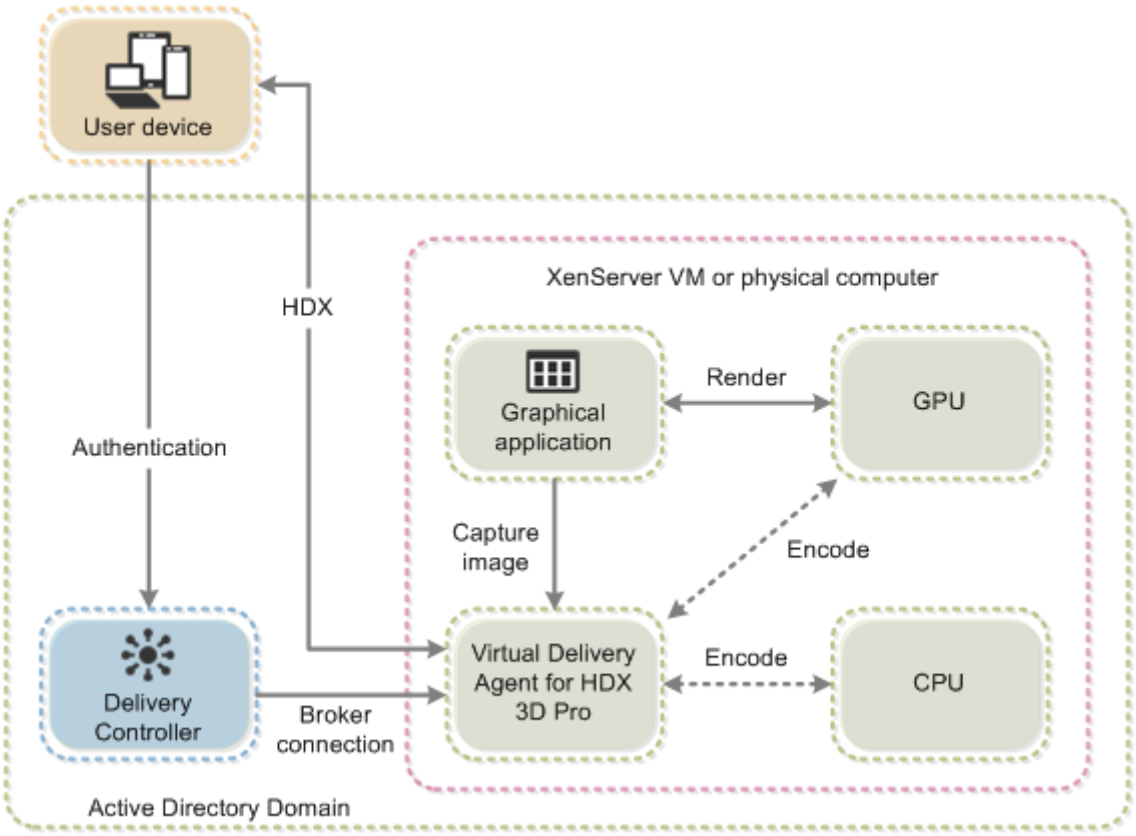
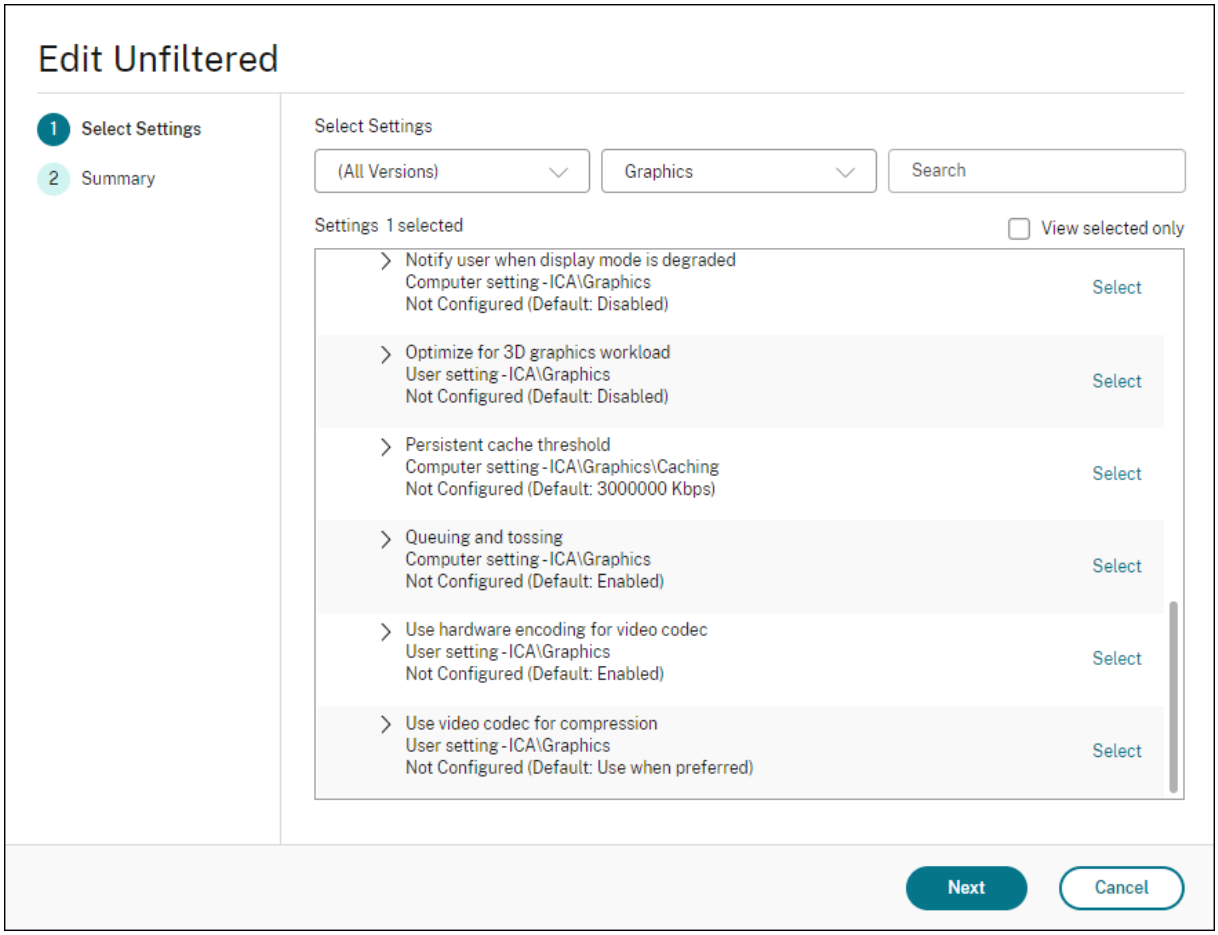
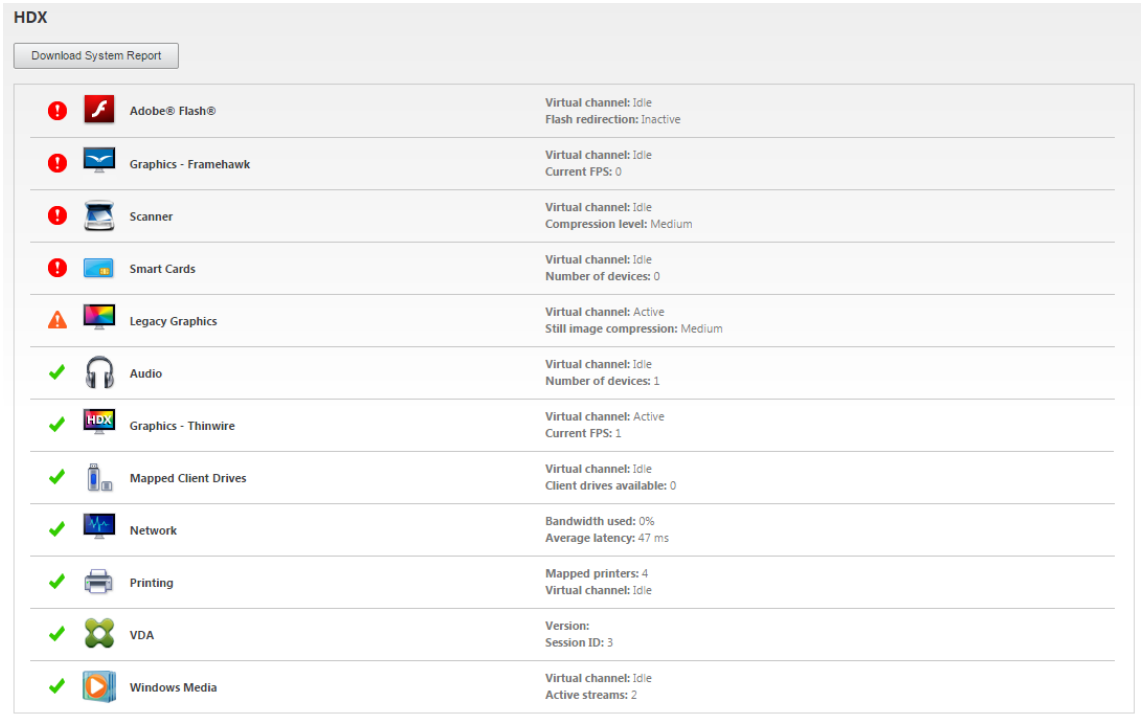
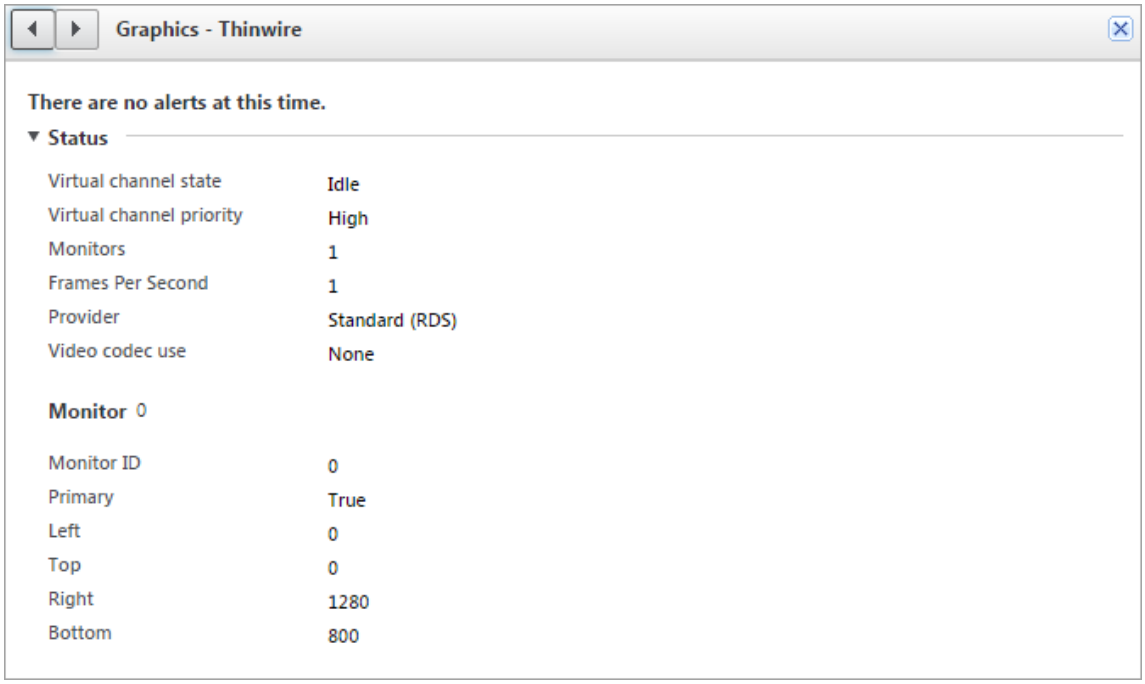
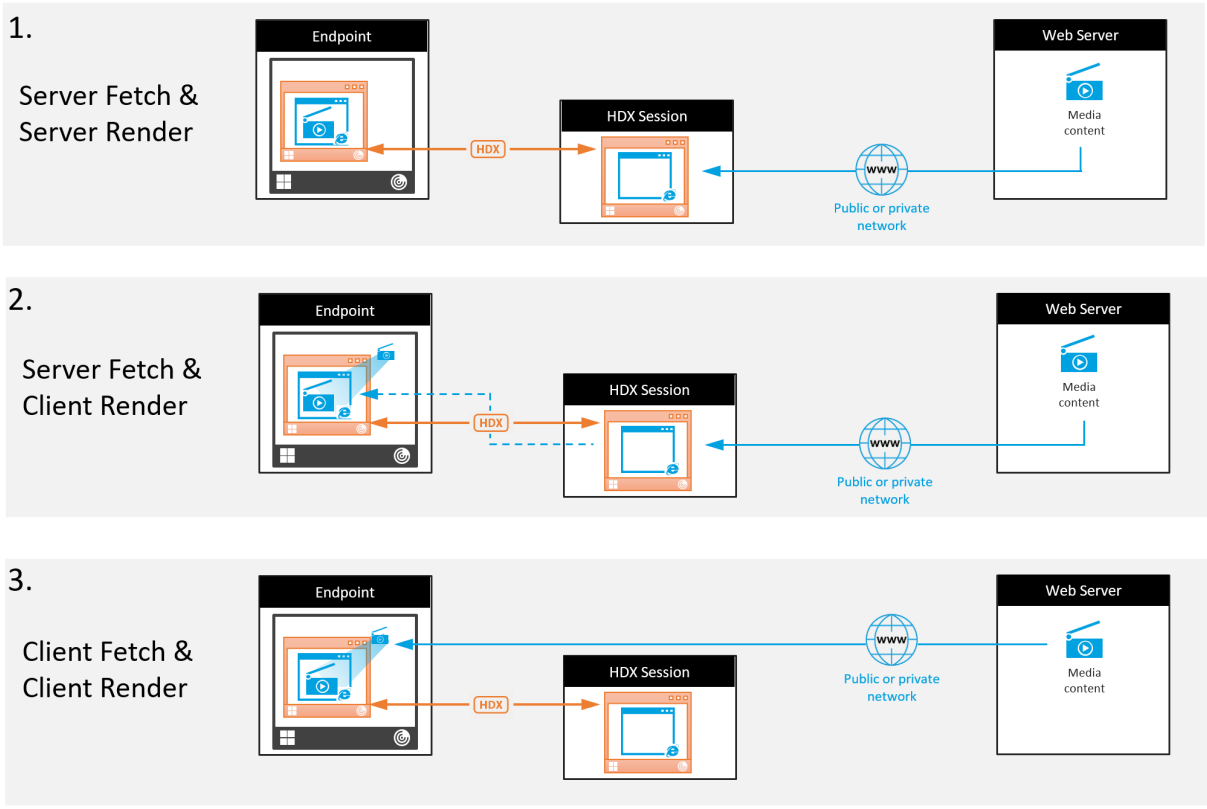
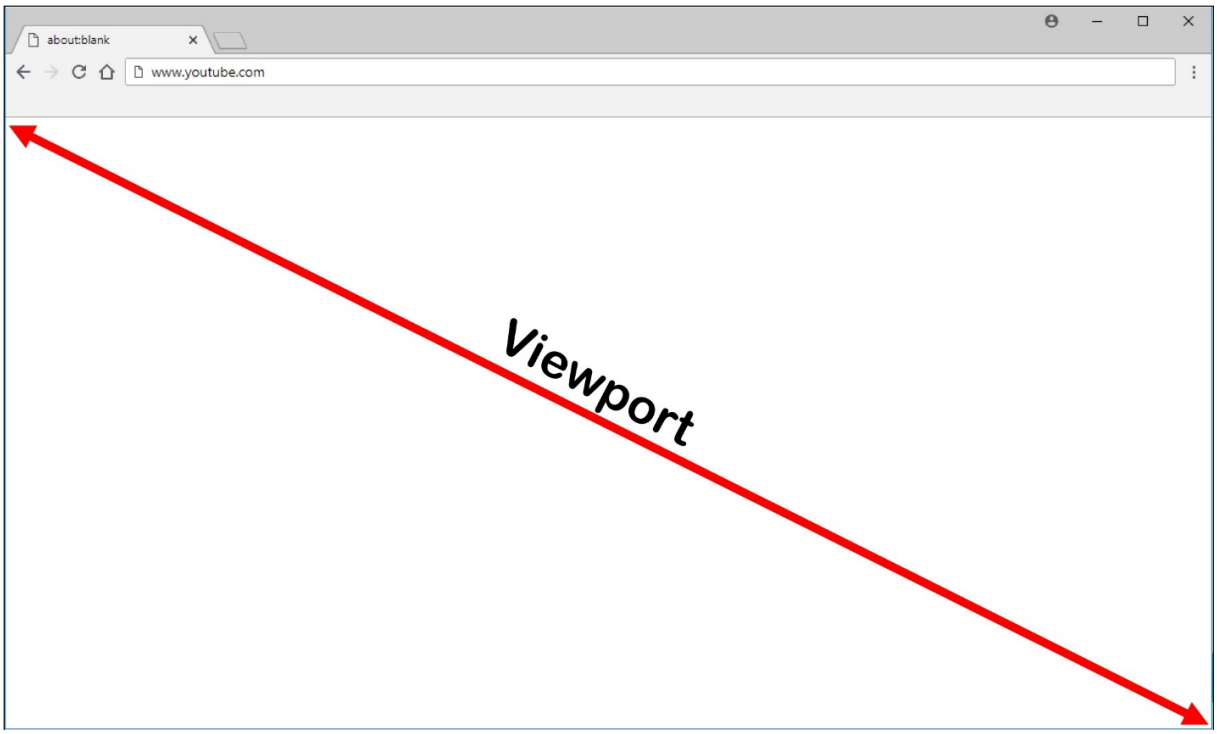
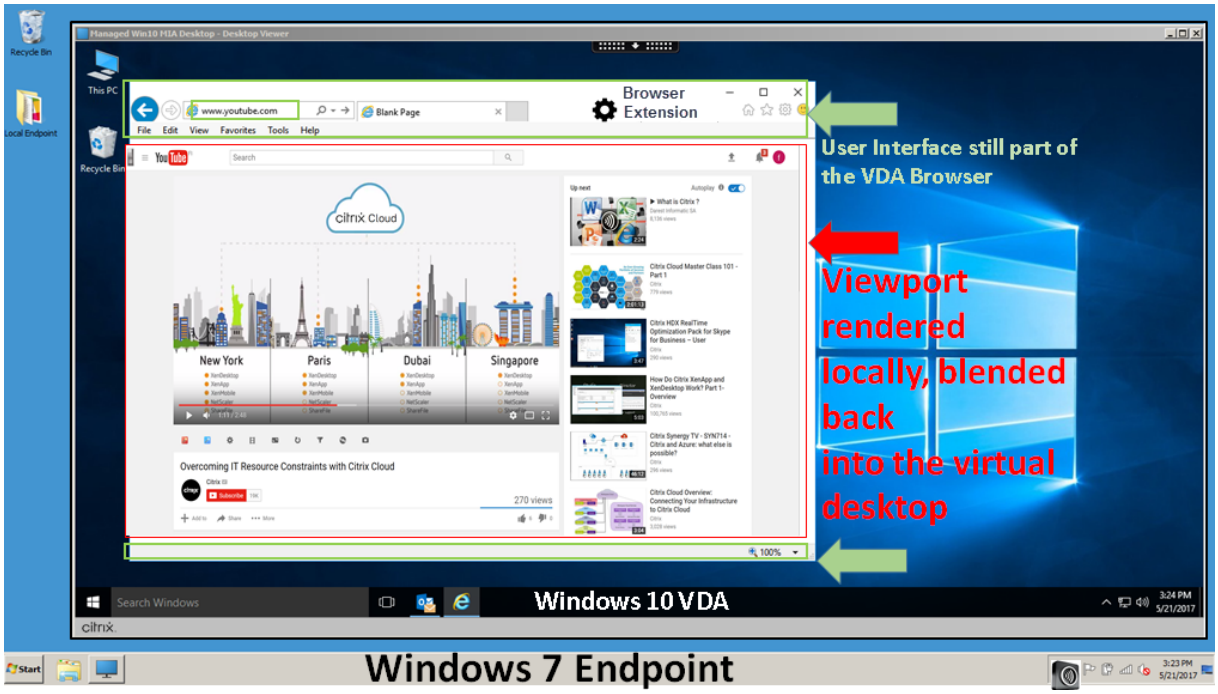
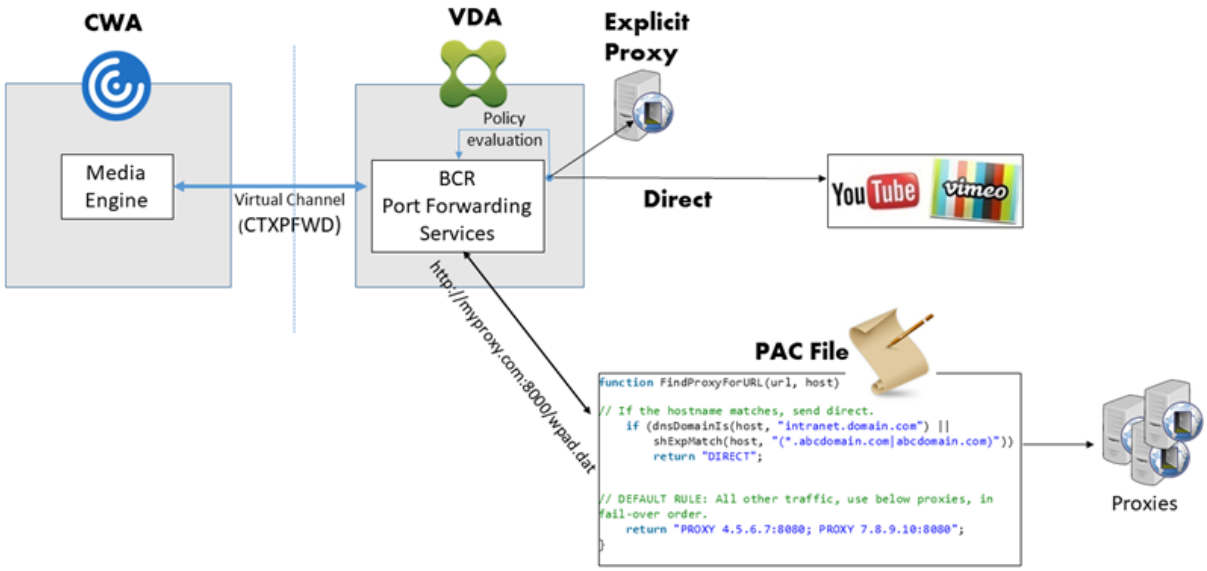
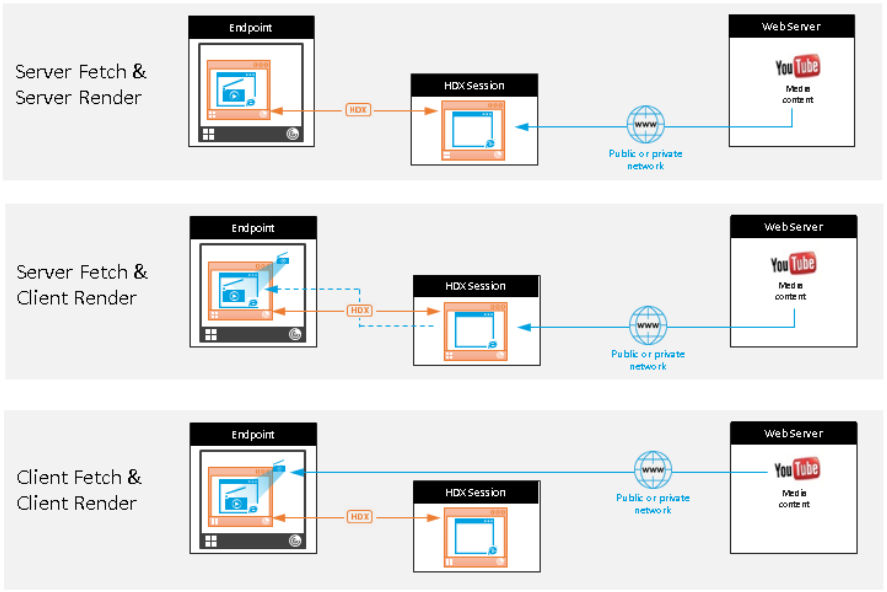
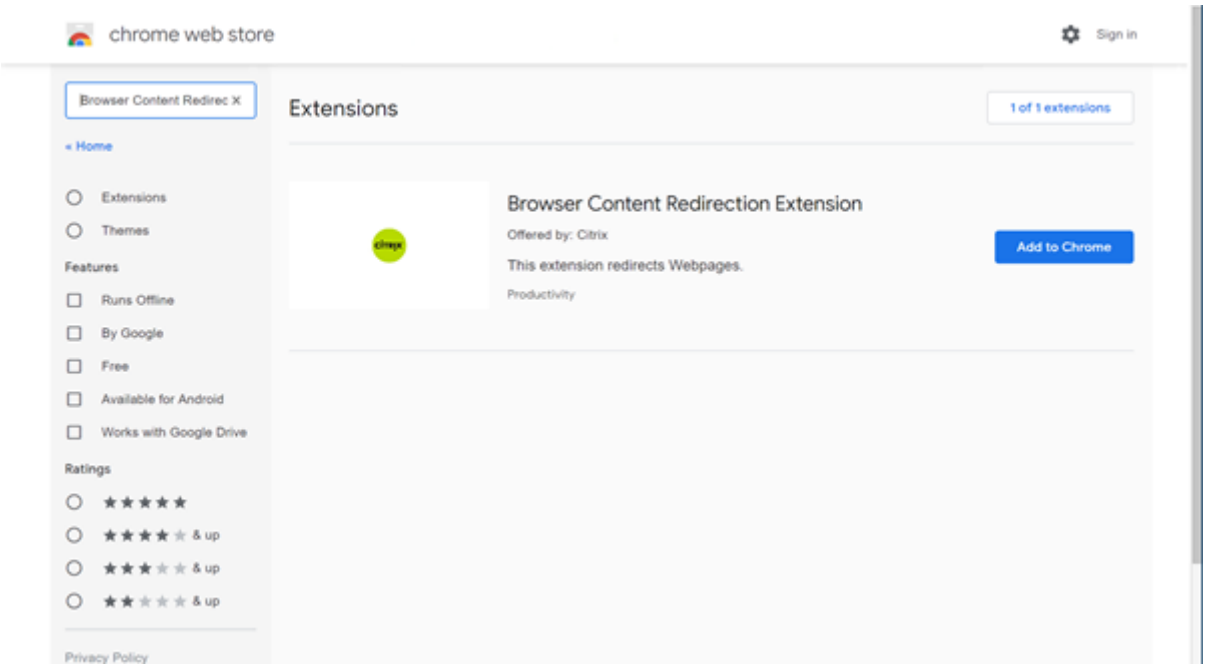
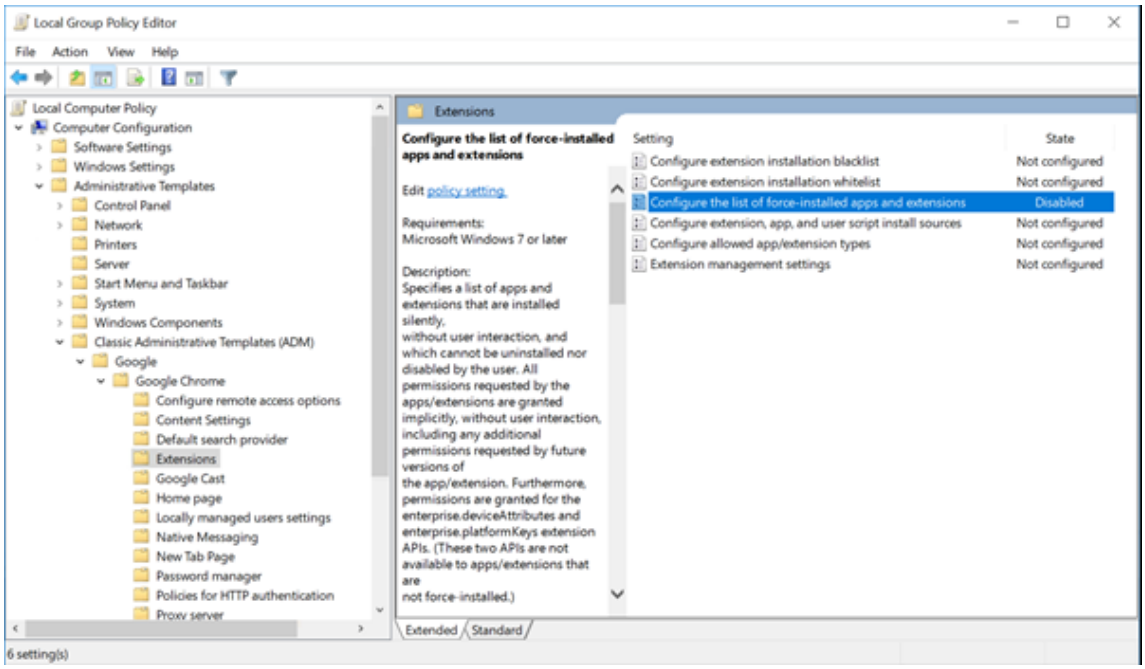
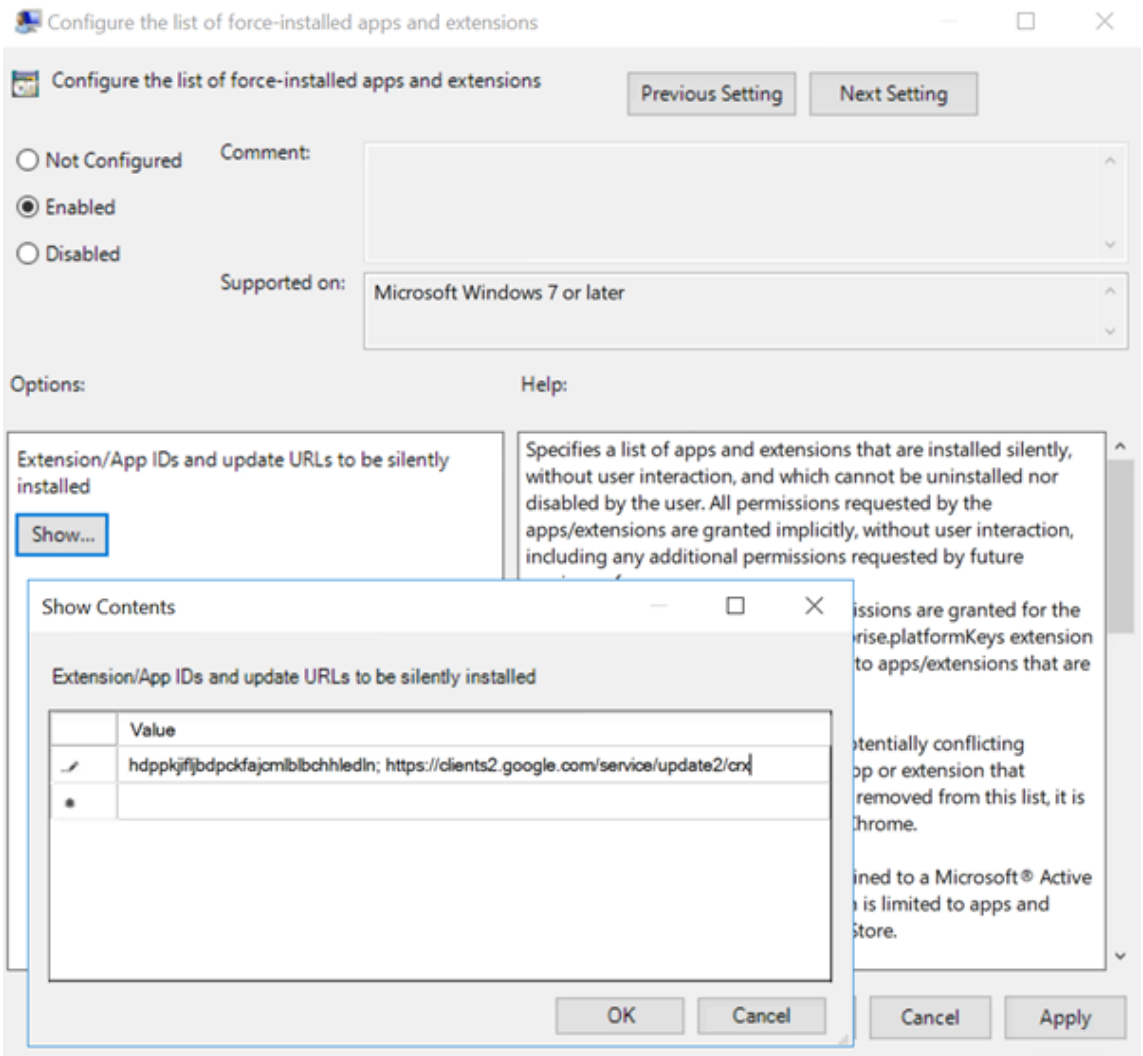
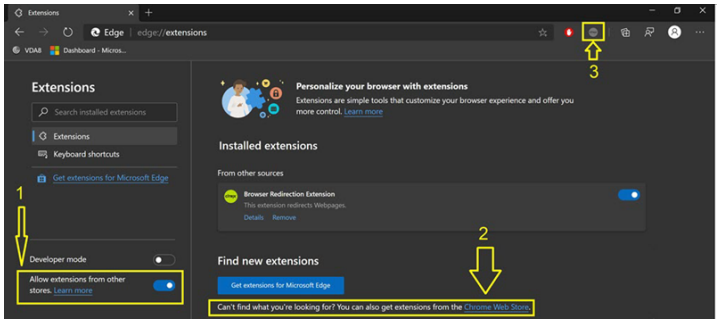
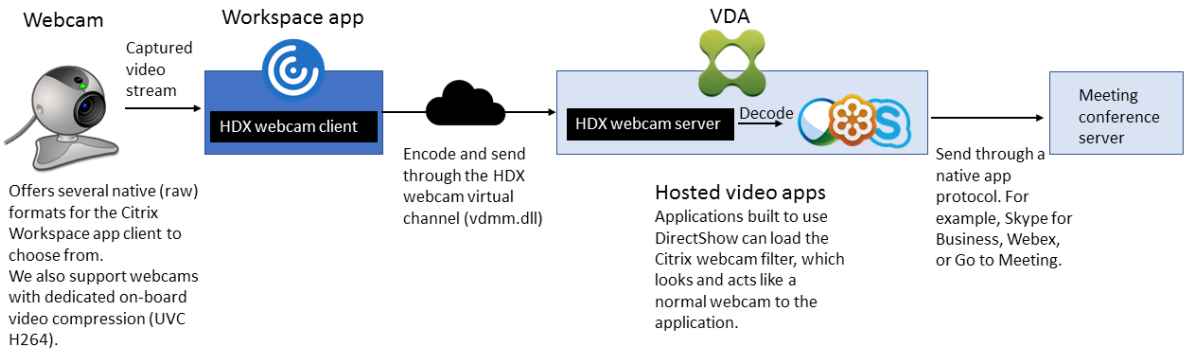
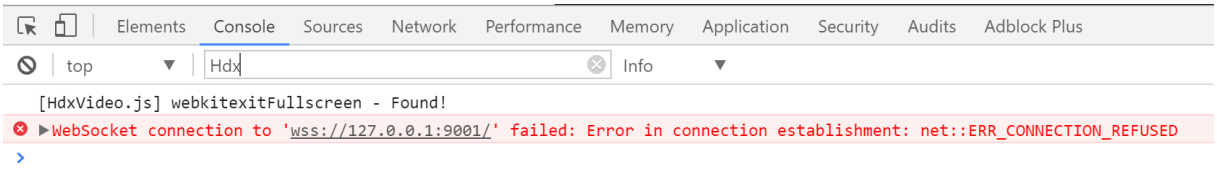
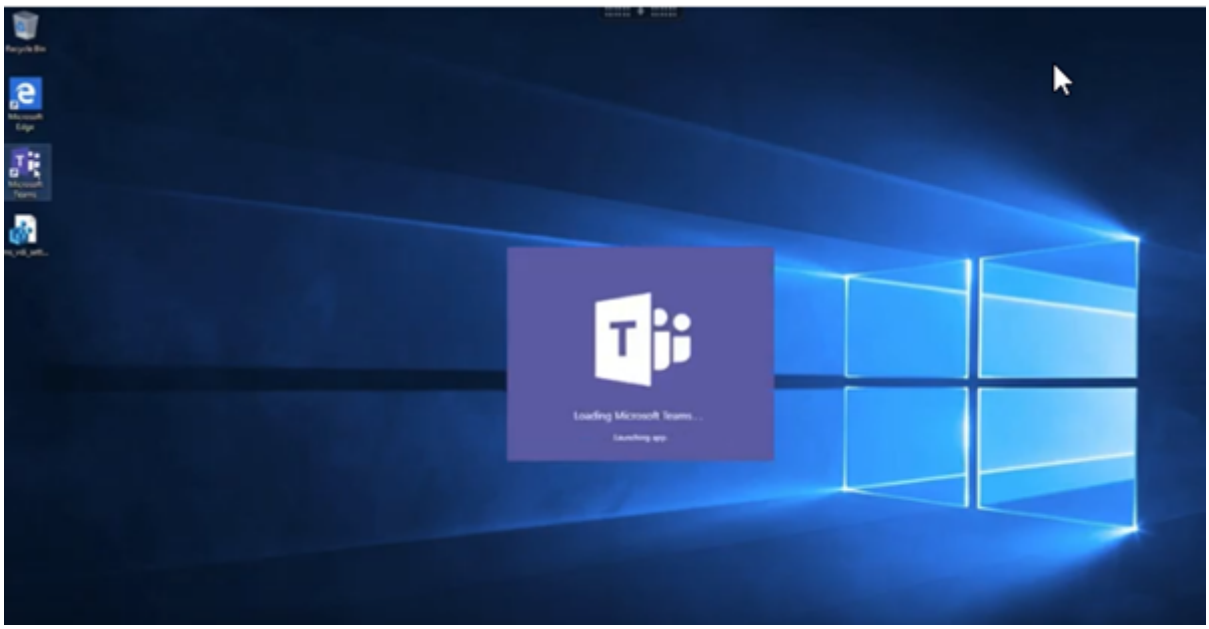
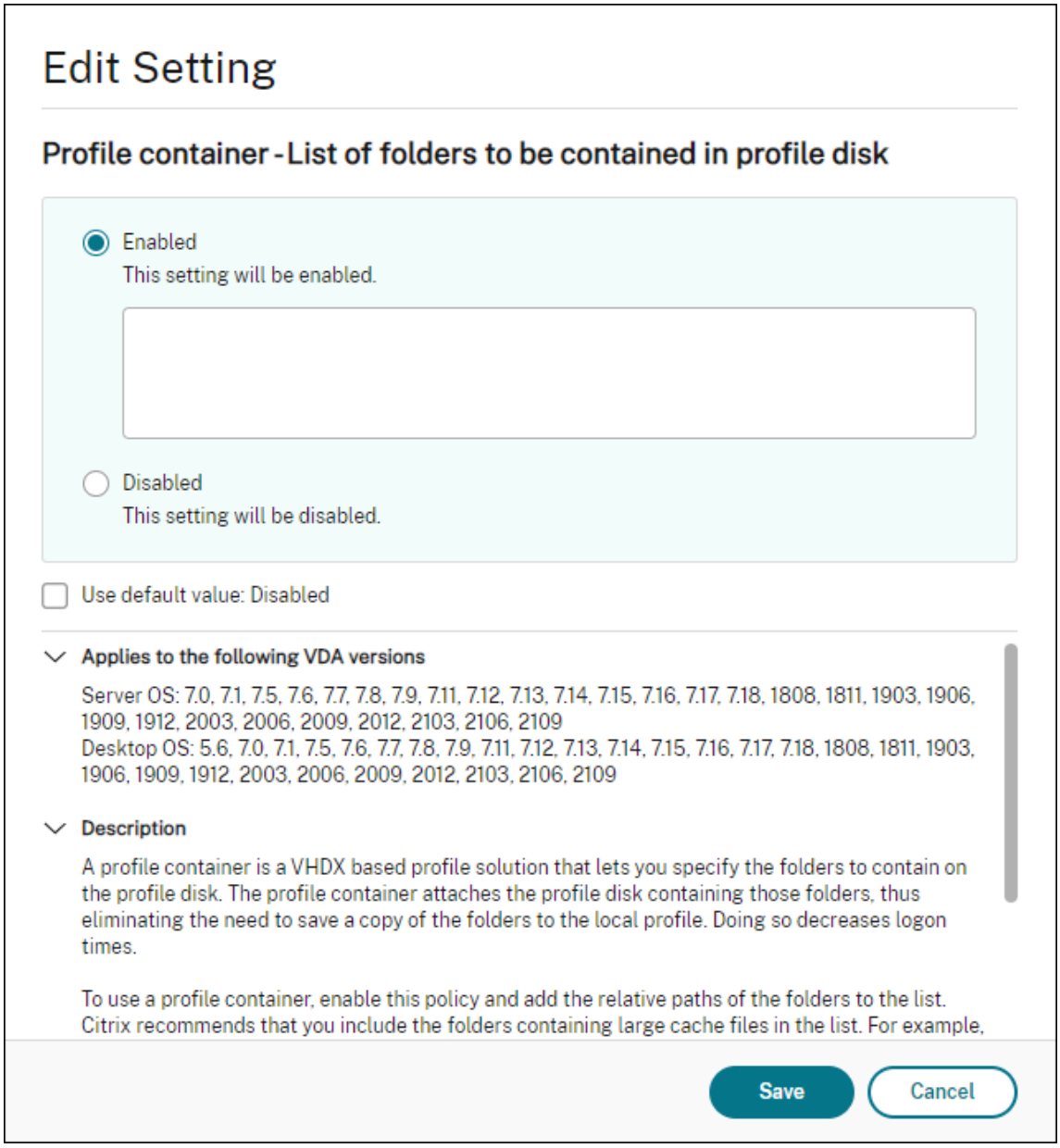
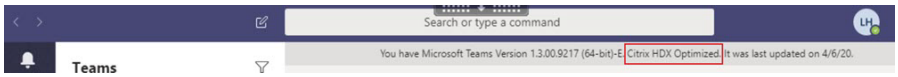
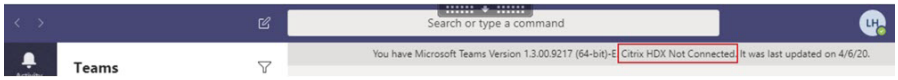
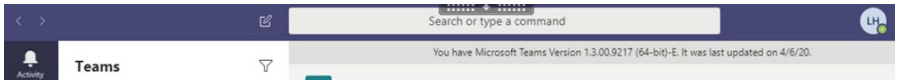
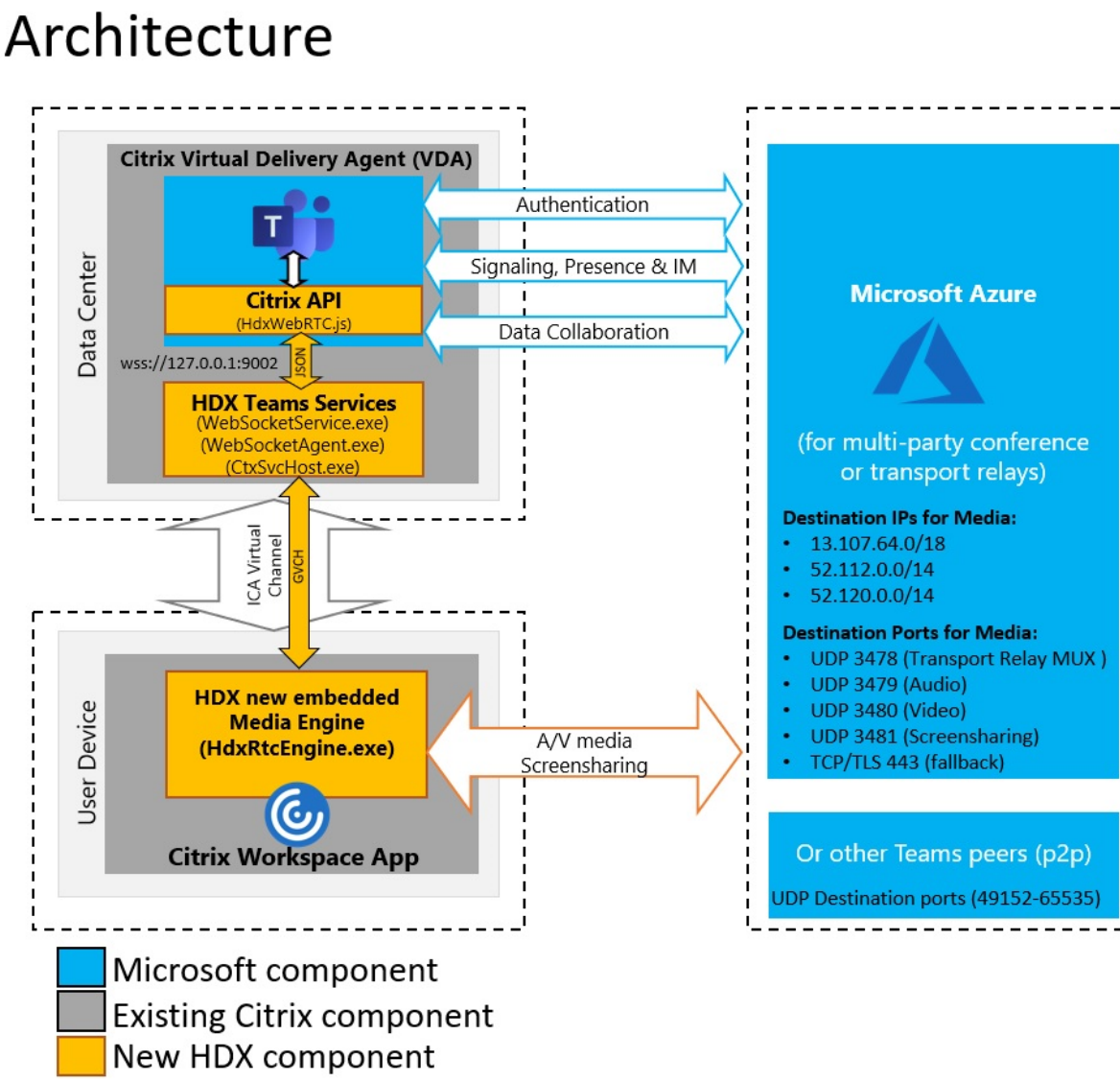
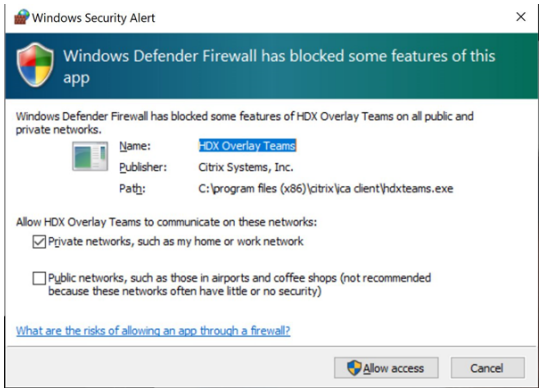
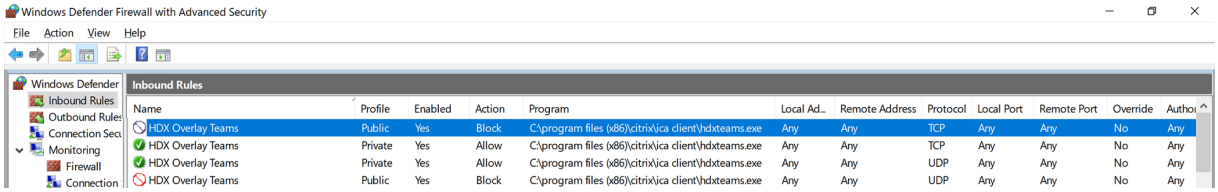
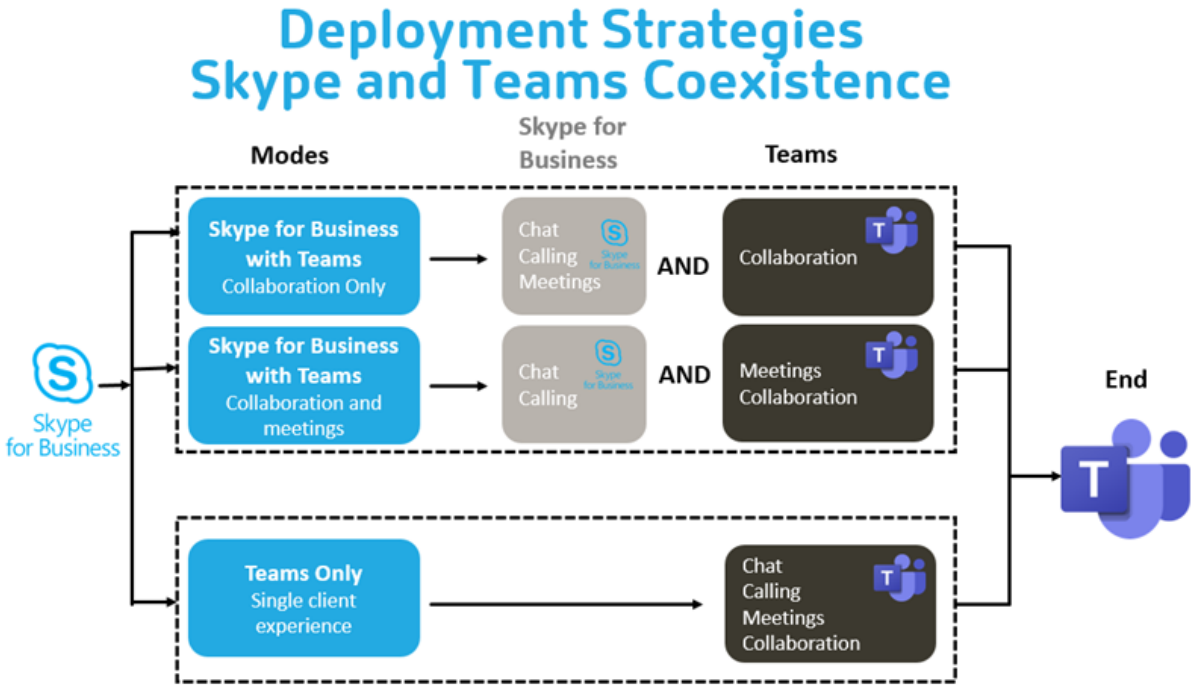
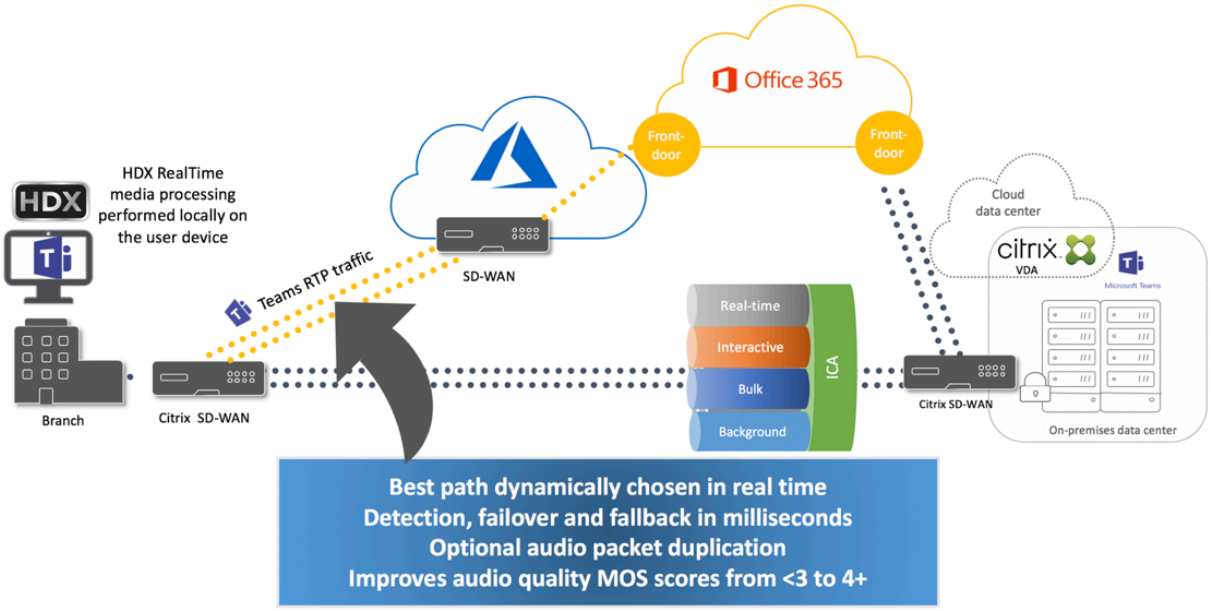
    - Edit Inventory
        - Create from existing
```



```
          -  Create new
          -  Remove

      -  Interaction
          -  Power off
          -  Power on
<!--NeedCopy-->
```

Microsoft Azure required permissions Image Portability requires your Azure service account to have the following permissions.

When the resource group to use for the Compositing Engine is specified (that is, in the *resourceGroup* property in a REST request or the *-AzureVmResourceGroup* parameter when using the Citrix.Workloads.Portability PowerShell commands) the following permissions are required at the scope of the resource group.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/delete
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/delete
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/read
<!--NeedCopy-->
```

When the resource group to use for the Compositing Engine is left unspecified the following permissions are required at the scope of the subscription.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
```



```
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```

The following permissions are required at the scope of the specified target resource group (that is, the resource group specified in the *targetDiskResourceGroupName* property in a REST request or the *-TargetResourceGroup* parameter when using PowerShell).

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

The following permissions are required at the scope of the specified virtual network resource group (that is, the resource group specified in the *virtualNetworkResourceGroupName* property in a REST request or the *-AzureVirtualNetworkResourceGroupName* parameter when using PowerShell).

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```

> **Important:**
>
> The `ceVmSku` option for 'prepare'and 'prepareAndPublish'jobs controls the type of Azure VM that the resulting managed disk is suitable for. You must select a ceVmSku with the same family and version as the VMs you intend to provision from the output image. The default value of `Standard_D2S_v3` is suitable to run on all v3 D family machines. Specifying machine SKUs that do not include a temp disk are not supported.

Google Cloud required permissions Image Portability requires your Google Cloud service account to have the following permissions:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
```



```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

AWS required permissions Image Portability requires that you attach a JSON policy document with the following configuration to the Identity and Access Management (IAM) user:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
```



```
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--NeedCopy-->
```

> **Note:**
>
> You might want to further reduce the scope of the Resource as needed.

Nutanix AHV required permissions Image Portability requires you to be a Cluster Admin in your Nutanix AHV configuration.

XenServer required permissions Image Portability requires you to have at a minimum the 'VM Admin'role for the pool the XenServer host is in.

Networking The Image Portability Service (IPS) creates a worker VM called the compositing engine (CE) to perform image operations. All of the connector appliances in the associated resource location must be able to communicate via HTTPS with the CE.
All communication between a connector appliance (CA) and the CE is initiated by the CA except for a single exception in the case of vSphere where there's bi-directional HTTPS communication between the CE and CA.

In cloud environments (Azure, AWS, Google Cloud) the CE is created with a private IP address. Hence the CE must be on the same virtual network as the CA or on a virtual network reachable from the CA.

Furthermore, for jobs that involve files on an SMB share (for example, export jobs), the CE must be on a network with connectivity to the SMB share.

See the Image Portability Service API documentation for details on how to specify the network to use for the CE in each supported platform.

For 'prepare'jobs, the operating system contained in the image is booted (on the CE) to do specialization and other tasks. If the image contains management or security agents that phone-in to a control server, these processes can interfere with the preparation process.

If the domain unjoin option is specified, network connectivity can affect the results. If the compositing engine VM can reach the Active Directory domain controller over the network, unjoin removes the computer account from the domain. This breaks the domain membership for the source VM from which the image was extracted.

Therefore, we recommend isolating the network provided for the operation from other network resources. This can be done by subnet isolation or with firewall rules. See Network isolation for details.

In some on-premises hypervisor environments the hypervisor might be configured with a TLS server certificate, which is either not trusted by the CA's set of trusted root certificate authorities, or doesn't match the server's host name. For such situations, **IPS provides job request** properties which can be used to work around the problem. See TLS certificates for details.

Network proxies If the network traffic between the CA and the internet traverses a proxy that performs TLS introspection, then it may be necessary to add the proxy's Root Certificate Authority (that is, the certificate the proxy uses to sign the TLS certificates it generates) to the CA's set of root certificate authorities. See Register your Connector Appliance with Citrix Cloud for further information.

Network isolation

- Azure

  In Azure, the CE is by default created with a network security group (NSG) attached to its NIC if the Azure service principal used in the operation has the necessary Azure permissions [1].

  - Microsoft.Network/networkSecurityGroups/join/action
  - Microsoft.Network/networkSecurityGroups/read
  - Microsoft.Network/networkSecurityGroups/write

    Otherwise the following permissions at the scope of the subscription if no explicit resource group is being used:

    * Microsoft.Network/networkSecurityGroups/delete

        * Microsoft.Network/networkSecurityGroups/join/action
        * Microsoft.Network/networkSecurityGroups/read
        * Microsoft.Network/networkSecurityGroups/write

    This NSG is configured to block all traffic in/out of the CE except for:

        - SMB (port 445) outbound
        - HTTPS (port 443) inbound
        - that required for internal Azure services

    The use of the NSG can be forced by setting the *networkIsolation* property in the job request to *true*. In this case, the job fails if the service principal used in the operation doesn't have the necessary permissions. Use of the NSG can be disabled by setting the *networkIsolation* property to *false*.

- AWS

In AWS to achieve network isolation of the CE, you can create a network security group or groups which block all undesired traffic and then in the job request, assign the security groups to the CE instance using the *securityGroupIds* request parameter which takes a list of security group Ids as value.

- Google Cloud

In Google Cloud to achieve network isolation of the CE, you can create firewall rules that block all undesired traffic and then apply those rules to the CE via network tags. IPS creates the CE with the network tag *compositing-engine* and you can assign it other network tags using the *networkTags* job request parameter which takes a list of tags as a value.

TLS certificates If the hypervisor's server certificate is signed by an authority not trusted by the CA, two alternate approaches can be used to resolve the problem.

1. Specify in the job request an additional Root Certificate Authority certificate to use in certificate verification. This certificate must be the Root Certificate Authority used to sign the hypervisor's server certificate.
2. Specify in the job request the SHA-1 fingerprint of the hypervisor's server certificate. In this case certificate validation is done by verifying that the SHA-1 fingerprint of the certificate returned by the hypervisor matches that provided in the job request. This method might not work if there's a TLS intercepting proxy between the CE and the hypervisor.

The job request parameters for the above, given respectively below for each platform, are:

- vSphere

    1. vCenterSslCaCertificate
    2. vCenterSslFingerprint

- Nutanix
    1. prismSslCaCertificate
    2. prismSslFingerprint
- XenServer
    1. xenSslCaCertificate
    2. xenSslFingerprint

See the Image Portability Service API documentation for further details.

Certificate validation errors can also occur when there's a mismatch between the hypervisor server's hostname and the hostname in its certificate. In this case, hostname matching can be disabled by setting the following parameter to *true* in the job request:

- vSphere
    - vCenterSslNoCheckHostname
- Nutanix
    - prismSslNoCheckHostname
- XenServer
    - xenSslNoCheckHostname

Related documentation

- Image Portability Service API documentation
- Connector Appliance for Cloud Services
- Google Cloud documentation
- Google Cloud service accounts
- Microsoft Azure app registration and authentication

1. If an explicit resource group is being used for the operation then the following permissions at the scope of the resource group:

Print

March 22, 2022

Managing printers in your environment is a multistage process:

1. Become familiar with printing concepts, if you are not already.
2. Plan your printing architecture. This includes analyzing your business needs, your existing printing infrastructure, how your users and applications interact with printing today, and which printing management model best applies to your environment.
3. Configure your printing environment by selecting a printer provisioning method and then creating policies to deploy your printing design. Update policies when new employees or servers are added.
4. Test a pilot printing configuration before deploying it to users.
5. Maintain your Citrix printing environment by managing printer drivers and optimizing printing performance.
6. Troubleshoot issues that may arise.

For complete information about printing in a Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) environment, begin with Print. From that article, you can move on to:

- Printing configuration examples
- Best practices
- Printing policies and preferences
- Provison printers
- Maintain the printing environment

Install the Universal Print Server on your print servers

1. Ensure that each print server has Microsoft Virtual C++ Runtime 2017, 32-bit and 64-bit installed.
2. Navigate to the Citrix Universal Print Server download page and click **Download File**.
3. Run one of the following commands on each print server:
    - For a 32-bit operating system: **UpsServer_x86.msi**.
    - For a 64-bit operating system: **UpsServer_x64.msi**.

After you install the Universal Print Server, configure it using the guidance in Provision printers.

Policies

March 18, 2023

Policies are a collection of settings that define how sessions, bandwidth, and security are managed for a group of users, devices, or connection types.

You can apply policy settings to VDAs or to users. You can edit settings in Web Studio or in the Active Directory Group policy objects (GPOs). You can specify filters (object assignments) for policies. If you do not specifically assign policies to filters, settings are applied to all user sessions.



You can apply policies on different levels of the network. Policy settings placed at the Organizational Unit GPO level take the highest precedence on the network. Policies at the Domain GPO level override policies on the Site Group Policy Object level. The Site Group Policy Object level overrides any conflicting policies on both the Microsoft and Citrix Local Policies levels.

All Citrix Site Policies are created and managed in the Web Studio console and stored in the Site Database. Group Policies are created and managed by using the Microsoft Group Policy Management Console (GPMC) and stored in the Active Directory. Microsoft Local Policies are created in the Windows Operating System and are stored in the registry.

Web Studio uses a Modeling Wizard to help administrators compare configuration settings within templates and policies to help eliminate conflicting and redundant settings.

Settings are merged according to priority and their condition. Any disabled setting overrides a lower-ranked enabled setting. Unconfigured policy settings are ignored and do not override lower-ranked settings.

Web Studio policies can also have conflicts with group policies in the Active Directory, which might override each other depending on the situation.

All policies are processed in the following order:

1. From the Citrix Workspace app, the end user logs on to a VDA using domain credentials.
2. Citrix policies are processed for the end user and for the VDA
3. Policies are applied in the following order:
    a) Local policies
    b) Site policies
    c) Domain policies
    d) OU (Organizational unit) policies

> **Note:**
>
> - All policies might not be present at the four levels. For most of the customers, only site policies are used. Local policies require the user to log on to VDA to edit policies. Hence, these policies are almost never used.
> - We do not support mixing Windows and Citrix policies in the same GPO.

For complete information about Citrix policies, see the following:

- Work with policies
- Policy templates
- Create policies
- Prioritize, model, compare, and troubleshoot policies
- Default policy settings
- Policy settings reference

  > **Note:**
  >
  > The policy settings references for Citrix DaaS are the same as the policy settings for Citrix Virtual Apps and Desktops. So, you can refer to the Policy settings reference section in the Citrix Virtual Apps and Desktops documentation for Citrix DaaS also.

Work with policies

May 15, 2023

Configure Citrix policies to control user access and session environments. Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple settings.

Tools for working with Citrix policies

- Studio - Policies that are created using Studio are stored in the site database, and the updates are pushed to the VDA either of the following happens:
  - When that VDA registers with Controller
  - When a user launches a session
- Group Policy Management Console -If your network environment uses Active Directory and you have permission to manage group policy, you can use the Group Policy Management Console (GPMC) to create and edit policies for your Site. In the console, you can configure Group Policy Objects (GPOs) with your desired settings and filters. These policies will take priority over policies configured in Studio. For more information, see CTX238166.

Policy processing order and precedence

Group policy settings are processed in the following order:

1. Citrix DaaS Site GPO (stored in the Site database)
2. Domain-level GPOs
3. Organizational Units

However, if different settings are applied for the same policy in two GPOs, the policy settings processed last overwrite the settings processed earlier. This configuration means that policy settings take precedence in the following order:

1. Organizational Units
2. Domain-level GPOs
3. Citrix DaaS site GPO (stored in the Site database)

When using multiple policies, you can prioritize policies that contain conflicting settings. For more information, see Prioritize, model, compare, and troubleshoot policies.

Workflow for Citrix policies

The process for configuring policies is as follows:

1. Create the policy.
2. Configure policy settings.
3. Assign the policy to machine and user objects.
4. Prioritize the policy.
5. Verify the effective policy by running the Citrix Group Policy Modeling wizard.

> **Note:**
>
> You open the Citrix Group Policy Modeling wizard by navigating to the **Policies > Modeling** tab and then clicking **Launch Modeling Wizard** in the **Actions** pane. The **Modeling** tab is available in Web Studio hosted in Citrix Cloud per customer request.

Navigate Citrix policies and settings

Policy settings are sorted into categories based on the functionality or feature they affect. For example, the Profile Management section includes policy settings for Profile Management.

- Computer settings (policy settings applying to machines) define the behavior of virtual desktops and are applied when a virtual desktop starts. These settings apply even when there are no active user sessions on the virtual desktop.
- User settings define the user experience. User settings are applied when a user connects or reconnects

To access policies, settings, or templates, select **Policies** in the Web Studio navigation pane.

- The **Policies** tab lists all policies. When you select a policy, tabs to the bottom display:
  - Overview - Lists name, priority, enabled/disabled status, and description
  - Settings - Lists all configured settings
  - Assigned To - Lists delivery group. You can edit or remove assigned to settings. Apply policy based on the delivery group membership of the desktop running the session. For more information, see Create policies.
- The **Templates** tab lists Citrix-provided and custom templates that you created. When you select a template, tabs to the bottom display:
  - Description (why you might want to use the template)
  - Settings (list of configured settings). For more information, see Policy templates.
  - The **Comparison** tab enables you to compare the settings in a policy or template with those settings in other policies or templates. For example, you might want to verify setting values to ensure compliance with best practices. For more information, see Prioritize, model, compare, and troubleshoot policies.
  - From the **Modeling** tab, you can simulate connection scenarios with Citrix policies. For more information, see Prioritize, model, compare, and troubleshoot policies.

  To search for a setting in a policy or template:

  1. Select the policy or template.
  2. Select **Edit policy** or **Edit Template** tab.

3. On the **Select Settings** page, begin to type the name of the setting.

You can refine your search by selecting:

- A category (for example, Bandwidth)
- The **View selected only** check box
- To search only the settings that have been added to the selected policy.

- To search for a setting within a policy:

1. Select the policy.
2. Select the **Settings** tab and type the name of the setting.

A policy, once created, is independent of the template used. You can use the **Description** field on a new policy to track the source template used.

Policy templates

October 27, 2022

Templates are a source for creating policies from a predefined starting point. Built-in Citrix templates, optimized for specific environments or network conditions, can be used as:

- A source for creating your own policies and templates to share between sites.
- A reference for easier comparison of results between deployments as you are able to quote the results, for example, "…when using Citrix template x or y…".
- A method for communicating policies with Citrix Support or trusted third parties. You can do it by importing or exporting templates.

Built-in Citrix templates

The following policy templates are available:

- **Very High Definition User Experience**. This template enforces default settings that maximize the user experience. Use this template in scenarios where multiple policies are processed in order of precedence.
- **High Server Scalability**. Apply this template to economize on server resources. This template balances user experience and server scalability. It offers a good user experience while increasing the number of users that you can host on a single server. This template does not use a video codec for compression of graphics and prevents server side multimedia rendering.

- **High Server Scalability-Legacy OS**. This High Server Scalability template applies only to VDAs running Windows Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode which is more efficient for those operating systems.
- **Optimized for NetScaler SD-WAN.** Apply this template for users working from branch offices with NetScaler SD-WAN for optimizing delivery of Citrix Virtual Desktops. (NetScaler SD-WAN is the new name for CloudBridge).
- **Optimized for WAN**. This template intends for task workers in branch offices who uses shared WAN or remote locations with low bandwidth connections. The workers access applications with graphically simple user interfaces and little multimedia content. This template trades off video playback experience and some server scalability for optimized bandwidth efficiency.
- **Optimized for WAN-Legacy OS**. This template applies only to VDAs running Windows Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode which is more efficient for those operating systems.
- **Security and Control**. Use this template in environments with low tolerance to risk, to minimize the features enabled by default in Citrix DaaS. This template includes settings that disable access to the following:

  - Printing
  - Clipboard
  - Peripheral devices
  - Drive mapping
  - Port redirection
  - Flash acceleration on user devices

  Applying this template might use more bandwidth and reduce user density per server.

While we recommend using the built-in Citrix templates with their default settings, there are settings that do not have a specific recommended value. For example, **Overall session bandwidth limit**, included in the Optimized for WAN templates. In this case, the template exposes the setting so the administrator understands this setting is likely to apply to the scenario.



Consider that you are working with a deployment (policy management and VDAs) earlier than XenApp and XenDesktop 7.6 FP3. Also, require High Server Scalability and Optimized for WAN templates. In this case, use the Legacy OS versions of these templates when they apply.

> **Note:**
>
> Citrix creates and updates built-in templates. You cannot modify or delete these templates.

Create and manage templates using Web Studio

To create a template based on a template:

1. Select **Policies** in the Web Studio navigation pane.



2. Select the **Templates** tab and then select the template from which you create the template.

3. Select **Create Template** tab. The **Select Settings** screen appears.



4. Select and configure the policy settings to include in the template.
5. Click **Next**. The **Summary** screen appears.
6. Enter a name for the template.
7. Click **Finish**. The new template appears on the Templates tab

To create a template based on a policy:

1. Select **Policies** in the Web Studio navigation pane.
2. Select the **Policies** tab and then select the policy from which you create the template.



3. Click **More** tab.
4. Select **Save as Template**. The **Select Settings** screen appears.



5. Select and configure any new policy settings to include in the template.
6. Click **Next**. The **Summary** screen appears.



7. Enter a name and description for the template, and then click **Finish**.

Create policies

October 18, 2023

Before creating a policy, decide which group of users or devices it might affect. You might want to create a policy that is based on user job function, connection type, user device, or geographic location.

If you already created a policy that applies to a group, consider editing that policy instead of creating another policy. After editing the policy, configure the appropriate settings. Avoid creating a policy solely to enable a specific setting or to exclude the policy from applying to certain users.

When you create a policy, you can base it on settings in a policy template and customize settings as needed. You can also create it without using a template and add all the settings you need.

In Citrix Studio, new policies created are set to Disabled unless the **Enable policy** check box is explicitly checked.

During policy creation and when configuring the settings, the system provides an option to view the settings type. You can view the following settings type:

- All settings - View all settings for all VDA versions
- Current settings only - View settings for only the current VDA versions
- Legacy settings only - View settings for only the deprecated VDA versions

To view the settings while configuring the settings:

1. Log in to DaaS Premium.
2. In the left-navigation, click **Policies**.
3. In the **Policies** tab, click **Create Policy**.
4. In the **Select Settings** table, click the drop-down next to **Settings**.
5. Select one of the following options from the drop down:
    - All settings - View all settings for all VDA versions
    - Current settings only - View settings for only the current VDA versions
    - Legacy settings only - View settings for only the deprecated VDA versions
6. The Settings table lists the settings available based on the previous step.

Policy settings

Policy settings can be enabled, disabled, or not configured. By default, policy settings aren't configured, which means they aren't added to a policy. Settings are applied only when they're added to a policy.

When configuring the settings for creating or editing a policy, if all delivery groups are disabled, then the system displays a **None of the elements in this filter is enabled** warning notification sign. If at least one delivery group is enabled, the system does not display the warning sign.

To view the warning while creating a policy:

1. Log in to DaaS Premium.

2. In the left-navigation, click **Policies**.
3. In the **Policies** tab, click **Create Policy**.
4. In the **Select Settings** table, select any setting and click **Next**.
5. In the **Assign Policy To** table, select a filter from the drop-down.
6. Unselect the **Enable** checkbox and click **Save**.

> **Note:**
>
> Not all filters support unselecting the **Enable** checkbox.
> In the **Filters** table, the filter displays the warning.

To view the warning while editing a policy:

1. Log in to DaaS Premium.
2. In the left-navigation, click **Policies**.
3. In the **Policies** tab, select any of the policies listed and click **Edit Policy**.
4. In the **Edit Policy** page, click **Assign Policy To** in the left navigation.
5. In the **Filter** table, select or click **Edit** for the required filter:
   - If a filter does not have the **Edit** button, select the filter.
   - If a filter has the edit button, click **Edit**.
6. Unselect the **Enable** option and click **Save**.

> **Note:**
>
> Not all filters support unselecting the **Enable** checkbox.
> In the **Filters** table, the filter displays the warning.

Some policy settings can be in one of the following states:

```
- Allowed or Prohibited allows or prevents the action controlled by
  the setting. Sometimes users are allowed or prevented from managing
  the setting's action in a session. For example, if the menu
  animation setting is set to Allowed, users can control menu
  animations in their client environment
- Enabled or Disabled turns the setting on or off. If you disable a
  setting, it is not enabled in lower-ranked policies.
```

In addition, some settings control the effectiveness of dependent settings. For example, Client drive redirection controls whether users are allowed to access the drives on their devices. Both this setting and the **Client network drives** setting must be added to the policy to allow users to access their network drives. If the **Client drive redirection** setting is disabled, users can't access their network drives, even if the **Client network drives** setting is enabled.

In general, policy setting changes that impact machines go into effect either when the virtual desktop restarts or when a user logs on. Policy setting changes that impact users go into effect the next time users log on.

For some policy settings, you can enter or select a value when you add the setting to a policy. You can limit the configuration of the setting by selecting Use default value. This selection disables the configuration of the setting and allows only the setting's default value to be used when the policy is applied. This selection is regardless of the value that was entered before selecting Use default value.

As best practice:

- Assign policies to groups rather than individual users. If you assign policies to groups, assignments are updated automatically when you add or remove users from the group.
- Disable unused policies. Policies with no settings added create unnecessary processing.

Policy assignments

When creating a policy, you assign it to certain users and machine objects. That policy is applied to connections according to specific criteria or rules. In general, you can add as many assignments as you want to a policy, based on a combination of criteria. If you specify no assignments, the policy is applied to all connections.

If you do not specify any assignments, or specify assignments but disable them, the policy is applied to **all** connections.

> **Note:**
>
> Policy assignments are also known as policy filters. For additional information, see the following topics:
>
> - Create, modify, or delete a filter for a policy
> - How do filters get applied?

The following table lists the available assignments:

Assignment name	Applies a policy based on
Access Control	Access control conditions through which a client is connecting. *Connection type* - Whether to apply the policy to connections made with or without NetScaler Gateway. *NetScaler Gateway farm name* - Name of the NetScaler Gateway virtual server. *Access condition* - Name of the end point analysis policy or session policy to use.
Citrix SD-WAN	Whether a user session is launched through Citrix SD-WAN. **Note:** You can add only one Citrix SD-WAN assignment to a policy.
Client IP Address	IP address of the user device used to connect to the session: IPv4 examples: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6 examples: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Client Name	Name of the user device. Exact match: ClientABCName. Using wildcard: Client*Name.
Delivery Group	Delivery Group membership.
Delivery Group type	Type of desktop or application: private desktop, shared desktop, private application, or shared application.
Organizational Unit (OU)	Organizational unit.
Tag	Tags. **Note:** Apply this policy to all tagged machines. Application tags aren't included.
User or Group	User or group name.

When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy. Any policy setting that is disabled takes precedence over a lower-ranked setting that is enabled. Policy settings that are not configured are ignored.

> **Important:**
>
> When configuring both Active Directory and Citrix policies using the Group Policy Management Console, assignments and settings might not be applied as expected. For more information, see CTX127461.

A policy named "Unfiltered"is provided by default.

- If you use Web Studio to manage Citrix policies, the settings you add to the Unfiltered policy are applied to all servers, desktops, and connections in a Site.
- The Sites and connections must be within the scope of the Group Policy Objects (GPOs) that includes the policy. For example, the Sales OU includes a GPO called Sales-US that includes all members of the US sales team. The Sales-US GPO is configured with an Unfiltered policy that includes several user policy settings. When the US Sales manager logs on to the Site, the settings in the Unfiltered policy are automatically applied to the session. This configuration is because the user is a member of the Sales-US GPO.

An assignment's mode determines if the policy is applied only to connections that match all the assignment criteria. If the mode is set to Allow (the default), the policy is applied only to connections that match the assignment criteria. If the mode is set to Deny, the policy is applied if the connection does not match the assignment criteria. The following examples illustrate how assignment modes affect Citrix policies when multiple assignments are present.

- **Example: Assignments of like type with differing modes** - In policies with two assignments of the same type, one set to Allow and one set to Deny, the assignment set to Deny takes precedence, provided the connection satisfies both assignments. For example:

  Policy 1 includes the following assignments:

  - Assignment A specifies the Sales group. The mode is set to Allow.
  - Assignment B specifies the Sales manager's account. The mode is set to Deny.

  Because the mode for Assignment B is set to Deny, the policy isn't applied when the Sales manager logs on to the Site, even though the user is a member of the Sales group.

- **Example: Assignments of differing type with like modes** - In policies with two or more assignments of differing types, set to Allow, the connection must satisfy at least one assignment of each type for the policy to be applied. For example:

  Policy 2 includes the following assignments:

  - Assignment C is a User assignment that specifies the Sales group. The mode is set to Allow.
  - Assignment D is a Client IP Address assignment that specifies 10.8.169.* (the corporate network). The mode is set to Allow.

  When the Sales manager logs on to the Site from the office, the policy is applied because the connection satisfies both assignments.

  Policy 3 includes the following assignments:

  - Assignment E is a User assignment that specifies the Sales group. The mode is set to Allow.

- Assignment F is an Access Control assignment that specifies NetScaler Gateway connection conditions. The mode is set to Allow.

When the Sales manager logs on to the Site from the office, the policy isn't applied because the connection doesn't meet the requirements of Assignment F.

Policy sets (Preview)

May 6, 2024

Policy sets are objects in Citrix DaaS which aggregates policies to allow for simplified, role-based access, and easy management. You can create policy sets to mirror logical divisions in your administrator team and company. For example, you can create a policy set for each geographic region, business-unit, or for specific use case. Once created, scopes and delivery groups are assigned to policy sets so that only authorized administrators can manage the policies that apply to their relevant users and machines.

Benefits

- Role-based access control for distributed administrator teams
- Simplified mergers, acquisitions, and consolidations
- Limited fault domain
- Multitenant support for policies

Enable policy sets

From the **Manage** tab of Citrix DaaS, navigate to **Settings** and turn on the **Policy sets** setting.



> **Note:**

> You must enable policy sets before creating a policy set.

Feature comparison

Before applying policy sets	After applying policy sets
Policies, settings, filters, and policy priorities for the entire site are configured in one place within Citrix Studio.	Policies, settings, filters, and policy priorities are configured separately for each policy set.
If you manage one policy, you must manage every policy.	Full administrators can delegate to lower-level admins the ability to manage a particular policy set on an individual basis.
Policies in large and distributed environments become complex and difficult to manage.	Policies in large and distributed environments can be divided and managed easily.

How do policy sets work?

General overview

- Policy sets are assigned to delivery groups
- Policy sets have one or multiple scopes
- Delivery groups with no policy set assigned receive the default policy set
- A delivery group can have only one policy set assigned to it
- Multiple delivery groups can use the same policy set
- Even though policy sets are assigned to delivery groups, the policies maintain their filters

For more information, see How do filters get applied?. There is no change in the way that policy assignments or policy filters work for policy sets. That is, they work the same way as they do for policies.

Default policy set

- When the policy set setting is turned on, all existing policies are grouped within the default policy set
- Every delivery group receives the default policy set unless the administrator team creates a policy set and assigns that to a delivery group.
- Once a delivery group has a different policy set assigned to it, it will no longer get policies from the default policy set

Policy set creation

Policy sets can be created in the following two ways:

- Create policy set - this action creates an empty policy set
- Clone policy set - this action creates a policy set based on an existing policy set

Create policy sets

1. On the Citrix DaaS configuration page, click the **Manage** tab.
2. Click the **Policies** tab.



3. Select **Create Policy Set**. The **Introduction** tab appears.
4. Click **Next** or click **Name and Description** tab.
5. Enter the name and description of the policy set.
6. Click **Next** or click the **Assignments** tab.
7. Select one or more delivery groups to which you want to assign the policy set.
8. Click **Next** or click **Scopes** tab.
9. Select the scopes of the policy set.
10. Click **Create**. The policy set is created with the defined assignment and scope.

Clone policy sets

1. On the Citrix DaaS configuration page, click the **Manage** tab.
2. Click the **Policies** tab.
3. Select **Clone Policy Set**.
4. Modify the name of the policy set.
5. Modify or create assignments for the policy set and click **Next**.
6. Select or deselect policies to include in the cloned policy set.

7. Modify the scope of the policy.
8. Click **Create**. The policy set is created.

Edit policy sets

1. On the Citrix DaaS configuration page, click the **Manage** tab.
2. Click the **Policies** tab.
3. Select **Edit Policy Set**.
4. Modify the name of the policy set and click **Next**.
5. Modify or create assignments for the policy set and click **Next**.
6. Modify the scope of the policy.
7. Click **Create**.

Policy set assignment

Policy sets are assigned to delivery groups. You can configure assignments when the policy set is created or edited. You can also configure assignments when delivery groups are created or edited.

Policy set scopes

Administrators can define the scope of the policy set so that only authorized administrators can view or edit it. You can configure scopes when the policy set is created or edited.

With the introduction of Policy Sets, you can also create and manage Citrix Policy using API. For more information, see How to create a policy set in Citrix DaaS.



Prioritize, model, compare, and troubleshoot policies

July 1, 2024

You can use policies to customize your environment to meet the needs of users based on the following:

- Job functions
- Geographic locations
- Connection types

For example, for improved security, place restrictions on user groups who regularly interact with sensitive data.

You can also create a policy that prevents users from saving sensitive files on their local client drives. You can create another policy for users in the user group who needs to access to their local drives. You then rank the two policies to control which one takes precedence. When using many policies, you must determine:

- How to prioritize the policies
- How to create exceptions
- How to view the effective policy when policies conflict

Prioritize policies

Prioritizing policies allows you to define the precedence of policies when they contain conflicting settings. The identification of all policies that match the assignments for the connection happens when a user signs on to the system. The identified policies and their associated settings are sorted into priority order. Each setting is applied according to the priority ranking of the policy.

You can prioritize policies by giving them different priority numbers in the **Web Studio**. By default, a new policy gets the lowest priority. If there are conflicts among settings of policies, a policy with a higher priority overrides a policy with a lower priority. A policy with the priority number of 1 is the highest priority policy. Policy settings are merged according to the following:

- Priorities of the policies
- Conditions specified in the filters of the policies

To prioritize policies, follow these steps:

1. Select **Policies** in the left pane.
2. On the **Policies** tab, select **Change Policy Priorities** in the action bar. The **Change Policy Priorities** page appears.

3. In the priority list, use the following ways to change the priority for a policy:
    - Drag the policy to a desired position.
    - To move it up or down by one position, click the Up or Down arrow icon respectively.
    - To move it to the top or bottom of the list, click the Top or Bottom arrow icon respectively.
    - To change the priority number, click the **Edit** icon, enter a number as needed, and then click **Save**.
4. Click **Save**.

Exceptions

When you create policies and use filters to assign them to groups of users, user devices, or machines, you might find that some members of the group need exceptions to some policy settings. You can create exceptions by:

- Creating a policy only for specific group members who need exceptions and then ranking that policy higher than the policy for the entire group
- Using the *Deny* mode for an assignment added to the policy

An assignment with the mode set to *Deny* applies a policy only to connections that don't match the assignment criteria. For example, a policy includes the following assignments:

- *Assignment A* is a client IP address assignment that specifies the range `208.77.88.*`. The mode is set to *Allow*.
- *Assignment B* is a user assignment that specifies a particular user account. The mode is set to *Deny*.

The policy applies to all users who signs n to the site with IP addresses in the range that is specified in *Assignment A*. However, the policy doesn't apply to the user who signs on to the site with the user account specified in *Assignment B*.

> **Note:**
>
> During the **Assign Policy** step, if you deselect the enable check box, assignment is disabled for the policy. If the only assignment for the policy is disabled, it is the same as not having any assignment, and, therefore, the policy applies to all objects in the site.

Determine which policies apply to a connection

Sometimes a connection does not respond as expected because multiple policies apply. If a higher priority policy applies to a connection, it can override the settings you configure in the original policy.

You can calculate the **Resultant Set of Policy** and determine how the final policy settings are merged for a connection.

You can calculate the **Resultant Set of Policy** in the following ways:

- Use the **Citrix Group Policy Modeling Wizard** to simulate a connection scenario and discern how Citrix policies might be applied. You can specify conditions for a connection scenario such as:
  - Users
  - Citrix policy assignment evidence values
- Use **Group Policy Results** to create a report describing the Citrix policies in effect for a given user and Virtual Delivery Agent (VDA).

Site policy settings created using **Web Studio** aren't included in the **Resultant Set of Policy** when you run the **Citrix Group Policy Modeling** wizard from the **Group Policy Management** console. To verify that you obtain the most comprehensive **Resultant Set of Policy**, Citrix recommends starting the **Citrix Group Policy Modeling** wizard from the **Web Studio**, unless you create policies using only the **Group Policy Management** console.

Use the policy modeling wizard

Policy modeling helps you simulate enabled policies with filters for planning and testing purposes. Only enabled policies with filters are modeled. Disabled policies are never applied and enabled policies without filters are always applied.

Perform the following steps to open the **Policy Modeling** wizard:

1. In Full Configuration, select **Policies**.
2. Select the **Modeling** tab.
3. Select **Policy Modeling** in the action bar.
4. Read the **Introduction** page and click **Next**.
5. Select users or computers. You can browse for containers or specific users or computers. Click **Next**.
6. Choose your filter evidence. You can optionally get more granular with your simulation by entering additional details, such as **Delivery group**, **Tags**, **Client IP address**, and so on. Click **Next**.
7. Review the summary of your selections and click **Run**.

After you click **Run**, the wizard generates a report of the modeling results. While viewing this report, you can:

- Select if you would like to view **All settings**, **Computer settings**, or **User settings** in the drop-down menu.

- Use the search bar to look for specific settings.
- Click a specific setting to view details of that setting. For example, if all user settings were not applied for a specific policy, the **Details** pane shows you the reason why the settings were not applied.
- Click **Export** to export the modeling results in JSON format, HTML format, or both.

After running policy modeling, more options become available to you. You can:

- **View Modeling Report**: This opens the same modeling report from above so you can view it again or export it.
- **Rerun Policy Modeling**: This allows you to rerun policy modeling with the same set of criteria selected previously and generate new modeling results. This is useful if some policies have changed and you would like to see how those changes affect your current model.
- **Delete Modeling Report**: This deletes the current modeling report.

Compare policies and templates

You can compare the settings in a policy or template with the settings of the other policies or templates. For example, you might want to verify setting values to maintain compliance with best practices. You might also want to compare settings in a policy or template with the default settings.

1. Select **Policies** in the **Web Studio** navigation pane.
2. Click the **Comparison** tab and then click **Select**.
3. Choose the policies or templates to compare. To include default values in the comparison, select the **Compare to default settings** check box.
4. After you click **Compare**, the configured settings are displayed in columns.
5. To see all settings, select **Show All Settings**. To return to the default view, select **Show Common Settings**.

Troubleshoot policies

Users, IP addresses, and other assigned objects can have multiple policies that apply simultaneously. This scenario can result in conflicts where a policy might not behave as expected. When you run the **Citrix Group Policy Modeling** wizard, you might discover that no policies apply to user connections. In such a scenario, policy settings doesn't apply to the users who connect to their applications and desktops under conditions that match the evaluation criteria of the policy. This situation happens when:

- No policies have assignments that match the evaluation criteria of the policy.
- Policies that match the assignment don't have any settings configured.
- Policies that match the assignment are disabled.

If you want to apply policy settings to the connections that meet the specified criteria, make sure:

- The policies you want to apply to those connections are enabled.
- The policies you want to apply have the appropriate settings configured.

> **Note:**
>
> In the second hop of double-hop scenarios, consider that a single-session OS VDA connects to multi-session OS VDA. In this case, Citrix policies act on the single-session OS VDA as if it were the user device. For example, consider policies are set to cache images on the user device. In this example, the images cached for the second hop in a double-hop scenario are cached on the single-session OS VDA machine.

Director

Non-administrators can use the Director to view policies that applies to a user session.

HDX overview

May 9, 2023

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Citrix HDX represents a broad set of technologies that deliver a high-definition experience to users of centralized applications and desktops, on any device and over any network.



HDX is designed around three technical principles:

- Intelligent redirection
- Adaptive compression
- Data de-duplication

Applied in different combinations, they optimize the IT and user experience, decrease bandwidth consumption, and increase user density per hosting server.

- **Intelligent redirection** - Intelligent redirection examines screen activity, application commands, endpoint device, and network and server capabilities to instantly determine how and where to render an application or desktop activity. Rendering can occur on either the endpoint device or hosting server.
- **Adaptive compression** - Adaptive compression allows rich multimedia displays to be delivered on thin network connections. HDX first evaluates several variables, such as the type of input, device, and display (text, video, voice, and multimedia). It chooses the optimal compression codec and the best proportion of CPU and GPU usage. It then intelligently adapts based on each unique user and basis. This intelligent adaptation is per user, or even per session.



- **Data de-duplication** - De-duplication of network traffic reduces the aggregate data sent between client and server. It does so by taking advantage of repeated patterns in commonly accessed data such as bitmap graphics, documents, print jobs, and streamed media. Caching these patterns allows only the changes to be transmitted across the network, eliminating duplicate traffic. HDX also supports multicasting of multimedia streams, where a single transmission from the source is viewed by multiple subscribers at one location, rather than a one-to-one connection for each user.

For more information, see Boost productivity with a high-definition user workspace.

At the device

HDX uses the computing capacity of user devices to enhance and optimize the user experience. HDX technology ensures that users receive a smooth, seamless experience with multimedia content in their virtual desktops or applications. Workspace control enables users to pause virtual desktops and applications and resume working from a different device at the point where they left off.

On the network

HDX incorporates advanced optimization and acceleration capabilities to deliver the best performance over any network, including low-bandwidth and high-latency WAN connections.

HDX features adapt to changes in the environment. The features balance performance and bandwidth. They apply the best technologies for each user scenario, whether the desktop or application is accessed locally on the corporate network or remotely from outside the corporate firewall.

In the data center

HDX uses the processing power and scalability of servers to deliver advanced graphical performance, regardless of the client device capabilities.

HDX channel monitoring provided by Citrix Director displays the status of connected HDX channels on user devices.

HDX Insight

HDX Insight is the integration of NetScaler Network Inspector and Performance Manager with Director. It captures data about ICA traffic and provides a dashboard view of real time and historical details. This data includes client-side and server-side ICA session latency, bandwidth use of ICA channels, and the ICA round-trip time value of each session.

You can enable NetScaler to use the HDX Insight virtual channel to move all the required data points in an uncompressed format. If you disable this feature, the NetScaler device decrypts and decompresses the ICA traffic spread across various virtual channels. Using the single virtual channel lessens complexity, enhances scalability, and is more cost effective.

Minimum requirements:

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp and XenDesktop 7.17
- NetScaler version 12.0 Build 57.x
- Citrix Workspace app for Windows 1808
- Citrix Receiver for Windows 4.10
- Citrix Workspace app for Mac 1808
- Citrix Receiver for Mac 12.8

Enable or disable HDX Insight virtual channel

To disable this feature, set the Citrix NetScaler Application Flow service properties to Disabled. To enable, set the service to Automatic. In either case, we recommend that you restart the server machine

after changing these properties. By default, this service is enabled (Automatic).



Experience HDX capabilities from your virtual desktop

- To see how browser content redirection, one of four HDX multimedia redirection technologies, accelerates delivery of HTML5 and WebRTC multimedia content:

  1. Download the Chrome browser extension and install it on the virtual desktop.
  2. To experience how browser content redirection accelerates the delivery of multimedia content to virtual desktops, view a video on your desktop from a website containing HTML5 videos, such as YouTube. Users don't know when browser content redirection is running. To see whether browser content redirection is being used, drag the browser window quickly. You'll see a delay or out of frame between the viewport and the user interface. You can also right-click on the webpage and look for **About HDX Browser Redirection** in the menu.

- To see how HDX delivers high definition audio:

  1. Configure your Citrix client for maximum audio quality; see the Citrix Workspace app documentation for details.
  2. Play music files by using a digital audio player (such as iTunes) on your desktop.

HDX provides a superior graphics and video experience for most users by default, and configuration isn't required. Citrix policy settings that provide the best experience for most use cases are enabled by default.

- HDX automatically selects the best delivery method based on the client, platform, application, and network bandwidth, and then self-tunes based on changing conditions.
- HDX optimizes the performance of 2D and 3D graphics and video.
- HDX enables user devices to stream multimedia files directly from the source provider on the internet or intranet, rather than through the host server. If the requirements for this client-side

content fetching are not met, media delivery falls back to server-side content fetching and multimedia redirection. Usually, adjustments to the multimedia redirection feature policies aren't needed.
- HDX delivers rich server-rendered video content to virtual desktops when multimedia redirection is not available: View a video on a website containing high definition videos, such as http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Good to know:

- For support and requirements information for HDX features, see the System requirements article. Except where otherwise noted, HDX features are available for supported Windows Multi-session OS and Windows Single-session OS machines, plus Remote PC Access desktops.
- This content describes how to optimize the user experience, improve server scalability, or reduce bandwidth requirements. For information about using Citrix policies and policy settings, see the Citrix policies documentation for this release.
- For instructions that include editing the registry, use caution: editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Auto client reconnect and session reliability

When accessing hosted applications or desktops, network interruption might occur. To experience a smoother reconnection, we offer auto client reconnect and session reliability. In a default configuration, session reliability starts and then auto client reconnect follows.

Auto client reconnect:

Auto client reconnect relaunches the client engine to reconnect to a disconnected session. Auto client reconnect closes (or disconnects) the user session after the time specified in the setting. If auto client reconnect is in progress, the system sends application and desktops network interruption notification to the user as follows:

- **Desktops.** The session window is grayed out and a countdown timer shows the time until the reconnections occur.
- **Applications.** The session window closes and a dialog appears to the user containing a countdown timer showing the time until the reconnections are attempted.

During auto client reconnect, sessions relaunch expecting network connectivity. User cannot interact with sessions while auto client reconnect is in progress.

On reconnection, the disconnected sessions reconnect using saved connection information. The user can interact with the applications and desktops normally.

Default auto client reconnect settings:

- Auto client reconnect timeout: 120 seconds
- Auto client reconnect: Enabled
- Auto client reconnect authentication: Disabled
- Auto client reconnect Logging: Disabled

For more information, see Auto client reconnect policy settings.

Session reliability:

Session reliability reconnects ICA sessions seamlessly across network interruptions. Session reliability closes (or disconnects) the user session after the time specified in the setting. After the session reliability timeout, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session. When session reliability is in progress, application and desktops network interruption notification are sent to the user as follows:

- **Desktops.** The session window becomes translucent and a countdown timer shows the time until the reconnections occur.
- **Applications.** The window becomes translucent along with connection interrupted pop ups from the notification area.

While session reliability is active, the user cannot interact with the ICA sessions. However, user actions like keystrokes are buffered for few seconds immediately after the network interruption and retransmitted when the network is available.

On reconnection, the client and the server resume at the same point where they were in their exchange of protocol. The session windows lose translucency and appropriate notification area pop ups are shown for applications.

Default session reliability settings

- Session reliability timeout: 180 seconds
- Reconnection UI opacity level: 80%
- Session reliability connection: Enabled
- Session reliability port number: 2598

For more information, see Session reliability policy settings.

NetScaler with auto client reconnect and session reliability:

If Multistream and Multiport policies are enabled on the server and any or all these conditions are true, auto client reconnect does not work:

- Session reliability is disabled on NetScaler Gateway.
- A failover occurs on the NetScaler appliance.
- NetScaler SD-WAN is used with NetScaler Gateway.

HDX adaptive throughput

HDX adaptive throughput intelligently fine-tunes the peak throughput of the ICA session by adjusting output buffers. The number of output buffers is initially set at a high value. This high value allows data to be transmitted to the client more quickly and efficiently, especially in high latency networks. Providing better interactivity, faster file transfers, smoother video playback, higher framerate and resolution results in an enhanced user experience.

Session interactivity is constantly measured to determine whether any data streams within the ICA session are adversely affecting interactivity. If that occurs, the throughput is decreased to reduce the impact of the large data stream on the session and allow interactivity to recover.

> **Important:**
>
> HDX adaptive throughput changes the way that output buffers are set by moving this mechanism from the client to the VDA, and no manual configuration is necessary.

This feature has the following requirements:

- VDA version 1811 or later
- Workspace app for Windows 1811 or later

Improve the image quality sent to user devices

The following visual display policy settings control the quality of images sent from virtual desktops to user devices.

- Visual quality. Controls the visual quality of images displayed on the user device: medium, high, always lossless, build to lossless (default = medium). The actual video quality using the default setting of medium depends on available bandwidth.
- Target frame rate. Specifies the maximum number of frames per second that are sent from the virtual desktop to the user device (default = 30). For devices that have slower CPUs, specifying a lower value can improve the user experience. The maximum supported frame rate per second is 60.
- Display memory limit. Specifies the maximum video buffer size for the session in kilobytes (default = 65536 KB). For connections requiring more color depth and higher resolution, increase the limit. You can calculate the maximum memory required.

Improve video conference performance

Several popular video conferencing applications are optimized for delivery from Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) through multimedia redirection (see, for example, HDX RealTime Optimization Pack). For applications that are not optimized, HDX webcam video compression

improves bandwidth efficiency and latency tolerance for webcams during video conferencing in a session. This technology streams webcam traffic over a dedicated multimedia virtual channel. This technology uses less bandwidth compared to the isochronous HDX Plug-n-Play USB redirection support, and works well over WAN connections.

Citrix Workspace app users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting **Don't use my microphone or webcam**. To prevent users from switching from HDX webcam video compression, disable USB device redirection by using the policy settings under ICA policy settings > USB Devices policy settings.

HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing
- Windows Media Redirection

If a webcam supports hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding might consume more bandwidth than software encoding. To force software compression, add the following DWORD key value to the registry key: `HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1`.

Network traffic priorities

Priorities are assigned to network traffic across multiple connections for a session using Quality of Service supported routers. Four TCP streams and two User Datagram Protocol (UDP) streams are available to carry ICA traffic between the user device and the server:

- TCP streams - real time, interactive, background, and bulk
- UDP streams - voice and Framehawk display remoting

Each virtual channel is associated with a specific priority and transported in the corresponding connection. You can set the channels independently, based on the TCP port number used for the connection.

Multiple channel streaming connections are supported for Virtual Delivery Agents (VDAs) installed on Windows 10 and Windows 8 machines. Work with your network administrator to ensure the Common Gateway Protocol (CGP) ports configured in the Multi-Port Policy setting are assigned correctly on the network routers.

Quality of Service is supported only when multiple session reliability ports, or the CGP ports, are configured.

> **Warning:**
>
> Use transport security when using this feature. Citrix recommends using Internet Protocol Security (IPsec) or Transport Layer Security (TLS). TLS connections are supported only when the connections traverse a NetScaler Gateway that supports multi-stream ICA. On an internal corporate network, multi-stream connections with TLS are not supported.

To set Quality of Service for multiple streaming connections, add the following Citrix policy settings to a policy (see Multi-stream connections policy settings for details):

- Multi-Port policy - This setting specifies ports for ICA traffic across multiple connections, and establishes network priorities.
  - Select a priority from the CGP default port priority list. By default, the primary port (2598) has a High priority.
  - Type more CGP ports in CGP port1, CGP port2, and CGP port3 as needed, and identify priorities for each. Each port must have a unique priority.

  Explicitly configure the firewalls on VDAs to allow the additional TCP traffic.
- Multi-Stream computer setting - This setting is disabled by default. If you use Citrix NetScaler SD-WAN with Multi-Stream support in your environment, you do not need to configure this setting. Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service.
- Multi-Stream user setting - This setting is disabled by default.

For policies containing these settings to take effect, users must log off and then log on to the network.

Show or hide the remote language bar

The language bar displays the preferred input language in an application session. If this feature is enabled (default), you can show or hide the language bar from the **Advanced Preferences > Language bar** UI in Citrix Workspace app for Windows. By using a registry setting on the VDA side, you can disable client control of the language bar feature. If this feature is disabled, the client UI setting doesn't take effect, and the per user current setting determines the language bar state. For more information, see Improve the user experience.

To disable client control of the language bar feature from the VDA:

1. In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
2. Create a DWORD value key, SeamlessFlags, and set it to 0x40000.

Unicode keyboard mapping

Non-Windows Citrix Receivers use the local keyboard layout (Unicode). If a user changes the local keyboard layout and the server keyboard layout (scan code), they might not be in sync and the output is incorrect. For example, User1 changes the local keyboard layout from English to German. User1 then changes the server-side keyboard to German. Even though both keyboard layouts are German, they might not be in sync causing incorrect character output.

Enable or disable Unicode keyboard layout mapping

By default, the feature is disabled on the VDA side. To enable the feature, toggle on the feature by using registry editor regedit on the VDA. Add the following registry key:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: EnableKlMap

Type: DWORD

Value: 1

To disable this feature, set **EnableKlMap** to 0 or delete the **CtxKlMap** key.

Enable Unicode keyboard layout mapping compatible mode

By default, Unicode keyboard layout mapping automatically hooks some windows API to reload the new Unicode keyboard layout map when you change the keyboard layout on the server side. A few applications cannot be hooked. To keep compatibility, you can change the feature to compatible mode to support these non-hooked applications. Add the following registry key:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: DisableWindowHook

Type: DWORD

Value: 1

To use normal Unicode keyboard layout mapping, set **DisableWindowHook** to 0.

Citrix ICA virtual channels

February 19, 2024

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of a Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

What are ICA virtual channels?

A large portion of the functionality and communication between the Citrix Workspace app and the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) servers occurs over virtual channels. Virtual channels are a necessary part of the remote computing experience with the Citrix DaaS servers. Virtual channels are used for:

- Audio
- COM ports
- Disks
- Graphics
- LPT ports
- Printers
- Smart cards
- Third-party custom virtual channels
- Video

New virtual channels are sometimes released with Citrix DaaS and Citrix Workspace app products to provide more functionality.



A virtual channel consists of a client-side virtual driver that communicates with a server-side application. Citrix DaaS ships with various virtual channels included. They're designed to allow customers and third-party vendors to create their own virtual channels by using one of the provided Software Development Kits (SDKs).

Virtual channels provide a secure way to accomplish various tasks. For example, an application that is running on a Citrix Virtual Apps server that is communicating with a client-side device or an application that is communicating with the client-side environment.

On the client side, virtual channels correspond to virtual drivers. Each virtual driver provides a specific function. Some are required for normal operation, and others are optional. Virtual drivers operate at the presentation layer protocol level. There can be several protocols active at any time by multiplexing channels that are provided by the Windows Station (WinStation) protocol layer.

The following functions are contained in the VirtualDriver registry value under this registry path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\
Advanced\Modules\ICA 3.0
```

or

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (for 64-bit)

- Thinwire3.0 (Required)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Clipboard
- ClientComm
- ClientAudio
- LicenseHandler (Required)
- TWI (Required)
- SmartCard
- ICACTL (Required)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Note:**
>
> You can disable specific client functionality by removing one or more of these values from the registry key. For example, if you wanted to remove the Client Clipboard, remove the word **Clipboard**.

This list contains the client virtual driver files and their respective functions. Citrix Virtual Apps and Citrix Workspace app for Windows use these files. They are in the form of Dynamic Link Libraries (user mode), and not Windows drivers (kernel mode) except for Generic USB as described in Generic USB virtual channel.

- vd3dn.dll –Direct3D virtual channel used for desktop composition redirection
- vdcamN.dll –Bidirectional audio
- vdcdm30n.dll –Client drive mapping
- vdcom30N.dll - Client COM port mapping
- vdcpm30N.dll –Client printer mapping
- vdctln.dll –ICA controls channel
- vddvc0n.dll –Dynamic virtual channel
- vdeuemn.dll - End user experience monitoring
- vdgusbn.dll –Generic USB virtual channel
- vdkbhook.dll –Transparent key pass-through
- vdlfpn.dll –Framehawk display channel over UDP like transport
- vdmmn.dll –Multimedia support

- vdmrvc.dll –Mobile Receiver virtual channel
- vdmtchn.dll - Multi-touch support
- vdscardn.dll –Smartcard support
- vdsens.dll –Sensors virtual channel
- vdspl30n.dll –Client UPD
- vdsspin.dll –Kerberos
- vdtuin.dll –Transparent UI
- vdtw30n.dll –Client Thinwire
- vdtwin.dll –Seamless
- vdtwn.dll –Twain

Some virtual channels are compiled into other files. For example Clipboard Mapping is available in wfica32.exe

64-bit compatibility

Citrix Workspace app for Windows is 64-bit compatible. As with most of the binaries compiled for 32 bit, these client files have 64-bit compiled equivalents:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Generic USB virtual channel

Generic USB virtual channel implementation uses two kernel mode drivers along with virtual channel driver vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

How ICA virtual channels work

Virtual channels are loaded in multiple ways. The Shell (WfShell for the server and PicaShell for the workstation) load some virtual channels. Some virtual channels are hosted as windows services.

Virtual channel modules loaded by the Shell, for example:

- EUEM
- Twain
- Clipboard
- Multimedia
- Seamless session sharing
- Time Zone

Some are loaded as kernel mode, for example:

- CtxDvcs.sys –Dynamic virtual channel
- Icausbb.sys –Generic USB redirection
- Picadm.sys –Client drive mapping
- Picaser.sys –COM port redirection
- Picapar.sys –LPT port redirection

Graphics virtual channel on the server side

Starting with XenApp 7.0 and XenDesktop7.0, `ctxgfx.exe` hosts the graphics virtual channel for both workstation and terminal server based sessions. `Ctxgfx` hosts platform specific modules that interact with the corresponding driver (`Icardd.dll` for RDSH and `vdod.dll` and `vidd.dll` for workstation).

For XenDesktop 3D Pro deployments an OEM graphics driver is installed for the corresponding GPU on the VDA. `Ctxgfx` loads specialized adaptor modules to interact with the OEM graphics driver.

Hosting specialized channels in windows services

On Citrix DaaS servers, various channels are hosted as windows services. Such hosting provides one-to-many semantics for multiple applications in a session and multiple sessions on the server. Examples of such services include:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service

- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops only)
- Citrix ICA Status Channel Service

The audio virtual channel on Citrix Virtual Apps is hosted using Windows Audio service.

On the server side, all client virtual channels are routed through the WinStation driver, Wdica.sys. On the client side, the corresponding WinStation driver, built into wfica32.exe, polls the client virtual channels. This image illustrates the virtual channel client-server connection.



This overview contains a client-server data exchange using a virtual channel.

1. The client connects to the Citrix DaaS server. The client passes information about the virtual channels it supports to the server.
2. The server-side application starts, obtains a handle to the virtual channel, and optionally queries for additional information about the channel.
3. The client virtual driver and server-side application pass data using the following two methods:
    - If the server application has data to send to the client, the data is sent to the client immediately. When the client receives the data, the WinStation driver de-multiplexes the virtual

channel data from the ICA stream and immediately passes it to the client virtual driver.
- If the client virtual driver has data to send to the server, the data is sent the next time the WinStation driver polls it. When the server receives the data, it is queued until the virtual channel application reads it. There is no way to alert the server virtual channel application that data was received.

4. When the server virtual channel application is completed, it closes the virtual channel and frees any allocated resources.

Creating your own virtual channel using the Virtual Channel SDK

Creating a virtual channel using the Virtual Channel SDK requires intermediate programming knowledge. Use this method to provide a major communication path between the client and the server. For example, if you are implementing usage of a device on the client side, such as a scanner, to be used with a process in the session.

> **Note:**
>
> - The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.
> - Because of enhanced security for Citrix DaaS, you must specify which virtual channels are allowed to be opened in an ICA session. For more information, see Virtual channel allow list policy settings.

Creating your own virtual channel using the ICA Client Object SDK

Creating a virtual channel using the ICA Client Object (ICO) is easier than using the Virtual Channel SDK. Use the ICO by creating a named object in your program using the **CreateChannels** method.

> **Important:**
>
> Because of enhanced security starting with the 10.00 version of the Citrix Receiver for Windows and later (and Citrix Workspace apps for Windows), you must take an extra step when creating an ICO virtual channel.

For more information, see Client Object API Specification Programmer's Guide.

Pass-through functionality of virtual channels

Most virtual channels that Citrix provides operate unmodified when you use the Citrix Workspace app for Windows within an ICA session (also known as a pass-through session). There are considerations when using the client in extra hops.

The following functions operate the same way in single or multiple hops:

- Client COM port mapping
- Client drive mapping
- Client printer mapping
- Client UPD
- End user experience monitoring
- Generic USB
- Kerberos
- Multimedia support
- Smartcard support
- Transparent key pass-through
- Twain

As the inherent nature of latency and factors such as compression and decompression and rendering being performed at each hop, performance might be affected with each additional hop that the client undergoes. The affected areas are:

- Bidirectional audio
- File transfers
- Generic USB redirection
- Seamless
- Thinwire

> **Important:**
>
> By default, the client drives mapped by an instance of the client running in a pass-through session are restricted to the client drives of the connecting client.

Pass-through functionality of virtual channels between a Citrix Virtual Desktop session and a Citrix Virtual App session

Most virtual channels provided by Citrix operate unmodified when you use Citrix Workspace app for Windows within an ICA session on a Citrix Virtual Desktops server (also known as a pass-through session).

Specifically, on the Citrix Virtual Desktops server, there is a VDA hook that runs **picaPassthruHook**. This hook makes the client think it's running on a CPS server, and placing the client into its traditional pass-through mode.

We support the following traditional virtual channels and their functionality:

- Client
- Client COM port mapping

- Client drive mapping
- Client printer mapping
- Generic USB (limited due to performance)
- Multimedia support
- Smartcard support
- SSON
- Transparent key pass-through

Security and ICA virtual channels

Securing usage is an important part of planning, developing, and implementing virtual channels. There are several references to specific areas of security located throughout this document.

Best practices

Open virtual channels when you **Connect** and **Reconnect**. Close virtual channels when you log off and **Disconnect**.

Keep the following guidelines in mind when you create scripts that use virtual channel functions.

Naming the Virtual Channels:

You can create a maximum of 32 virtual channels. Seventeen of the 32 channels are reserved for special purposes.

- Virtual channel names must not be more than seven characters in length.
- The first three characters are reserved for the vendor name, and the next four for the channel type. For example, **CTXAUD** represents the Citrix audio virtual channel.

Virtual channels are referred to by a seven-character (or shorter) ASCII name. In some previous versions of the ICA protocol, virtual channels were numbered. The numbers are now assigned dynamically based on the ASCII name, making implementation easier. Users who are developing virtual channel code for internal use only can use any seven-character name that does not conflict with existing virtual channels. Use only numbers and upper and lowercase ASCII. Follow the existing naming convention when adding your own virtual channels. There are several predefined channels. The predefined channels begin with the OEM identifier CTX and are for use only by Citrix.

Double-Hop Support:

Virtual Channel	Is double hop supported?
Audio	No

Virtual Channel	Is double hop supported?
Browser Content Redirection	No
CDM	Yes
CEIP	No
Clipboard	Yes
Continuum (MRVC)	No
Control VC	Yes
HTML5 Video Redirection (v1)	Yes
Keyboard, Mouse	Yes
MultiTouch	No
NSAPVC	No
Printing	Yes
SensVC	No
Smartcard	Yes
Twain	Yes
USB VC	Yes
WAYCOM devices -K2M using USB VC	Yes
Webcam Video Compression	Yes
Windows Media Redirection	Yes

See also

- ICA Virtual Channel SDK
- The Citrix Developer Network is the home for all technical resources and discussions involving the use of Citrix SDKs. In this network, you can find access to SDKs, sample code and scripts, extensions and plug-ins, and SDK documentation. Also included are the Citrix Developer Network forums, where technical discussions take place around each of the Citrix SDKs.

Double hop in Citrix DaaS

March 22, 2022

In the context of a Citrix client session, the term "double hop" refers to a Citrix Virtual App session that is running within a Citrix Virtual Desktop session. The following diagram illustrates a double hop.



In a double hop scenario, when the user connects to a Citrix Virtual Desktop running on a single-session OS VDA (known as VDI) or a multi-session OS VDA (known as a published desktop), that is considered the first hop. After the user connects to the virtual desktop, the user can launch a Citrix Virtual Apps session. That is considered the second hop.

You can use a double hop deployment model to support various use cases. The case where the Citrix Virtual Desktop and the Citrix Virtual Apps environments are managed by different entities is one common example. This method can also be effective in resolving application compatibility issues.

System requirements

All Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) editions support double hop.

The first hop must use a supported version of the single-session or multi-session OS VDA and the Citrix Workspace App. The second hop must use a supported version of the multi-session OS VDA. See the Product Matrix page for supported versions.

For best performance and compatibility, Citrix recommends using a Citrix client of the same version or newer than the VDA versions in use.

In environments where the first hop involves a third-party (non-Citrix) virtual desktop solution in combination with a Citrix Virtual Apps session, support is limited to the Citrix Virtual Apps environment. In the event of any issues related to the third-party virtual desktop, including - but not limited to - Citrix Workspace app compatibility, redirection of hardware devices, and session performance, Citrix can provide technical support in a limited capacity. A Citrix Virtual Desktop at the first hop might be required as part of troubleshooting.

Deployment considerations for HDX in double hop

In general, each session in a double hop is unique and client-server functions are isolated to a given hop. This section includes areas that require special consideration by Citrix administrators. Citrix

recommends that customers conduct thorough testing of required HDX capabilities to ensure user experience and performance is adequate for a given environment configuration.

Graphics

Use default graphics settings (selective encoding) on the first and second hops. In the case of HDX 3D Pro, Citrix highly recommends that all applications that require graphics acceleration run locally in the first hop with the appropriate GPU resources available to the VDA.

Latency

End-to-end latency can impact the overall user experience. Consider the added latency between the first and second hops. This is especially important with redirection of hardware devices.

Multimedia

Server-side (in session) rendering of audio and video content performs best in the first hop. Video playback in the second hop requires decoding and re-encoding at the first hop, increasing bandwidth and hardware resource utilization as a result. Audio and video content must be limited to the first hop whenever possible.

USB device redirection

HDX includes generic and optimized redirection modes to support a wide array of USB device types. Pay special attention to the mode in use at each hop and use the following table as reference for best results. For more information about generic and optimized redirection modes, see Generic USB devices.

First hop (VDI or published desktop)	Second hop (Virtual apps)	Support notes
Optimized	Optimized	Recommended (based on device support). For example, USB mass storage, TWAIN scanners, Webcam, Audio.
Generic	Generic	For devices where the optimized option is not available.

First hop (VDI or published desktop)	Second hop (Virtual apps)	Support notes
Generic	Optimized	While technically possible, it is recommended to use the optimized mode across both hops when device support is available.
Optimized	Generic	Not supported

> **Note:**
>
> Due to the inherent chattiness of USB protocols, performance may decrease across hops. Functionality and results vary depending on specific device and application requirements. Validation testing is highly recommended in all cases of device redirection and especially important in double hop scenarios.

Support exceptions

Double hop sessions support most HDX features and capabilities except for the following:

- Browser content redirection
- Local App Access
- RealTime Optimization Pack for Skype for Business
- Optimization for Microsoft Teams

HDX connectivity

April 25, 2024

Citrix HDX represents a broad set of technologies that deliver a high-definition experience to users of centralized applications and desktops, on any device and over any network.

HDX is designed around three technical principles:

- Intelligent redirection
- Adaptive compression
- Data de-duplication

Applied in different combinations, they optimize the IT and user experience, decrease bandwidth consumption, and increase user density per hosting server.

Within the HDX offering, you can connect over a unique, proprietary transport protocol, utilize the maximum transmission units when establishing sessions, and optimize connectivity with Citrix SD-WAN.

Adaptive transport

May 3, 2024

Adaptive Transport is a mechanism in Citrix Virtual Apps and Desktops that allows establishing connections for HDX sessions using a preferred transport protocol while providing a fallback to TCP if connectivity with the preferred protocol is unavailable.

The following transport protocols are supported:

- Enlightened Data Transport (EDT)
- Transmission Control Protocol (TCP)

Configuration

Adaptive Transport is enabled by default. You can configure Adaptive Transport to operate in the following modes:

- **Preferred**: (Default) The client attempts to connect with the preferred protocol and falls back to TCP if connectivity with the preferred protocol is unavailable.
- **Diagnostic mode**: The client only attempts to connect using the preferred protocol. Fall back to TCP is disabled.
- **Off**: The client only attempts to connect using TCP.

How it works

When **Adaptive Transport** is set to `Preferred`, the client attempts to connect to the session with both the preferred protocol and TCP in parallel. This allows optimizing the connection time if it's not possible to connect with the preferred protocol and the client must fall back to using TCP. If the connection is established using TCP, the client attempts to connect with the preferred protocol in the background every five minutes.

When **Adaptive Transport** is set to `Diagnostic mode`, the client connects to the session only with the preferred protocol. If the client is unable to establish a connection using the preferred protocol, it doesn't fall back to using TCP, and the connection fails.

When **Adaptive Transport** is set to `Off`, **Adaptive Transport** is disabled, and the client connects to the session using TCP only.





System requirements

The following are the requirements for using Adaptive Transport and EDT:

- Control plane
  - Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
  - Citrix Virtual Apps and Desktops: currently supported version

- Virtual Delivery Agent
  - Windows: currently supported version (2402 or later recommended)
  - Linux: currently supported version (2402 or later recommended)
- Citrix Workspace app
  - Windows: currently supported version (2402 or later recommended)
  - Linux: currently supported version (2402 or later recommended)
  - Mac: currently supported version (2402 or later recommended)
  - iOS: latest version available in the Apple App Store
  - Android: latest version available in Google Play
- Citrix NetScaler Gateway
  - 14.1.12.30 or later (recommended)
  - 13.1.17.42 or later (13.1-52.19 or later recommended)

> **Note:**
>
> For details on Linux VDA, please see the Linux Virtual Delivery Agent documentation.

Network requirements

The following sections are the network requirements for using EDT with Adaptive Transport:

Session hosts

If your session hosts have a firewall such as Windows Defender Firewall, you must allow the following inbound traffic for internal connections.

Description	Source	Protocol	Port
Internal connection - Session Reliability enabled	Client	UDP	2598
Internal connection - Session Reliability disabled			1494
Internal connection - HDX Direct or VDA SSL			443

> **Note:**
>
> The VDA installer adds the appropriate inbound rules to the Windows Defender Firewall. If you use a different firewall, you must add the rules above.

Internal network

The following table depicts the firewall rules required for using EDT in your network:

Description	Protocol	Source	Destination	Destination port
Direct internal connection - Session Reliability enabled	UDP	Client network	VDA network	2598
Direct internal connection - Session Reliability disabled				1494
Direct internal connection - HDX Direct or VDA SSL				443
NetScaler Gateway		NetScaler SNIP		2598
NetScaler Gateway - VDA SSL				443

> **Note:**
>
> If you are using Citrix Gateway Service, you must enable **Rendezvous** to use EDT as your transport protocol. See the Rendezvous documentation for system and network requirements.

Client network

The following table outlines the connectivity requirements for client devices:

Description	Protocol	Source	Destination	Destination port
Internal connection - Session Reliability enabled	UDP	Client IP	VDA network	2598
Internal connection - Session Reliability disabled				1494
Internal connection - HDX Direct or SSL VDA				443
External connection - NetScaler Gateway			NetScaler Gateway public IP address	443
External connection - Citrix Gateway Service			Citrix Gateway Service	443

> **Note:**
>
> If you are using Citrix Gateway Service, clients must be able to reach https://*.*.nssvc.net. If you can't allow all subdomains using https://*.*.nssvc.net, you can use https://*.c.nssvc.net and https://*.g.nssvc.net instead. For more information, see Knowledge Center article CTX270584.

Enlightened Data Transport

April 25, 2024

Enlightened Data Transport (EDT) is a Citrix-proprietary transport protocol built on top of User Datagram Protocol (UDP). It delivers a superior user experience on challenging long-haul connections while maintaining server scalability. EDT improves data throughput for all ICA virtual channels on unreliable networks, providing a better and more consistent user experience.

When **Adaptive Transport** is enabled, EDT is the preferred protocol.

Things to know

- **Session Reliability** must be enabled to use **MTU Discovery** and EDT with NetScaler Gateway and Citrix Gateway Service.
- Packet fragmentation can cause performance degradation or even failure to open sessions in some cases. To prevent this, you must adjust the EDT MTU to a value adequate for your networks. You can use EDT MTU Discovery or a manual workaround described in How to configure MSS when using EDT on networks with non-standard MTU.
- For details on enabling the use of EDT with NetScaler Gateway, see Configure NetScaler Gateway to support Enlightened Data Transport.

EDT MTU Discovery

MTU Discovery allows EDT to automatically determine the Maximum Transmission Unit (MTU) when establishing a session. Doing so prevents EDT packet fragmentation that might result in performance degradation or failure to establish a session.

MTU Discovery is enabled by default. If you need to disable it, see HDX features managed through the registry for details.

> **Note:**
>
> - **Session Reliability** must be enabled for MTU Discovery to work.
> - MTU Discovery with Multi-Stream ICA is available with VDA versions 2209 and later.

Troubleshooting

April 29, 2024

To confirm that EDT is being used as the transport protocol for the session, you can use Director or the `CtxSession.exe` command-line utility on the VDA.

In Director, look up the session and select **Details**. If the **Connection type** is HDX and the **Protocol** is UDP, EDT is being used as the transport protocol for the session.



To use the CtxSession.exe utility, launch a Command Prompt or PowerShell within the session and run `ctxsession.exe`. To see verbose statistics, run `ctxsession.exe -v`. If EDT is in use, the transport protocol shows one of the following:

- **UDP > ICA** (Session Reliability disabled)
- **UDP > CGP > ICA** (Session Reliability enabled)
- **UDP > DTLS > CGP > ICA** (ICA is DTLS-encrypted end-to-end)



When sessions fail to connect with EDT

To troubleshoot **Adaptive Transport** and **EDT**, we suggest the following:

1. Review the System requirements, Network requirements, Known issues, and Things to know, and ensure that all items have been addressed.
2. Check if there are Citrix policies in Studio or GPO overwriting the desired **HDX Adaptive Transport** setting.
3. Check if there are settings on the client overwriting the desired HDX Adaptive Transport setting. This can be a GPO preference, a setting configured using the optional Workspace app administrative template, or a manual configuration of the **HDXoverUDP** setting in the registry or client's configuration file.
4. On multi-session VDA machines, ensure that the UDP listeners are active. Open a command prompt in the VDA machine and run `netstat -a -p udp`. For more information, see How to Confirm HDX Enlightened Data Transport Protocol.
5. Check if the appropriate firewall rules have been configured in both network firewalls and firewalls running on the VDA machines.
6. Launch a direct session internally, bypassing the NetScaler Gateway or Citrix Gateway Service, and check the protocol in use. If the session uses EDT, the VDA is ready to use EDT for external connections through NetScaler Gateway or Citrix Gateway Service.

7. If EDT works for direct internal connections and not for sessions going through NetScaler Gateway or Citrix Gateway Service:

   - Ensure that **Session Reliability** is enabled.
   - If using NetScaler Gateway, ensure that your configuration adheres to the required configuration outlined in Configure NetScaler Gateway to support Enlightened Data Transport and HDX Insight.

8. If using Citrix Gateway Service, ensure that Rendezvous is enabled and working.

9. Check if your users' connections require a non-standard MTU. Connections with an effective MTU lower than 1500 bytes cause EDT packet fragmentation, which in turn can affect performance or even cause session launch failures. This issue is common when using VPNs, some Wi-Fi access points, and mobile networks, such as 4G and 5G. Ensure that you either have MTU Discovery enabled or are setting a custom MTU as outlined in How to configure MSS when using EDT on networks with non-standing MTU.

Known issues

- Asymmetrical network paths can cause MTU Discovery to fail for connections that do not go through NetScaler Gateway or Citrix Gateway Service. To address this issue, upgrade to VDA version 2103 or later. [CVADHELP-16654]
- When using NetScaler Gateway, asymmetrical network paths can cause MTU Discovery to fail. This is due to an issue on Gateway that causes the Don't Fragment (DF) bit in the EDT packets' header not to be propagated. A fix for this issue is available, starting with firmware release 13.1 build 17.42. For details on how to enable the fix, see the NetScaler Gateway documentation. [CGOP-18438]
- MTU Discovery can fail for users that connect through a DS-Lite network. Some modems fail to honor the DF bit when packet processing is enabled, preventing MTU Discovery from detecting fragmentation. In this situation, the following are the available options:

  - Disable packet processing on the user's modem.
  - Disable **MTU Discovery** and use a hardcoded MTU as described in How to configure MSS when using EDT on networks with non-standing MTU.
  - Disable **Adaptive Transport** to force sessions to use TCP. If only a subset of users are affected, consider disabling it on the client side so that other users can continue to use EDT.

Rendezvous protocol

April 4, 2023

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud Connectors to connect directly and securely with the Citrix Cloud control plane.

There are two types of traffic to consider:

1. Control traffic for VDA registration and session brokering.
2. HDX session traffic.

There are two versions of Rendezvous available:

- Version 1 (V1): supports bypassing the Citrix Cloud Connectors for HDX session traffic only.
- Version 2 (V2): supports bypassing the Citrix Cloud Connectors for both control traffic and HDX session traffic.

For details about system requirements, considerations, and configuration for each of the Rendezvous versions, review their respective documentation.

Rendezvous V1 documentation

Rendezvous V2 documentation

Rendezvous V1

April 4, 2023

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud Connectors to connect directly and securely with the Citrix Cloud control plane.

Requirements

- Access to environment using Citrix Workspace and Citrix Gateway service.
- Control Plane: Citrix DaaS (Citrix Cloud).
- VDA: Version 1912 or later.
  - Version 2012 is the minimum required for EDT Rendezvous.
  - Version 2012 is the minimum required for non-transparent proxy support (no PAC file support).

  - Version 2103 is the minimum required for proxy configuration with a PAC file.

- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- The VDAs must have access to `https://*.nssvc.net`, including all subdomains. If you can't add all subdomains to the allow list in that manner, use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see the Internet Connectivity Requirements section of the Citrix Cloud documentation (under Citrix DaaS) and the Knowledge Center article CTX270584.
- The VDAs must be able to connect to the addresses mentioned previously on TCP 443 and UDP 443 for TCP Rendezvous and EDT Rendezvous, respectively.
- Cloud Connectors must obtain the VDAs' FQDNs when brokering a session. Accomplish this task in one of these two ways:
  - **Enable DNS resolution for the site.** Navigate to **Full Configuration > Settings** and turn on the **Enable DNS resolution** setting. Alternatively, use the Citrix Virtual Apps and Desktops Remote PowerShell SDK and run the command `Set-BrokerSite -DnsResolutionEnabled $true`. For more information about the Citrix Virtual Apps and Desktops Remote PowerShell SDK, see SDKs and APIs.
  - **DNS Reverse Lookup Zone with PTR records for the VDAs.** If you choose this option, we recommend that you configure VDAs to always attempt to register PTR records. To do so, use the Group Policy Editor or Group Policy Object, navigate to **Computer Configuration > Administrative Templates > Network > DNS Client**, and set **Register PTR Records** to **Enabled and Register**. If the connection's DNS suffix does not match the domain's DNS suffix, you must also configure the **Connection-specific DNS suffix** setting for the machines to register PTR records successfully.

> **Note:**
>
> If using the DNS resolution option, the Cloud Connectors must be able to resolve the fully qualified domain names (FQDNs) of the VDA machines. In the case that internal users connect directly to the VDA machines, the client devices also must be able to resolve the VDA machines' FQDNs.
>
> If using a DNS reverse lookup zone, the FQDNs in the PTR records must match the FQDNs of the VDA machines. If the PTR record contains a different FQDN, the Rendezvous connection fails. For example, if the machine's FQDN is `vda01.domain.net`, the PTR record must contain `vda01.domain.net`. A different FQDN such as `vda01.sub.domain.net` does not work.

Proxy configuration

The VDA supports establishing Rendezvous connections through a proxy.

Proxy considerations

Consider the following when using proxies with Rendezvous:

- Transparent proxies, non-transparent HTTP proxies, and SOCKS5 proxies are supported.
- Packet decryption and inspection are not supported. Configure an exception so that the ICA traffic between the VDA and the Gateway Service is not intercepted, decrypted, or inspected. Otherwise, the connection breaks.
- HTTP proxies support machine-based authentication by using Negotiate and Kerberos or NT LAN Manager (NTLM) authentication protocols.

  When you connect to the proxy server, the Negotiate authentication scheme automatically selects the Kerberos protocol. If Kerberos isn't supported, Negotiate falls back to NTLM for authentication.

  > **Note:**
  >
  > To use Kerberos, you must create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the format `HTTP/<proxyURL>` when establishing a session, where the proxy URL is retrieved from the **Rendezvous proxy** policy setting. If you don't create an SPN, authentication falls back to NTLM. In both cases, the VDA machine's identity is used for authentication.

- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, you must configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Transparent proxy

If using a transparent proxy in your network, no additional configuration is required on the VDA.

Non-transparent proxy

If using a non-transparent proxy in your network, configure the Rendezvous proxy configuration setting. When the setting is enabled, specify the HTTP or SOCKS5 proxy address, or enter the path to the

PAC file so the VDA knows which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>` or `socks5://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path>/<filename>.pac`

If you use the PAC file to configure the proxy, define the proxy using the syntax required by the Windows HTTP service: `PROXY [<scheme>=]<URL or IP>:<port>`. For example, `PROXY socks5=<URL or IP>:<port>`.

Rendezvous validation

If you meet all requirements, follow these steps to validate if Rendezvous is in use:

1. Launch PowerShell or a command prompt within the HDX session.
2. Run `ctxsession.exe –v`.
3. The transport protocols in use indicate the type of connection:
    - TCP Rendezvous: **TCP > SSL > CGP > ICA**
    - EDT Rendezvous: **UDP > DTLS > CGP > ICA**
    - Proxy through Cloud Connector: **TCP > CGP > ICA**

Other considerations

Windows cipher suite order

For a custom cipher suite order, make sure that you include the VDA-supported cipher suites from the following list:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

If the custom cipher suite order does not contain these cipher suites, the Rendezvous connection fails.

Zscaler Private Access

If using Zscaler Private Access (ZPA), it is recommended that you configure bypass settings for the Gateway Service to avoid increased latency and the associated performance impact. To do so, you must define application segments for the Gateway Service addresses –specified in the requirements –and set them to always bypass. For information on configuring application segments to bypass ZPA, see the Zscaler documentation.

Rendezvous V2

April 19, 2024

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud Connectors to connect directly and securely with the Citrix Cloud control plane.

Rendezvous V2 is supported with standard domain joined machines, Hybrid Azure AD joined machines, Azure AD joined machines, and non-domain joined machines.

> **Note:**
>
> Currently, connectorless deployments are possible with *Azure AD joined* and *non-domain joined* machines only. Standard AD domain joined machines and Hybrid Azure AD joined machines still require Cloud Connectors for VDA registration and session brokering. However, there are no DNS requirements for using Rendezvous V2.
>
> Cloud Connector requirements for other functions not related to VDA communication, such as connecting to your on-prem AD domain, MCS provisioniong to on-prem hypervisors, etc., remain the same.

Requirements

The requirements for using Rendezvous V2 are:

- Access to the environment using Citrix Workspace and Citrix Gateway Service
- Control plane: Citrix DaaS
- VDA version 2203
- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- Session Reliability must be enabled on the VDAs
- The VDA machines must have access to:
  - `https://*.xendesktop.net` on `TCP 443`. If you can't allow all subdomains in that manner, you can use `https://<customer_ID>.xendesktop.net`, where <customer_ID> is your Citrix Cloud customer ID as shown in the Citrix Cloud administrator portal.
  - `https://*.*.nssvc.net` on `TCP 443` for the control connection with Gateway Service.
  - `https://*.*.nssvc.net` on `TCP 443` and `UDP 443` for HDX sessions over TCP and EDT, respectively.

> **Note:**
>
> If you can't allow all subdomains using `https://*.*.nssvc.net`, you can use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see Knowledge Center article CTX270584.

Proxy configuration

The VDA supports connecting through proxies for both control traffic and HDX session traffic when using Rendezvous. The requirements and considerations for both types of traffic are different, so review them carefully.

Control traffic proxy considerations

- Only HTTP proxies are supported.
- Packet decryption and inspection are not supported. Configure an exception so the control traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Proxy authentication is not supported.

HDX traffic proxy considerations

- HTTP and SOCKS5 proxies are supported.
- EDT can only be used with SOCKS5 proxies.
- By default, HDX traffic uses the proxy defined for control traffic. If you must use a different proxy for HDX traffic, whether a different HTTP proxy or a SOCKS5 proxy, use the Rendezvous proxy configuration policy setting.
- Packet decryption and inspection are not supported. Configure an exception so the HDX traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Machine-based authentication is supported only with HTTP proxies and if the VDA machine is AD domain joined. It can use Negotiate/Kerberos or NTLM authentication.

  > **Note:**
  >
  > To use Kerberos, create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the format `HTTP/<proxyURL>` when establishing a session, where the proxy URL is retrieved from the Rendezvous proxy configuration policy setting. If you don't create an SPN, authentication

> falls back to NTLM. In both cases, the VDA machine's identity is used for authentication.

- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Transparent proxy

If using a transparent proxy in your network, no additional configuration is required on the VDA.

Non-transparent proxy

If using a non-transparent proxy in your network, specify the proxy during the VDA installation so that control traffic can reach the Citrix Cloud control plane. Make sure to review the control traffic proxy considerations before proceeding with the installation and configuration.

In the VDA installation wizard, select **Rendezvous Proxy Configuration** in the **Additional Components** page. This option makes the **Rendezvous Proxy Configuration** page available later in the installation wizard. Once here, enter the proxy address or the path to the PAC file for the VDA to know which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path/<filename>.pac`

As stated in the HDX traffic proxy considerations, HDX traffic uses the proxy defined during the VDA installation by default. If you must use a different proxy for HDX traffic, whether a different HTTP proxy or a SOCKS5 proxy, use the Rendezvous proxy configuration policy setting. When the setting is enabled, specify the HTTP or SOCKS5 proxy address. You can also enter the path to the PAC file so the VDA knows which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>` or `socks5://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path/<filename>.pac`

If you use the PAC file to configure the proxy, define the proxy using the syntax required by the Windows HTTP service: `PROXY [<scheme>=]<URL or IP>:<port>`. For example, `PROXY socks5=<URL or IP>:<port>`.

How to configure Rendezvous

Following are the steps for configuring Rendezvous in your environment:

1. Make sure that all requirements are met.
2. If you must use a non-transparent HTTP proxy in your environment, configure it during the VDA installation. Refer to the proxy configuration section for details.
3. Reboot the VDA machine after installation is complete.
4. Create a Citrix policy, or edit an existing one:
    - Set the **Rendezvous Protocol** setting to **Allowed**.
    - If you must configure an HTTP or SOCKS5 proxy for HDX traffic, configure the **Rendezvous proxy configuration** setting.
    - Ensure that the Citrix policy filters are set properly. The policy applies to the machines that need Rendezvous enabled.
5. Ensure that the Citrix policy has the correct priority so that it does not overwrite another one.

> **Note:**
>
> If you are using VDA version 2308 or older, V1 is used by default. For more information on how to configure the version to use, see HDX features managed through the registry.

Rendezvous validation

If you meet all requirements and have completed the configuration, follow these steps to validate if Rendezvous is in use:

1. Within the virtual desktop, open a command prompt or PowerShell.
2. Run `ctxsession.exe -v`.
3. The transport protocols displayed indicate the type of connection:
    - TCP Rendezvous: TCP > SSL > CGP > ICA
    - EDT Rendezvous: UDP > DTLS > CGP > ICA
    - Not Rendezvous: TCP > CGP > ICA
4. The Rendezvous version reported indicates the version in use.

Other considerations

Windows cipher suite order

If the cipher suite order has been modified in the VDA machines, make sure that you include the VDA-supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

If the custom cipher suite order does not contain these cipher suites, the Rendezvous connection fails.

Zscaler Private Access

If using Zscaler Private Access (ZPA), it is recommended that you configure bypass settings for the Gateway Service to avoid increased latency and the associated performance impact. To do so, you must define application segments for the Gateway Service addresses –specified in the requirements –and set them to always bypass. For information on configuring application segments to bypass ZPA, see the Zscaler documentation.

Known Issues

VDA 2203 installer does not allow entering a slash (/) for the proxy address

As a workaround, you can configure the proxy in the registry after the VDA is installed:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
Value type: String
Value name: ProxySettings
Value data: Proxy address or path to pac file. For example:
    Proxy address: http://squidk.test.local:3128
    Pac file: http://file.test.com/config/proxy.pac
```

Rendezvous traffic flow

The following diagram illustrates the sequence of steps about Rendezvous traffic flow.



1. The VDA establishes a WebSocket connection with Citrix Cloud and registers.
2. The VDA registers with Citrix Gateway Service and obtains a dedicated token.
3. The VDA establishes a persistent control connection with the Gateway Service.
4. The user navigates to Citrix Workspace.
5. Workspace evaluates authentication configuration and redirects users to the appropriate IdP for authentication.
6. The user enters their credentials.
7. After successfully validating the user credentials, the user is redirected to Workspace.
8. Workspace counts resources for the user and displays them.
9. The user selects a desktop or application from Workspace. Workspace sends the request to Citrix DaaS, which brokers the connection and instructs the VDA to prepare for the session.
10. The VDA responds with the Rendezvous capability and its identity.
11. Citrix DaaS generates a launch ticket and sends it to the user device through Workspace.
12. The user's endpoint connects to the Gateway Service and provides the launch ticket to authenticate and identify the resource to connect to.
13. The Gateway Service sends the connection information to the VDA.
14. The VDA establishes a direct connection for the session with the Gateway Service.
15. The Gateway Service completes the connection between the endpoint and the VDA.
16. The VDA verifies licensing for the session.
17. Citrix DaaS sends applicable policies to the VDA.

HDX Direct (Preview)

May 22, 2024

When accessing Citrix-delivered resources, HDX Direct allows both internal and external client devices to establish a secure direct connection with the session host if direct communication is possible.

> **Important:**
>
> HDX Direct is currently in preview. This feature is provided without support and is not yet recommended for use in production environments. To submit feedback or report issues, use this form.

System requirements

The following are the system requirements for using HDX Direct:

- Control plane
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 or later
- Virtual Delivery Agent (VDA)
  - Windows: version 2402 or later
- Workspace app
  - Windows: version 2402 or later
- Access tier
  - Citrix Workspace with Citrix Gateway Service
  - Citrix Workspace with NetScaler Gateway
- Other
  - Adaptive Transport must be enabled for external direct connections

Network requirements

The following are the network requirements for using HDX Direct.

Session hosts

If your session hosts have a firewall such as Windows Defender Firewall, you must allow the following inbound traffic for internal connections.

Description	Source	Protocol	Port
Direct internal connection	Client	TCP	443
Direct internal connection	Client	UDP	443

> Note:
>
> The VDA installer adds the appropriate inbound rules to Windows Defender Firewall. If you use a different firewall, you must add the rules above.

Client network

The following table describes the client network for internal and external users.

Internal users

Description	Protocol	Source	Source port	Destination	Destination port
Direct internal connection	TCP	Client network	1024–65535	VDA network	443
Direct internal connection	UDP	Client network	1024–65535	VDA network	443

External users

Description	Protocol	Source	Source port	Destination	Destination port
STUN (external users only)	UDP	Client network	1024–65535	Internet (see note below)	3478, 19302

Description	Protocol	Source	Source port	Destination	Destination port
External user connection	UDP	Client network	1024–65535	Data center's public IP address	1024–65535

Data center network

The following table describes the data center network for internal and external users.

Internal users

Description	Protocol	Source	Source port	Destination	Destination port
Direct internal connection	TCP	Client network	1024–65535	VDA network	443
Direct internal connection	UDP	Client network	1024–65535	VDA network	443

External users

Description	Protocol	Source	Source port	Destination	Destination port
STUN (external users only)	UDP	VDA network	1024–65535	Internet (see note below)	3478, 19302
External user connection	UDP	DMZ / Internal network	1024–65535	VDA network	55000–55250
External user connection	UDP	VDA network	55000–55250	Client's public IP	1024–65535

> **Note:**
>
> Both the VDA and Workspace app attempt to send STUN requests to the following servers in the same order:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478

> - stun.l.google.com:19302
>
> If you change the default port range for external user connections using the **HDX Direct port range** policy setting, the corresponding firewall rules must match your custom port range.

Configuration

HDX Direct is disabled by default. You can configure this feature using the **HDX Direct** setting in the Citrix policy.

- **HDX Direct**: To enable or disable a feature.
- **HDX Direct mode**: Determines if **HDX Direct** is available for internal clients only or for both internal and external clients.
- **HDX Direct port range**: Defines the port range that the VDA uses for connections from external clients.

Considerations

The following are considerations for using HDX Direct:

- HDX Direct for external users is only available with EDT (UDP) as the transport protocol. Therefore, **Adaptive Transport** must be enabled.
- If you are using **HDX Insight**, note that using **HDX Direct** prevents the HDX Insight data collection, as the session would no longer be proxied through NetScaler Gateway.
- When using non-persistent machines for your virtual apps and desktops, Citrix recommends enabling **HDX Direct** on the session hosts instead of in the master/template image so that each machine generates its own certificates.
- Using your own certificates with HDX Direct is not currently supported.

How it works

HDX Direct allows clients to establish a direct connection to the session host when direct communication is available. When direct connections are made using HDX Direct, self-signed certificates are used to secure the direct connection with network level-encryption (TLS/DTLS).

Internal users

The following diagram depicts the overview of the HDX Direct connection process of internal users.

1. The client establishes an HDX session through the Gateway Service.

2. Upon a successful connection, the VDA sends to the client the VDA machine's FQDN, a list of its IP addresses, and the VDA machine's certificate via the HDX connection.
3. The client probes the IP addresses to see if it can reach the VDA directly.
4. If the client can reach the VDA directly with any of the IP addresses shared, the client establishes a direct connection with the VDA, secured with (D)TLS using a certificate that matches the one exchanged in step (2).
5. Once the direct connection is successfully established, the session is transferred to the new connection, and the connection to the Gateway Service is terminated.

> **Note:**
>
> After establishing the connection in step 2, above, the session is active. The subsequent steps do not delay or interfere with the user's ability to use the virtual application or desktop. If any of the subsequent steps fail, the connection through the Gateway is maintained without interrupting the user's session.

External users

The following diagram depicts the overview of the HDX Direct connection process for external users:

1. The client establishes an HDX session through the Gateway Service.
2. Upon a successful connection, both the client and the VDA send a STUN request to discover their public IP addresses and ports.
3. The STUN server responds to the client and VDA with their corresponding public IP addresses and ports.
4. Through the HDX connection, the client and the VDA exchange their public IP addresses and UDP ports, and the VDA sends its certificate to the client.
5. The VDA sends UDP packets to the client's public IP address and UDP port. The client sends UDP packets to the VDA's public IP address and UDP port.
6. Upon receipt of a message from the VDA, the client responds with a secure connection request.
7. During the DTLS handshake, the client verifies that the certificate matches the certificate exchanged in step (4). After validation, the client sends its authorization token. A secure direct connection is now established.
8. Once the direct connection is successfully established, the session is transferred to the new connection, and the connection to the Gateway Service is terminated.

> **Note:**
>
> After establishing the connection in step 2, above, the session is active. The subsequent steps do not delay or interfere with the user's ability to use the virtual application or desktop. If any of the

> subsequent steps fail, the connection through the Gateway is maintained without interrupting the user's session.

Certificate management

Session host

The following two services on the VDA machine handle certificate creation and management, both of which are set to run automatically at machine startup:

- Citrix ClxMtp Service: Responsible for CA certificate key generation and rotation.
- Citrix Certificate Manager Service: Responsible for generating and managing the self-signed root CA certificate and the machine certificates.

The following steps depict the certificate management process:

1. The services start at machine startup.
2. `Citrix ClxMtp Service` creates keys if none has been created already.
3. Citrix Certificate Manager Service checks if **HDX Direct** is enabled. If not, the service stops itself.
4. If **HDX Direct** is enabled, the Citrix Certificate Manager Service checks if a self-signed root CA certificate exists. If not, a self-signed root certificate is created.
5. Once a root CA certificate is available, the Citrix Certificate Manager Service checks if a self-signed machine certificate exists. If not, the service generates keys and creates a new certificate using the machine's FQDN.
6. If there is an existing machine certificate created by the Citrix Certificate Manager Service and the subject name does not match the machine's FQDN, a new certificate is generated.

> **Note:**
>
> The Citrix Certificate Manager Service generates RSA certificates that leverage 2048-bit keys.

Client device

To successfully establish a secure **HDX Direct** connection, the client must trust the certificates used to secure the session. To facilitate this, the client receives the CA certificate for the session through the ICA file (supplied by Workspace), so it is not necessary to distribute CA certificates to the client devices' certificate stores.

NAT Compatibility

May 22, 2024

To establish a direct connection between an external user device and the session host, HDX Direct leverages hole punching for NAT traversal and STUN to facilitate the exchange of the public IP address and port mappings for the client device and session host. This is similar to how VoIP, unified communications, and P2P solutions work.

As long as firewalls and other network components are configured to allow the UDP traffic for the STUN requests and the HDX sessions, HDX Direct for external users is expected to work. However, there are certain scenarios where the NAT types of the user and session host networks lead to an incompatible combination, thus causing HDX Direct to fail.

Validations

You can validate the NAT type on the client and the session host by using STUNTMAN's STUN client utility:

1. Download the appropriate package for the target platform from stunprotocol.org, and extract the contents.
2. Open a terminal prompt and navigate to the directory where the contents were extracted.
3. Run the following command:
   ```
   .\stunclient.exe stunserver.stunprotocol.org --mode behavior
   ```
4. Take note of the output.

If the binding and behavior tests are successful, both **binding test** and **behavior test** report the success and a NAT behavior is specified:

If the tests fail, both **binding test** and **behavior test** report the failure.

See the following table to determine if HDX Direct for external users is expected to work based on the test results of both the client and session host:

Client device	Session host	Expected to work?
Endpoint Independent Mapping	Endpoint Independent Mapping	Yes
Endpoint Independent Mapping	Endpoint Dependent Mapping	Yes
Endpoint Dependent Mapping	Endpoint Independent Mapping	Yes
Endpoint Dependent Mapping	Endpoint Dependent Mapping	No
Address and port dependent mapping	Any NAT type	No

Client device	Session host	Expected to work?
Any NAT type	Address and port dependent mapping	No
fail	Any NAT type	No
Any NAT type	fail	No
fail	fail	No

Troubleshooting

December 21, 2023

To confirm that **HDX Direct** successfully established a direct connection, you can use the `CtxSession.exe` utility on the VDA machine.

To use the `CtxSession.exe` utility, launch a Command Prompt or PowerShell within the session and run `ctxsession.exe -v`. If the **HDX Direct** connection is successfully established, **HDX Direct Status** is `Connected`.

You can also look at the session host's event logs for information on whether the HDX Direct connection was established successfully or failed. See the **Event Logs** section for details.

> Note:
>
> Depending on the environment and the number of IP addresses available to the session hosts, it can take up to 5 minutes for the HDX Direct connection to be established.

When HDX Direct fails to establish a direct connection

If HDX Direct is failing to establish a direct connection, review the following steps:

1. Ensure that the VDA version and Workspace app version in use support the feature per the system requirements.
2. Confirm that you have a policy applied to the VDA that enables HDX Direct and that there are no other policies with higher priority disabling the feature.
3. Confirm that you have a policy applied to the VDA that sets the desired HDX Direct mode and that there are no other policies with higher priority overwriting the configuration.
4. Ensure that the Citrix ClxMtp Service is running on the session host.

5. Ensure that the Citrix Certificate Manager Service is running on the session host. If it's not running, try to start it manually. The service automatically stops if HDX Direct is disabled.
6. Check if the session host has its self-signed Root CA certificate:
    a) Issued to: `CA-<hostname>` (For example, CA-FTLW11-001)
    b) Issued by: `CA-<hostname>` (For example, CA-FTLW11-001)
    c) Issuer details: The organization is Citrix Systems, Inc.
7. Check if the session host has its self-signed server certificate:
    a) Issued to: `<host FQDN>` (For example, FTLW11-001.ctxlab.net)
    b) Issued by: `CA-<hostname>` (For example, CA-FTLW11-001)
    c) Issuer details: The organization is Citrix Systems, Inc.
8. If the certificates are missing, contact Citrix Tech Support.
9. If the certificates are present:
    a) Stop the Citrix Certificate Manager Service on the session host.
    b) Delete both the self-signed Root CA certificate and the self-signed server certificate.
    c) Start the Citrix Certificate Manager Service on the session host. The service creates new certificates once it starts.
10. For internal users:
    a) Ensure the session host's firewall is not blocking inbound traffic on UDP 443 or TCP 443, for HDX over EDT and HDX over TCP, respectively.
    b) Ensure that your network firewall is not blocking traffic on UDP 443 and TCP 443 between your clients' network and session hosts' network.
11. For external users:
    a) Check the NAT type for the client and the session host, and ensure that the combination is expected to work. See the NAT Compatibility section for details.
    b) If the NAT test fails on either the client or the session host:
        i. If there is a firewall running on the system, ensure it is not blocking outbound traffic on UDP 3478.
        ii. Ensure that your network firewalls are not blocking outbound traffic on UDP 3478.
        iii. Ensure the firewalls are not blocking the STUN server's response.
    c) Ensure that your network firewalls have the appropriate rules configured to allow all necessary traffic. See the Network Requirements section for details.
    d) If you change the default port range using the HDX Direct port range policy setting, ensure that your firewall rules are set for the custom port range.

Event logs

The following events are logged in the VDA machine's event log:

Log	ID	Source	Level	Description
Applications and Services Logs > Citrix-HostCore-HDX Direct/Operational	1	HDX Direct	Information	HDX Direct connection for internal user <username> established.
Applications and Services Logs > Citrix-HostCore-HDX Direct/Operational	2	HDX Direct	Information	HDX Direct connection for external user <username> established.
Applications and Services Logs > Citrix-HostCore-HDX Direct/Operational	3	HDX Direct	Information	HDX Direct connection for user <username> failed.

Known issues

HDX Direct might stop working after performing an in-place upgrade of the VDA on a machine that already has **HDX Direct** enabled.
To resolve the issue, complete the following steps:

1. Stop the Citrix Certificate Manager Service on the session host.
2. Delete the self-signed Root CA certificate and the self-signed server certificate.
3. Open the registry.
4. Delete the `HKLM\Software\Citrix\HDX-Direct` key.
5. Go to `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Set the **SSLEnabled** value to `0`.
7. Delete the contents of the **SSLThumbprint** value.
8. Start the **Citrix Certificate Manager Service**.

Secure HDX (Preview)

May 31, 2024

Secure HDX is an Application Level Encryption (ALE) solution that prevents any network elements in the traffic path from being able to inspect the HDX traffic. It does this by providing true End-to-End Encryption (E2EE) at the application level between the Citrix Workspace app (client) and the VDA (session host) using AES-256-GCM encryption.

> **Important:**
>
> Secure HDX is currently in preview. This feature is provided without support and is not yet recommended for use in production environments. To submit feedback or report issues, use this form.

System requirements

The following list depicts the system requirements for using Secure HDX.

- Control plane
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 or later
- Virtual Delivery Agent (VDA)
  - Windows: version 2402 or later
- Workspace app
  - Windows: version 2402 or later
- Access tier
  - Citrix Workspace
  - Citrix StoreFront 2402 or later

Configuration

Secure HDX is disabled by default. You can configure this feature using the Secure HDX setting in Citrix policy:

Secure HDX: Defines whether to enable the feature for all sessions, only for direct connections, or disable it.

Considerations

The following are considerations for using Secure HDX:

- If a user tries to connect to a session host with Secure HDX enabled using a client that does not support the feature, the connection will be denied.
- If you use HDX Insight, note that using Secure HDX prevents HDX Insight data collection as the NetScaler is not able to inspect the encrypted HDX traffic. If you must use HDX Insight, you can set Secure HDX to be enabled only for direct connections.
- Service Continuity is not currently supported with Secure HDX. If you have Service Continuity enabled in your Citrix Cloud environment, you might not be able to connect to any session hosts that have Secure HDX enabled if there is a Cloud service outage.
- If you use SmartControl, note that using Secure HDX prevents SmartControl from working as the NetScaler is unable to inspect the encrypted HDX traffic. If you must use SmartControl, you can set Secure HDX to be enabled only for direct connections.
- Multi-Stream ICA is not supported when Secure HDX is enabled.
- If you use any third-party solutions that rely on inspecting HDX traffic, they would no longer work if you enable Secure HDX since HDX traffic is encrypted.

Troubleshooting

To confirm that Secure HDX is active, you can use the `ctxsession.exe` utility on the VDA machine.

To use the `CtxSession.exe` utility, open a Command Prompt or PowerShell within the session and run `ctxsession.exe -v`. If Secure HDX is in use, ICA Encryption displays `SecureHDX AES-256 GCM`.



When Secure HDX does not get enabled in the session

- Ensure the VDA version in use supports the feature per the system requirements.
- Confirm that you have a policy applied to the VDA that enables Secure HDX and that there are no other policies with higher priority disabling the feature.
- If the client device is connecting through NetScaler Gateway or Gateway Service, ensure that Secure HDX is not set to "Direct Connections Only".
- If the session host was already running when you configured Secure HDX, restart the machine to ensure changes take effect.

Virtual channel allow list

April 25, 2024

The virtual channel allow list is a feature that allows you to control which non-Citrix virtual channels are allowed in your environment. By default, the virtual channel allow list feature is enabled. As a result, only Citrix virtual channels are allowed to open in Citrix Virtual Apps and Desktops sessions. If there is a need to use custom virtual channels, whether homegrown or from a third party, these need to be explicitly added to the allow list.

Configuration

The virtual channel allow list is enabled by default. You can configure this feature using the following settings in the Citrix policy:

- **Virtual channel allow list**: to enable or disable the feature and to add virtual channels to the list.
- **Virtual channel allow list log throttling**: sets the throttling period for the virtual channel allow list event logging.
- **Virtual channel allow list logging**: sets the logging level for the virtual channel allow list.

Adding virtual channels to the allow list

To add a virtual channel to the allow list, you need the following information:

1. The virtual channel name as defined in the code, which can be up to seven characters long. For example, `CTXCVC1`.
2. The paths to the processes that open the virtual channel on the VDA machine. For example, `C:\Program Files\Application\run.exe`.

Once you have the required information, you must add the virtual channel to the allow list using the Virtual channel allow list policy setting. To add a virtual channel to the list, enter the virtual channel name followed by a comma, and then the path to the process that accesses the virtual channel. If there are multiple processes, you can add these processes by separating each process with commas.

For single processes

Using the previous examples, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe
```


For multiple processes

If there are multiple processes, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

Using wildcards

The use of wildcards (*) is supported. You can use wildcards when the names of directories or executables change based on the version of the application, or if the third-party component is installed in the users' profiles.

You can use wildcards in the following scenarios:

- To replace the full directory name.
  For example: `C:\Program Files\Application\*\run1.exe`
- To replace part of the directory name.
  For example: `C:\Program Files\Application\v*\run1.exe`
- To replace the executable's name.
  For example: `C:\Program Files\Application\v1.2\*.exe`
- To replace part of the executable's name.
  For example: `C:\Program Files\Application\v1.2\run*.exe`

The following restrictions apply:

- The wildcard can only be used to replace a single directory. For example, if the executable is located in `C:\Program Files\Application\v1.2\run1.exe`
  - Allowed: `C:\Program Files\Application\*\run1.exe`
  - Not allowed: `C:\Program Files\*\run1.exe`
- Entries must contain the file name extension.
  - Allowed: `C:\Program Files\Application\v1.2\*.exe`
  - Not allowed: `C:\Program Files\Application\v1.2\*`
- All paths must be local.

> **Note:**
>
> - Network paths are not allowed.
> - Wildcard support is available from Citrix Virtual Apps and Desktops 2206.
> - Wildcard support is available in Citrix Virtual Apps and Desktops 2203 LTSR from CU2.

Using system environment variables

You can use system environment variables to simplify the definition of the trusted processes in your allow list. You can use any of the out-of-box variables, such as %programfiles%, %programfiles(x86)%, %systemdrive%, and %systemroot%.

You can also use custom environment variables as long as they are defined at the system level.

The following examples depict out-of-box environment variables:

- %programfiles%\Application\v1.2\run.exe
- %programfiles%\Application*\run.exe
- %programfiles(x86)%\Application\v1.*\run.exe

The following example depicts a custom system environment variable:

- Custom variable name: app
- Custom variable value: %programfiles%\Application\
- Allow list entry: CTXCVC1,%app%\run.exe

> **Note:**
>
> User environment variables are not supported.
>
> Environment variable support is available from Citrix Virtual Apps and Desktops version 2209.

Obtain virtual channel names and processes

The easiest way to obtain the name of the virtual channel and the process that opens it on the VDA machine is to get the information from the developer or a third-party vendor that provided the virtual channel.

Alternatively, you can obtain information by applying the feature's logs and following these steps:

1. Once the client and server components of the custom virtual channel are in place, launch a virtual application or virtual desktop.
2. In the VDA machine's System event log, look for the custom virtual channel's name and the process that tried to open it. For more information on available events, see Event logs.
3. Log out from the session.
4. Add an entry in the virtual channel allow list policy settings for the identified virtual channel and process.
5. Restart the machine.
6. Once the VDA is registered, run the virtual application or virtual desktop to validate that the custom virtual channels open successfully.

Considerations for Citrix virtual channels

All built-in Citrix virtual channels are trusted and allowed to open without further configuration. However, the following two features require explicit entries in the allow list because of external dependencies:

- Multimedia Redirection
- HDX RealTime Optimization Pack for Skype for Business

Multimedia Redirection

If you use a media player other than Windows Media Player as your system media player, you need to add it to the allow list as a trusted process. The following information is required for the allow list entry:

- Virtual channel name: `CTXMM`
- Process: Path to the media player used in your VDA machine. For example, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Allow list entry: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

The following information is required for the allow list entry:

- Virtual channel name: `CTXRMEP`
- Process: Path to the Skype for Business executable in your VDA machine, which can vary based on the version of Skype for Business or if you used a custom installation path. For example, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Allow list entry: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Troubleshooting

April 25, 2024

If your custom virtual channel fails to open, review the following steps:

1. Ensure you are using the correct VDA version.

2. Confirm that you have a policy applied to the VDA with the custom virtual channel in the virtual channel allow list and that there are no other policies with higher priority overwriting this configuration.
3. Check the event log in the VDA and confirm that the virtual channel name reported matches the one defined in the allow list.

    a) If you have multiple processes, ensure these are defined properly as described in Adding virtual channels to the allow list.
    b) If you are using wildcards in the defined process path, ensure you are adhering to the guidelines for Using wildcards.
    c) If you are using environment variables in the defined process path, ensure you are adhering to the guidelines in Using system environment variables.

Event logs

The following events are logged in the VDA machine's event log.

Single-session VDA

The following events are logged in the single-session VDA machine's event log:

Log Name	Id	Source	Level	Description
System	2001	Picadd	Information	Custom virtual channel <vcName> has been opened by process <processName>
System	2002	Picadd	Warning	Custom virtual channel <vcName> cannot be opened by process <processName>

Log Name	Id	Source	Level	Description
System	2003	Picadd	Information	<username> opened custom virtual channel <vcName>
System	2004	Picadd	Warning	<username> tried to open custom virtual channel <vcName>
System	2005	Picadd	Error	Path given in policy < pathInPolicy > cannot resolve to process path
System	2007	Picadd	Information	Loaded process path is < processPath>
System	2008	Picadd	Error	Environment variable <varName> in VC policy path is not found

Multi-session VDA

The following events are logged in the multi-session VDA machine's event log:

Log Name	Id	Source	Level	Description
System	13	Rpm	Information	Custom virtual channel <vcName> has been opened by process < processName>

Log Name	Id	Source	Level	Description
System	14	Rpm	Warning	Custom virtual channel <vcName> cannot be opened by process < processName>
System	15	Rpm	Information	<username> opened custom virtual channel <vcName>
System	16	Rpm	Warning	<username> tried to open custom virtual channel <vcName>
System	17	Rpm	Error	Path given in policy < pathInPolicy > cannot resolve to process path
System	18	Rpm	Information	Loaded process path is < processPath>
System	19	Rpm	Error	Environment variable <varName> in VC policy path is not found

Known third-party virtual channels

April 25, 2024

The following are known third-party solutions that use custom Citrix virtual channels. This list does not include every solution that uses a custom Citrix virtual channel.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings for VDI
- Ultima IA-Connect

To obtain details for adding the associated virtual channels to the allow list, reach out to the solutions' vendors. Alternatively, follow the steps outlined in the Obtaining virtual channel names and processes section.

Devices

August 3, 2023

HDX provides a high-definition user experience on any device, at any location. The articles in the Devices section describe these devices:

- Client Drive Mapping
- Generic USB device
- Mobile and touch screen devices
- Serial devices
- Specialty keyboards
- TWAIN devices
- Webcams
- WIA devices

Optimized vs. generic USB device

An optimized USB device is one for which Citrix Workspace app has specific support. For example, the ability to redirect webcams using the HDX Multimedia virtual channel. A generic device is a USB device for which there is no specific support in Citrix Workspace app.

By default, generic USB redirection can't redirect USB devices with optimized virtual channel support unless put into Generic mode.

In general, you get better performance for USB devices in Optimized mode than in Generic mode. However, there are cases where a USB device doesn't have full functionality in Optimized mode. It might be necessary to switch to Generic mode to gain full access to its features.

With USB mass storage devices, you can use either client drive mapping or generic USB redirection, or both, controlled by Citrix polices. The main differences are:

If both generic USB redirection and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it's redirected using client drive mapping.

When these conditions are true, the mass storage device is redirected using generic USB redirection:

- Both generic USB redirection and the client drive mapping policies are enabled.
- A device is configured for automatic redirection.
- A mass storage device is inserted either before or after a session starts.

For more information, see http://support.citrix.com/article/CTX123015.

Feature	Client drive mapping	Generic USB redirection
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Encrypted device access	Yes, if encryption is unlocked before the device is accessed on the virtual session.	Citrix Virtual Desktops only

Scanning

June 27, 2024

Scanner is a device that optically scans images, printed text, handwriting or an object and converts it to a digital image.

If you're using a scanner and your computer is running windows, there's a good chance you're using the WIA scanner driver. This driver is responsible for communicating between your computer and scanner.

- **Windows Image Acquisition** (WIA) is Microsoft's driver model and application programming interface (API) that enables software to communicate with imaging hardware like scanners.
- **TWAIN** (Windows and Mac) is another protocol which is a scanning protocol that connects scanners and applications together by providing standard interface. TWAIN allows applications to acquire images from TWAIN compliant devices (scanners, digital cameras, etc.).

TWAIN Redirection

June 27, 2024

Introduction

TWAIN is a scanning protocol used to link image software to scanners or digital cameras.

How TWAIN works

- Scan your documents using any of the 32-bit applications in your Citrix session.

  > **Note:**
  >
  > Use a locally attached TWAIN-compliant scanner to scan the documents.

- The Citrix scanning module redirects the TWAIN request to the client's scanner.
- Once the scan is complete, the session host is notified.

Requirements

Citrix Control Plane

- Citrix Virtual Apps and Desktops 1912 or later
- Citrix DaaS

Session Host

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Windows Server 2022 or later
- VDA
  - Version 1912 or later
- Application
  - 32-bit application

Client Device

- Operating system
  - Windows 10 1809 or later
  - Windows 11
- Workspace app
  - Windows: version 1912 or later
- Scanner
  - TWAIN-compliant scanner

Configuration

- Install TWAIN drivers on the client endpoint.
- Set up devices or applications to select the required scanning protocol if they support both TWAIN and WIA.
- Attach the scanner to the client endpoint locally (through USB).
- Redirect TWAIN devices to the session via USB redirection if needed.

> **Note:**
>
> TWAIN devices don't work well with USB redirection leading to poor scan quality.

Policy Settings

Policy settings to set up TWAIN redirection and improve scanning.

- **Client TWAIN device redirection:** to enable or disable TWAIN redirection.

  > **Note:**
  >
  > By default, TWAIN redirection is enabled.

- **TWAIN compression level:** to set compression levels for images from client to host.

For more details, see TWAIN devices policy settings.

Troubleshooting

Try out TWAIN with the public test app Twacker, which can be downloaded from this URL.

Follow the steps to validate TWAIN within a published desktop session:

1. Install **Twacker** on the VDA.
2. Launch **Twacker** (32-bit version).
3. Click **File > Select Source** and select your scanner from the list.
4. Click **File > Acquire**.
5. Click the **Scan button** to test your scanner.

If **Twacker** can scan successfully, it confirms that the **Citrix Virtual Apps and Desktops** setup is:

- Configured for USB redirection
- Using TWAIN devices
- Meeting all local client device requirements

If you still have scanning issues within a particular application, then it's likely to be a software issue.

WIA devices

June 27, 2024

Requirements

- The scanner must be WIA compliant.
- Install the WIA drivers on the local device. They are not required on the server.

- Attach the scanner locally (for example, through USB).
- Ensure that the scanner is using the local Windows Image Acquisition service and not the TWAIN driver.
- Ensure that there is no policy applied to the user account that is used for the test, and which is limiting the bandwidth within the ICA session. For example, client USB redirection bandwidth limit.

Windows Image Acquisition application allow list

An allow list lets you control which applications on the VDA can access the Windows Image Acquisition scanner redirection. The Registry Editor uses input from the allow list setting on each VDA that contains Windows Image Acquisition. By default, no applications have access to Windows Image Acquisition.

To adjust Windows Image Acquisition for applications on the VDA, see the Windows Image Acquisition application allow list setting in the list of features managed through the registry.

For information about policy settings, see WIA devices policy settings.

Generic USB devices

June 27, 2024

HDX technology provides **optimized support** for most popular USB devices. These devices include:

- Monitors
- Mice
- Keyboards
- Voice over Internet Protocol phones
- Headsets
- Webcams
- Scanners
- Cameras
- Printers
- Drives
- Smart card readers
- Drawing tablets
- Signature pads

Optimized support offers an improved user experience with better performance and bandwidth efficiency over a WAN. Optimized support is usually the best option, especially in high latency or security-sensitive environments.

HDX technology provides **generic USB redirection** for specialty devices that don't have optimized support or where it is unsuitable. For more information about generic USB redirection, see Generic USB redirection.

For more information about USB devices and Citrix Workspace app for Windows, see Configuring composite USB device redirection and Configuring USB support.

Configuration

June 27, 2024

USB redirection is disabled by default. You can configure generic USB redirection using the following settings in Citrix policy:

- **Client USB device redirection**: to enable or disable USB redirection
- **Client USB device redirection rules**: to specify specific device action i.e. to allow or deny access to a particular device
- **Client USB device redirection rules (Version 2)**: to specify rules for filtering, splitting and auto-connecting USB devices
- **Client USB device optimization rules**: to disable optimization or change the optimization mode
- **Allow existing USB devices to be automatically connected**: to allow or prevent automatic connection of existing USB devices that are connected to a client endpoint at the start of an HDX session
- **Allow newly arrived USB devices to be automatically detected**: to allow or prevent automatic connection of USB devices that are connected to a client endpoint during an HDX session

See, USB Policy Settings for more details.

How to configure USB redirection

By default, USB redirection configuration is disabled. To use it, USB redirection policy and specific redirection rules must be enabled and configured on the DDC.

> **Note:**
>
> If you are using any components older than version 2212 or you are using Workspace App for

> Linux/Mac, see Legacy USB Redirection Configuration for details on how to configure USB redirection.

Enabling Generic USB Redirection

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the **Client USB device redirection policy**.
4. Select **Allowed** and click **Save**.

Creating USB Redirection Policy Rules

When the user tries to redirect a USB device to Virtual Desktop, it is checked against each USB policy rule in turn until a match is found. The first match for any devices is considered final. If the first match is an **Allow** rule, the matched device is allowed to be redirected to the virtual desktop. If the first match is a **Deny** rule, the matched device is only available in the local desktop. If no match is found, default rules are used.

Device Rules As with regular USB devices, device rules set in the policy or client Citrix Workspace app configuration on the end point select the devices for forwarding. Citrix Workspace app uses these rules to decide which USB devices to allow or prevent from forwarding to the remote session.

Each rule consists of an action keyword (**Allow, Connect, or Deny**), a colon (:), and zero or more filter parameters that match actual devices at the endpoints USB subsystem. These filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

Device rules are clear text with each rule on a single line and an optional comment after a # character. Rules are matched top down (descending priority order). The first rule that matches the device or child interface is applied. Subsequent rules that select the same device or interface are ignored.

Example: ALLOW VID=1050 PID=0421 #Device1
Example: CONNECT VID=xxxx PID=yyyy Class=03 #Device2

Keyword	Description
CONNECT	Use this keyword to allow devices to be redirected over the USB virtual channel as well as enable them to be auto-redirected during session launch and upon insertion.

Keyword	Description
ALLOW	Use this keyword to allow devices to be redirected over the USB virtual channel
DENY	Use this keyword to deny devices from being redirected over the USB virtual channel



Setting the policy on the DDC:

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the **Client USB device redirection rules** (**Version 2**).
4. Set the value based on the examples provided in the description for each usb device that needs to be redirected and click Save.

   For Example: Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Mass Storage

> **Note:**
>
> If a Citrix admin checks **Use default value** and clicks on **Save**, the default rules can be found in the following registry in the VDA.
>
> **Caution!**
>
> Refer to the Disclaimer at the end of this article before using the Registry Editor.

`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **Note:**
>
> Policies can still be set on the client device using group policy device rules but that is no longer needed on newer versions of CVAD and CWA.
>
> For legacy configuration of USB devices, see Legacy USB Redirection Configuration.

Configure automatic redirection of USB devices (Optional)

USB devices are automatically redirected when USB support is enabled. Also, the USB user preference settings are set to automatically connect USB devices. It is not always best to redirect all USB devices. Users can explicitly redirect devices from the USB device list that are not automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules on either the client endpoint or the DDC policy.
This policy can be set either on the DDC, on the client using a GPO, using Citrix Workspace Preferences or the Connections tab under CDViewer. All of these methods are described below:

Setting the policy on the DDC:

There are two policies on the DDC that can be set to allow auto redirection of USB devices-

- Allow existing USB devices to be automatically connected
- Allow newly arrived USB devices to be automatically connected

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the setting **Allow** existing USB devices to be automatically connected.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
5. Edit the setting **Allow** newly arrived USB devices to be automatically connected.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Composite Devices and Device Splitting

June 27, 2024

A composite USB device is a single device that acts like multiple independent USB devices connected to a computer. It has a single USB connector but it can expose multiple interfaces to the computer with each having its own set of functionalities. When a user plugs in a composite USB device, the host device checks for all functions (interfaces) against each policy rule. If the first match for any function(interface) is a Deny rule, the rule is considered definitive for the composite device and the device is denied. If the first match for a function (interface) is an Allow rule, the host device continues to match the rules against the next function (interface). The composite device is allowed if no function (interface) is denied by a policy rule. If definitive match for composite device is a Deny Rule, the device is available only to the local desktop otherwise the device is remoted to the virtual desktop. If no match is found, default rules are used.



We can split the composite device using the appropriate rules in the Device redirection rules (Version 2) policy to allow only specific functionality of a composite device. For instance, we may want to use just the HID functions of a FIDO2 key but not the smartcard functionality. In that case, we would set the rules as illustrated below:

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 allowed FIDO2 HID functions.
2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 smartcard function blocked.

> **Tip:**
>
> When creating new policy rules, refer to the USB Class Codes, available on the USB web site.

Configuring a signature pad

1. Install the appropriate device driver on the VDA host.
2. Turn On the **Client USB device redirection policy** in **Citrix Web Studio**.
3. Edit the **Client USB device redirection rules** (**Version 2**) policy.
    a) Set the **VID** and **PID** information for the signature pad that needs to be redirected and click **Save**. For example: **Connect**: VID=056A PID=00A4 #STU-430
4. Edit the policy **Client USB device optimization rules**.
    a) Set the mode along with other device information. For example: Mode=00000004 VID=056A PID=00A4 class=03 #Input device operating in capture mode
5. Edit the policy **Allow existing USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
7. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
8. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Once these policies are set in the Studio console, subsequent session launches will have the device getting automatically redirected and will not require any additional end user action.

> **Note:**
>
> Replace the VID and PID with the actual VID and PID of the device to be redirected.

Configuring Bloomberg keyboard using USB redirection

1. Turn On the **Client USB device redirection policy** in **Citrix Web Studio**.
2. Bloomberg 5 keyboards are set by default in the Client USB device redirection rules (Version 2) policy and no additional admin action is needed.
3. Edit the policy **Allow existing USB devices to be automatically connected**.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

5. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Once these policies are set in the Studio console, Bloomberg keys will automatically be presented in subsequent HDX sessions and will not require any additional end user action.

Configuring a FIDO2 key using USB redirection

Citrix recommends using FIDO2 redirection for using FIDO2 keys in your HDX sessions. However, there might be situations in which you must redirect FIDO2 keys using USB redirection instead. These include scenarios where FIDO2 redirection is not available because the feature is not supported by the client, the VDA, or the operating system (e.g. Windows Server 2016).

There can also be situations in which the key has multiple modes enabled, but you only want to allow a subset of those in your HDX sessions. For example, you might want to allow FIDO2 and OTP, but block the smart card.

The following steps illustrate how you can configure a FIDO2 key using USB redirection (Yubikey vid=1050, pid=0407).

1. turn On the **Client USB device redirection policy** in **Citrix Web Studio**.
2. Edit the **Client USB device redirection rules** (Version 2) policy.
    a) Set the **VID** and **PID** information as well as the split device configuration for the FIDO2 key to be redirected in the session and click **Save**.
    b) **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 allowed FIDO2 HID functions.
    c) **Deny**: VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 smartcard function blocked.
3. Edit the policy **Allow existing USB devices to be automatically connected**.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
5. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Once these policies are set in the Studio console, FIDO2 keyboards will automatically be presented in subsequent HDX sessions and will not require any additional end user action.

Configuring a 3-d mouse using USB redirection

Today, the 3dConnexion space mouse drivers are only supported on workstation OSes (Win 10 and Win11). They do not work on server OS. The following are the steps to configure a SpaceMouse Enterprise on a workstation OS (vid=046D, pid=C016).

1. Install the latest Windows driver on the VDA host.
2. Turn On the **Client USB device redirection policy** in **Citrix Web Studio**.
3. Edit the **Client USB device redirection rules** (**Version 2**) policy.
    a) Set the **VID** and **PID** information for the signature pad that needs to be redirected and click **Save**. For example: **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise
4. Edit the policy **Client USB device optimization rules**.
    a) Set the mode along with other device information. For example: Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. Edit the policy **Allow existing USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
7. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
8. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Troubleshooting

June 27, 2024

The following steps should be followed to triage USB redirection related issues:

1. Validate system requirements are being met for USB redirection. This includes correct CVAD and CWA versions, supported devices and device drivers on the OS platform under consideration.
2. Ensure the configuration is appropriate based on the components' versions and platforms in use in your environment. See the note in Legacy USB Redirection Configuration for details on components that require legacy configuration settings.
3. Validate that device is listed under devices that the client has enumerated.

a) Workspace Preferences toolbar: Look at the devices enumerated in the Devices tab of the Workspace app Preferences toolbar (Right click **CWA icon > Connection Center > Preferences**...Click on **Devices** tab).

b) `CtxUsbDiagnostics.exe` (Recommended): Run this tool in a command prompt window. The output gives you device specific information for a specific session. It will tell you if a device is being redirected or not. It will also tell you if a device rule set is causing the device to not be redirected. See, Diagnostics Tool for more information.

c) USBView or other 3rd party tools: Run a 3rd party tool like USBView in the endpoint / client machine to ensure that the device is detected at the endpoint.

4. If you see the device being enumerated:

a) If you see a Deny rule in the CtxUsbDiagnostics tool output for a particular device, check the policies configured in Studio and ensure that the rules are correctly set in Version 2 policy. If the deny rule doesn't appear in the studio policy, check the client side policy and finally the client side defaults in that order to find the matching deny rule.

b) If there is no deny rule in the CtxUsbDiagnostics output, then CWA will allow redirection of the device by checking / clicking the appropriate button in the devices tab of the Preferences window (Devices > Manage devices). A device once redirected will be available in the session. This can be verified by checking the device manager / USBView or similar application in the HDX session.

5. If you do not see the device being presented inside the session:

a) It is possible that the correct device driver is not installed correctly on the VDA host. Ensure that the latest versions of device drivers are correctly installed on the VDA host. Some device drivers are not supported on terminal server machines so ensure that is not the case with the device you are trying to redirect.

b) Ensure that the device is not being used on the client endpoint. Some devices require drivers to be installed on the client endpoint as well and this could prevent them from being redirected in the session.

6. Validate USB related rules are set correctly on the client endpoint:

a) **CWA for Windows** :

i. Validate that group policy on the client (add more detail and SS for this) is appropriately set and does not conflict with the rules set in Studio.

ii. Validate that default rules in the client's registry.



(`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`)are appropriately set and not in conflict with the rules set in Studio and client group policy.

b) CWA for Linux - To triage CWA for Linux issues, see USB documentation for CWA for Linux

c) CWA for Mac - To triage CWA for Mac issues, see CWA for Mac

Note:

- On TSVDA, audio devices are blocked by default from using USB redirection. The recommended way to use those devices is using the optimized Audio VC.
- Sometimes, USB composite devices might not be split automatically even though a correct device redirection rule is set to split the device. This issue occurs because the device is in low power mode. In these instances, the child device that enters low power mode might not be present in the device list. You can use the following workarounds to overcome this issue:
  - Disconnect the session, insert the USB device, and reconnect to the session.

  - Unplug the USB device and plug it back in. This action results in the device moving out of low power mode.

- Sometimes, USB battery saver settings may be enabled to optimize battery life. If the client endpoint goes to sleep, the USB device may get disconnected. In such a scenario, you might have to disconnect and reconnect the device in order to present the device again in the session.

Event Logs

Administrators can now monitor for unauthorized devices that users may attempt to redirect and can take the appropriate action. Here are some of the event messages that will be logged in the Event viewer on the VDA host for devices that are allowed to be redirected and for devices that are not.

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB Diagnostics Tool

June 27, 2024

`CtxUsbDiagnostics.exe` is a command-line tool on the VDA to help Citrix admins diagnose and resolve USB device redirection issues experienced on the client in an expedited manner. This utility tool collects vital information required to triage configuration issues associated with USB devices attached to the client that are failing to redirect inside an HDX session.

```
> **Note :**
>
> Running Command Prompt or Powershell as an administrator is required to ensure the tool has the necessary permissions to perform system-level operations.
```


Requirements

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows 11 21H2 or later
  - Windows Server 2016 or later
- VDA
  - Windows: Citrix Virtual Apps and Desktops Version 2311 or later

Client device

- Operating system
  - Windows 10 1809 or later
- Workspace App
  - Windows: version 2311 or later

What does the tool do?

The tool currently provides:

- SessionID
- VDA device policies (device rules set in Studio)
- Client devices and client device policies (device rules)
- List of devices, their redirection state, and why they were allowed or denied



> **Note :**
>
> The administrator can see device information for all active sessions.

Information Displayed

- **Citrix Studio rules - Version 1/2**
  - The DDC rules indicate the use of the legacy "**Client USB device redirection rules**"or "**Client USB device redirection rules (Version 2)**"policy in Studio. The information listed in this section lists all the rules configured by the Citrix admin.

- **Client Default Device Rules**
  - This section lists the rules that are set in the registry on the client.



- **Device optimization rules**
  - The section lists the device optimization rules as set in “Client USB device optimization rules.



Device List

This section lists valuable information about each device that is connected to the client endpoint, the hardware information, whether it is being redirected or not, whether the correct device redirection rule is set or not, and so on.

Tag Name	Description
displayName	Lists the common name of the device.
vid	Vendor ID
pid	Product ID
Interfaces	This subsection lists all the interfaces in case the composite device has been split into multiple child devices.
InterfaceNum	Indicates the index of the interface descriptor
class	Class code
subclass	Subclass Code

Tag Name	Description
protocol	Protocol
redirectionState	**Local** indicates that the device is not redirected in the ICA session. **ThisSession** indicates that the device is redirected in the ICA session. **OtherSession** indicates that the device is redirected in another ICA session.
optiEnabled	**true** indicates that the device is optimized. **false** indicates that the device is not optimized and the data transfer happens over the USB virtual channel.
deviceType	**generic** indicates that the device does not have an optimized virtual channel and the traffic is flowing through the USB virtual channel. **optimized** implies that the data transfer associated with the device is happening over a dedicated virtual channel.
isDenied	**true** indicates that the device is not redirected because of a policy rule set by the admin. `false` indicates that the device is redirected because of applied policy.
denyRule	This field is useful if **isDenied** is set to `true`. It tells the admin the specific rule set in the policy that is resulting in the device not getting redirected.

Legacy USB Redirection Configuration

June 27, 2024

If you are using any components older than version 2212 or if you are using CWA for Linux, follow this guide for configuring USB redirection in your environment.

Enabling Generic USB Redirection

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the **Client USB device redirection policy**.
4. Select **Allowed** and click **Save**.

Creating USB Redirection Policy Rules

When the user tries to redirect a USB device to Virtual Desktop, it is checked against each USB policy rule in turn until a match is found. The first match for any devices is considered final. If the first match is an Allow rule, the matched device is allowed to be redirected to the virtual desktop. If the first match is a Deny rule, the matched device is only available in the local desktop. If no match is found, default rules are used.

Setting the policy on the DDC:

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the **Client USB device redirection rules**.
4. Set the value based on the examples provided in the description for each usb device that needs to be redirected and click Save.
   For Example:
   Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Mass Storage

   > **Note:**
   >
   > If a Citrix admin checks Use default value and clicks on Save, the default rules can be found in the following registry in the VDA.
   >
   > **Caution!:**
   >
   > Refer to the Disclaimer at the end of this article before using the Registry Editor.
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

Using GPOs on the client:

1. Open the **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**.

2. Open the **USB Device Rules setting** and enable the setting. Add the USB Device rule as in this example,
   The Allow: VID=1230 PID=0007 rule allows the device with Vendor ID 1230 and Product ID 0007.

> **Note:**
>
> Use the Allow: VID=xxxx PID=xxxx rule when a specific device must be on top of the device rules list.



> **Note:**
>
> A tool like USBView or even the Connection toolbar can be used to determine the device details like VID and PID (include SS here).

Configure automatic redirection of USB devices

USB devices are automatically redirected when USB support is enabled. Also, the USB user preference settings are set to automatically connect USB devices. It is not always best to redirect all USB devices. Users can explicitly redirect devices from the USB device list that are not automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules on either the client endpoint or the DDC policy.

This policy can be set either on the DDC, on the client using a GPO, using Citrix Workspace Preferences or the Connections tab under CDViewer. All of these methods are described below:

Setting the policy on the DDC:

There are two policies on the DDC that can be set to allow auto redirection of USB devices- "Allow existing USB devices to be automatically connected, Allow newly arrived USB devices to be automatically connected'

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the setting **Allow existing USB devices to be automatically connected**.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
5. Edit the setting **Allow newly arrived USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Using GPOs on the client:

1. Open **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**.
2. Open **New USB Devices**, select **Enabled**, and click **OK**.
3. Open **Existing USB Devices**, select **Enabled**, and click **OK**.



Using Citrix Connection Center:

1. Go to **Citrix Workspace Preferences > Connections**.
2. Ensure that the following options are selected:

    a) When a session starts, connect devices automatically
    b) When a new device is connected while a session is running, connect the device automatically.

3. Click **OK**.

Using CDViewer Connection toolbar:

1. After a session starts, click on the **CDViewer** dropdown and select the **Citrix Workspace Preferences > Connections** tab.
2. Ensure that the following options are selected:

    a) When a session starts, connect devices automatically
    b) When a new device is connected while a session is running, connect the device automatically.

3. Click **Apply** and **OK** to save the policy.



For the client based configurations, the registry keys are set to the client device at the following location:

> **Caution!:**
>
> Refer to the Disclaimer at the end of this article before using the Registry Editor.
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

Graphics

March 22, 2022

Citrix HDX graphics include an extensive set of graphics acceleration and encoding technologies that optimizes the delivery of rich graphics applications from Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). The graphic technologies provide the same experience as using a physical desktop when working remotely with virtual applications that are graphics intensive.

You can use software or hardware for graphics rendering. Software rendering requires a third-party library called software rasterizer. For example, Windows includes the WARP rasterizer for DirectX based graphics. Sometimes, you might want to use an alternative software renderer. Hardware rendering (hardware acceleration) requires a graphics processor (GPU).

HDX Graphics offers a default encoding configuration that is optimized for the most common use cases. By using Citrix policies, IT administrators can also configure various graphics-related settings to meet different requirements and provide the desired user experience.

Thinwire

Thinwire is the Citrix default display remoting technology used in Citrix DaaS.

Display remoting technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display. Graphics are generated as a result of user input, for example, keystrokes or mouse actions.

HDX 3D Pro

The HDX 3D Pro capabilities in Citrix DaaS enable you to deliver desktops and applications that perform best using a graphics processing unit (GPU) for hardware acceleration. These applications include 3D professional graphics applications based on OpenGL and DirectX. The standard VDA supports GPU acceleration of DirectX only.

GPU acceleration for Windows Single-session OS

By using HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Single-session OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and GPU Passthrough and GPU virtualization technologies offered by XenServer, vSphere, and Hyper-V (passthrough only) hypervisors.

Using GPU Passthrough, you can create VMs that have exclusive access to dedicated graphics processing hardware. You can install multiple GPUs on the hypervisor and assign VMs to each of these GPUs on a one-to-one basis.

Using GPU virtualization, multiple virtual machines can directly access the graphics processing power of a single physical GPU.

GPU acceleration for Windows Multi-session OS

HDX 3D Pro allows graphics-heavy applications running in Windows Multi-session OS sessions to render on the server graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server GPU, graphics rendering doesn't slow down the server CPU. Also, the server is able to process more graphics because the workload is split among the CPU and GPU.

Framehawk

> **Important:**
>
> As of Citrix Virtual Apps and Desktops 7 1903, Framehawk is no longer supported. Instead, use Thinwire with adaptive transport enabled.

Framehawk is a display remoting technology for mobile workers on broadband wireless connections (Wi-Fi and 4G/LTE cellular networks). Framehawk overcomes the challenges of spectral interference and multipath propagation and delivers a fluid and interactive user experience to users of virtual apps and desktops.

Text-based session watermark

Text-based session watermarks help to deter and enable tracking data theft. This traceable information appears on the session desktop as a deterrent to those using photographs and screen captures to steal data. You can specify a watermark that is a layer of text. The watermark can display over the entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

Related information

- HDX 3D Pro
- GPU acceleration for Windows Single-session OS
- GPU acceleration for Windows Multi-session OS
- Thinwire
- Text-based session watermark

HDX 3D Pro

December 12, 2023

The HDX 3D Pro capabilities of Citrix Virtual Apps and Desktops enable you to deliver desktops and applications that perform best using a graphics processing unit (GPU) for hardware acceleration. These applications include 3D professional graphics applications based on OpenGL and DirectX. The standard VDA supports GPU acceleration of DirectX only.

For the HDX 3D Pro policy settings, see Optimize for 3D graphics workload.

All supported Citrix Workspace apps can be used with 3D graphics. For best performance with complex 3D workloads, high-resolution monitors, multi-monitor configurations, and high frame rate applications, we recommend the latest versions of Citrix Workspace app for Windows and Citrix Workspace

app for Linux. For more information on supported versions of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app.

Examples of 3D professional applications include:

- Computer-aided design, manufacturing, and engineering (CAD/CAM/CAE) applications
- Geographical Information System (GIS) software
- Picture Archiving Communication System (PACS) for medical imaging
- Applications using the latest OpenGL, DirectX, NVIDIA CUDA, and OpenCL and WebGL versions
- Computationally intensive non-graphical applications that use NVIDIA Compute Unified Device Architecture (CUDA) GPUs for parallel computing

HDX 3D Pro provides the best user experience over any bandwidth:

- On WAN connections: Deliver an interactive user experience over WAN connections with bandwidths as low as 1.5 Mbps.
- On LAN connections: Deliver a user experience equivalent to that of a local desktop on LAN connections.

  You can replace complex and expensive workstations with simpler user devices by moving the graphics processing into the data center for centralized management.

HDX 3D Pro provides GPU acceleration for Windows single-session OS machines and Windows multi-session OS machines. For more information, see GPU acceleration for Windows single-session OS and GPU acceleration for Windows multi-session OS.

HDX 3D Pro is compatible with GPU passthrough and GPU virtualization technologies offered by the following hypervisors, in addition to bare metal:

- XenServer
  - GPU passthrough with NVIDIA GRID, AMD, and Intel GVT-d
  - GPU virtualization with NVIDIA GRID, AMD, and Intel GVT-g
  - See hardware compatibility at Hypervisor Hardware Compatibility List.

Use the HDX Monitor tool to validate the operation and configuration of HDX visualization technologies and to diagnose and troubleshoot HDX issues. To download the tool and learn more about it, see https://taas.citrix.com/hdx/download/.

GPU acceleration for Windows multi-session OS

December 12, 2023

HDX 3D Pro allows graphics-heavy applications running in Windows Multi-session OS sessions to render on the server's graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server's GPU, graphics rendering does not slow the server's CPU. Also, the server is able to process more graphics because the workload is split between the CPU and GPU.

Since Windows Server is a multi-user operating system, multiple users can share a GPU accessed by Citrix Virtual Apps without the need for GPU virtualization (vGPU).

For procedures that involve editing the registry, use caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

GPU sharing

GPU Sharing enables GPU hardware rendering of OpenGL and DirectX applications in remote desktop sessions. It has the following characteristics:

- Can be used on bare metal or virtual machines to increase application scalability and performance.
- Enables multiple concurrent sessions to share GPU resources (most users do not require the rendering performance of a dedicated GPU).
- Requires no special settings.

A GPU can be assigned to the Windows Server virtual machine in either full pass-through or virtual GPU (vGPU) modes following Hypervisor and GPU vendor requirements. Bare-metal deployments on physical Windows Server machines are also supported.

GPU Sharing does not depend on any specific graphics card.

- For virtual machines, select a graphics card that is compatible with the Hypervisor in use. For a XenServer hardware compatibility list, see Hypervisor Hardware Compatibility List.
- When running on bare metal, it is recommended to have a single display adapter enabled by the operating system. If multiple GPUs are installed on the hardware, disable all but one of them using Device Manager.

Scalability using GPU Sharing depends on several factors:

- The applications being run
- The amount of video RAM they consume
- The graphics card's processing power

Some applications handle video RAM shortages better than others. If the hardware becomes overloaded, instability or a crash of the graphics card driver might occur. Limit the number of concurrent users to avoid such issues.

To confirm that GPU acceleration is occurring, use a third-party tool such as GPU-Z. GPU-Z is available at http://www.techpowerup.com/gpuz/.

- Access to a high-performance video encoder for NVIDIA GPUs and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature and allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA fall backs to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

DirectX, Direct3D, and WPF rendering

DirectX, Direct3D, and WPF rendering are only available on servers with a GPU that supports a display driver interface (DDI) version of 9ex, 10, or 11.

- On Windows Server 2008 R2, DirectX and Direct3D require no special settings to use a single GPU.
- On Windows Server 2012 and later, Remote Desktop Services (RDS) sessions on the RD Session Host server use the Microsoft Basic Render Driver as the default adapter. To use the GPU in RDS sessions on Windows Server 2012 and later, enable the **Use the hardware default graphics adapter for all Remote Desktop Services sessions** setting in the group policy **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Remote Session Environment**.
- To enable WPF applications to render using the server's GPU, create the settings in the registry of the server running Windows Multi-session OS sessions. For information on the registry setting, see Windows Presentation Foundation (WPF) rendering in the list of features managed through the registry.

GPU acceleration for CUDA or OpenCL applications

GPU acceleration of CUDA and OpenCL applications running in a user session is disabled by default.

To use the CUDA acceleration POC features, enable the registry settings. For information, see GPU acceleration for CUDA or OpenCL applications in the list of features managed through the registry.

GPU acceleration for Windows single-session OS

December 12, 2023

With HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Single-session OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and GPU Passthrough and GPU virtualization technologies offered by XenServer, vSphere, Nutanix, and Hyper-V (passthrough only) hypervisors.

HDX 3D Pro offers the following features:

- Adaptive H.264-based or H.265-based deep compression for optimal WAN and wireless performance. HDX 3D Pro uses CPU-based full-screen H.264 compression as the default compression technique for encoding. Hardware encoding with H.264 is used with NVIDIA, Intel, and AMD cards that support NVENC. Hardware encoding with H.265 is used with NVIDIA cards that support NVENC.
- Lossless compression option for specialized use cases. HDX 3D Pro also offers a CPU-based lossless codec to support applications where pixel-perfect graphics are required, such as medical imaging. True lossless compression is recommended only for specialized use cases because it consumes more network and processing resources.

  When using lossless compression:

  - The lossless indicator, a notification area icon, notifies the user if the screen displayed is a lossy frame or a lossless frame. This icon helps when the **Visual Quality** policy setting specifies **Build to lossless**. The lossless indicator turns green when the frames sent are lossless.
  - The lossless switch enables the user to change to Always Lossless mode anytime within the session. To select or deselect **Lossless anytime within a session**, right-click the icon and click **Switch to pixel perfect** or use the shortcut ALT+SHIFT+1.

    For lossless compression: HDX 3D Pro uses the lossless codec for compression regardless of the codec selected through policy.

    For lossy compression: HDX 3D Pro uses the original codec, either the default or the one selected through policy.

    Lossless switch settings are not retained for subsequent sessions. To use a lossless codec for every connection, select **Always lossless** in the **Visual quality** policy setting.
- You can override the default shortcut, ALT+SHIFT+1, to select or deselect Lossless within a session. Configure a new registry setting at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKEY_LOCAL_MACHINE_HotKey, Type: String

  - The format to configure a shortcut combination is C=0|1, A=0|1, S=0|1, W=0|1, K=val. Keys must be comma ","separated. The order of the keys does not matter.
  - A, C, S, W and K are keys, where C=Control, A=ALT, S=SHIFT, W=Win, and K=a valid key. Allowed values for K are 0–9, a–z, and any virtual key code.
  - For example:
    * For F10, set K=0x79
    * For Ctrl + F10, set C=1, K=0x79
    * For Alt + A, set A=1, K=a or A=1, K=A or K=A, A=1
    * For Ctrl + Alt + 5, set C=1, A=1, K=5 or A=1, K=5, C=1
    * For Ctrl + Shift + F5, set A=1, S=1, K=0x74

> **Caution:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- Multiple and high resolution monitor support. For Single-session OS machines, HDX 3D Pro supports user devices with up to four monitors. Users can arrange their monitors in any configuration and can mix monitors with different resolutions and orientations. The number of monitors is limited by the capabilities of the host computer GPU, the user device, and the available bandwidth. HDX 3D Pro supports all monitor resolutions and is limited only by the capabilities of the GPU on the host computer.
- Dynamic resolution. You can resize the virtual desktop or application window to any resolution. **Note**: The only supported method to change the resolution is by resizing the VDA session window. Changing resolution from within the VDA session (using **Control Panel > Appearance** and **Personalization > Display > Screen Resolution) is not supported**.
- Support for NVIDIA vGPU architecture. HDX 3D Pro supports NVIDIA vGPU cards. For information, see NVIDIA vGPU for GPU passthrough and GPU sharing. NVIDIA vGPU enables multiple VMs to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.
- Support for VMware vSphere and VMware ESX using Virtual Direct Graphics Acceleration (vDGA) - You can use HDX 3D Pro with vDGA for both RDS and VDI workloads.
- Support for VMware vSphere/ESX using NVIDIA vGPU and AMD MxGPU.
- Support for Microsoft HyperV using Discrete Device Assignment in Windows Server 2016.
- Support for Data Center Graphics with Intel Xeon Processor E3 Family. HDX 3D Pro supports multi-monitors (up to 3), console blanking, custom resolution, and high frame-rate with the

supported family of Intel processors. For more information, see http://www.citrix.com/intel and http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.

- Support for AMD RapidFire on the AMD FirePro S-series server cards. HDX 3D Pro supports multi-monitors (up to 6), console blanking, custom resolution, and high frame-rate. Note: HDX 3D Pro support for AMD MxGPU (GPU virtualization) works with VMware vSphere vGPUs only. XenServer and Hyper-V are supported with GPU passthrough. For more information, see AMD Virtualization Solution.
- Access to a high-performance video encoder for NVIDIA GPUs, AMD GPUs, and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature. The feature allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA falls back to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

As shown in the following figure:

- When a user logs on to Citrix Workspace app and accesses the virtual application or desktop, the Controller authenticates the user. The Controller then contacts the VDA for HDX 3D Pro to broker a connection to the computer hosting the graphical application.

The VDA for HDX 3D Pro uses the appropriate hardware on the host to compress views of the complete desktop or of just the graphical application.

- The desktop or application views and the user interactions with them are transmitted between the host computer and the user device. This transmission is done through a direct HDX connection between Citrix Workspace app and the VDA for HDX 3D Pro.



Optimize the HDX 3D Pro user experience

To use HDX 3D Pro with multiple monitors, ensure that the host computer is configured with at least as many monitors as are attached to user devices. The monitors attached to the host computer can be either physical or virtual.

Do not attach a monitor (either physical or virtual) to a host computer while a user is connected to the virtual desktop or application providing the graphical application. Doing so can cause instability during a user's session.

Let your users know that changes to the desktop resolution (by them or an application) are not supported while a graphical application session is running. After closing the application session, a user can change the resolution of the Desktop Viewer window in the Citrix Workspace app - Desktop Viewer Preferences.

When multiple users share a connection with limited bandwidth (for example, at a branch office), we recommend that you use the **Overall session bandwidth limit** policy setting to limit the bandwidth available to each user. Using this setting ensures that the available bandwidth does not fluctuate widely as users log on and off. Because HDX 3D Pro automatically adjusts to use all the available bandwidth, large variations in the available bandwidth over the course of user sessions can negatively impact performance.

For example, if 20 users share a 60 Mbps connection, the bandwidth available to each user can vary between 3 Mbps and 60 Mbps, depending on the number of concurrent users. To optimize the user experience in this scenario, determine the bandwidth required per user at peak periods and limit users to this amount always.

For users of a 3D mouse, we recommend that you increase the priority of the Generic USB Redirection virtual channel to 0. For information about changing the virtual channel priority, see the Knowledge Center article CTX128190.

Thinwire

May 9, 2023

Introduction

Thinwire, a part of Citrix HDX technology, is the Citrix default display remoting technology used in Citrix Virtual Apps and Desktops.

Display remoting technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display.

A successful display remoting solution provides a highly interactive user experience that is similar to that of a local PC. Thinwire achieves this experience by using a range of complex and efficient image analysis and compression techniques. Thinwire maximizes server scalability and consumes less bandwidth than other display remoting technologies.

Because of this balance, Thinwire meets most general business use cases and is used as the default display remoting technology in Citrix Virtual Apps and Desktops.

HDX 3D Pro

In its default configuration, Thinwire can deliver 3D or highly interactive graphics and use a graphics processing unit (GPU), if present. However, we recommend enabling HDX 3D Pro mode using the **Optimize for 3D graphics workload** or **Visual quality > Build to lossless** policies for scenarios when GPUs are present. These policies configure Thinwire to use a video codec (H.264 or H.265) to encode the entire screen using hardware acceleration if a GPU is present. Doing so provides a more fluid experience for 3D professional graphics. For more information, see H.264 Build to lossless, HDX 3D Pro, and GPU acceleration for Windows Single-session OS.

Requirements

Thinwire is optimized for modern operating systems, including Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows 10. For Windows Server 2008 R2, legacy graphics mode is recommended. Use the built-in Citrix policy templates, High Server Scalability-Legacy OS and Optimized for WAN-Legacy OS to deliver the Citrix recommended combinations of policy settings for these use cases.

> **Note:**
>
> We do not support legacy graphics mode in this release. It is included for backward compatibility when using XenApp 7.15 LTSR, XenDesktop 7.15 LTSR, and previous VDA releases.

- The policy setting which drives the behavior of Thinwire, **Use video codec for compression**, is available on VDA versions in Citrix Virtual Apps and Desktops 7 1808 or later and XenApp and XenDesktop 7.6 FP3 and later. The **Use video codec when preferred** option is the default setting on VDA versions Citrix Virtual Apps and Desktops 7 1808 or later and XenApp and XenDesktop 7.9 and later.
- All Citrix Workspace apps support Thinwire. Some Citrix Workspace apps might support features of Thinwire that others do not, for example, 8-bit or 16-bit graphics for reduced bandwidth usage. Support for such features is automatically negotiated by Citrix Workspace app.
- Thinwire uses more server resources (CPU, memory) in multi-monitor and high-resolution scenarios. It is possible to tune the amount of resources Thinwire uses, however, bandwidth usage might increase as a result.
- In low bandwidth or high latency scenarios, consider enabling 8-bit or 16-bit graphics to improve interactivity. Visual quality might be affected, especially at 8-bit color depth.

Encoding methods

Thinwire can operate in two different encoding modes depending on policy and client capabilities:

- Thinwire full screen H.264 or H.265
- Thinwire with selective H.264 or H.265

Legacy GDI remoting uses the XPDM remoting driver and not a Thinwire bitmap encoder.

Configuration

Thinwire is the default display remoting technology.

The following Graphics policy setting sets the default and provides alternatives for different use cases:

- Use video codec for compression
  - **Use video codec when preferred**. This is the default setting. No additional configuration is required. Keeping this setting as the default ensures that Thinwire is selected for all Citrix connections, and is optimized for scalability, bandwidth, and superior image quality for typical desktop workloads. This is functionally equivalent to **For actively changing regions**.
- Other options in this policy setting continue to use Thinwire with other technologies for different use cases. For example:
  - **For actively changing regions**. The adaptive display technology in Thinwire identifies moving images (video, 3D in motion) and uses H.264 or H.265 only in the part of the screen where the image is moving.
  - **For the entire screen**. Delivers Thinwire with full-screen H.264 or H.265 to optimize for improved user experience and bandwidth in cases with heavy use of 3D graphics. In the case of H.264 4:2:0 (the **Visually lossless** policy is disabled), the final image is not pixel perfect (lossless) and might not be suitable for certain scenarios. In such cases, consider using H.264 Build to lossless instead.



Various other policy settings, including the following Visual display policy settings can be used to fine tune the performance of display remoting technology. Thinwire supports them all.

- Preferred color depth for simple graphics
- Target frame rate
- Visual quality

To get the Citrix recommended combinations of policy settings for different business use cases, use the built-in Citrix Policy templates. The **High Server Scalability** and **Very High Definition User Experience** templates both use Thinwire with the optimum combinations of policy settings for your organization's priorities and your users' expectations.

Monitoring Thinwire

You can monitor the use and performance of Thinwire from Citrix Director. The HDX virtual channel details view contains useful information for troubleshooting and monitoring Thinwire in any session. To view Thinwire-related metrics:

1. In Director, search for a user, machine or endpoint, open an active session and click **Details**. Or, you can select **Filters > Session > All Sessions**, open an active session and click **Details**.
2. Scroll down to the **HDX** panel.



3. Select **Graphics - Thinwire**.



Lossless compression codec (MDRLE)

In a typical desktop session, most of the imagery is simple graphics or text regions. Thinwire determines where these regions are and selects these areas for lossless encoding using the 2DRLE codec. At the Citrix Workspace app client side, these elements are decoded using the Citrix Workspace app-side 2DRLE decoder for session display.

In XenApp and XenDesktop 7.17, we added a higher compression ratio MDRLE codec that consumes less bandwidth in typical desktop sessions than the 2DRLE codec. This new codec does not impact server scalability.

Lower bandwidth usually means improved session interactivity (especially on shared or constrained links) and reduced costs. For example, the expected bandwidth consumption when using the MDRLE codec is approximately 10–15% less compared with XenApp and XenDesktop 7.15 LTSR for typical Office-like workloads.

Configuration isn't required for the MDRLE codec. If Citrix Workspace app supports MDRLE decoding, the VDA uses the VDA MDRLE encoding and the Citrix Workspace app MDRLE decoding. If Citrix Workspace app doesn't support MDRLE decoding, the VDA automatically falls back to 2DRLE encoding.

MDRLE Requirements:

- Citrix Virtual Apps and Desktops minimum version 7 1808 VDAs
- XenApp and XenDesktop minimum version 7.17 VDAs
- Citrix Workspace app for Windows minimum version 1808
- Citrix Receiver for Windows minimum version 4.11

Progressive Mode

Citrix Virtual Apps and Desktops 1808 introduced progressive mode and enabled it by default. In constrained network conditions (default: bandwidth < 2 Mbps, or latency > 200 ms), Thinwire increased the compression of text and static imagery to improve interactivity during screen activity. The heavily compressed text and images are then progressively sharpened, in a random block fashion, when screen activity stopped. While compressing and sharpening this way improves overall interactivity, it reduces cache efficiency and increases bandwidth usage.

As of Citrix Virtual Apps and Desktops 1906, progressive mode is disabled by default. We now use a different approach. The quality of still images is now based on network conditions and floats between a pre-defined minimum and maximum value for each **Visual quality** setting. Because there is no explicit sharpening step, Thinwire optimizes image delivery and maintains cache efficiency, while providing nearly all of the benefits of progressive mode.

Changing progressive mode behavior

You can change the progressive mode state with the registry key. For information, see Progressive mode in the list of features managed through the registry.

H.264 Build to lossless

Build to lossless is a special Thinwire configuration that optimizes graphics delivery for interactivity and final image quality. You can enable this setting by setting the **Visual quality** policy to **Build to lossless**.

Build to lossless compresses the screen using H.264 (or H.265) during screen activity and sharpens to pixel perfect (lossless) when activity stops. The H.264 (or H.265) image quality adapts to available resources to maintain the best possible frame rate. The sharpening step is performed gradually, giving an immediate response if the user begins screen activity shortly after sharpening starts. For example, selecting a model and rotating it.

H.264 **Build to lossless** offers all the advantages of full screen H.264 or H.265, including hardware acceleration, but with the added benefit of a final, guaranteed lossless screen. This is critical for 3D-type workloads that require a final pixel-perfect image. For example, manipulating medical imagery. Also, H.264 **Build to lossless** uses fewer resources than full screen H.264 4:4:4. As a result, using **Build to lossless** usually results in a higher frame rate than Visually lossless H.264 4:4:4.

> **Note:**
>
> In addition to the **Visual quality** policy, set the **Use video codec** policy to **Use when preferred** (default) or **For actively changing regions**. You can revert to non-H.264 Build to lossless by

> setting the **Use video codec** policy to **Do not use video codec**. This results in moving images being encoded with JPEG instead of H.264 (or H.265).

Text-based session watermark

March 23, 2022

Text-based session watermarks help to deter and enable tracking data theft. This traceable information appears on the session desktop as a deterrent to those using photographs and screen captures to steal data. You can specify a watermark that is a layer of text, which displays over the entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

> **Important:**
>
> Text-based session watermarking is not a security feature. The solution does not prevent data theft completely, but it provides some level of deterrent and traceability. Although we do not guarantee complete information traceability when using this feature, we recommend that you combine this feature with other security solutions as applicable.

The session watermark is text and is applied to the session that is delivered to the user. The session watermark carries information for tracking data theft. The most important data is the identity of the logon user of the current session in which the screen image was taken. To trace the data leakage more effectively, include other information such as server or client internet protocol address and a connect time.

To adjust the user experience, use the Session Watermark policy settings to configure the placement and watermark appearance on the screen.

Requirements:

Virtual Delivery Agents:

Multi-session OS 7.17
Single-session OS 7.17

Limitations:

- Session watermarks are not supported in sessions where Local App Access, Windows media redirection, MediaStream, browser content redirection, and HTML5 video redirection are used. To use session watermark, ensure that these features are disabled.
- Session watermark is not supported and doesn't appear if the session is running in full-screen hardware accelerated modes (full-screen H.264 or H.265 encoding).

- If you set these HDX policies, watermark settings don't take effect and a watermark isn't displayed in the session display.

Use hardware encoding for video codec to **Enabled**
Use video codec for compression to **For the entire screen**

- If you set these HDX policies, the behavior is undetermined and the watermark might not display.

  Use hardware encoding for video codec to **Enabled**
  Use video codec for compression to **Use video codec when preferred**

  To ensure the watermark displays, set **Use hardware encoding for video codec** to **Disabled**, or set **Use video codec for compression** to **For actively changing regions** or **Do not use video codec**.

- Session watermark supports only the Thinwire graphics mode.
- If you use Session Recording, the recorded session doesn't include the watermark.
- If you use Windows remote assistance, the watermark is not shown.
- If a user presses the **Print Screen** key to capture the screen, the screen captured at the VDA side doesn't include the watermarks. We recommend that you take measures to avoid the captured image being copied.

Multimedia

March 22, 2022

The HDX technology stack supports the delivery of multimedia applications through two complementary approaches:

- Server-side rendering multimedia delivery
- Client-side rendering multimedia redirection

This strategy ensures that you can deliver a full range of multimedia formats, with a great user experience, while maximizing server scalability to reduce the cost-per-user.

With server-rendered multimedia delivery, audio and video content is decoded and rendered on the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server by the application. The content is then compressed and delivered using ICA protocol to Citrix Workspace app on the user device. This method provides the highest rate of compatibility with various applications and media formats. Because video processing is compute-intensive, server-rendered multimedia delivery benefits greatly from the onboard hardware acceleration. For example, support for DirectX Video Acceleration (DXVA)

offloads the CPU by performing H.264 decoding in separate hardware. Intel Quick Sync, AMD Rapid-Fire, and NVIDIA NVENC technologies provide hardware-accelerated H.264 encoding.

Because most servers do not offer any hardware acceleration for video compression, server scalability is negatively impacted if all video processing is done on the server CPU. You can maintain high server scalability, by redirecting many multimedia formats to the user device for local rendering.

- Windows Media redirection offloads the server for a wide variety of media formats typically associated with the Windows Media Player.
- HTML5 video has become popular, and Citrix introduced a redirection technology for this type of content. We recommend the browser content redirection for websites using HTML5, HLS, DASH, or WebRTC.
- You can apply the general contact redirection technologies Host-to-client redirection and Local App Access to the multimedia content.

Putting these technologies together, if you don't configure redirection, HDX does Server-Side Rendering.
If you configure redirection, HDX uses either Server Fetch and Client Render or Client Fetch and Client Render. If those methods fail, HDX falls back to Server-Side Rendering as needed and is subject to the Fallback Prevention Policy.

Example scenarios



Scenario 1. (Server Fetch and Server Rendering):

1. The server fetches the media file from its source, decodes, and then presents the content to an audio device or display device.
2. The server extracts the presented image or sound from the display device or audio device respectively.
3. The server optionally compresses it, and then transmits it to the client.

This approach incurs a high CPU cost, high bandwidth cost (if the extracted image/sound isn't compressed efficiently), and has low server scalability.

Thinwire and Audio virtual channels handle this approach. The advantage of this approach is that it reduces the hardware and software requirements for the clients. Using this approach the decoding happens on the server and it works for a wider variety of devices and formats.

Scenario 2. (Server Fetch and Client Render):

This approach relies on being able to intercept the media content before it is decoded and presented to the audio or display device. The compressed audio/video content is instead sent to the client where it is then decoded and presented locally. The advantage of this approach is that the are offloaded to the client devices, saving CPU cycles on the server.

However, it also introduces some additional hardware and software requirements for the client. The client must be able to decode each format that it might receive.

Scenario 3. (Client Fetching and Client Rendering):

This approach relies on being able to intercept the media content URL before it's fetched from the source. The URL is sent to the client where the media content is fetched, decoded, and presented locally. This approach is conceptually simple. Its advantage is that it saves both CPU cycles on the server and bandwidth because the server sends only control commands. However, the media content is not always accessible to the clients.

Framework and platform:

Single-session operating systems (Windows, Mac OS X, and Linux) provide multimedia frameworks that enable the faster development of multimedia applications. This table lists some of the more popular multimedia frameworks. Each framework divides media processing into several stages and uses a pipelined-based architecture.

Framework	Platform
DirectShow	Windows (98 and later)
Media Foundation	Windows (Vista and later)
Gstreamer	Linux
Quicktime	Mac OS X

Double hop support with media redirection technologies

	Audio redirection	No
	Browser content redirection	No
	HDX webcam redirection	Yes
	HTML5 Video redirection	Yes
	Windows Media redirection	Yes

Audio features

September 19, 2022

You can configure and add the following Citrix policy settings to a policy that optimizes HDX audio features. For usage details plus relationships and dependencies with other policy settings, see Audio policy settings and Bandwidth policy settings and Multi-stream connections policy settings.

> **Important:**
>
> We recommend delivering audio using User Datagram Protocol (UDP) rather than TCP. Only Windows Virtual Delivery Agent (VDA) supports audio over UDP.
>
> UDP audio encryption using DTLS is available only between Citrix Gateway and Citrix Workspace app. Therefore, sometimes it might be preferable to use TCP transport. TCP supports end-to-end TLS encryption from the VDA to Citrix Workspace app.

Audio quality

In general, higher sound quality consumes more bandwidth and server CPU utilization by sending more audio data to user devices. Sound compression allows you to balance sound quality against overall session performance; use Citrix policy settings to configure the compression levels to apply to sound files.

By default, the **Audio quality policy** setting is set to High - high definition audio when TCP transport is used. The policy is set to Medium - optimized-for-speech when UDP transport (recommended) is used. The **High Definition audio** setting provides high fidelity stereo audio, but consumes more bandwidth than other quality settings. Do not use this audio quality for non-optimized voice chat or video chat applications (such as softphones). The reason being that it might introduce latency into the audio path that is not suitable for real-time communications. We recommend the optimized for speech policy setting for real-time audio, regardless of the selected transport protocol.

When the bandwidth is limited, for example satellite or dial-up connections, reducing audio quality to **Low** consumes the least possible bandwidth. In this situation, create separate policies for users on low-bandwidth connections so that users on high-bandwidth connections are not adversely impacted.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device.

Bandwidth guidelines for audio playback and recording:

- High quality (default)

  - Bitrate: ~100 kbps (min 75, max 175 kbps) for playback / ~70 kbps for microphone capture
  - Number of Channels: 2 (Stereo) for playback, 1 (mono) for microphone capture
  - Frequency: 44100 Hz
  - Bit-depth: 16-bit

- Medium quality (recommended for VoIP)
  - Bitrate: ~16 kbps (min 20, max 40 kbps) for playback, ~16 kbps for microphone capture
  - Number of Channels: 1 (Mono) for both playback and capture
  - Frequency: 16000 Hz (wideband)
  - Bit-depth: 16-bit

- Low quality
  - Bitrate: ~ 11 kbps (min 10; max 25 kbps) for playback, ~11 kbps for microphone capture
  - Number of Channels: 1 (Mono) for both playback and capture
  - Frequency: 8000 Hz (narrowband)
  - Bit-depth: 16-bit

Client audio redirection

To allow users to receive audio from an application on a server through speakers or other sound devices on the user device, leave the **Client audio redirection** setting at **Allowed**. This is the default.

Client audio mapping puts extra load on the servers and the network. However, prohibiting client audio redirection disables all HDX audio functionality.

For setting details, see Audio policy settings. Remember to enable client audio settings on the user device.

Client microphone redirection

To allow users to record audio using input devices such as microphones on the user device, leave the **Client microphone redirection** setting at its default (Allowed).

For security, user devices alert their users when servers they don't trust try to access microphones. Users can choose to accept or reject access before using the microphone. Users can disable this alert on Citrix Workspace app.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device.

Audio Plug N Play

The Audio Plug N Play policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is **Enabled** by default. Audio Plug N Play enables audio devices to be recognized. The devices are recognized even if they are not plugged in until after the user session has started.

This setting applies only to Windows Multi-session OS machines.

For setting details, see Audio policy settings.

Audio redirection bandwidth limit and audio redirection bandwidth limit percent

The Audio redirection bandwidth limit policy setting specifies the maximum bandwidth (in kilobits per second) for a playing and recording audio in a session.

The Audio redirection bandwidth limit percent setting specifies the maximum bandwidth for audio redirection as a percentage of the total available bandwidth.

By default, zero (no maximum) is specified for both settings. If both settings are configured, the one with the lowest bandwidth limit is used.

For setting details, see Bandwidth policy settings. Remember to enable Client audio settings on the user device.

Audio over UDP Real-time Transport and Audio UDP port range

By default, Audio over User Datagram Protocol (UDP) Real-time Transport is allowed (when selected at the time of installation). It opens up a UDP port on the server for connections that use Audio over UDP Real-time Transport. If there is network congestion or packet loss, we recommend configuring UDP/RTP for audio to ensure the best possible user experience. For any real time audio such as soft-phone applications, UDP audio is preferred to EDT. UDP allows for packet loss without retransmission, ensuring that no latency is added on connections with high packet loss.

> **Important:**
>
> When Citrix Gateway is not in the path, audio data transmitted with UDP is not encrypted. If Citrix Gateway is configured to access Citrix Virtual Apps and Desktops resources, then audio traffic between the endpoint device and Citrix Gateway is secured using DTLS protocol.

The Audio UDP port range specifies the range of port numbers that the Windows VDA uses to exchange audio packet data with the user device.

By default, the range is 16500 through 16509.

For setting details about Audio over UDP Real-time Transport, see Audio policy settings. For details about Audio UDP port range, see Multi-stream connections policy settings. Remember to enable Client audio settings on the user device.

Audio over UDP requires the Windows VDA. For supported policies on the Linux VDA, see Policy support list.

Audio setting policies for user devices

1. Load the group policy templates by following Configuring the Group Policy Object administrative template.
2. In the Group Policy Editor, expand **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.
3. For **Client audio settings**, select **Not Configured**, **Enabled**, or **Disabled**.
   - **Not Configured**. By default, Audio Redirection is enabled using high quality audio or the previously configured custom audio settings.
   - **Enabled**. Enables audio redirection using the selected options.
   - **Disabled**. Disables audio redirection.
4. If you select **Enabled**, choose a sound quality. For UDP audio, use **Medium** (default).
5. For UDP audio only, select **Enable Real-Time Transport** and then set the range of incoming ports to open in the local Windows firewall.
6. To use UDP Audio with Citrix Gateway, select **Allow Real-Time Transport Through gateway**. Configure Citrix Gateway with DTLS. For more information, see this article.

As an Administrator, if you do not have control on endpoint devices to make these changes, use the default.ica attributes from StoreFront to enable UDP Audio. For example, for bring your own devices or home computers.

1. On the StoreFront machine, open C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica with an editor such as notepad.
2. Make the following entries under the [Application] section.

   ; This text enables Real-Time Transport

   EnableRtpAudio=true

   ; This text allows Real-Time Transport Through gateway

   EnableUDPThroughGateway=true

   ; This text sets audio quality to Medium

   AudioBandwidthLimit=1

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

If you enable User Datagram Protocol (UDP) audio by editing default.ica, then UDP audio is enabled for all users who are using that store.

Avoid echo during multimedia conferences

Users in audio or video conferences might hear an echo. Echoes usually occur when speakers and microphones are too close to each other. For that reason, we recommend the use of headsets for audio and video conferences.

HDX provides an echo cancellation option (enabled by default) that minimizes any echo. The effectiveness of echo cancellation is sensitive to the distance between the speakers and the microphone. Ensure that the devices aren't too close or too far away from each other.

You can change a registry setting to disable echo cancellation. For information, see Avoid echo during multimedia conferences in the list of features managed through the registry.

Softphones

A softphone is software acting as a phone interface. You use a softphone to make calls over the internet from a computer or other smart device. By using a softphone, you can dial phone numbers and carry out other phone-related functions using a screen.

Citrix Virtual Apps and Desktops support several alternatives for delivering softphones.

- **Control mode**. The hosted softphone controls a physical telephone set. In this mode, no audio traffic goes through the Citrix Virtual Apps and Desktops server.
- **HDX RealTime optimized softphone support (recommended)**. The media engine runs on user device, and Voice over Internet Protocol traffic flows peer-to-peer. For examples, see:
  - HDX Optimization for Microsoft Teams
  - HDX RealTime Optimization Pack, which optimizes the delivery of Microsoft Skype for Business
  - Cisco Jabber Softphone for VDI (formerly known as VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (formerly known as VDI Communicator)
  - Zoom VDI Plugin
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic dictation device

- **Local App Access**. A Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) feature that allows an application such as a softphone to run locally on the Windows user device yet appear seamlessly integrated with their virtual/published desktop. This feature offloads all audio processing to the user device. For more information, see Local App Access and URL redirection.
- **HDX RealTime generic softphone support.** Voice over Internet Protocol-over-ICA.

Generic softphone support

Generic softphone support, enables you to host an unmodified softphone on XenApp or XenDesktop in the data center. The audio traffic goes over the Citrix ICA protocol (preferably using UDP/RTP) to the user device running the Citrix Workspace app.

Generic softphone support is a feature of HDX RealTime. This approach to softphone delivery is especially useful when:

- An optimized solution for delivering the softphone is not available and the user is not on a Windows device where Local App Access can be used.
- The media engine that is needed for optimized delivery of the softphone isn't installed on the user device or isn't available for the operating system version running on the user device. In this scenario, Generic HDX RealTime provides a valuable fallback solution.

There are two softphone delivery considerations using Citrix Virtual Apps and Desktops:

- How the softphone application is delivered to the virtual/published desktop.
- How the audio is delivered to and from the user headset, microphone, and speakers, or USB telephone set.

Citrix Virtual Apps and Desktops include numerous technologies to support generic softphone delivery:

- Optimized-for-Speech codec for fast encode of the real-time audio and bandwidth efficiency.
- Low latency audio stack.
- Server-side jitter buffer to smooth out the audio when the network latency fluctuates.
- Packet tagging (DSCP and WMM) for Quality of Service.
  - DSCP tagging for RTP packets (Layer 3)
  - WMM tagging for Wi-Fi

The Citrix Workspace app versions for Windows, Linux, Chrome, and Mac also are Voice over Internet Protocol capable. Citrix Workspace app for Windows offers these features:

- Client-side jitter buffer - Ensures smooth audio even when the network latency fluctuates.
- Echo cancellation - Allows for greater variation in the distance between microphone and speakers for workers who do not use a headset.

- Audio plug-n-play - Audio devices do not need to be plugged in before starting a session. They can be plugged in at any time.
- Audio device routing - Users can direct ringtone to speakers but the voice path to their headset.
- Multi-stream ICA - Enables flexible Quality of Service-based routing over the network.
- ICA supports four TCP and two UDP streams. One of the UDP streams supports the real-time audio over RTP.

For a summary of Citrix Workspace app capabilities, see Citrix Receiver Feature Matrix.

System configuration recommendations

Client Hardware and Software:
For optimal audio quality, we recommend the latest version of Citrix Workspace app and a good quality headset that has acoustic echo cancellation (AEC). Citrix Workspace app versions for Windows, Linux, and Mac support Voice over Internet Protocol. Also, Dell Wyse offers Voice over Internet Protocol support for ThinOS (WTOS).

CPU Considerations:
Monitor CPU usage on the VDA to determine if it is necessary to assign two virtual CPUs to each virtual machine. Real-time voice and video are data intensive. Configuring two virtual CPUs reduces the thread switching latency. Therefore, we recommend that you configure two vCPUs in a Citrix Virtual Desktops VDI environment.

Having two virtual CPUs does not necessarily mean doubling the number of physical CPUs, because physical CPUs can be shared across sessions.

Citrix Gateway Protocol (CGP), which is used for the Session Reliability feature, also increases CPU consumption. On high-quality network connections, you can disable this feature to reduce CPU consumption on the VDA. Neither of the preceding steps might be necessary on a powerful server.

UDP Audio:
Audio over UDP provides excellent tolerance of network congestion and packet loss. We recommend it instead of TCP when available.

LAN/WAN configuration:
Proper configuration of the network is critical for good real-time audio quality. Typically, you must configure virtual LANs (VLANs) because excessive broadcast packets can introduce jitter. IPv6-enabled devices might generate many broadcast packets. If IPv6 support is not needed, you can disable IPv6 on those devices. Configure to support Quality of Service.

Settings for use WAN connections:
You can use voice chat over LAN and WAN connections. On a WAN connection, audio quality depends on the latency, packet loss, and jitter on the connection. If delivering softphones to users on a WAN connection, we recommend using the NetScaler SD-WAN between the data center and the remote office. Doing so maintains a high Quality of Service. NetScaler SD-WAN supports Multi-Stream ICA,

including UDP. Also, for a single TCP stream, it's possible to distinguish the priorities of various ICA virtual channels to ensure that high priority real-time audio data receives preferential treatment.

Use Director or the HDX Monitor to validate your HDX configuration.

Remote user connections:
Citrix Gateway supports DTLS to deliver UDP/RTP traffic natively (without encapsulation in TCP). Open firewalls bidirectionally for UDP traffic over Port 443.

Codec selection and bandwidth consumption:
Between the user device and the VDA in the data center, we recommend using the **Optimized-for-Speech** codec setting, also known as Medium Quality audio. Between the VDA platform and the IP-PBX, the softphone uses whatever codec is configured or negotiated. For example:

- G711 provides good voice quality but has a bandwidth requirement of from 80 kilobits per second through 100 kilobits per second per call (depending on Network Layer2 overheads).
- G729 provides good voice quality and has a low bandwidth requirement of from 30 kilobits per second through 40 kilobits per second per call (depending on Network Layer 2 overheads).

Delivering softphone applications to the virtual desktop

There are two methods by which you can deliver a softphone to the XenDesktop virtual desktop:

- The application can be installed in the virtual desktop image.
- The application can be streamed to the virtual desktop using Microsoft App-V. This approach has manageability advantages because the virtual desktop image is kept uncluttered. After being streamed to the virtual desktop, the application runs in that environment as if it was installed in the usual manner. Not all applications are compatible with App-V.

Delivering audio to and from the user device

Generic HDX RealTime supports two methods of delivering audio to and from the user device:

- **Citrix Audio Virtual Channel**. We generally recommend the Citrix Audio Virtual Channel because it's designed specifically for audio transport.
- **Generic USB Redirection**. Supports audio devices having buttons or a display (or both), human interface device (HID), if the user device is on a LAN or LAN-like connection back to the Citrix Virtual Apps and Desktops server.

Citrix audio virtual channel

The bidirectional Citrix Audio Virtual Channel (CTXCAM) enables audio to be delivered efficiently over the network. Generic HDX RealTime takes the audio from the user headset or microphone and compresses it. Then, it sends it over ICA to the softphone application on the virtual desktop. Likewise, the audio output of the softphone is compressed and sent in the other direction to the user headset or speakers. This compression is independent of the compression used by the softphone itself (such

as G.729 or G.711). It is done using the Optimized-for-Speech codec (Medium Quality). Its characteristics are ideal for Voice over Internet Protocol. It features quick encode time, and it consumes only approximately 56 Kilobits per second of network bandwidth (28 Kbps in each direction), peak. This codec must be explicitly selected in the service's Manage console because it is not the default audio codec. The default is the HD Audio codec (High Quality). This codec is excellent for high fidelity stereo soundtracks but is slower to encode compared to the Optimized-for-Speech codec.

Generic USB Redirection

Citrix Generic USB Redirection technology (CTXGUSB virtual channel) provides a generic means of remoting USB devices, including composite devices (audio plus HID) and isochronous USB devices. This approach is limited to LAN-connected users. This reason being that the USB protocol tends to be sensitive to network latency and requires considerable network bandwidth. Isochronous USB redirection works well when using some softphones. This redirection provides excellent voice quality and low latency. However, Citrix Audio Virtual Channel is preferred because it is optimized for audio traffic. The primary exception is when you're using an audio device with buttons. For example, a USB telephone attached to the user device that is LAN-connected to the data center. In this case, Generic USB Redirection supports buttons on the phone set or headset that control features by sending a signal back to the softphone. There isn't an issue with buttons that work locally on the device.

Limitation

After you install an audio device on your client, enable the audio redirection, and start an RDS session, the audio files might not play audio. As a workaround, add the registry key on the RDS machine, and then restart the machine. For information, see Audio limitation in the list of features managed through the registry.

Browser content redirection

June 15, 2022

Browser content redirection prevents the rendering of webpages in the allow list on the VDA side. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL.

> **Note:**
>
> You can specify that webpages be redirected to the VDA side (and not redirected on the client side) by using a block list.

This overlay web layout engine runs on the endpoint device instead of on the VDA and uses the endpoint CPU, GPU, RAM, and Network.

Only the browser viewport is redirected. The viewport is the rectangular area in your browser where content displays. The viewport doesn't include things like the Address Bar, Favorites Toolbar, Status Bar. Those items are in the user interface, which are still running on the browser in the VDA.



1. Configure a policy in the Manage > Full Configuration interface that specifies the Access Control List containing the URLs for redirection from the allow or block lists. For the browser on the VDA to detect that the URL that the user is navigating to matches the allow list or does not match a block list, a browser extension performs the comparison. The browser extension (BHO) for Internet Explorer 11 is included in the installation media and is installed automatically. For Chrome, the browser extension is available in the Chrome Web Store, and you can deploy it using the Group Policies and ADMX files. Chrome extensions are installed on a per-user basis. Updating a golden image to add or remove an extension is not required.
2. If a match is found in the allow list (for example `https://www.mycompany.com/`), and there is no match to a URL in the block list (for example `https://www.mycompany.com/engineering`), a virtual channel (CTXCSB) instructs Citrix Workspace app that a redirection is required and relays the URL. Citrix Workspace app then instantiates a local rendering engine and displays the website.
3. Citrix Workspace app then blends back the website into the virtual desktop browser content area seamlessly.

The color of the logo specifies the status of the Chrome extension. It is one of these three colors:

- Green: Active and connected.
- Gray: Not active/idle on the current tab.
- Red: Broken/Not working.

You can debug logging by using **Options** in the extensions menu.



Here are scenarios of how Citrix Workspace app fetches content:

- **Server fetch and server render**: There is no redirection because you didn't add the site to the allow list or the redirection failed. We fall back to rendering the webpage on the VDA and use Thinwire to remote the graphics. Use policies to control the fallback behavior. High CPU, RAM, and bandwidth consumption on the VDA.
- **Server fetch and client render**: Citrix Workspace app contacts and fetches content from the web server through the VDA using a virtual channel (CTXPFWD). This option is useful when the client doesn't have internet access (for example, thin clients). Low CPU and RAM consumption on the VDA, but bandwidth is consumed on the ICA virtual channel.

  There are three modes of operation for this scenario. The term proxy refers to a proxy device that the VDA accesses to gain Internet access.

  Which policy option to choose:

  - Explicit Proxy - If you have a single explicit proxy in your Datacenter.
  - Direct or Transparent - If you do not have proxies, or if you use transparent proxies.
  - PAC files - If you rely on PAC files so browsers in the VDA can automatically choose the appropriate proxy server for fetching a specified URL.



- **Client fetch and client render**: Because Citrix Workspace app contacts the web server directly, it requires internet access. This scenario offloads all the network, CPU, and RAM usage from your XenApp and XenDesktop Site.

Redirection scenarios



Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

Fallback mechanism:

There might be times when client redirection fails. For example, if the client machine does not have direct internet access, an error response might go back to the VDA. In such cases, the browser on the

VDA can then reload and render the page on the server.

You can suppress server rendering of video elements by using the existing **Windows media fallback prevention** policy. Set this policy to **Play all content only on client** or **Play only client-accessible content on client**. These settings block video elements from playing on the server if there are failures in client redirection. This policy takes effect only when you enable browser content redirection and the **Access Control List** policy contains the URL that falls back. The URL can't be in the block list policy.

System requirements:

Windows endpoints:

- Windows 10 or 11
- Citrix Workspace app 1809 for Windows or later

> **Note:**
>
> Browser content redirection is supported only on the Current Release of Citrix Workspace app for Windows, but not on the Citrix Workspace app LTSR releases, 1912 and 2203.1.

Linux endpoints:

- Citrix Workspace app 1808 for Linux or later
- Citrix Receiver for Linux 13.9 or later
- Thin client terminals must include WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 and XenApp and XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- VDA operating system: Windows 10 (minimum version 1607), Windows Server 2012 R2, Windows Server 2016
- Browser on the VDA:
  - Google Chrome v66 or higher (Chrome requires Citrix Workspace app 1809 for Windows on the user endpoint, Citrix Virtual Apps and Desktops 7 1808 VDA, and the browser content redirection extension)
  - Internet Explorer 11 and configure these options:
    - Clear **Enhanced Protected Mode** under: **Internet Options** > **Advanced > Security**
    - Check **Enable third-party browser extensions** under: **Internet Options > Advanced > Browsing**

Troubleshooting

For troubleshooting information, see the Knowledge Center article https://support.citrix.com/article/CTX230052

Browser content redirection Chrome extension

To use browser content redirection with Chrome, add the browser content redirection extension from the Chrome Web Store. Click **Add to Chrome** in the Citrix Virtual Apps and Desktops environment.

The extension is **not** required on the user's client machine –only in the VDA.

System requirements

- Chrome v66 or higher
- Browser content redirection extension
- Citrix Virtual Apps and Desktops 7 1808 or higher
- Citrix Workspace app 1809 for Windows or higher

> **Note:**
>
> Browser content redirection is supported only on the Current Release of Citrix Workspace app for Windows, but not on the Citrix Workspace app LTSR releases, 1912 and 2203.1.



This method works for individual users. To deploy the extension to a large group of users in your organization, deploy the extension using Group Policy.

Deploy the extension using Group Policy

1. Import the Google Chrome ADMX files into your environment. For information about downloading policy templates and installing and configuring the templates into your Group Policy Editor,

see Set Chrome Browser policies on managed PCs.

2. Open your Group Policy Management console and go to **User Configuration \ Administrative Templates\Classic Administrative Templates (ADM) \ Google\ Google Chrome \ Extensions**. Enable the **Configure the list of force-installed apps and extensions** setting.



3. Click **Show** and type the following string, which corresponds to the extension ID. Update the URL for the browser content redirection extension.

```
hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
```




4. Apply the setting and after a **gpupdate** refresh, the user automatically receives the extension. If you launch the Chrome browser in the user's session, the extension is already applied and they cannot remove it.

   Any updates to the extension are automatically installed on the users'machines through the update URL that you specified in the setting.

   If the **Configure the list of force-installed apps and extensions** setting is set to **Disabled**, the extension is automatically removed from Chrome for all users.

Browser content redirection Edge Chromium extension

To install the browser content redirection extension in Edge, make sure you have version **83.0.478.37** or higher of the Edge browser installed.

1. Click the **Extensions** option in the menu and turn on **Allow extensions from other stores**.

2. Click the **Chrome Web Store** link and the extension appears at the bar on the top right. For more info on Microsoft Edge extensions, see Extensions.



Browser content redirection and DPI

When using browser content redirection with the DPI (scaling) set to anything over 100% on the user's machine, the redirected browser content screen displays incorrectly. To avoid this issue, do not set the DPI when using browser content redirection. Another way to avoid the issue is by disabling browser content redirection GPU acceleration for Chrome by creating the registry key on the user's machine. For information, see Browser content redirection and DPI in the list of features managed through the registry.

User-agent request header

The user-agent header helps identify HTTP requests sent from browser content redirection. This setting can be useful when you configure proxy and firewall rules. For example, if the server blocks the requests sent from browser content redirection, you can create a rule that contains the user-agent header to bypass certain requirements.

Only Windows devices support the user-agent request header.

By default, the user-agent request header string is disabled. To enable the user-agent header for client-rendered content, use the Registry editor. For information, see User-agent request header in the list of features managed through the registry.

HDX video conferencing and webcam video compression

March 23, 2022

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Webcams can be used by applications running within the virtual session by using HDX webcam video compression or HDX plug-n-play generic USB redirection. Use **Citrix Workspace app > Preferences > Devices** to switch between modes. Citrix recommends you always use HDX webcam video compression if possible. HDX generic USB redirection is recommended only when there are application compatibility issues with HDX video compression or when you require advanced native functionalities of the webcam. For better performance, Citrix recommends the Virtual Delivery Agent to have at least two virtual CPUs.

To prevent users from switching from HDX webcam video compression, disable USB device redirection by using the policy settings under **ICA policy settings > USB Devices policy** settings. Citrix Workspace app users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting **Don't use my microphone or webcam**.

HDX webcam video compression

HDX webcam video compression is also called **Optimized** webcam mode. This type of webcam video compression sends the H.264 video directly to the video conferencing application running in the virtual session. To optimize VDA resources, HDX webcam compression doesn't encode, transcode, and decode webcam video. This feature is enabled by default.

To disable direct video streaming from the server to the video conferencing app, set the registry key to 0 on the VDA. For information, see Webcam video compression in the list of features managed through the registry.

If you disable the default functionality for streaming video resources, HDX webcam video compression uses the multimedia framework technology that is part of the client operating system to intercept video from capture devices, transcode, and compress it. Manufacturers of capture devices supply the drivers that plug into the OS kernel streaming architecture.

The client handles communication with the webcam. The client then sends the video only to the server that can display it properly. The server doesn't deal directly with the webcam, but its integration gives you the same experience in your desktop. Workspace app compresses the video to save bandwidth and provide better resiliency on WAN scenarios.



HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Multimedia conferencing
- Windows Media Redirection

If a webcam supports hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding might consume more bandwidth than software encoding. To force software compression, edit the registry key on the client. For information, see Webcam software compression in the list of features managed through the registry.

HDX webcam video compression requirements

HDX webcam video compression supports the following versions of Citrix Workspace app:

Platform	Processor
Citrix Workspace app for Windows	Citrix Workspace app for Windows supports webcam video compression for 32-bit and 64-bit apps on XenApp and XenDesktop 7.17 and later. On earlier versions, Citrix Workspace app for Windows supports only 32-bit apps.
Citrix Workspace app for Mac	Citrix Workspace app for Mac 2006 or later supports webcam video compression for 64-bit apps on XenApp and XenDesktop 7.17 and later. On earlier versions, Citrix Workspace app for Mac supports only 32-bit apps.
Citrix Workspace app for Linux	Citrix Workspace app for Linux supports only 32-bit apps on the virtual desktop.

Platform	Processor
Citrix Workspace app for Chrome	Because some ARM Chromebooks don't support H.264 encoding, only 32-bit apps can use the optimized HDX webcam video compression.

Media foundation-based video applications support HDX webcam video compression on Windows 8.x or higher and Windows Server 2012 R2 and higher. For more information, see Knowledge Center article CTX132764.

Other user device requirements:

- Appropriate hardware to produce sound.
- DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding capable reduce client-side CPU usage.
- For HDX webcam video compression, install webcam drivers on the client, obtained from the camera manufacturer, if possible. Installation of the device drivers isn't required on the server.

Different webcams offer different frame rates and have different levels of brightness and contrast. Adjusting the contrast of the webcam can reduce upstream traffic significantly. Citrix uses the following webcams for initial feature validation:

- Microsoft LifeCam VX models (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

To adjust the preferred video frame rate, edit the registry key on the client. For information, see Webcam video compression frame rate in the list of features managed through the registry.

High-definition webcam streaming

The video conferencing application on the server selects the webcam format and resolution based on the supported format types. When a session starts, the client sends the webcam information to the server. Choose a webcam from the application. When the webcam and the video conferencing application support high-definition rendering, the application uses high-definition resolution. We support webcam resolutions up to 1920x1080.

This feature requires the Citrix Workspace app for Windows, minimum version 1808 or Citrix Receiver for Windows, minimum version 4.10.

You can use a registry key to disable and enable the feature. For information, see High-definition webcam streaming in the list of features managed through the registry.

If the media type negotiation fails, HDX falls back to the default resolution of 352x288 CIF. You can use registry keys on the client to configure the default resolution. Ensure that the camera supports the specified resolution. For information, see High-definition webcam resolution in the list of features managed through the registry.

HDX webcam video compression uses significantly less bandwidth compared to plug-n-play generic USB redirection and works well over WAN connections. To adjust the bandwidth, set the registry key on the client. For information, see High-definition webcam bandwidth in the list of features managed through the registry.

Enter a value in bits per second. If you don't specify the bandwidth, the video conferencing applications use 350000 bps by default.

HDX plug-n-play generic USB redirection

HDX plug-n-play generic USB redirection (isochronous) is also called **Generic** webcam mode. The benefit of HDX plug-n-play generic USB redirection is that you don't have to install drivers on your thin client/endpoint. The USB stack is virtualized such that anything you plug into the local client is sent to the remote VM. The remote desktop acts as if you plugged it in natively. The Windows desktop handles all the interaction with the hardware and runs through the plug-n-play logic to find the correct drivers. Most webcams work if the drivers exist on the server and can work over ICA. Generic webcam mode uses significantly more bandwidth (many Megabits per second) because you are sending uncompressed video down with USB protocol over the network.

HTML5 multimedia redirection

May 9, 2024

HTML5 multimedia redirection extends the multimedia redirection features of HDX MediaStream to include HTML5 audio and video. Because of growth in online distribution of multimedia content, especially to mobile devices, the browser industry has developed more efficient ways to present audio and video.

Flash has been the standard, but it requires a plug-in, doesn't work on all devices, and has higher battery usage in mobile devices. Companies like YouTube, NetFlix.com, and newer browsers versions of Mozilla, Google, and Microsoft are moving to HTML5 making it the new standard.

HTML5-based multimedia has many advantages over proprietary plug-ins, including:

- Company-independent standards (W3C)
- Simplified digital rights management (DRM) workflow
- Better performance without the security issues raised by plug-ins

HTTP progressive downloads

HTTP progressive download is an HTTP-based pseudo-streaming method that supports HTML5. In a progressive download, the browser plays back a single file (encoded at a single quality) while it is being downloaded from an HTTP web server. The video is stored on the drive as it's received and is played from the drive. If you rewatch the video, the browser can load the video from cache.

For an example of a progressive download, see the HTML5 video redirection test page. To inspect the video elements in the webpage and find the sources (mp4 container format) in HTML5 video tags, use the developer tools in your browser:

Comparing HTML5 and Flash

Feature	HTML5	Flash
Requires a proprietary player	No	Yes
Runs on mobile devices	Yes	Some
Running speed on different platforms	High	Slow
Supported by iOS	Yes	No
Resource usage	Less	More
Load faster	Yes	No

Requirements

We support only redirection for progressive downloads in mp4 format. We don't support WebM and Adaptive bitrate streaming technologies like DASH/HLS.

We support the following, and use policies to control them. For more information, see Multimedia policy settings.

- Server side render
- Server fetch client render
- Client side fetching and rendering

Minimum versions of Citrix Workspace app and Citrix Receiver:

- Citrix Workspace app 1808 for Windows
- Citrix Receiver for Windows 4.5
- Citrix Workspace app 1808 for Linux
- Citrix Receiver for Linux 13.5

Minimum VDA browser version	Windows OS version/build/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Firefox 47 Manually add the certificates to the Firefox certificate store or configure Firefox to search for certificates from a Windows trusted certificate store. For more information, see https://wiki.mozilla.org/CA:AddRootToFirefox	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Components of the HTML5 video redirection solution

- **HdxVideo.js** - JavaScript hook intercepting video commands on the website. HdxVideo.js communicates with WebSocketService using Secure WebSockets (SSL/TLS).
- **WebSocket SSL Certificates**
  - For the CA (root): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    Location: Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
  - For the end-entity (leaf): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Location: Certificates (Local Computer) > Personal > Certificates.
- **WebSocketService.exe** - Runs on the local system and performs SSL termination and user session mapping. TLS Secure WebSocket listening on 127.0.0.1 port 9001.

- **WebSocketAgent.exe** - Runs on the user session and renders the video as instructed from WebSocketService commands.

How do I enable HTML5 video redirection?

In this release, this feature is available for controlled webpages only. It requires the addition of the HdxVideo.js JavaScript (included in the Citrix Virtual Apps and Desktops Installation media) to the webpages where the HTML5 multimedia content is available. For example, videos on an internal training site.

Websites like youtube.com, which are based on Adaptive Bitrate technologies (for example, HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (DASH)), are not supported.

For more information, see *Multimedia policy settings*.

Troubleshooting Tips

Errors might occur when the webpage tries to run HdxVideo.js. If the JavaScript fails to load, the HTML5 redirection mechanism fails. Ensure that there are no errors related to HdxVideo.js by inspecting the console in the developers tool windows of your browser. For example:



Optimization for Microsoft Teams

May 9, 2024

> **Note:**
>
> The new Microsoft Teams 2.1 is now generally available for VDA. This Microsoft Teams version is compatible with Citrix Microsoft Teams Optimization using WebRTC (VDI 1.0).
>
> If you are using Citrix Virtual Apps and Desktops 2402, you don't need to manually configure the `msedgewebview2.exe` registry entry as it's whitelisted by default.
>
> Published apps are now supported with the new Microsoft Teams.
>
> If you are using Citrix Virtual Apps and Desktops 2311 or earlier, a new registry configuration setting is required in the VDA to enable the new Microsoft Teams to access the Citrix virtual channel.

> To enable Microsoft Teams 2.1 optimization, configure the following registry key in the VDA:
>
> **Location**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
>
> **Key** (REG_Multi_SZ): `ProcessWhitelist`
>
> **Value**: `msedgewebview2.exe`
>
> For more information, see the Microsoft documentation.

Citrix delivers optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops and Citrix Workspace app. By default, we bundle all the necessary components into the Citrix Workspace app and the Virtual Delivery Agent (VDA).

Our optimization for Microsoft Teams includes VDA-side HDX services and an API to interface with the Microsoft Teams hosted app to receive commands. These components open a control virtual channel (CTXMTOP) to the Citrix Workspace app-side media engine. The endpoint decodes and provides the multimedia locally, moving the Citrix Workspace app window back into the hosted Microsoft Teams app.

Authentication and signaling occur natively on the Microsoft Teams-hosted app, just like the other Microsoft Teams services (for example chat or collaboration). Audio/video redirection doesn't affect them.

The `CTXMTOP` is a command and control virtual channel. That means that media isn't exchanged between the Citrix Workspace app and the VDA.

Only client-fetch/client-render is available.

This video demo gives you an idea of how Microsoft Teams works in a Citrix virtual environment.



Microsoft Teams installation

Citrix and Microsoft recommend the latest available version of Microsoft Teams and to keep it up to date.
Microsoft Teams desktop app versions with release dates that are more than 90 days older than the current version's release date aren't supported.
Unsupported Microsoft Teams desktop app versions show a blocking page to users and request to update the app.

For information on the latest available versions, see Update history for Teams App (Desktop and Mac).

We recommend that you follow the Microsoft Teams machine-wide installation guidelines. Also, avoid using the .exe installer that installs Microsoft Teams in `AppData`. Instead, install in `C:\Program Files (x86)\Microsoft\Teams` by using the `ALLUSER=1` flag from the command line.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

This example also uses the `ALLUSERS=1` parameter. When you set this parameter, the Microsoft Teams Machine-Wide Installer appears in **Programs and Features** in the **Control Panel**. Also, in **Apps & features** in Windows Settings for all users of the computer. All users can then uninstall Microsoft Teams if they have administrator credentials.

It's important to understand the difference between `ALLUSERS=1` and `ALLUSER=1`. You can use the `ALLUSERS=1` parameter in non-VDI and VDI environments. Use the `ALLUSER=1` parameter only in VDI environments to specify a per-machine installation.

In `ALLUSER=1` mode, the Microsoft Teams application doesn't auto-update whenever there's a new version. We recommend this mode for non-persistent environments, such as hosted shared apps or desktops out of a Windows Server or Windows 10 random/pooled catalogs. For more information, see Install Microsoft Teams using MSI (VDI Installation section).

Suppose you have Windows 10 dedicated persistent VDI environments. You want the Microsoft Teams application to auto-update and prefer Microsoft Teams to install per-user under `Appdata/Local`. In this case, use the `.exe` installer or the MSI without `ALLUSER=1`.

> **Note:**
>
> We recommend installing the VDA before installing Microsoft Teams in the golden image. This installation order is needed for the `ALLUSER=1` flag to take effect. If you installed Microsoft Teams in the virtual machine before installing the VDA, uninstall and reinstall Microsoft Teams.

For Remote PC Access

We recommend that you install Microsoft Teams version 1.4.00.22472 or later after installing the VDA. Otherwise, you need to sign out and sign in again for Microsoft Teams to detect the VDA as expected. Version 1.4.00.22472 and later includes augmented logic run at Microsoft Teams launch time and sign in time for VDA detection. These versions also include active session type identification (HDX, RDP or locally connected to the client machine). If you're locally connected, previous versions of Microsoft Teams might fail to detect and disable certain features or UI elements. For example, Breakout Rooms, pop out windows for meetings and chat, or meeting reactions.

> **Important:**
>
> When you roam from a local session to an HDX session and if Microsoft Teams is kept open and running on the background, you must exit and relaunch Microsoft Teams to optimize with HDX correctly.
> Conversely, if you use Microsoft Teams remotely via an optimized HDX session, disconnect the HDX session and reconnect to the same Windows session locally at the device. When working from the office, you must relaunch Microsoft Teams so it can correctly detect the Remote PC state (HDX or local). Because Microsoft Teams can only assess VDI mode at app launch time, and not while it is already running on the background. Without a restart, Microsoft Teams might fail to load features like pop out Windows, Breakout Rooms, or meeting reactions.

For App Layering

If using Citrix App Layering to manage VDA and Microsoft Teams installations in different layers, you must create a new registry key on Windows VDAs before installing Microsoft Teams with the `ALLUSER=1` flag from the command line. For more information, see the *Optimization for Microsoft Teams with Citrix App Layering* section under Multimedia.

Profile Management recommendations

We recommend using the machine-wide installer for Windows Server and Pooled VDI Windows 10 environments.

When the **ALLUSER=1** flag is passed to the MSI from the command line (the machine-wide installer), the Microsoft Teams app installs under `C:\Program Files (x86)` (~300 MB). The app uses `AppData\Local\Microsoft\TeamsMeetingAddin` for logs and `AppData\Roaming\Microsoft\Teams` (~600–700 MB) for user specific configurations, caching of elements in the user interface, and so forth.

> **Important:**
>
> If you don't pass the **ALLUSER=1** flag, the MSI places the Teams.exe installer and `setup.json` under `C:\Program Files (x86)\Teams Installer`. A registry key (TeamsMachineInstaller) is added under: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> A subsequent user logon triggers the final installation in **AppData** instead.

Machine-wide installer

The following is an example of folders, desktop shortcuts, and registries created by installing Microsoft Teams machine-wide installer on a Windows Server 2016 64-bit VM:

Folder:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Desktop Shortcut:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registry:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Name: `Teams`
- Type: `REG_SZ`
- Value: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Note:**
>
> The registry location varies based on the underlying Operating Systems and bitness.

Recommendations

- We recommend disabling auto-start by deleting the Microsoft Teams registry keys. Doing so prevents many logons that occur at the same time (for example, at the beginning of your work day) from spiking up the VM's CPU.

- If the virtual desktop does not have a GPU/vGPU, we recommend setting **Disable GPU hardware acceleration** in the Microsoft Teams **Settings** to improve performance. This setting (`"disableGpu":true`) is stored in `%Appdata%\Microsoft\Teams` in `desktop-config.json`. You can use a logon script to edit that file and set the value to **true**.
- If using Citrix Workspace Environment Management (WEM), enable **CPU Spikes Protection** to manage processor consumption for Microsoft Teams.

Per-user installer

When using the `.exe` installer, the installation process differs. All the files are placed in AppData.

Folder:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Desktop shortcut:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"
```

Registry:

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Best Practices

The best practice recommendations are based on the use-case scenarios.
Using Microsoft Teams with a non-persistent setup requires a profile caching manager for efficient Microsoft Teams runtime data synchronization. With a profile caching manager, the appropriate user-specific information is cached during the user session. For example, the user-specific information includes, user data, profile, and settings. Synchronize the data in these two folders:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Microsoft Teams cached content exclusion list for non-persistent setup Exclude the files and directories from the Microsoft Teams caching folder as described in the Microsoft documentation. This action helps you to reduce the user caching size to further optimize your non-persistent setup.

Use case: single-session scenario In this scenario, the end user uses Microsoft Teams in one location at a time. They don't need to run Microsoft Teams in two Windows sessions at the same time. In a common virtual desktop deployment, each user is assigned to one desktop, and Microsoft Teams is deployed in the virtual desktop as one application.
We recommend enabling the Citrix Profile container and redirecting the per-user directories listed in Per-user installer into the container.

1. Deploy the Microsoft Teams machine-wide installer (**ALLUSER=1**) in the golden image.
2. Enable Citrix Profile Management and set up the user profile store with the proper permissions.
3. Enable the following Profile Management policy setting: **File system > Synchronization > Profile container –List of folders to be contained in profile disk**.



List all the per-user directories into this configuration. You can also configure these settings using the Citrix Workspace Environment Management (WEM) service.

4. Apply the settings to the correct delivery group.
5. Log in to validate the deployment.

System requirements

Minimum recommended version - Delivery Controller (DDCs) 1906.2

If you're using an earlier version, see Enable optimization of Microsoft Teams:

Supported operating systems:

- Windows Server 2022, 2019, 2016, 2012R2 Standard and data center Editions, and with the Server Core option

Minimum version - Virtual Delivery Agents (VDAs) 1906.2

Supported operating systems:

- Windows 11.
- Windows 10 64-bit, versions 1607 and later. VM hosted apps are supported in Citrix Workspace app for Windows 2109.1 and later.
- Windows Server 2022, 2019, 2016, and 2012 R2 (Standard and data center Editions).

Requirements:

- BCR_x64.msi - the MSI that includes the Microsoft Teams optimization code and starts automatically from the GUI. If you're using the command line interface for the VDA installation, don't exclude it.

Recommended version –Citrix Workspace app for Windows latest CR and Minimum version - Citrix Workspace app 1907 for Windows

- Windows 11.
- Windows 10 (32-bit and 64-bit editions, including Embedded editions) (Support for Windows 7 stopped at Version 2006) (Support for Windows 8.1 stopped at version 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) and 2019 LTSC (v1809).
- Processor (CPU) architectures supported: x86 and x64 (ARM isn't supported).
- Endpoint requirement: Approximately 2.2–2.4 GHz dual core CPU that can support 720p HD resolution during a peer-to-peer video conference call.

- Dual or quad-core CPUs with lower base speeds (~1.5 GHz) equipped with Intel Turbo Boost or AMD Turbo Core that can boost up to at least 2.4 GHz.
- HP Thin Clients verified: t630/t640, t730/t740, mt44/mt45.
- Dell Thin Clients verified: 5070, 5470 Mobile TC and AIO.
- 10ZiG Thin Clients verified: 4510 and 5810q.
- For a complete list of verified endpoints, see Thin Clients.
- Citrix Workspace app requires at least 600 MB free disk space and 1 GB RAM.
- Microsoft .NET Framework minimum requirement is version 4.8. Citrix Workspace app automatically downloads and installs .NET Framework if it's not present in the system.

Administrators can enable/disable Microsoft Teams starting in optimized mode by changing the Teams Optimization policy. Users starting in optimized mode in Citrix Workspace app can't disable Microsoft Teams.

Minimum version - Citrix Workspace app 2006 for Linux

Software:

- `GStreamer` 1.0 or later or Cairo 2
- libc++-9.0 or later
- `libgdk` 3.22 or later
- OpenSSL 1.1.1d
- x64 Linux distribution

Hardware:

- Minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call
- Dual or quad-core CPU with a base speed of 1.8 GHz and a high Intel Turbo Boost speed of at least 2.9 GHz

For a complete list of verified endpoints, see Thin Clients.

For more information, see Prerequisites to install Citrix Workspace app.

You can disable Microsoft Teams optimization updating the value of the **VDWEBRTC** field to Off in the `/opt/Citrix/ICAClient/config/module.ini` file. The default is VDWEBRTC=On. After the update is complete, restart the Session. (Root permission is required).

Minimum version - Citrix Workspace app 2012 for Mac

Supported operating systems:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 and later.
- macOS Monterey.

Features supported:

- Audio
- Video
- Screen sharing optimization (incoming and outgoing)

> **Note:**
>
> Citrix Viewer app requires access to macOS Security and Privacy preferences for screen sharing to work. Users configure this preference in **Apple menu > System preferences > Security & Privacy > Privacy tab > Screen recording** and select **Citrix Viewer**.

Microsoft Teams optimization works by default with Citrix Workspace app 2012 and later and macOS 10.15.

If you want to disable Microsoft Teams optimization, run this command in a terminal and restart the Citrix Workspace app:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Minimum version - Latest version of Citrix Workspace app for Chrome OS running on the latest version of Chrome OS

Hardware:

- Processors that perform at par or better than Intel i3, quad core 2.4 GHz.

Features supported:

- Audio
- Video
- Screen sharing optimization (incoming and outgoing) - disabled by default. See these settings for instructions on how to turn it on.

Single Server Scalability

This section provides recommendations and guidance to estimate how many users or virtual machines (VMs) can be supported on a single physical host. This is commonly referred to as Citrix Virtual Apps and Desktops Single Server Scalability (SSS). In the context of Citrix Virtual Apps (CVA) or session virtualization, it is also commonly known as user density. The idea is to find out how many users or VMs can be ran on a single piece of hardware running a major hypervisor.

> **Note:**
>
> This section includes guidance to estimate SSS. Note that the guidance is high level and might not necessarily be specific to your unique situation or environment. The only way to truly understand Citrix Virtual Apps and Desktops SSS is to use a scalability or load testing tool such as Login VSI. Citrix recommends using this guidance and these simple rules to quickly estimate SSS only. However, Citrix recommends using Login VSI or the load testing tool of your choice to validate results, especially before purchasing hardware or making any financial decisions.

Hardware (system under test)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (max Turbo 3.70 GHz), 12 cores per socket, dual socket with Hyperthreading enabled
- 382 GB of RAM
- Local SSD RAID 0 storage (11 disk) 6 TB

Software

A single virtual machine (40 logical processors) with Windows 2019 (TSVDA) running Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

Terminology

- Knowledge worker workload: Includes Acrobat Reader, Freemind/Java, Photo viewer, Edge, and MS Office apps such as Excel, Outlook, PowerPoint, and Word.
- Baseline: Server Scalability tests run with knowledge worker workload (without Microsoft Teams).
- Microsoft Teams Workload: Knowledge worker typical workload + Microsoft Teams.

How Microsoft Teams is stress-tested

- Microsoft Teams is optimized with HDX. Hence, all the multimedia processing is offloaded to the endpoint or client and is not part of the measurement.
- All Microsoft Teams processes stopped or killed, before workload starts.
- Open Microsoft Teams (Cold start).
- Measure the time taken by Microsoft Teams to load and grab the focus of Microsoft Teams primary window.

- Switch to chat window using keyboard shortcuts.
- Switch to calendar window using keyboard shortcuts.
- Send the chat message to a specific user using keyboard shortcuts.
- Switch to Microsoft Teams window using keyboard shortcuts.

Results

- 40% scalability impact with Microsoft Teams Workload (81 users), when compared to Baseline (137 users).
- Increasing the server capacity by ~40% (in CPU) restores the number of users as with Baseline workload.
- 20% extra memory required with Microsoft Teams Workload, when compared to Baseline.
- Increase per user storage size by 512-1024 MB.
- ~50% increase in IOPS write, ~100% increase in IOPS reads. Microsoft Teams can have a significant impact in environment with slower storage.

Feature matrix and version support

Feature	Microsoft Teams (minimum version)	VDA (minimum version)	Citrix Workspace app for Windows CR (minimum version)	Citrix Workspace app for Mac (minimum version)	Citrix Workspace app for Linux (minimum version)	Citrix Workspace app for Chrome OS
Audio/Video (P2P and conference)	current version minus 90 days	1906	1907	2009	2004	2105.5
Screensharing	Current version minus 90 days	1906	1907	2012	2006	2105.5
i. Screen Indicator Red border	Current version minus 90 days	1906	2002	2012	2006	No

Feature	Microsoft Teams (minimum version)	VDA (minimum version)	Citrix Workspace app for Windows CR (minimum version)	Citrix Workspace app for Mac (minimum version)	Citrix Workspace app for Linux (minimum version)	Citrix Workspace app for Chrome OS
ii. Limit capture to Desktop Viewer	Current version minus 90 days	1906	2009.5	2012	2006	No
iii. Multi-monitor	Current version minus 90 days	1912 CU6+	2106 (1)	2106	2106	No
DTMF	Current version minus 90 days	N/A	2102	2101	2101	2111.1
Proxy Server support	Current version minus 90 days	N/A	2012 (2)	2104 (3)	2101 (3)	2305
App Sharing	Current version minus 90 days	2109	2109.1	2203.1	2209	No
Live Captions	Current version minus 90 days	N/A (4)	2109.1	2109	2109	2303
Dynamic e911	Current version minus 90 days	N/A	2112.1	2112	2112	2112
Give Control	Current version minus 90 days	N/A	2112.1	2203.1	No	No

Feature	Microsoft Teams (minimum version)	VDA (minimum version)	Citrix Workspace app for Windows CR (minimum version)	Citrix Workspace app for Mac (minimum version)	Citrix Workspace app for Linux (minimum version)	Citrix Workspace app for Chrome OS
Request Control	Current version minus 90 days	N/A	2112.1	2203.1	2203	2303
MultiWindow	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Meeting Transcriptions	Current version minus 90 days	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Background Blurring	Current version minus 90 days	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer in full screen mode only. SHIFT+F2 not supported.
2. Negotiate/Kerberos, NTLM, Basic, and Digest. Pac files are also supported.
3. Anonymous only.
4. If VDA is 2112 or higher, Live Captions will only work if Citrix Workspace app version is 2203.1 for MAC and 2203 Linux or 2112 for Windows. This is because Live Captions behave differently if Microsoft Teams is in Single Window UI mode or MultiWindow mode.
5. MultiWindow was introduced in 2112 VDA but was back-ported to the VDA 1912 LTSR CU6 release.

> **Note:**
>
> All features listed in **Citrix Workspace app for Windows 1912 CU6 (or later)** are applicable to Citrix Workspace app for Windows 2203.1 LTSR CU1.

Enable optimization of Microsoft Teams

To enable optimization for Microsoft Teams, use the Manage console policy described in the Microsoft Teams redirection policy. This policy is **ON** by default. In addition to this policy being

enabled, HDX checks to verify that the version of the Citrix Workspace app is at least the minimum required version. If you enabled the policy and the Citrix Workspace app version is supported, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** is set to **1** automatically on the VDA. Microsoft Teams reads the key to load in VDI mode.

> **Note:**
>
> If you're using version 1906.2 or later VDAs or with older controller versions (for example, version 7.15) that don't have the policy available in the Manage console (Studio), your VDA can still be optimized. HDX optimization for Microsoft Teams is enabled by default in the VDA.

If you click **About > Version**, the **Citrix HDX Optimized** legend displays:



If you see **Citrix HDX Not Connected**, the Citrix API is loaded in Microsoft Teams. Loading the API is the first step toward redirection. But there's an error in later parts of the stack. The error is most likely in the VDA services or the Citrix Workspace app.



If you don't see any legend, Microsoft Teams failed to load the Citrix API. Exit Microsoft Teams by right-clicking the notification area icon and restarting. Make sure that the Manage console policy isn't set to **Prohibited** and that the Citrix Workspace app version is supported.



> **Important: session reconnects**
>
> - You might require to relaunch Microsoft Teams to get an HDX optimized session when your connectivity changes. For example, if you are roaming from an unsupported endpoint (Workspace app for iOS, Android, or old versions of Windows/Linux/Mac) to a supported one (Workspace app for Windows/Linux/Mac/ChromeOS/HTML5), or the opposite way.
> - A Microsoft Teams relaunch is also required if you have installed the app using the Microsoft Teams .exe installer in the VDA. The .exe installer is recommended for persistent VDI deployments. In such cases, Microsoft Teams can auto-update while the HDX session is in the disconnected state. So, users reconnecting to an HDX session finds that the Microsoft Teams is not running optimized.
> - When you roam from a local session to an HDX session, you must relaunch Microsoft Teams to optimize with HDX. This action is required in a Remote PC Access scenario.

Network requirements

Microsoft Teams relies on Media Processor servers in Microsoft 365 for meetings or multiparty calls. Also, Microsoft Teams relies on Microsoft 365 Transport Relays for these scenarios:

- Two peers in a point-to-point call do not have direct connectivity
- A participant does not have direct connectivity to the media processor.

So the network health between the peer and the Microsoft 365 cloud determines the performance of the call. For detailed guidelines around network planning, see Microsoft 365 network connectivity principles.

We recommend evaluating your environment to identify any risks and requirements that can influence your overall cloud voice and video deployment.
Use the Skype for Business Network Assessment Tool to test if your network is ready for Microsoft Teams. For support information, see Support.

Summary of key network recommendations for Real Time Protocol (RTP) traffic

- Connect to the Microsoft 365 network as directly as possible from the branch office.
- Plan for and provide sufficient bandwidth at the branch office.
- Check each branch office for network connectivity and quality.
- If you must use any of the following at the branch office, make sure that RTP/UDP traffic (handled by HdxRtcEngine.exe in Citrix Workspace app) is.
  - Bypass proxy servers
  - Network SSL intercept
  - Deep packet inspection devices
  - VPN hairpins (use split tunneling if possible)

> **Important: VPN Split tunnel configuration**
>
> HdxRtcEngine.exe traffic has to be diverted from the VPN tunnel and allowed to use the user's local Internet connection to connect directly to the service. The manner in which this is accomplished will vary depending on the VPN product and machine platform used but most VPN solutions will allow some simple configuration of policy to apply this logic. For more information on VPN platform-specific split tunnel guidance, see this Microsoft article.

The WebRTC media engine in the Workspace app (HdxRtcEngine.exe) uses the Secure Real-time Transport Protocol (SRTP) for multimedia streams that are offloaded to the client. SRTP provides confidentiality and authentication to RTP. For this feature, symmetric keys (negotiated with DTLS) are used to encrypt media and control messages using the AES encryption cipher.

The following metrics are recommended for a positive user experience:

Metric	Endpoint to Microsoft 365
Latency (one way)	< 50 msec
Latency (RTT)	< 100 msec
Packet Loss	<1% during any 15s interval
Packet inter-arrival jitter	<30ms during any 15s interval

For more information, see Prepare your organization's network for Microsoft Teams.

For bandwidth requirements, optimization for Microsoft Teams can use a wide variety of codecs for audio (OPUS/G.722/PCM G711) and video (H264).

The peers negotiate these codecs during the call establishment process using the Session Description Protocol (SDP) Offer/Answer.
Citrix minimum recommendations per user are:

Type	Bandwidth	Codec
Audio (each way)	~ 90 kbps	G.722
Audio (each way)	~ 60 kbps	Opus*
Video (each way)	~ 700 kbps	H264 360p @ 30 fps 16:9
Screen sharing	~ 300 kbps	H264 1080p @ 15 fps

Opus and H264 are the preferred codecs for peer-to-peer and conference calls.

> **Important:**
>
> About performance, encoding is more expensive than decoding for CPU use at the client machine. You can hardcode the maximum encoding resolution in the Citrix Workspace app for Linux and Windows. See Encoder performance estimator and Optimization for Microsoft Teams.

Proxy servers

Depending on the location of the proxy, consider the following:

- Proxy configuration on the VDA:

  If you configure an explicit proxy server in the VDA and route connections to localhost through a proxy, redirection fails. To configure the proxy correctly, you must select the **Bypass proxy**

servers for local address setting in **Internet Options > Connections > LAN Settings > Proxy Servers** and bypass `127.0.0.1:9002`.

If you use a PAC file, your VDA proxy configuration script from the PAC file must return **DIRECT** for `wss://127.0.0.1:9002`. If not, optimization fails. To make sure that the script returns **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Proxy configuration on Citrix Workspace app:

  If the branch office is configured to access the internet through a proxy, these versions support proxy servers:

  - Citrix Workspace app for Windows version 2012 (Negotiate/Kerberos, NTLM, Basic, and Digest. `Pac` files are also supported)
  - Citrix Workspace app for Windows version 1912 CU5 (Negotiate/Kerberos, NTLM, Basic, and Digest. `Pac` files are also supported)
  - Citrix Workspace app for Linux version 2101 (anonymous authentication)
  - Citrix Workspace app for Mac version 2104 (anonymous authentication)

Client devices with earlier versions of Citrix Workspace app can't read proxy configurations. These devices send traffic directly to Microsoft 365 TURN servers.

> **Important:**
>
> - Verify that the client device can connect to the DNS server to do DNS resolutions. A client device must be able to resolve the following Microsoft Teams Relay server's FQDNs:
>
>   ```
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>   ```
>
> If DNS requests are unsuccessful, P2P calls with outside users and conference calls media establishment fails.
>
> - The location of the conference server is selected based on the first participant's virtual desktop location (and not the client).

Call establishment and media flow paths

When possible, the HDX WebRTC media engine in the Citrix Workspace app (HdxRtcEngine.exe) tries to establish a direct network Secure Real-time Transport Protocol (SRTP) connection over User Datagram

Protocol (UDP) in a peer-to-peer call. If the UDP high ports are blocked, the media engine falls back to TCP/TLS 443.

The HDX media engine supports ICE, Session Traversal Utilities for NAT (STUN), and Traversal Using Relays around NAT (TURN) for candidate discovery and establishing connection. This support means that the endpoint must be able to perform DNS resolutions.

Consider a scenario where there is no direct path between the two peers or between a peer and a conference server and you are joining a multi-party call or meeting. The HdxRtcEngine.exe uses a Microsoft Teams transport relay server in Microsoft 365 to reach the other peer or the media processor, where meetings are hosted. Your client machine must have access to three Microsoft 365 subnet IP address ranges and four UDP ports (or TCP/TLS 443 as fallback if UDP is blocked). For more information, see the Architecture diagram in the Call setup and Office 365 URLs and IP address ranges ID 11.

ID	Category	Addresses	Destination Ports
11	Optimize required	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (fallback)

These ranges include both Transport Relays and media processors, front-ended by an Azure Load Balancer.
The Microsoft Teams Transport Relays provide STUN and TURN functionality, but they aren't ICE endpoints. Also, the Microsoft Teams Transport Relays don't terminate media, TLS, or do any transcoding. They can bridge TCP (if HdxRtcEngine.exe uses TCP) to UDP when they forward traffic to other peers or media processors.

Workspace app WebRTC media engine contacts the closest Microsoft Teams Transport Relay in the Microsoft 365 cloud. The media engine uses anycast IP and port 3478–3481 UDP (different UDP ports per workload, though multiplexing can happen) or 443 TCP/TLS for fallbacks. Call quality depends on the underlying network protocol. Because UDP is always recommended over TCP, we advise you to design your networks to accommodate UDP traffic in the branch office.

If Microsoft Teams loaded in optimized mode and HdxRtcEngine.exe is running on the endpoint, ICE failures might cause a call setup failure or one-way-only audio/video. When a call can't be completed or the media streams aren't full duplex, check the **Wireshark trace** on the endpoint first. For more information about the ICE candidate gathering process, see "Collecting logs"in the Support section.

> **Note:**
>
> If the endpoints don't have internet access, the users might still be able to make a peer-to-peer

> call if they are both on the same LAN. Meetings fail. In this case, there's a 30-second timeout before the call setup begins.

Call setup

Use this architecture diagram as a visual reference for the call flow sequence. The corresponding steps are indicated in the diagram.



Architecture

1. Start Microsoft Teams.
2. Microsoft Teams authenticates to O365. Tenant policies are pushed down to the Microsoft Teams client, and relevant TURN and signaling channel information is relayed to the app.

3. Microsoft Teams detects that it's running in a VDA and makes API calls to the Citrix JavaScript API.
4. Citrix JavaScript in Microsoft Teams opens a secure WebSocket connection to WebSocketService.exe running on the VDA, which spawns WebSocketAgent.exe inside the user session.
5. WebSocketAgent.exe instantiates a generic virtual channel by calling into the Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe).
6. Citrix Workspace app's wfica32.exe (HDX engine) spawns a new process called HdxRtcEngine.exe, which is the new WebRTC engine used for Microsoft Teams optimization.
7. Citrix media engine and Teams.exe have a 2-way virtual channel path and can start processing multimedia requests.

   ——User calls——

8. **Peer A** clicks the **call** button. Teams.exe communicates with the Microsoft Teams services in Microsoft 365, establishing an end-to-end signaling path with **Peer B**. Microsoft Teams asks HdxRtcEngine for a series of supported call parameters (codecs, resolutions, and so forth, which is known as a Session Description Protocol (SDP) offer). These call parameters are then relayed using the signaling path to the Microsoft Teams services in Microsoft 365 and from there to the other peer.
9. The SDP offer/answer (single-pass negotiation) takes place through the signaling channel, and the ICE connectivity checks (NAT and Firewall traversal using STUN bind requests) complete. Then, Secure Real-time Transport Protocol (SRTP) media flows directly between HdxRtcEngine and the other peer (or Microsoft 365 conference servers if it's a meeting).

Microsoft Phone System

Phone System is Microsoft's technology that enables call control and PBX in the Microsoft 365 cloud with Microsoft Teams. Optimization for Microsoft Teams supports Phone System, using Microsoft 365 Calling Plans or Direct Routing. With Direct Routing, you connect your own supported session border controller to the Microsoft Phone System directly without any additional on-premises software.
Call queues, transfer, forward, hold, mute, and resume a call are supported.

DTMF

The dual-tone multi-frequency (DTMF) feature is supported with these versions of Citrix Workspace app (and later):

- Citrix Workspace app for Windows version 2102
- Citrix Workspace app for Windows LTSR 1912 CU5 (Windows 10 OS only)

- Citrix Workspace app for Linux version 2101
- Citrix Workspace app for Mac version 2101
- Citrix Workspace app for Chrome OS version 2111.1

Support for dynamic e911

Starting with version 2112, Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it allows you to do the following:

- Configure and route emergency calls.
- Notify security personnel.

The notification is provided based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client that runs on the VDA.

Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Microsoft Teams Optimization with HDX is compliant with Ray Baum's law when used with the following versions of Citrix Workspace app:

- Citrix Workspace app for Windows version 2112.1 and later
- Citrix Workspace app for Linux version 2112 and later
- Citrix Workspace app for Mac version 2112 and later
- Citrix Workspace app for Chrome OS version 2112 and later

To enable dynamic emergency calling, the administrator must use the Microsoft Teams Admin Center and configure the following to create a network or emergency location map:

- Network settings
- Location Information Service (LIS)

For more information on Dynamic emergency calling, see Microsoft's documentation.

The dispatchable location information that Citrix Workspace app relays to Microsoft Teams is:

- Chassis ID / Port ID using Link Layer Discovery Protocol (LLDP) for Ethernet/Switch connections. Ethernet/Switch (LLDP) is supported on:
  - Windows versions 8.1 and 10
  - macOS, which requires LLDP enablement software. To download the LLDP enablement software, go to `www.microsoft.com` and search for LLDP enablement software.
  - Linux, which requires the LLDP library to be included in the operating system(OS) distribution of the Thin Client.
- WLAN BBSID and {IPv4-IPv6; Subnet; MAC Address} of the endpoint where Citrix Workspace app is installed.

  - Subnet and WiFi-based locations are supported on the Workspace app for Windows, Linux, and Mac.

- Latitude and Longitude, if user permission is granted at the OS-level where Citrix Workspace app is installed.

  - Supported on all Workspace app platforms. However, for Citrix Workspace for Linux, you must include the `libgps` library in the OS distribution of the Thin Client (sudo apt-get install libgps23 gpsd lldpd).

Firewall considerations

When users start an optimized call using the Microsoft Teams client for the first time, they might notice a warning with the **Windows firewall** settings. The warning asks for users to allow communication for HdxTeams.exe or HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



The following four entries are added under **Inbound Rules** in the **Windows Defender Firewall > Advanced Security** console. You can apply more restrictive rules if you want.



Microsoft Teams and Skype for Business Coexistence

You can deploy Microsoft Teams and Skype for Business side by side as two separate solutions with overlapping capabilities.
For more information, see Understand Microsoft Teams and Skype for Business coexistence and interoperability.

Citrix RealTime Optimization Pack and HDX optimization for Microsoft Teams multimedia engines then honor the configuration set in your environment. Examples include island modes and Skype for Business with Microsoft Teams collaboration. Also, Skype for Business with Microsoft Teams collaboration and meetings.

Peripheral access can be granted only to a single application at the time. For example, webcam access by the RealTime Media Engine during a call locks the imaging device during a call. When the device is released, it becomes available for Microsoft Teams.



Citrix SD-WAN: optimized network connectivity for Microsoft Teams

Optimal audio and video quality require a network connection to the Microsoft 365 cloud that has low latency, low jitter, and low packet loss. Backhauling of Microsoft Teams audio-video RTP traffic from Citrix Workspace app users at branch office locations to a data center before going to the internet can add excessive latency. It might also cause congestion on WAN links. Citrix SD-WAN optimizes connectivity for Microsoft Teams following Microsoft 365 network connectivity principles. Citrix SD-WAN uses the Microsoft REST-based Microsoft 365 IP address and web service and proximate DNS. This use is to identify, categorize, and steer Microsoft Teams traffic.

Business broadband internet connections in many areas suffer from intermittent packet loss, periods of excessive jitter, and outages.

Citrix SD-WAN offers two solutions to preserve Microsoft Teams audio-video quality when network health is variable or degraded.

- If you use Microsoft Azure, a Citrix SD-WAN virtual appliance (VPX) deployed in the Azure VNET provides advanced connectivity optimizations. These optimizations include seamless link failover and audio packet racing.
- Citrix SD-WAN customers can connect to Microsoft 365 through the Citrix Cloud Direct service. This service provides reliable and secure delivery for all internet-bound traffic.

If the quality of the branch office internet connection isn't a concern, it might be enough to minimize latency. Steer Microsoft Teams traffic directly from the Citrix SD-WAN branch appliance to the nearest Microsoft 365 front door to minimize latency. For more information, see Citrix SD-WAN Office 365 optimization.



Multi-window meetings and chat

You can use multiple meetings or chat windows for Microsoft Teams in Windows. For details on the pop-out feature, see Microsoft Teams Pop-Out Windows for Chats and Meetings on the Microsoft 365 site.

> **Note:**
>
> This feature is supported with Citrix Workspace app for Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. It requires VDA 2112 or greater and was back-ported to 1912 CU6+ LTSR, and VDA 2112.

Background blurring and background effects

Citrix Workspace app for Windows, Mac, Linux, and ChromeOS/HTML5 supports background blurring and background effects in Microsoft Teams optimization with HDX.

You can either blur or replace the background with a default image and avoid unexpected distractions by helping the conversation stay focused on the silhouette (body and face). You can use this feature with P2P or conference calls.

> **Note:**
>
> This feature is integrated with the Microsoft Teams UI/buttons. MultiWindow support is a pre-requisite that requires a VDA update to 2112 or later. For more information, see Multi-window meetings and chat.

Microsoft Teams UI controls on background blurring and effects require the following minimum versions:

- Citrix Workspace app for Windows 2207
- Citrix Workspace app for Mac 2301
- Citrix Workspace app for Linux 2212
- Citrix Workspace app for ChromeOS 2303

Limitations:

- The client must be connected to the internet while replacing the background image with a Microsoft Teams default image.
- Admin and user-defined background image replacement is not supported in the Microsoft Teams UI. Custom background images can be configured using configuration settings on the client, if the image is also stored on the client.

Setting a custom background image

The following registry keys are only required if you don't plan to use the Microsoft Teams UI to control the feature, or if an admin wants to override default behaviors. For example, disable background blurring because the endpoint is not powerful enough.

On Windows To set a custom background image, administrators or end-users must configure the following registry key on the client or endpoint:

Location: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Name: VideoBackgroundEffect
- Type: DWORD

- Value: 0 (disabled), 1 (enabled), 2 (background image replacement)

Value set to 1 blurs the background. This value can be set either by the end-user, or the administrator.

Value set to 2 also requires the **VideoBackgroundImage** key to be present as well. Only the administrator can set this value. The following key is required only if you want to replace the background image and not for blurring:

- Name: VideoBackgroundImage
- Type: REG_SZ
- Value: my_image_name.jpeg

The video background image must be present in the `C:\Program Files (x86)\Citrix\ICA Client` directory.

This registry configuration can also be used to enable background blurring or image replacement in Citrix Workspace app 2206 without the Microsoft Teams UI selector. In other words, if your environment or VDA doesn't support multi-window, you can still apply the HKCU registry workaround with Citrix Workspace app 2206 or higher to achieve a similar result, although the user cannot control the functionality in the middle of the HDX session or Microsoft Teams call.

Registry key changes only take effect when the HDX session connects.

On Mac User downloaded picture location: */Users/username/Downloads/any_image.png*

Run the following commands to set the custom image as the default image:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

On Linux User downloaded picture location: */home/username/Downloads/any_image.jpg*

Create file */var/.config/citrix/hdx_rtc_engine/config.json* and add the following configuration keys in JSON format. For example,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

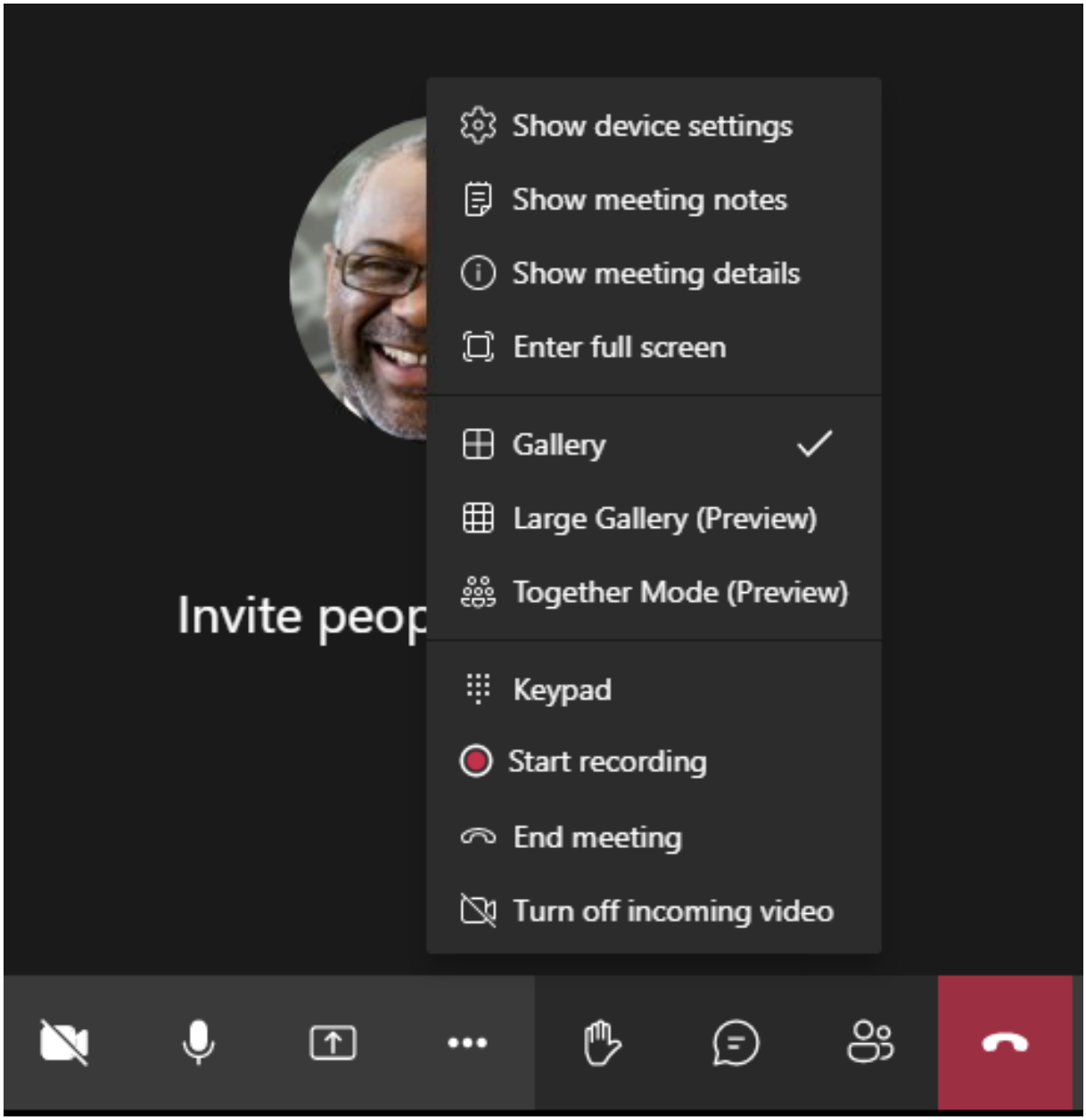
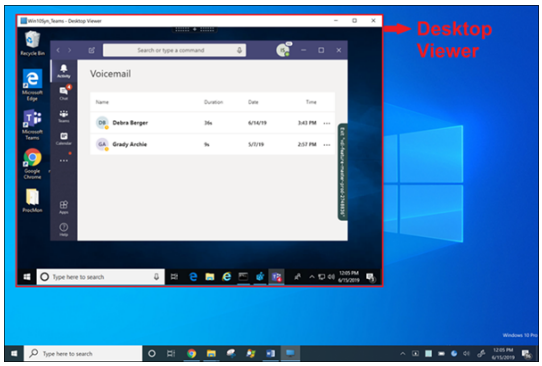
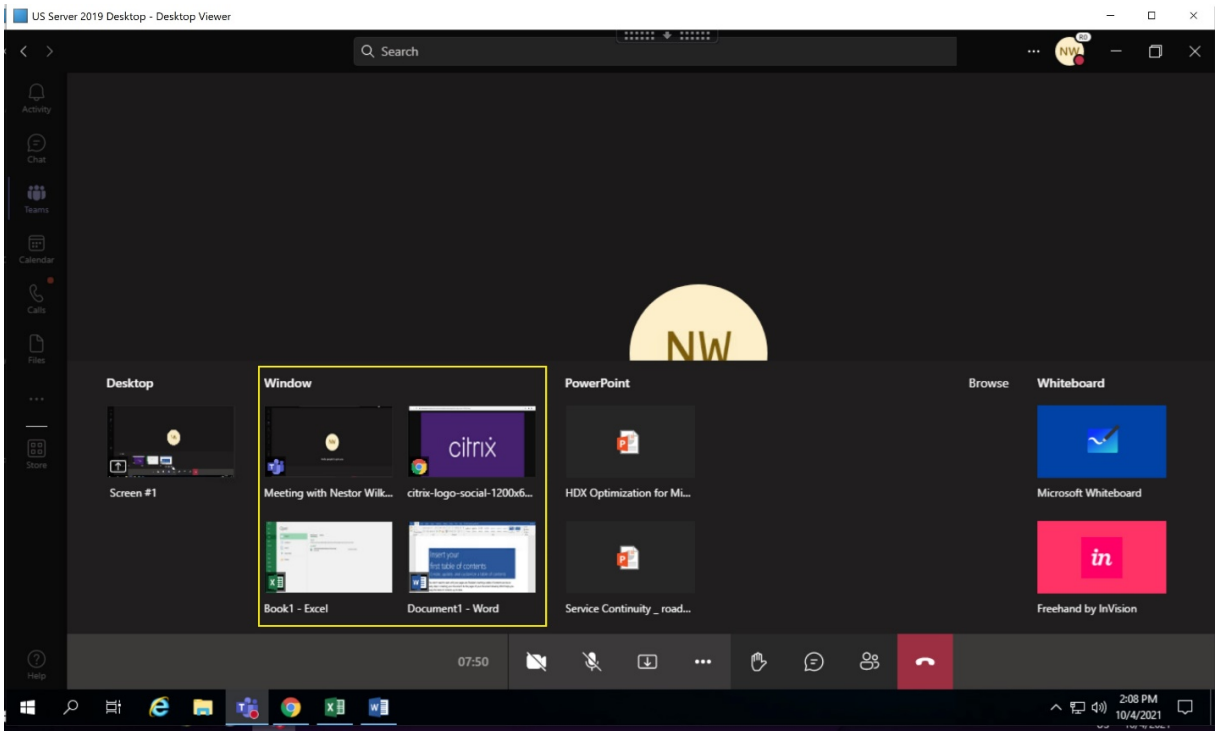
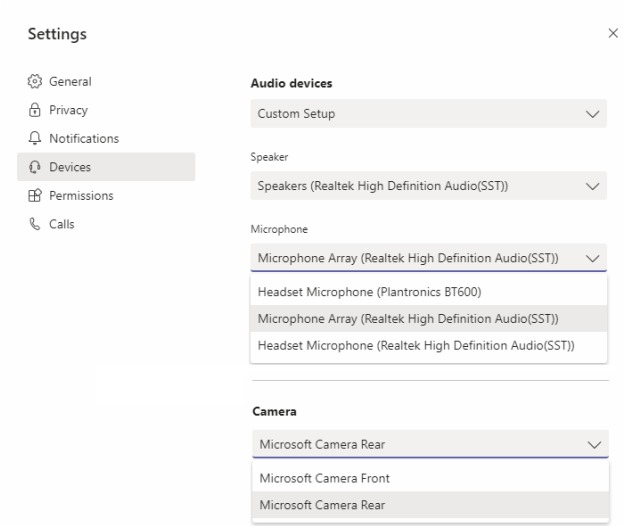
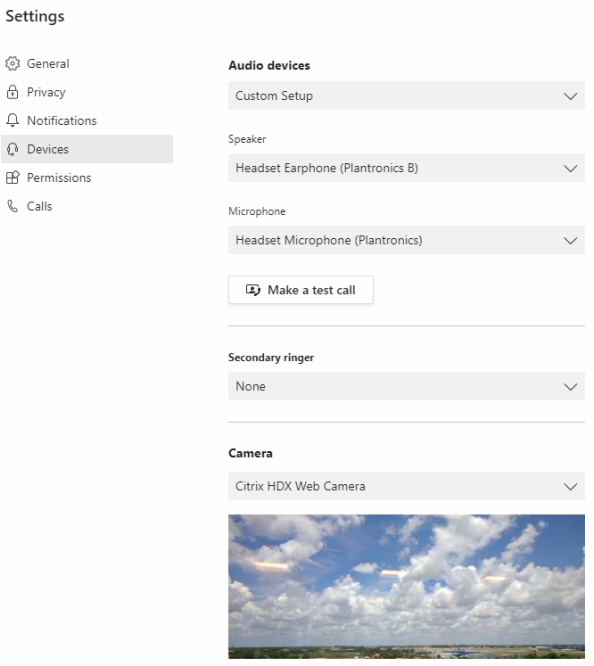
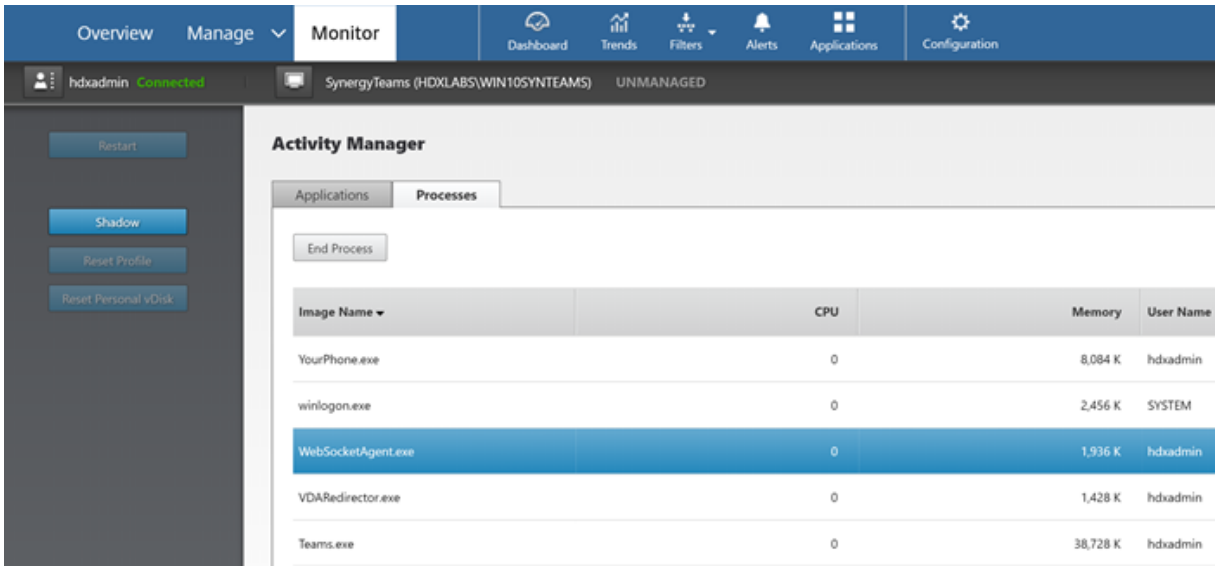
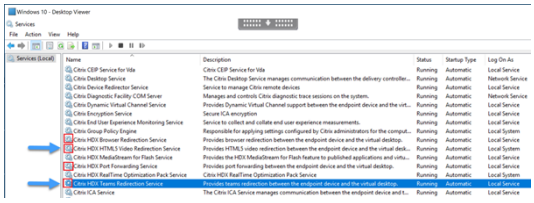
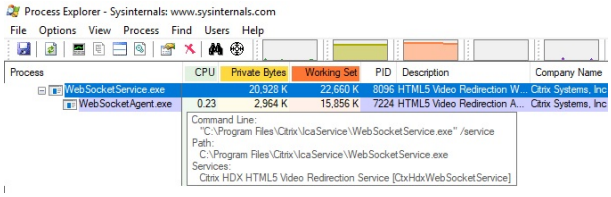
 }

<!--NeedCopy-->
```


On HTML5 For HTML5, background blurring is only supported. Custom image replacement is not supported.

For background blurring, do the following:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **backgroundEffects** attribute and set the attribute to **true**. For example,

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }

<!--NeedCopy-->
```

3. Save the changes.

Client CPU Consumption considerations

While the blurring feature is frugal on the CPU, you can expect an increase in consumption. For example, on a thin client with a 4 Core, 1.5 GHz Intel® Pentium® Silver chip with TurboBoost up to 2.8 GHz, the background blurring adds about 2% to the CPU usage. Average CPU usage is less than 20%.

Gallery view and active speakers in Microsoft Teams

Microsoft Teams supports **Gallery**, **Large gallery**, and **Together mode** layouts.

Microsoft Teams displays a 2x2 grid with video streams of four participants (known as **Gallery**). In this case, Microsoft Teams sends four video streams to the client device for decoding. When more than four participants share video, only the last four most active speakers appear on the screen.

Microsoft Teams also provides the large gallery view with a grid up to 7x7. As a result, the Microsoft Teams conference server composites a single video feed and sends it to the client device for decoding, resulting in lower CPU consumption. This single, matrix-style feed might include users' self-preview video as well.

Lastly, Microsoft Teams supports **Together mode**, which is part of the new meeting experience. Using AI segmentation technology to digitally place participants in a shared background, Microsoft Teams puts all participants in the same auditorium.

The user can control these modes during a conference call by selecting **Gallery**, **Large gallery**, or **Together mode** layouts in the ellipses menu.



Support for video aspect ratio constraints (CWA for Windows 2102, CWA for Linux 2106, CWA for MAC 2106 and later):

- The option **Fill to frame** is available in Gallery/Large Gallery View. This option crops the video size to fit it in the subwindow. **Fit to frame**, on the other hand, displays black bars (letterbox) on the sides of the video so there is no cropping.

The following table provides a comparison of Gallery and Large Gallery layouts:

	Gallery view 2x2 (default)	Large Gallery view
Layout / Grid	Displays a 2x2 grid with video streams of four participants. Only the last four most active speakers appear on the screen and other participants do not appear on the grid.	Displays a 7x7 grid with video streams of 49 participants.
Mixing technique	A media router forwards individual streams from each participant to every user.	A central conference server mixes and transcodes all audio or video to create a tailored composite layout for every participant. This action introduces some additional latency.
Active speaker	The new active speaker replaces the least active speaker in the grid.	Displays all participants irrespective of whether they are active or inactive.
Encoding at the endpoint	One or more video streams might be encoded at the endpoint if Simulcast is enabled. For more information on Simulcast support, see Simulcast.	One or more video streams might be encoded at the endpoint if Simulcast is enabled. For more information on Simulcast support, see Simulcast.
Decoding at the endpoint	Each participant gets up to four individual media streams. This increases CPU consumption at the endpoint by HdxRtcEngine.exe (for decoding/rendering).	Each participant gets only a single stream for audio and video. This setting lowers the CPU consumption at the endpoint.
Maximum resolution	720p. When four participants are sharing video, the maximum resolution is 360p per video feed. If fewer than four participants are sharing video, then the resolution per video feed might be higher.	720p for the composite layout or mixing. There's no need for a high-quality video stream per participant in a composite layout. Because of this condition, each sender reduces resolution or upload bitrate.

	Gallery view 2x2 (default)	Large Gallery view
'Slow-user'problem	Sender modifies each modality's (audio/video/screenshare) quality to the lowest common network quality among the participants. This multimedia stream is then forwarded to all other participants. As a result, a participant with poor network condition impacts the quality for everyone else in the call.	Less susceptible to the lowest common network quality scenario. The conference server provides different qualities based on the network conditions of individual participants.
Self-preview	Displays yourself in a small thumbnail in real time.	Displays yourself in thumbnail and mixed with the rest of the video feeds. As a result, you might see yourself included in the main video layout with some additional delay.

Screen sharing in Microsoft Teams

Microsoft Teams relies on video-based screen sharing (VBSS), effectively encoding the desktop being shared with video codecs like H264 and creating a high-definition stream. With HDX optimization, incoming screen sharing is treated as a video stream.

Starting from Citrix Workspace app 2109 or higher for Windows, Linux, Mac, and Citrix Workspace app 2303 for ChromeOS users can share their screens and video camera simultaneously.

With earlier versions, if you're in the middle of a video call and the other peer starts to share the desktop, the original camera video feed is paused. Instead, the screen sharing video feed shows. The peer must then manually resume the camera sharing.

> **Note for PowerPoint Live**
>
> This limitation does not exist if you're sharing content from PowerPoint Live. In that case, other peers can still see your webcam and content and navigate back and forth to review other slides. In this scenario, the slides are rendered on the VDA. To access a PowerPoint Live slide deck, click on the 'Share tray'button and select one of the suggested PowerPoint slides, or click 'Browse' and find a PowerPoint file on your computer or in OneDrive.

Outgoing screen sharing is also optimized and offloaded to Citrix Workspace app. In this case, the

media engine captures and transmits only the Citrix Desktop Viewer (CDViewer.exe) window, with a red border drawn around it. Any local application overlapping with Desktop Viewer isn't captured.

> **Note**
>
> Set specific permission in Citrix Workspace app for Mac to enable screen sharing. For more information, see System Requirements.

Multimonitor

If Desktop Viewer (CDViewer.exe) is in full-screen mode and spanning across multimonitor setups, Citrix Workspace app 2106 or later (Windows/Linux/Mac) allows the screen picker to select the monitor to share.

Known limitation:

- If Desktop Viewer is disabled or if Desktop Lock is being used, multimonitor selection isn't available in the Microsoft Teams screen picker. The Desktop Viewer might be disabled either by editing the `.ICA` file template or `StoreFront web.config`. SHIFT+F2 hotkey isn't compatible with multimonitor screen sharing.
- In Workspace app versions older than 2106, only the primary monitor is shared. Drag the application in the virtual desktop to the primary monitor for the other peer on the call to see it.
- Multimonitor screen sharing might not work if you configure the Citrix Workspace app with the virtual monitor layout feature (logical partition of a single physical monitor). In this case, all virtual monitors are shared as a composite image.
- Older versions of the Citrix Workspace app for Windows (1907 up to 2008) also shares a local application that runs in the client machine. This sharing is possible only if the local app was overlaid on top of Desktop Viewer. This behavior was removed in 2009.6 or higher, and 1912 CU5 or higher.
- While screen sharing, if you change from windowed mode to full-screen, screen sharing stops. You must stop and share again for screen sharing to work.



Screensharing from seamless application:

If you're publishing Microsoft Teams as a standalone, seamless application, screen sharing captures the local desktop of your physical endpoint. Citrix Workspace app minimum version 1909 is required.

App sharing

Starting with Citrix Workspace app for Windows 2112.1 and VDA 2112, Microsoft Teams supports app sharing.

Starting with Citrix Workspace app for Windows 2109, Mac 2203, Linux 2209, and VDA 2109, Microsoft Teams supports screen sharing of specific apps running in the virtual session. To share a specific app:

1. Navigate to the Microsoft Teams app within your remote session.
2. Click **Share content** in your Microsoft Teams UI.
3. Select an app to share in the meeting. The red border appears around an app you selected and the peers on the call can see the shared app.

To share a different app, click **Share content** again and select a new app.

If you want to disable app sharing, create the following registry key on the VDA at `HKLM\SOFTWARE\Citrix\Graphics`:
Name: `UseWsProvider`
Type: `DWORD`
Value: 0

> **Note:**
>
> - When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.
> - If you minimize an app, Microsoft Teams displays the last image from the shared app. You can maximize the window to resume screen sharing.
> - Screen sharing depends on the VDA-side capturing of the window. The content is then relayed at a maximum rate to the Citrix Workspace app. The maximm rate is 30 frames per second. The Citrix Workspace app forwards the content to the peers or conference server.



Known limitations with screen sharing of specific app:

- Mouse pointer isn't visible when you are screen sharing an app.
- If you minimize an app when you're sharing it, only the app icon appears in the screen picker. The thumbnail of the app isn't previewed in the screen picker. You can't share the content and the red border does not appear until you maximize the app.
- LAA apps shows a list of apps that can be shared with desktop apps in the optimized Microsoft Teams in the VDA. However, when you select the app from the list, the result might not be as expected.

Compatibility with app protection

The screen sharing of a specific app is compatible with the app protection feature in HDX optimized Microsoft Teams. You can screen share a specific app, if you've launched the app or desktop from a delivery group that has app protection enabled.

When you click **Share content** in the Microsoft Teams UI, the screen picker removes the **Desktop** option. You can only select the **Window** option to share any open app.

> **Note:**
>
> When you launch apps or desktops from a delivery group with app protection enabled, you aren't able to see the incoming video or screen sharing.

Give and Request control in Microsoft Teams This feature is supported in the following versions of Citrix Workspace app (there is no dependency on the VDA version or Operative System, single session

or multisession):

- Citrix Workspace app for Windows version 2112.1 and later
- Citrix Workspace app for Mac version 2203.1 and later
- Citrix Workspace app for Linux version 2203 and later
- Citrix Workspace app for ChromeOS version 2303 and later

You can request control during a Microsoft Teams call when a participant is sharing the screen. Once you have control, you can make selections, edits, or other keyboard and mouse activities to the shared screen.

To take control when a screen is being shared, click **Request control** button in the Microsoft Teams UI. The meeting participant who's sharing the screen can either allow or deny your request.

While you have control, you can make selections, edits, and other modifications to the shared screen. For these actions, you can use both keyboard and mouse. When you're done, click **Request control**.

> **Limitations:**
>
> - Give and Request control are not available if the user is sharing a single app (also known as App sharing). The full desktop or monitor must be shared.
> - The feature to pin the control bar to a specific location is not available.

Peripherals in Microsoft Teams

When optimization for Microsoft Teams is active, the Citrix Workspace app accesses the peripherals (headsets, microphones, cameras, speakers, and so forth). Then the peripherals are properly listed in the Microsoft Teams UI (**Settings > Devices**).



Microsoft Teams does not access the devices directly. Instead, it relies on the Workspace app WebRTC media engine for acquiring, capturing, and processing the media. Microsoft Teams lists the devices for the user to select.

The peripherals that are inserted while Microsoft Teams is active aren't selected by default. You've to manually select the peripherals from the **Settings** > **Devices** screen of the Microsoft Teams UI. After the peripheral is selected, Microsoft Teams caches the information of the peripherals. As a result, the peripherals are automatically selected when you reconnect to a session from the same endpoint.

Recommendations:

- Microsoft Teams certified headsets with built-in echo cancellation. In setups with extra peripherals, where microphone and speakers are on separate devices, there might be an echo. An example is a webcam with a built-in microphone and a monitor with speakers. When using external speakers, place them as far as possible from the microphone. Also, place them away from any surface that might refract the sound into the microphone.
- Microsoft Teams certified cameras, although Skype for Business certified peripherals are compatible with Microsoft Teams.
- Citrix Workspace app media engine can't take advantage of CPU offloading with webcams that perform on-board H.264 encoding -UVC 1.1 and 1.5.

> **Note:**
>
> Workspace app 2009.6 for Windows can now acquire peripherals with audio formats with 24-bit or with frequencies above 96 kHz.
>
> HdxTeams.exe (in the Citrix Workspace app for Windows 2009 or older) supports only these specific audio device formats (channels, bit depth, and sample rate):
>
> - Playback Devices: up to 2 channels, 16 bit, frequencies up to 96,000 Hz
> - Recording Devices: up to 4 channels, 16 bit, frequencies up to 96,000 Hz
>
> Even if one speaker or microphone does not match the expected settings, device enumeration in Microsoft Teams fails and **None** displays under **Settings > Devices**.
>
> **Webrpc** logs in **HdxTeams.exe** show this type of information:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing ...
> ```
>
> ```
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!
> ```
>
> As a workaround, disable the specific device or:
>
> 1. Open the **Sound Control Panel** (mmsys.cpl).

2. Select the playback or recording device.
3. Go to **Properties > Advanced** and change the settings to a supported mode.

Fallback mode

If Microsoft Teams fails to load in optimized VDI mode ("Citrix HDX Not Connected"in Teams/About/Version), the VDA falls back to legacy HDX technologies. The legacy HDX technologies might be webcam redirection and client audio and microphone redirection. If you're using a Workspace app version/platform OS that does not support Microsoft Teams optimization, fallback registry keys do not apply.
In fallback mode, the peripherals are mapped to the VDA. The peripherals appear to the Microsoft Teams app as if they were locally attached to the virtual desktop.

You can now granularly control the fallback mechanism by setting the registry keys in the VDA. For information, see Microsoft Teams fallback mode in the list of features managed through the registry.

This feature requires Microsoft Teams version 1.3.0.13565 or later.

To determine if you are in optimized or unoptimized mode when looking at the **Settings > Devices** tab in the Microsoft Teams app, the main difference is the camera name. If Microsoft Teams loaded in unoptimized mode, legacy HDX technologies launch. The webcam name has the **Citrix HDX** suffix as shown in the following graphic. The speaker and microphone device names might be slightly different (or truncated) when compared to the optimized mode.



When legacy HDX technologies are used, Microsoft Teams doesn't offload audio, video, and screen sharing processing to the endpoint's Citrix Workspace app WebRTC media engine. Instead, HDX tech-

nologies use server-side rendering. Expect high CPU consumption on the VDA when you turn on video. Real-time audio performance might not be optimal.

Known limitations

Citrix limitations

Limitations on Citrix Workspace app:

- HID buttons - Answer and end call aren't supported. Volume up and down are supported.
- QoS settings in the Admin Center for Microsoft Teams don't apply for VDI users.
- App protection add-on feature for the Citrix Workspace app prevents outgoing screen sharing and blocks incoming screen share and video.
- Users can't take screenshots of Microsoft Teams content while using a snipping tool on the VDA. However, if a snipping tool is used at the client side, the content can be captured.

Limitation on the VDA:

- When you configure the Citrix Workspace app High DPI setting to **Yes**, the redirected video window appears out of place. This limitation occurs when the monitor's DPI scaling factor is set to anything above 100%.

Limitations on Citrix Workspace app and the VDA:

- You can only control the volume of an optimized call using the volume bar on the client machine –not on the VDA.

Simulcast

Simulcast support is enabled for optimized Microsoft Teams video conference calls on Windows and Mac. For Linux check with your thin client vendor.
With Simulcast the quality and experience of video conference calls across different endpoints are improved by adapting to the proper resolution for the best call experience for all callers.

With this improved experience, each user might deliver multiple video streams in different resolutions (for example, 720p, 360p, and so on) depending on several factors including endpoint capability, network conditions, and so on. The receiving endpoint then requests the maximum quality resolution that it can handle thereby giving all users the optimum video experience.

> **Note:**
>
> This feature is available only after the roll-out of an update from Microsoft Teams. For information on ETA, https://www.microsoft.com/ go to and search for Microsoft 365 roadmap. When the

> update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

Microsoft limitations

- A 3x3 gallery view isn't supported. Microsoft Teams dependency –contact Microsoft for when to expect a 3x3 grid.
- Interoperability with Skype for Business is limited to audio calls, no video modality.
- Incoming and outgoing video stream maximum resolution is 720p. Microsoft Teams dependency –contact Microsoft for when to expect 1080p.
- PSTN call ringback tone isn't supported.
- Media bypass for Direct Routing isn't supported.
- Broadcast and live event producer and presenter roles aren't supported. Attendee role is supported but not optimized (renders on the VDA instead).
- The zoom in and zoom out function in Microsoft Teams isn't supported.
- Location-Based Routing and Media Bypass are not supported.
- Call merge is not supported (option not displayed in the user interface).

Citrix and Microsoft limitations

- When doing screen sharing, the option **include system audio** isn't available.
- Simulcast isn't supported on ChromeOS.

Upcoming Microsoft Teams Single-Window EOL

On January 31, 2024, Microsoft will retire the Microsoft Teams support for Single-window UI when using VDI Microsoft Teams optimization and support only the Multi-Window experience. Microsoft gave notice of this deprecation on 9/8/2023 in the M365s Admin Center (Post ID: MC674419).
Public details about the Multi-Window feature can be found in the Tech Community article: New Meeting and Calling Experience in Microsoft Teams.

You must upgrade your VDA and Citrix Workspace app to the supported versions to continue using Microsoft Teams in optimized mode for video and screen sharing. If you don't upgrade your infrastructure and endpoints to support multi-window, you can only establish audio calls. You will not be able to use the optimized video and screensharing functionality.

The following table illustrates the minimum, LTSR, and recommended versions of VDA and Citrix Workspace app required to continue using optimized calling in Microsoft Teams on Citrix VDI:

Component	Minimum version	LTSR supported version	Recommnded version
Microsoft Teams	1.5.00.11865	Not applicable	Latest
VDA	1912 CU6 LTSR, 2203 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+
Citrix Workspace app for Windows	2205 CR	2203 CU2+	2309 CR+
Citrix Workspace app for Mac	2209 CR	Not applicable	2308 CR+
Citrix Workspace app for Linux	2209 CR	Not applicable	2308 CR+
Citrix Workspace app for ChromeOS or HTML5	2303 CR	Not applicable	2309 CR+

Deprecation announcement of the SDP format (Plan B) from WebRTC

Citrix is planning to deprecate the current SDP format (Plan B) support from WebRTC in future releases. You must use Unified Plan in WebRTC to support optimized Microsoft Teams functionalities.

Products that are affected

In one of the future releases of the Citrix Workspace Application, calls between endpoints with the upcoming release for the Citrix Workspace app and endpoints with Citrix Workspace app 2108 or older versions will not be supported. This calling incompatibility includes 1912 LTSR Citrix Workspace app clients (CWA). The following CWA clients are impacted:

- Citrix Workspace app for Windows
- Citrix Workspace app for Linux
- Citrix Workspace app for Mac
- Citrix Workspace app for Chrome

Replacement for Plan B

If you are running the Citrix Workspace app version older than 2109, you must upgrade to a supported version (preferably the latest CR release). Otherwise, any calls with a future release or newer endpoints fail to connect. Calls between future releases and your federated communication partners might also fail to complete if the federated partner has not upgraded their Citrix Workspace.

Citrix Workspace app version 2108 has completed its support date in March 2023 and must be upgraded to a newer version. For more information, see Workspace App for details on Citrix Workspace app version support.

For more information on the Plan B deprecation, see the WebRTC documentation.

Additional information

- Monitor, troubleshoot, and support Microsoft Teams
- Deploy the Microsoft Teams desktop app to the VM
- Install Microsoft Teams using MSI (VDI Installation section)
- Thin clients
- Skype for Business Network Assessment Tool
- Understand Microsoft Teams and Skype for Business coexistence and interoperability

Monitor, troubleshoot, and support Microsoft Teams

April 10, 2024

Monitor Teams

This section provides guidelines for monitoring Microsoft Teams optimization with HDX.
If you're running in optimized mode and `HdxRtcEngine.exe` is running on the client machine, a process on the VDA called `WebSocketAgent.exe` is running in the session. Use the **Activity Manager** in Director to see the application.



With the VDA minimum version 1912, you can monitor active Teams calls using the Citrix HDX Monitor (minimum version 3.11). The Citrix Virtual Apps and Desktops product ISO contains the latest `hdxmonitor.msi` in the folder `layout\image-full\Support\HDX Monitor`.

For more information, see *Monitoring* in the Knowledge Center article CTX253754.

Troubleshoot

This section provides troubleshooting tips for issues that you might encounter when using optimization for Microsoft Teams. For more information, see CTX253754.

On the Virtual Delivery Agent

There are four services installed by BCR_x64.msi. Only two are responsible for Microsoft Teams redirection in the VDA.



- **Citrix HDX Teams Redirection Service** establishes the virtual channel used in Microsoft Teams. The service relies on CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** runs as WebSocketService.exe listening on 127.0.0.1:9002 TCP. WebSocketService.exe performs two main functions:

  i. **TLS termination for secure WebSockets** receives a secure WebSocket connection from vdiCitrixPeerConnection.js, which is a component inside the Microsoft Teams app. You can track it with the Process Monitor. For more information about certificates, see the section "TLS and HTML5 video redirection, and browser content redirection"under Communication between Controller and VDA.

  Some antivirus and desktop security software interferes with the proper functioning of `WebSocketService.exe` and its certificates. While the Citrix HDX HTML5 Video Redirection service might be running in the `services.msc` console, the localhost `127.0.0.1:9002` TCP socket is never in listening mode as seen in netstat. Trying to restart the service causes it to hang ("Stopping…"). Ensure you apply the proper exclusions for the `WebSocketService.exe` process.

ii. **User session mapping.** When the Microsoft Teams application starts, WebSocketService.exe starts the WebSocketAgent.exe process in the user's session in the VDA. WebSocketService.exe runs in Session 0 as a LocalSystem account.



You can use **netstat** to check if the WebSocketService.exe service is in an active listening state in the VDA.

Run `netstat -anob -p tcp` from an elevated command prompt window:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

On a successful connection, the state changes to ESTABLISHED:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> **Important:**
>
> WebSocketService.exe listens in two TCP sockets, 127.0.0.1:9001 and 127.0.0.1:9002. Port 9001 is used for browser content redirection and HTML5 video redirection. Port 9002 is used for Microsoft Teams redirection. Ensure that you don"t have any proxy configurations in the Windows OS of the VDA that can prevent a direct communication between Teams.exe and WebSocketService.exe. Sometimes, when you configure an explicit proxy in Internet Explorer 11 (**Internet Options > Connections > LAN settings > Proxy Server**), connections might flow through an assigned proxy server. Verify that **Bypass proxy server for local addresses** is checked when using a manual and explicit proxy setting.

Services locations and descriptions

Service	Path to executable in Windows Server OS	Log on as	Description
Citrix HTML5 Video Redirection Service	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	Local System account	Provides multiple HDX Multimedia services with the initial framework required to perform media redirection between the virtual desktop and the endpoint device.
Citrix HDX Browser Redirection Service	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	This account (local Service)	Provides browser content redirection between the endpoint device and the virtual desktop.
Citrix Port Forwarding Service	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	This account (local Service)	Provides port forwarding between the endpoint device and the virtual desktop for browser content redirection.
Citrix HDX Teams Redirection Service	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	Local System account	Provides Microsoft Teams redirection between the endpoint device and the virtual desktop.

Citrix Workspace app

On the user's endpoint, the Citrix Workspace app for Windows instantiates a new service called Hdx-Teams.exe. It does so when Microsoft Teams launches in the VDA and the user tries to call or access the peripherals in self-preview. If you don't see this service, check the following:

1. Ensure that you installed as a minimum the Workspace App version 1905 for Windows. Do you see HdxTeams.exe and the webrpc.dll binaries in the Workspace app installation path?
2. If you validated step1, do the following to check if HdxTeams.exe is getting launched.

    a) Exit Microsoft Teams on the VDA.

b) Start services.msc on VDA.
c) Stop the Citrix HDX Teams Redirection Service.
d) Disconnect the ICA session.
e) Connect the ICA session.
f) Start the Citrix HDX Teams Redirection Service.
g) Restart the Citrix HDX HTML5 Video Redirection Service.
h) Launch Microsoft Teams on the VDA.

3. If you still don't see HdxTeams.exe being launched on the client endpoint, do the following:

a) Restart the VDA.
b) Restart the client endpoint.

Support

Citrix and Microsoft jointly support the delivery of Microsoft Teams from Citrix Virtual Apps and Desktops using optimization for Microsoft Teams. This joint support is the result of close collaboration between the two companies. If you have valid support contracts and you experience an issue with this solution, open a support ticket with the vendor whose code you suspect to be causing the issue. That is, Microsoft for Teams or Citrix for the optimization components.

Citrix or Microsoft receives the ticket, triages the issue, and escalates as appropriate. There is no need for you to contact each company's support team.

When you have a problem, we recommend you click **Help > Report a Problem** in the Teams UI. VDA-side logs are automatically shared between Citrix and Microsoft to resolve technical issues faster.

Collecting logs

HDX media engine logs can be found on the user's machine (not on the VDA). In case of any issues, make sure you attach logs to your support case.

Windows logs:

You can locate Windows logs at %TEMP% inside the **HDXTeams** folder (AppData/Local/Temp/HDX-Teams or AppData/Local/Temp/HdxRtcEngine). Look for a .txt file called webrpc_Day_Month_timestamp_Year.txt. If you are using newer versions of Citrix Workspace app, for example Citrix Workspace app 2009.5 or later, store the logs in AppData\Local\Temp\HdxRtcEngine.

Each session creates a separate folder for logs.

Mac logs:

1. VDWEBRTC log - records the execution of the virtual channel.

Location /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine log - records the execution of the processes on HdxRtcEngine.

   Location: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine log is enabled by default.

3. Webrpc logs - are the most important logs that record the execution of the wrap-up of the webrtc library.

   Location: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

Linux logs:

You can locate Linux logs in the /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/ folders.
Webrtc log: /tmp/webrpc/<current date>/webrtc.log
Kernel log: /var/log/syslog

ICE/STUN/TURN/ logs:

When establishing a call, these four ICE phases are required:

- Candidate gathering
- candidate exchange
- Connectivity checks (STUN bind requests)
- Candidate promotion

In the HdxRtcEngine.exe logs, the following entries are the relevant Interactive Connectivity Establishment (ICE) entries. These entries must be there for a call set-up to succeed. See the following sample snippet for the gathering stage:

```
RPCStubs Info: -> device id = \\?\display#int3470#4&1835d135&0&uid13424
   #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 \{
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[...]

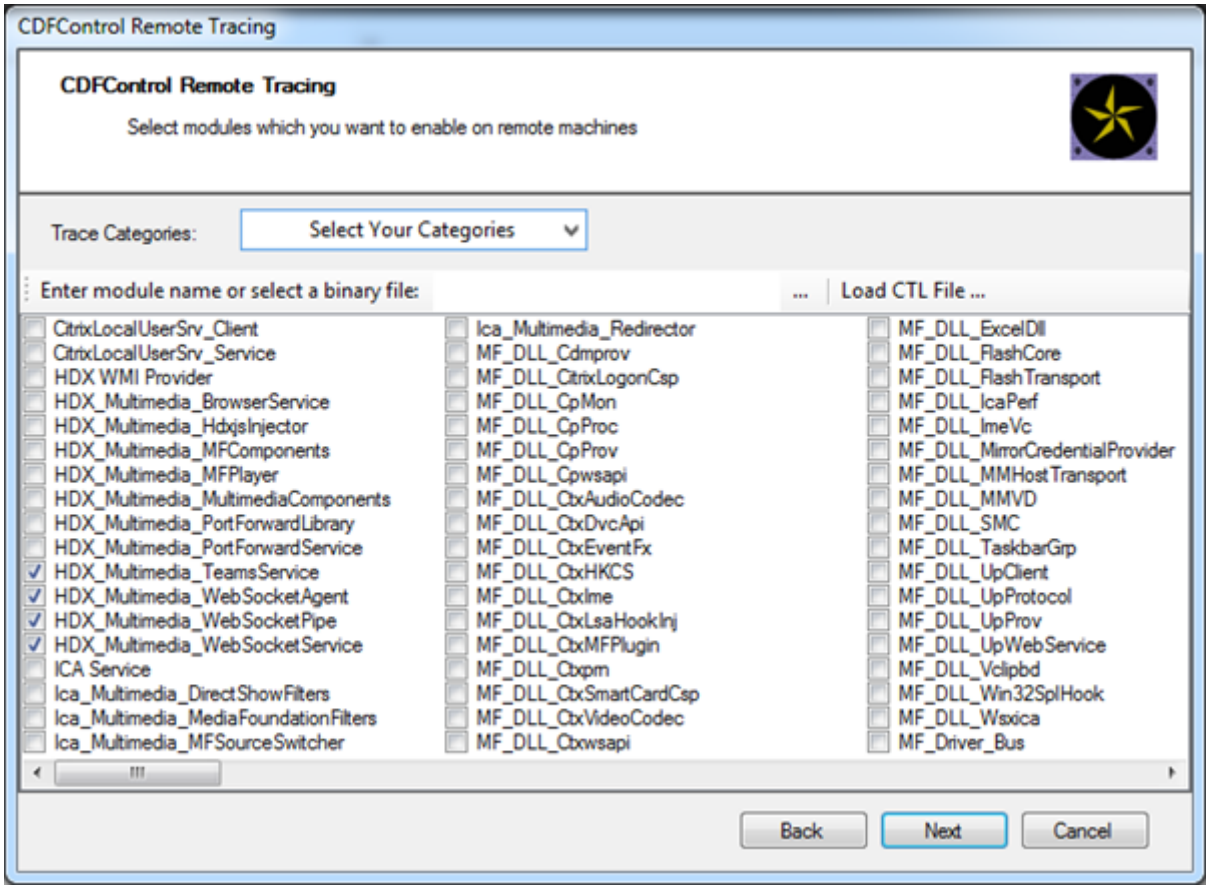
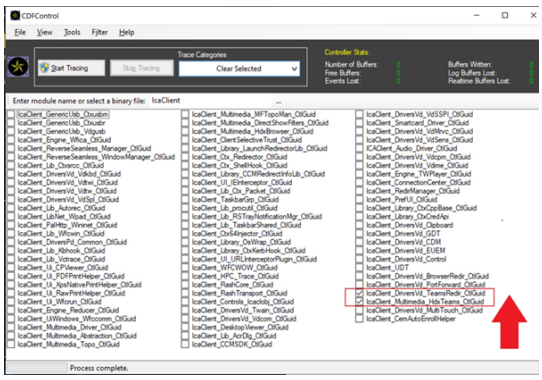
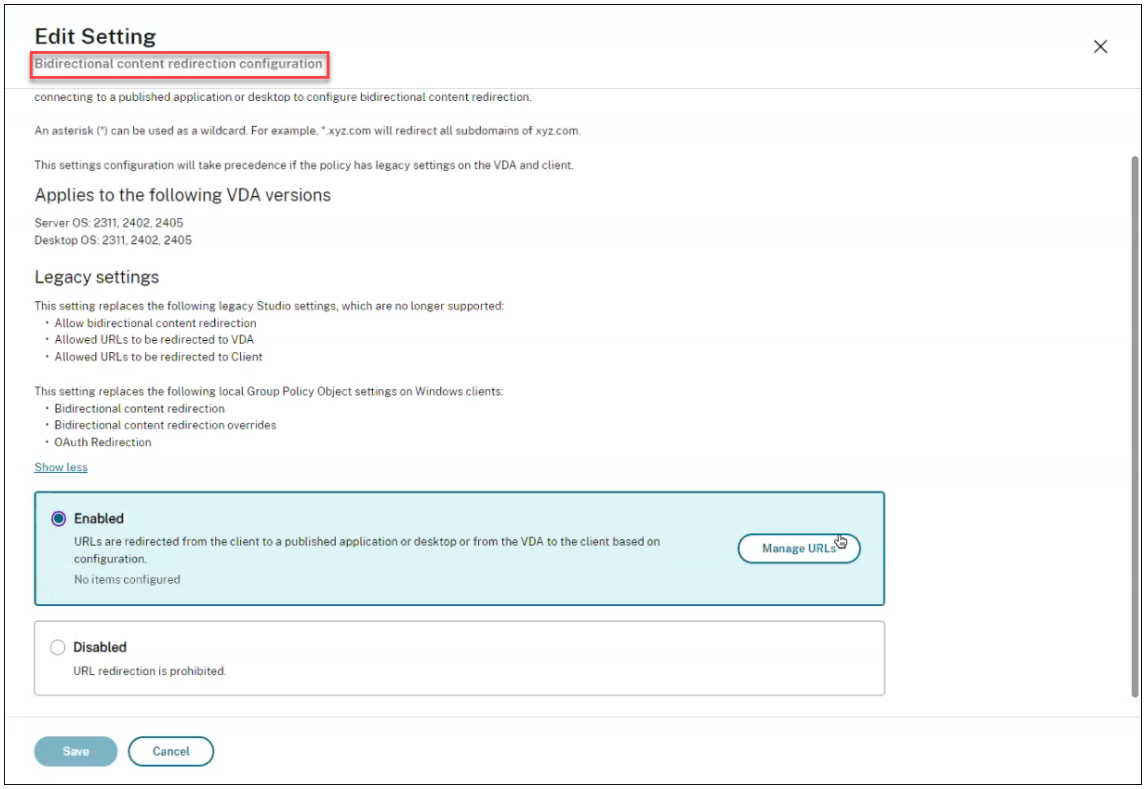
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
   HaveLocalOffer

```



```
webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering

[...]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[...]
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[...]

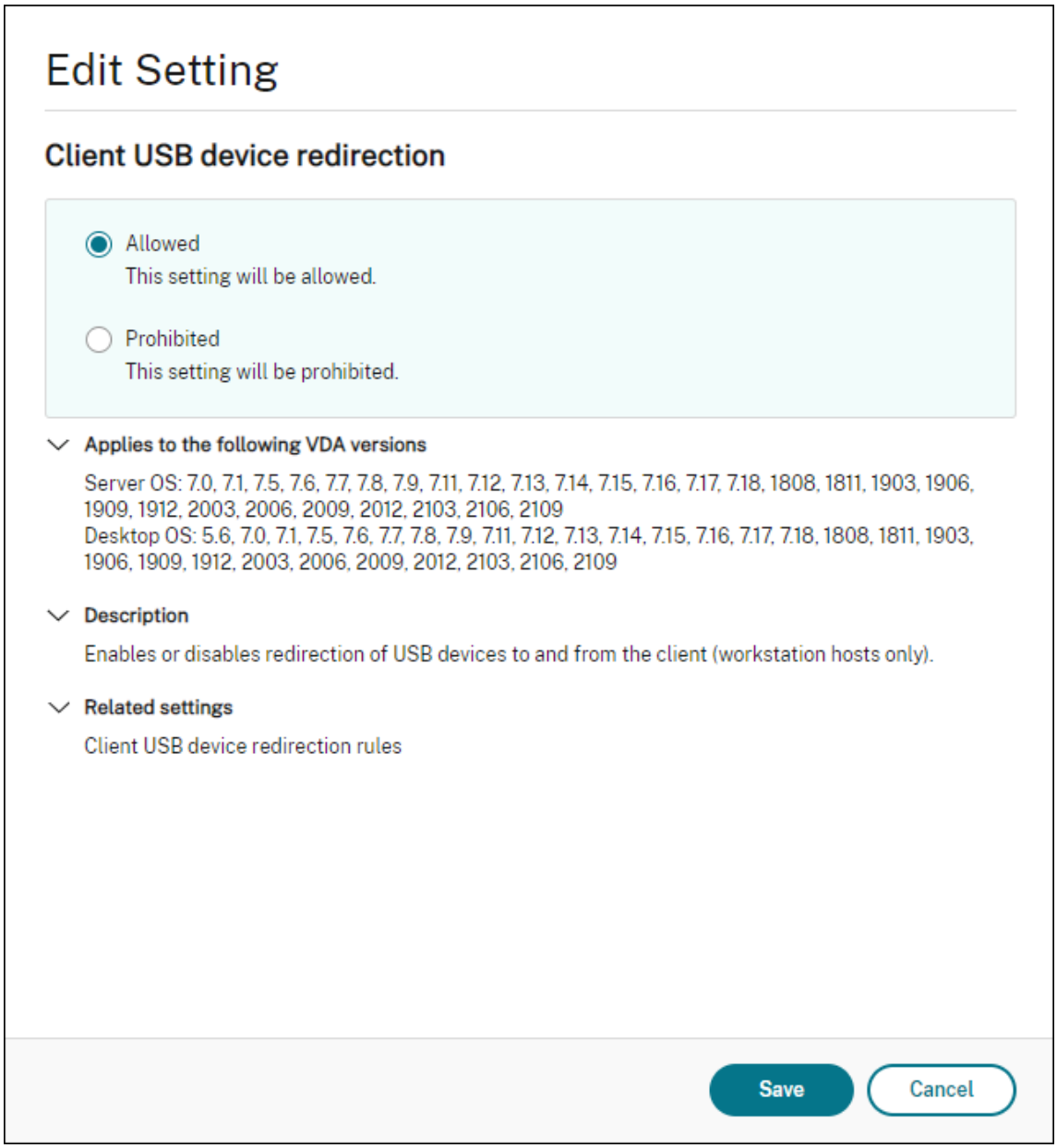
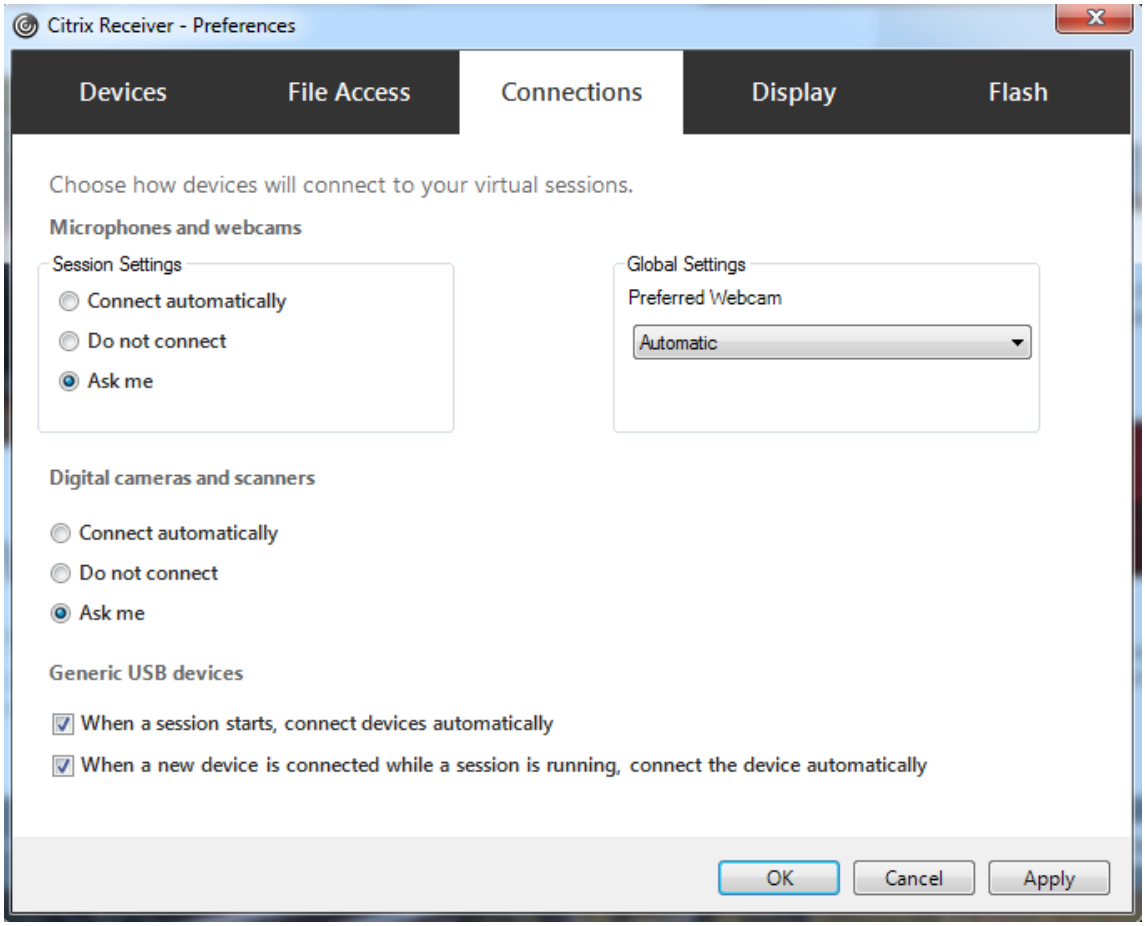
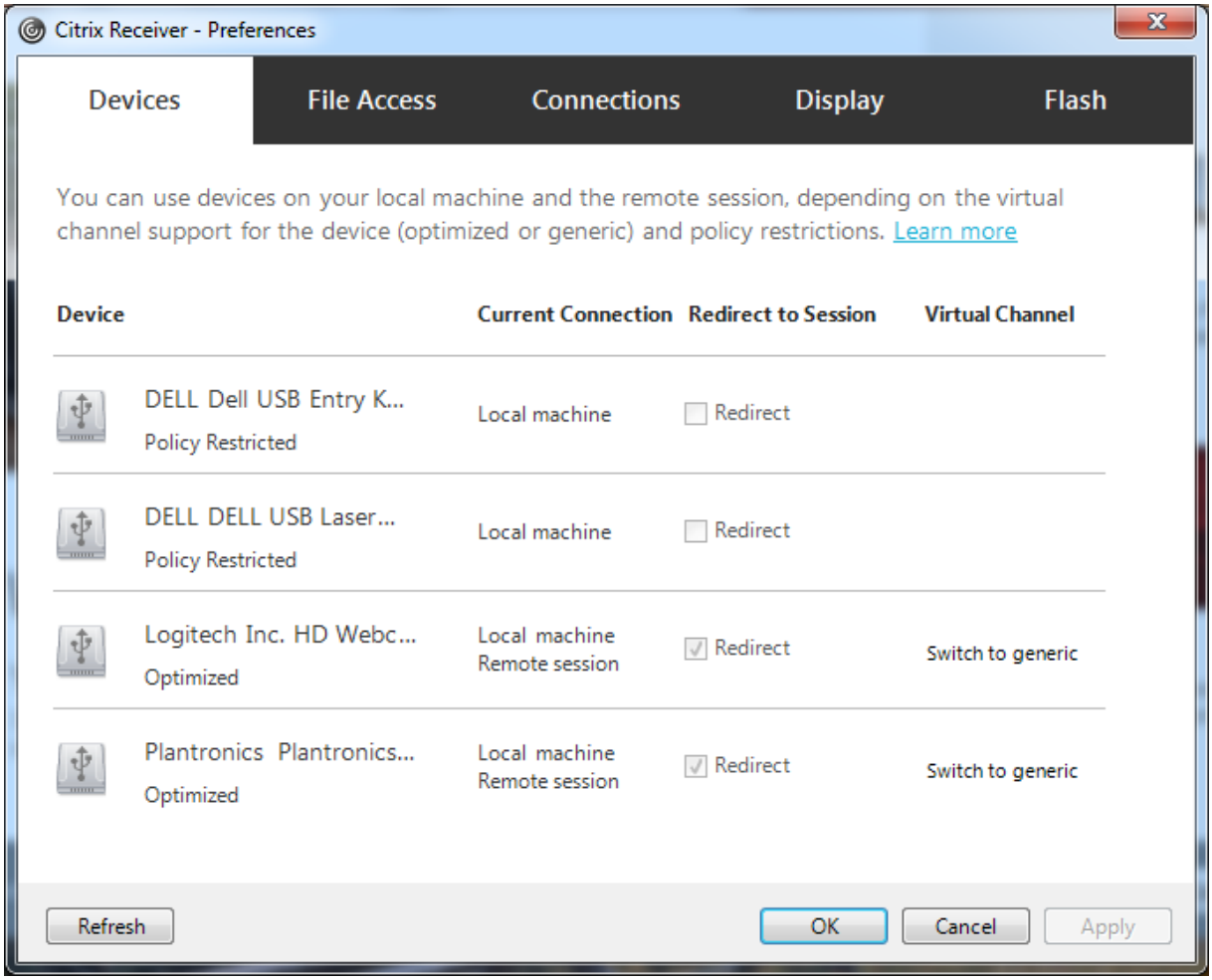
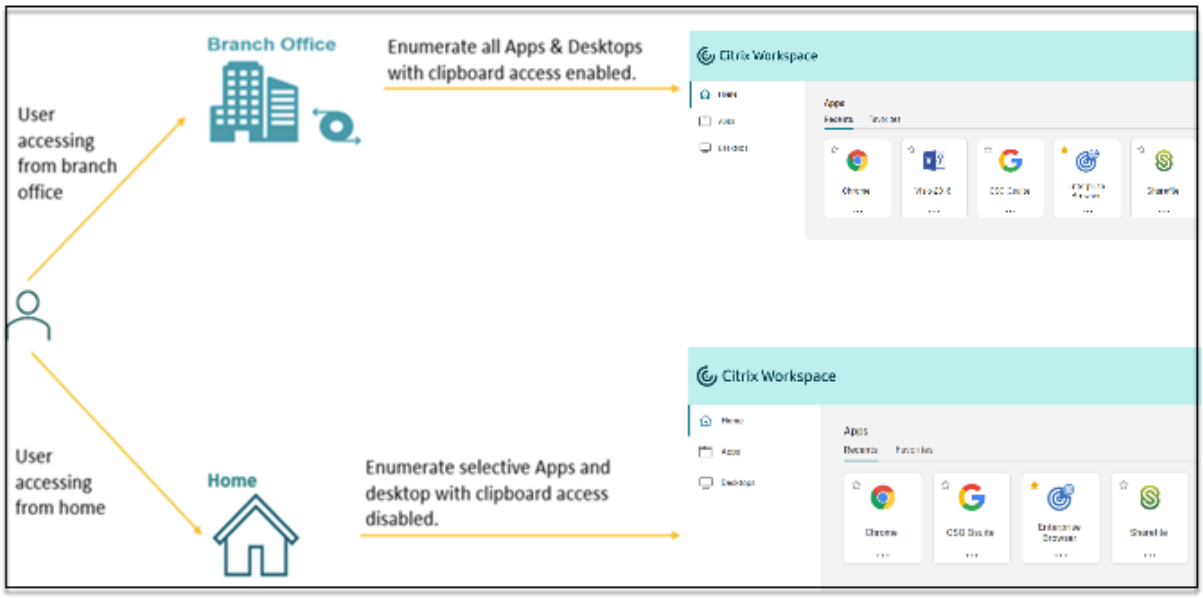
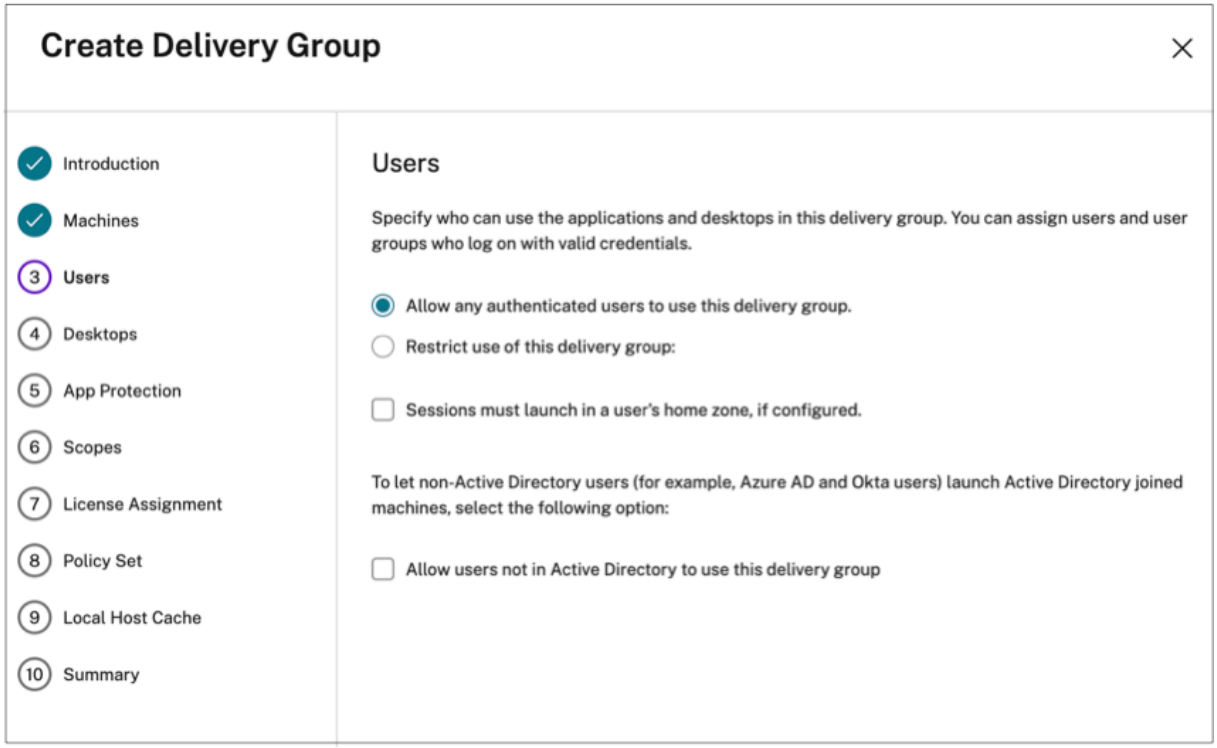
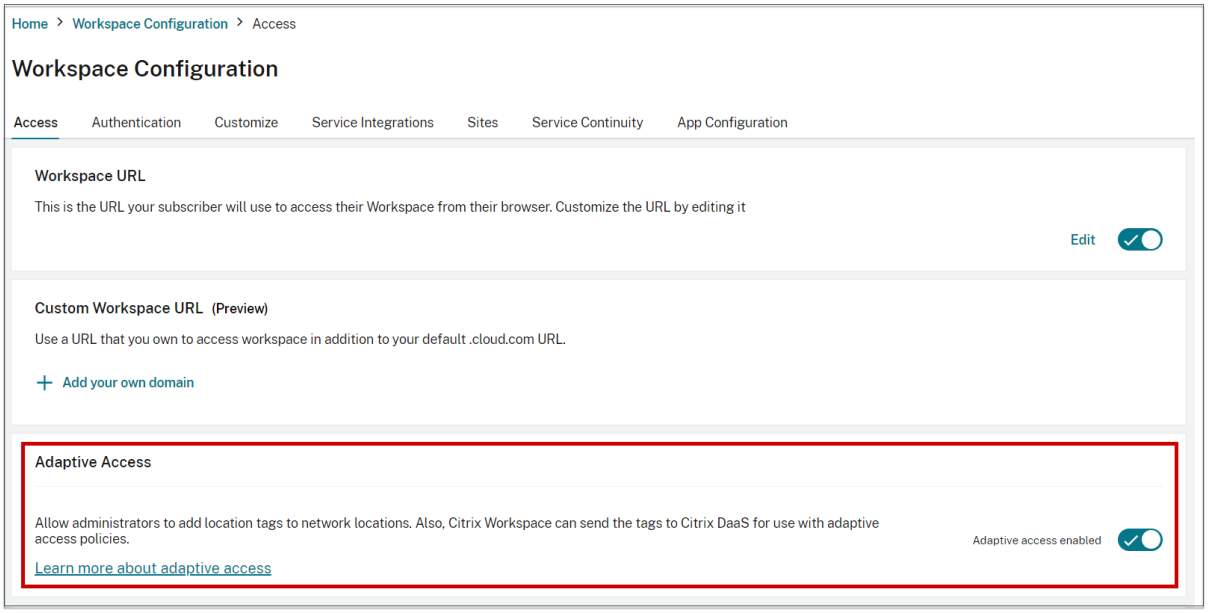
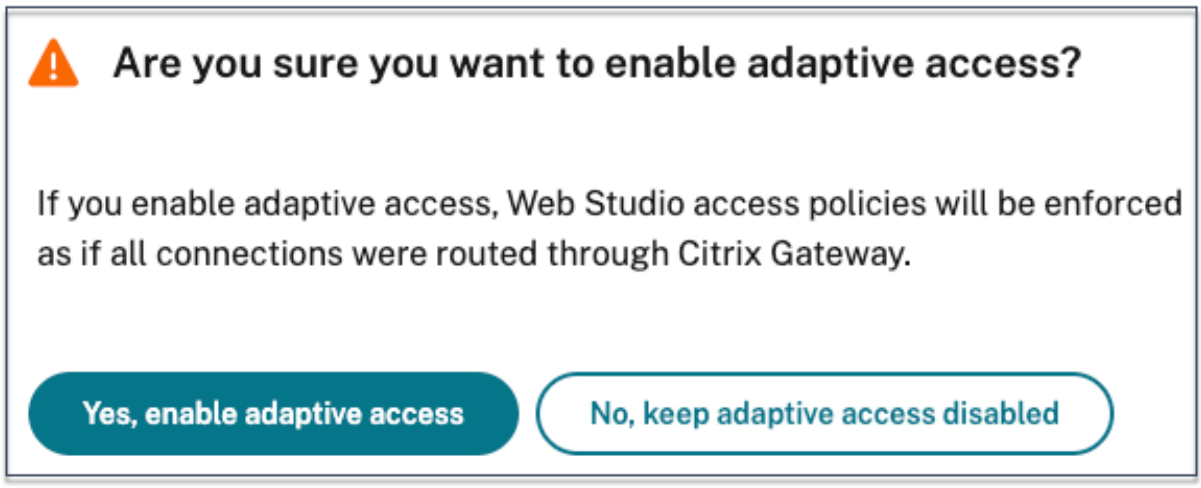
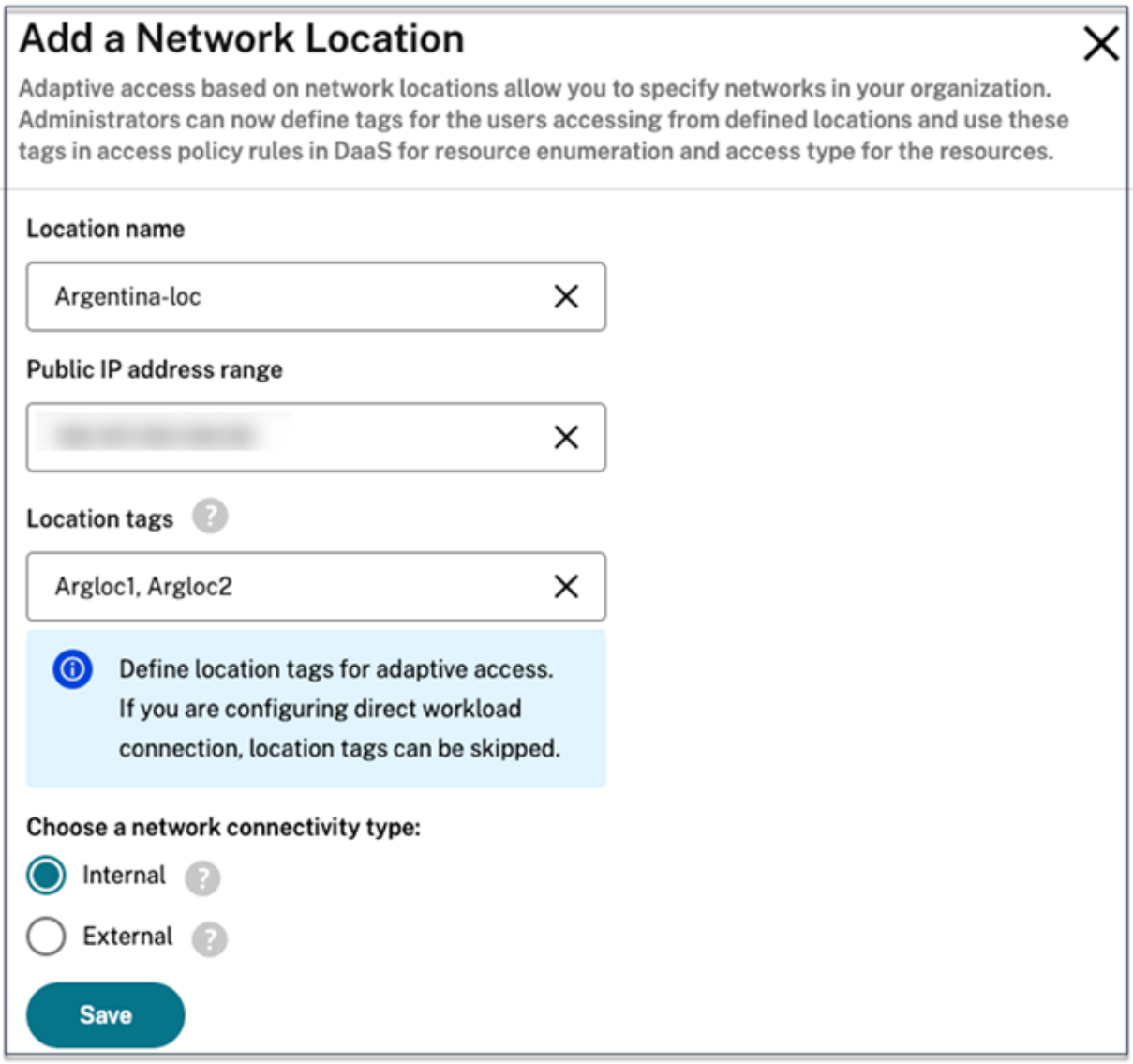
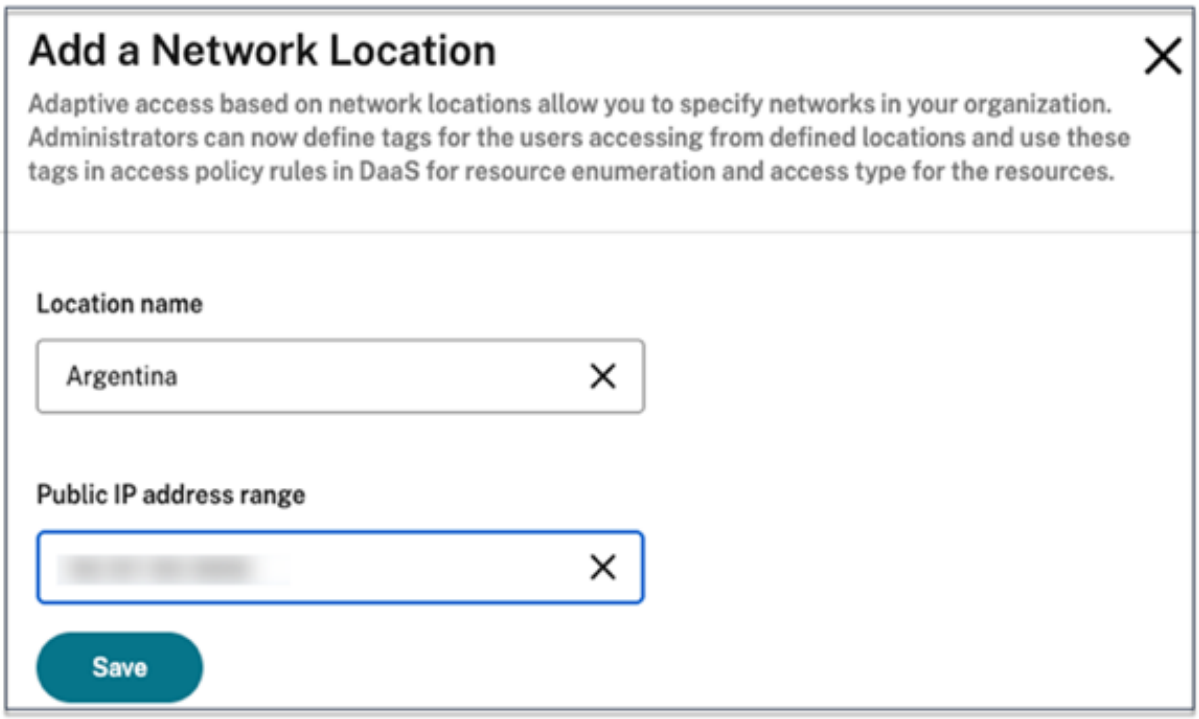
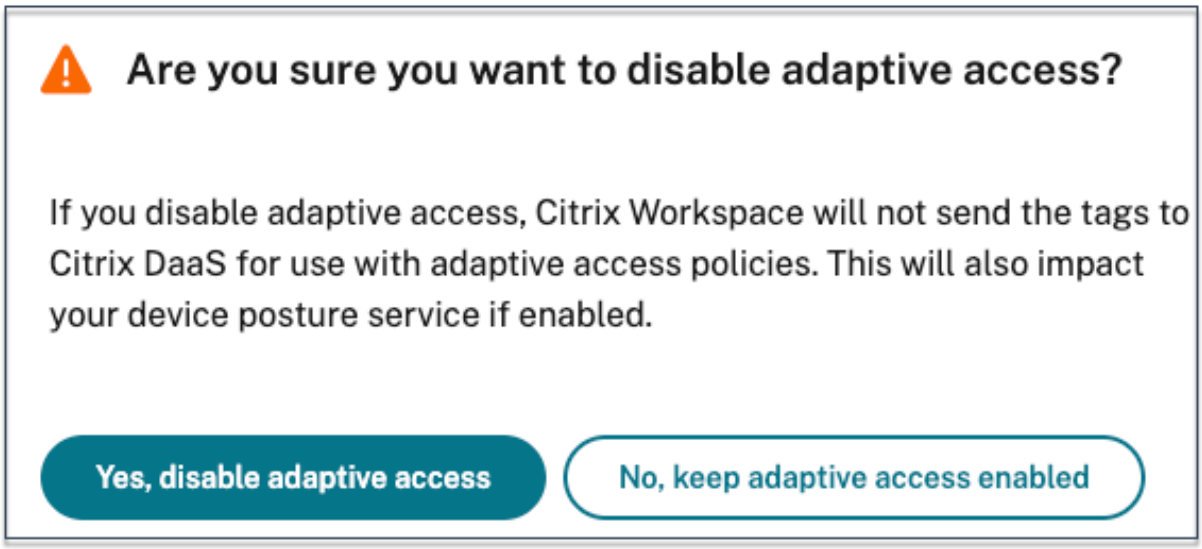
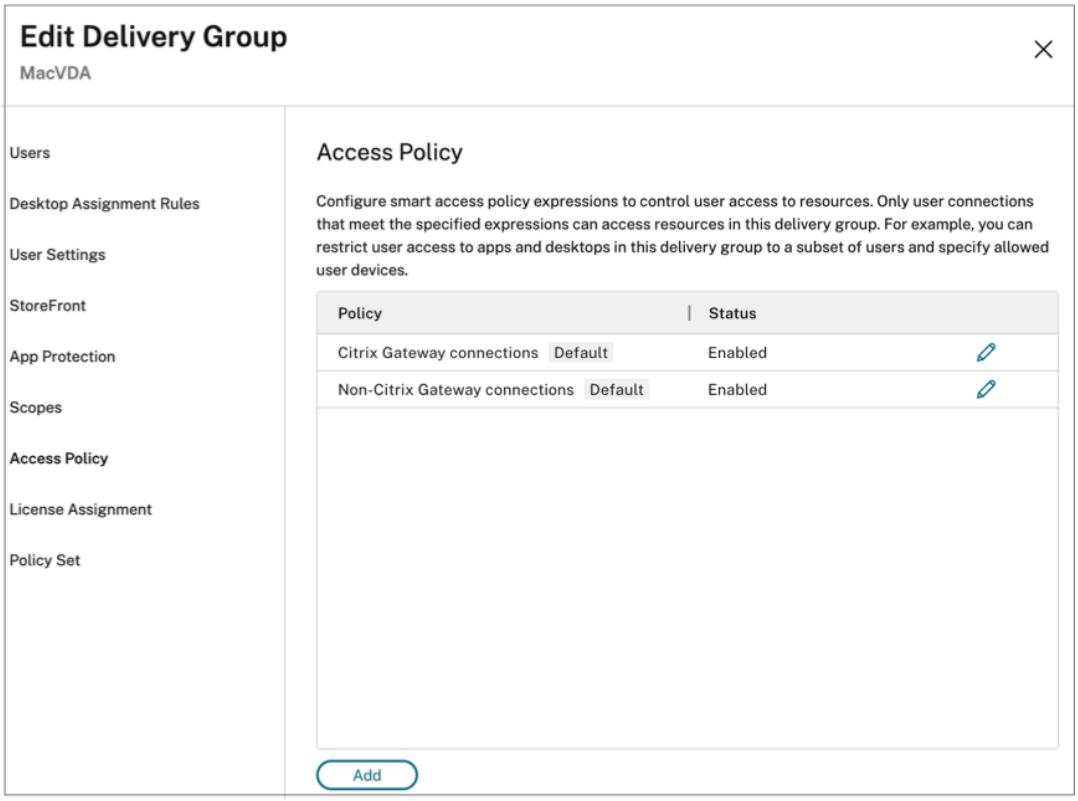
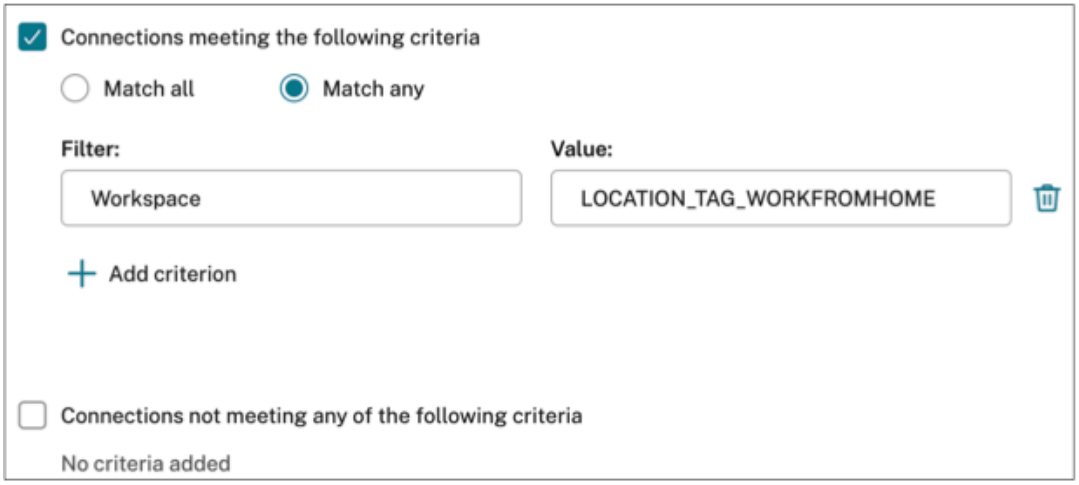
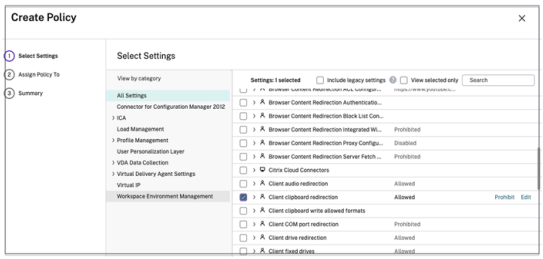
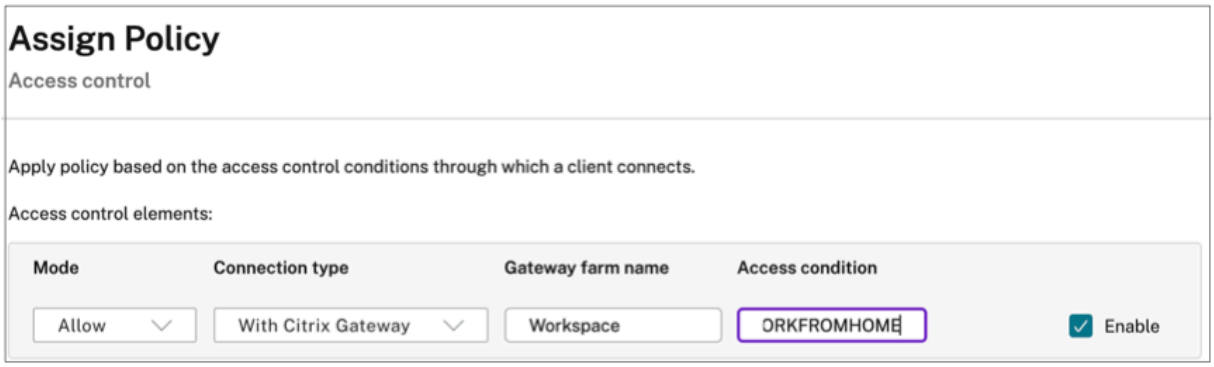
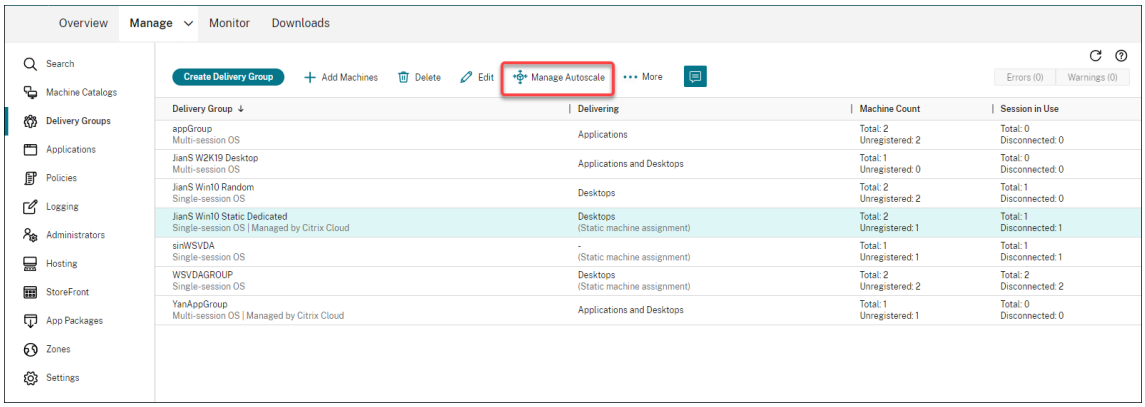
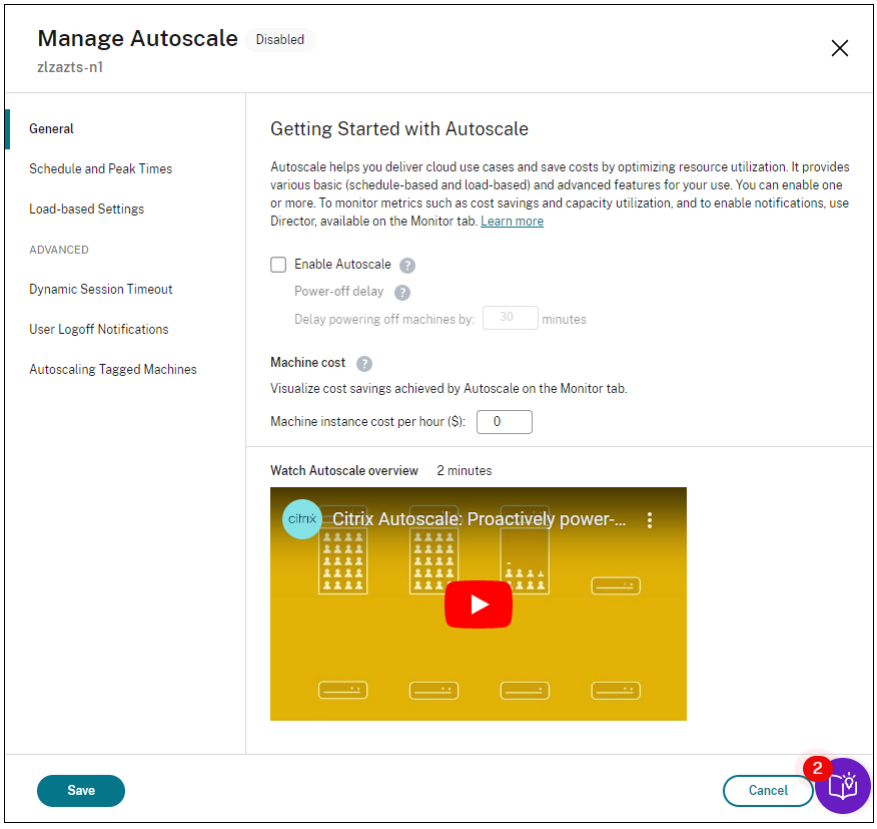
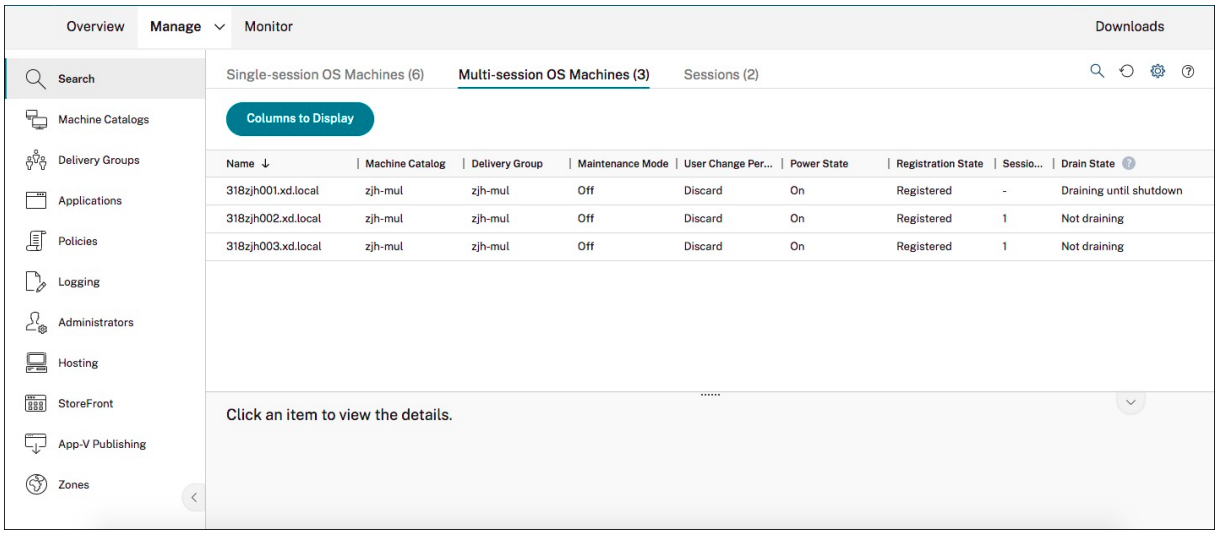
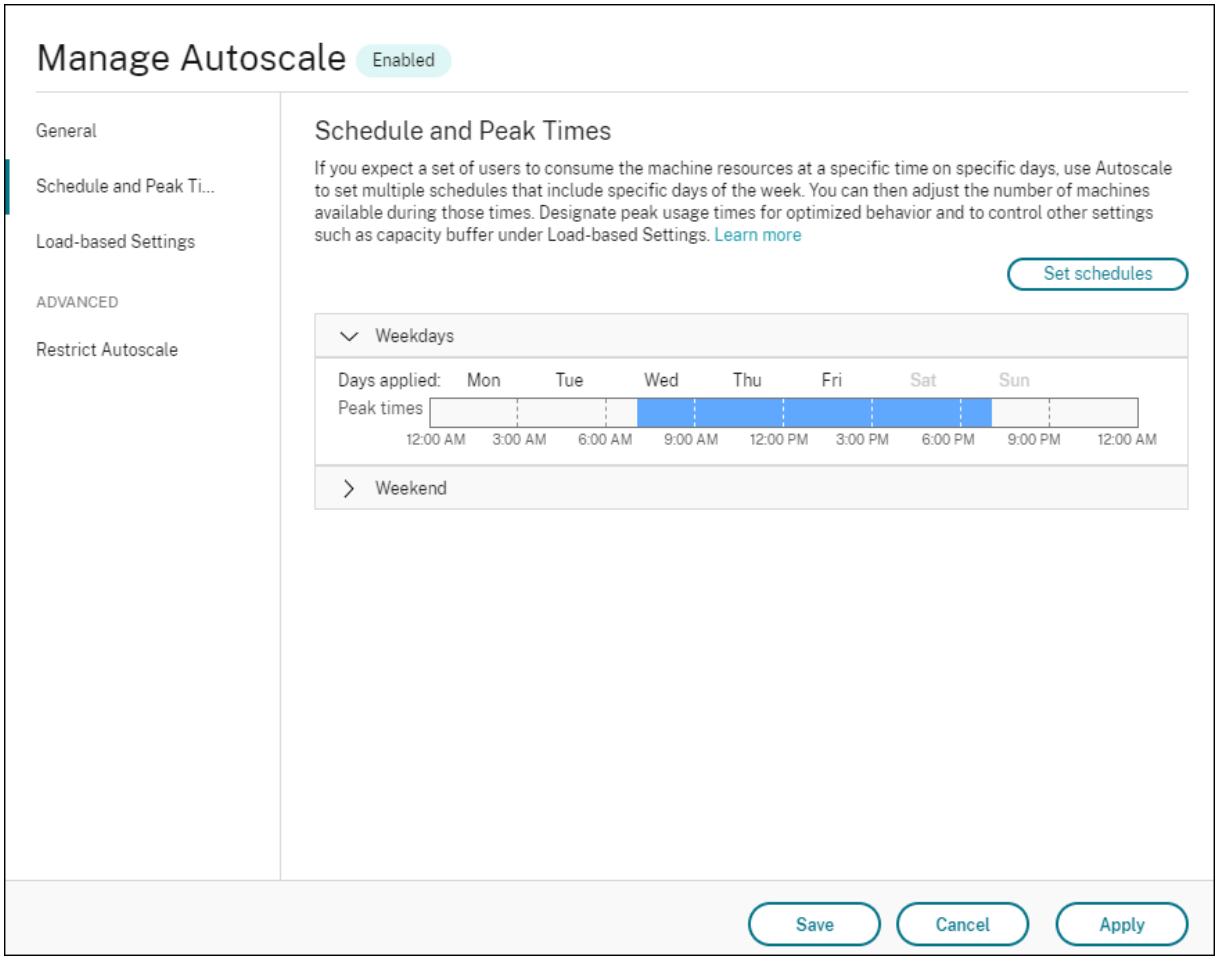
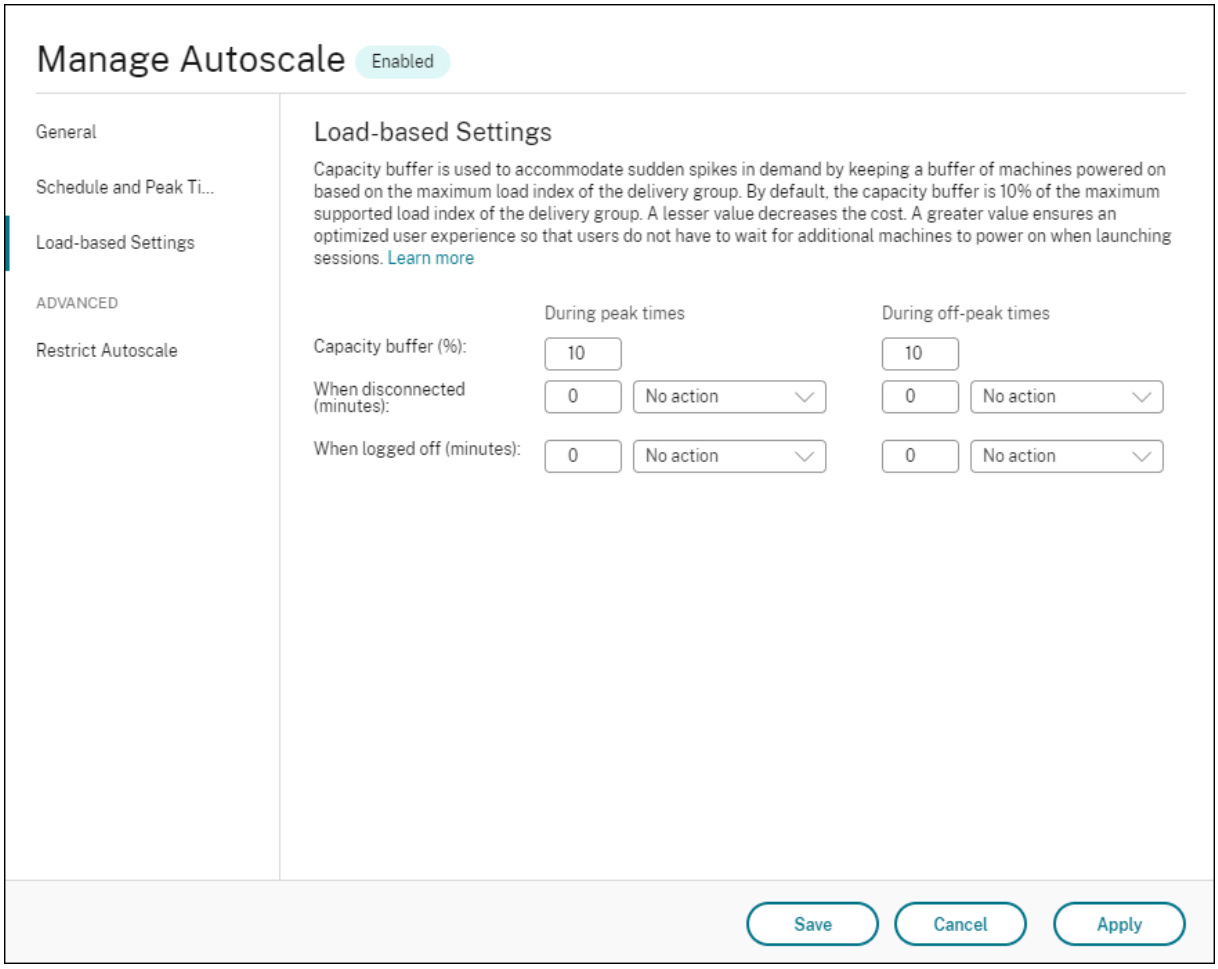
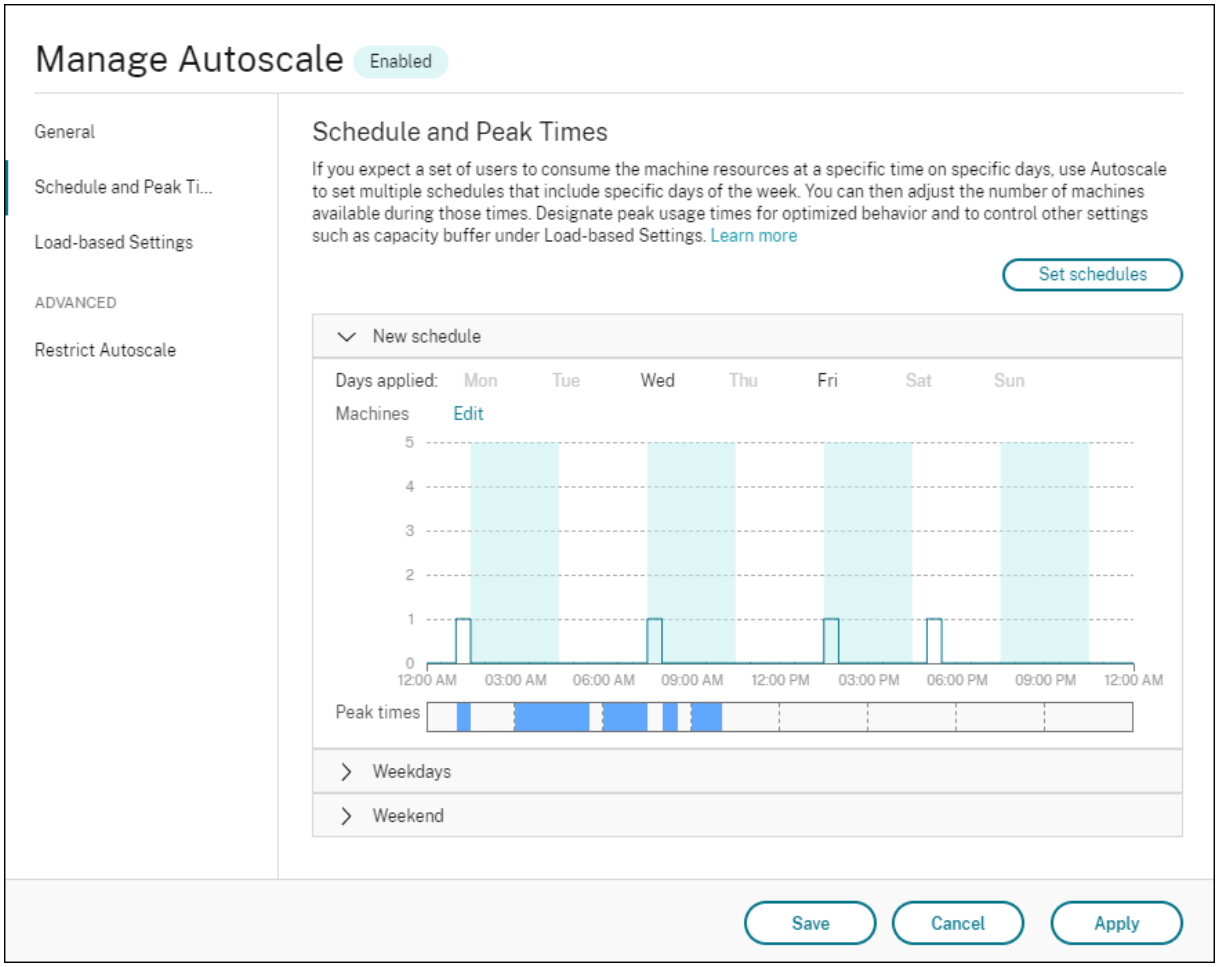
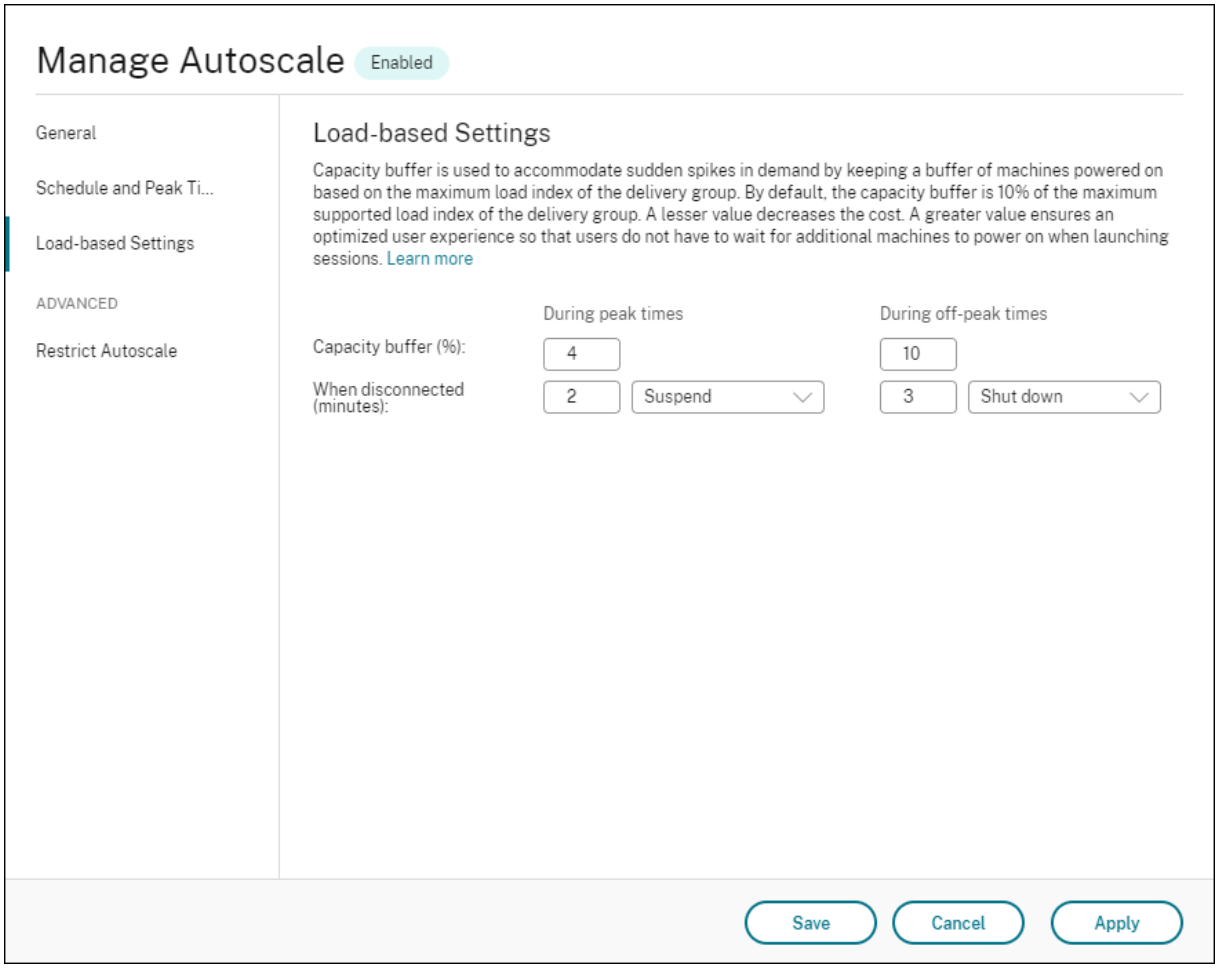
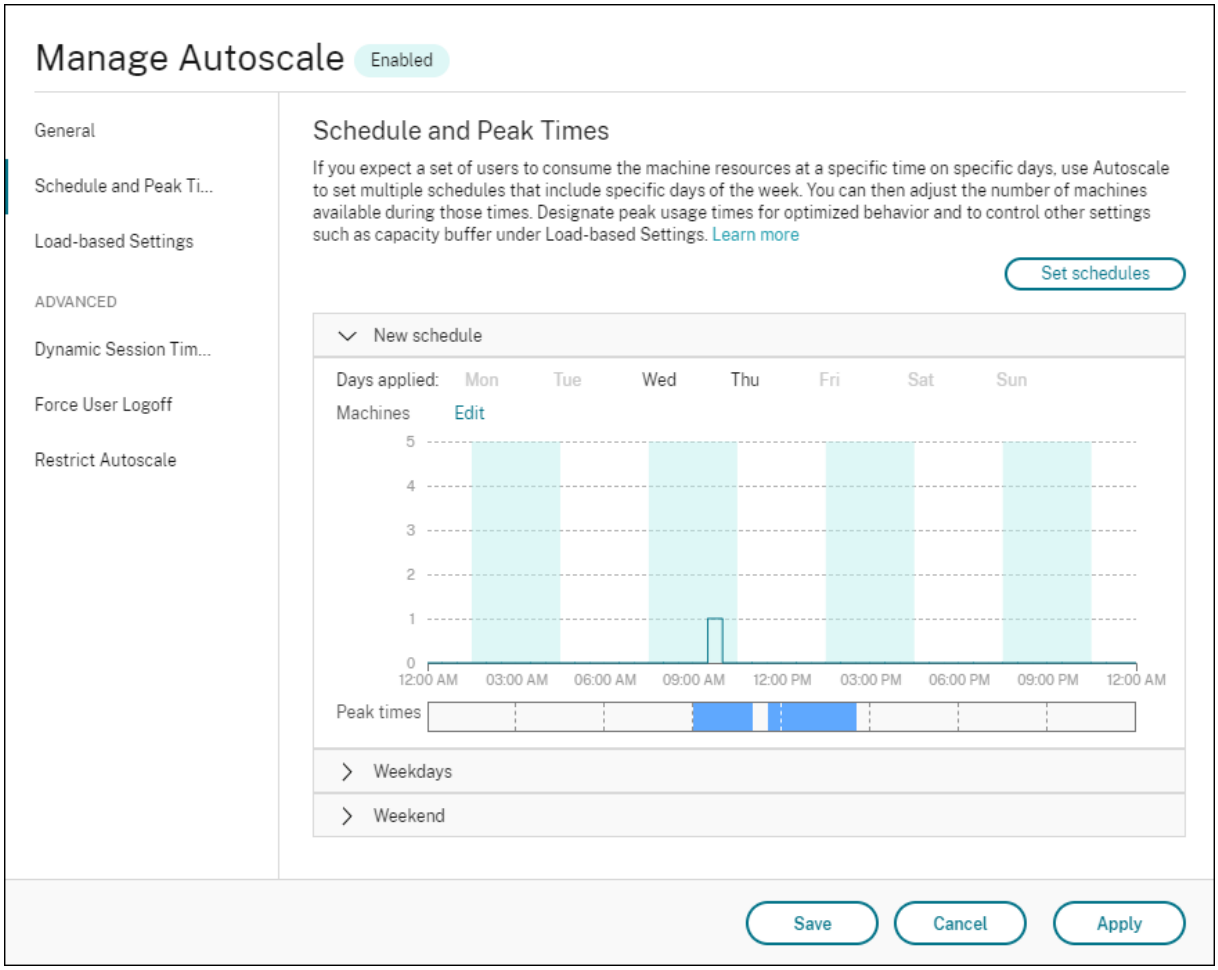
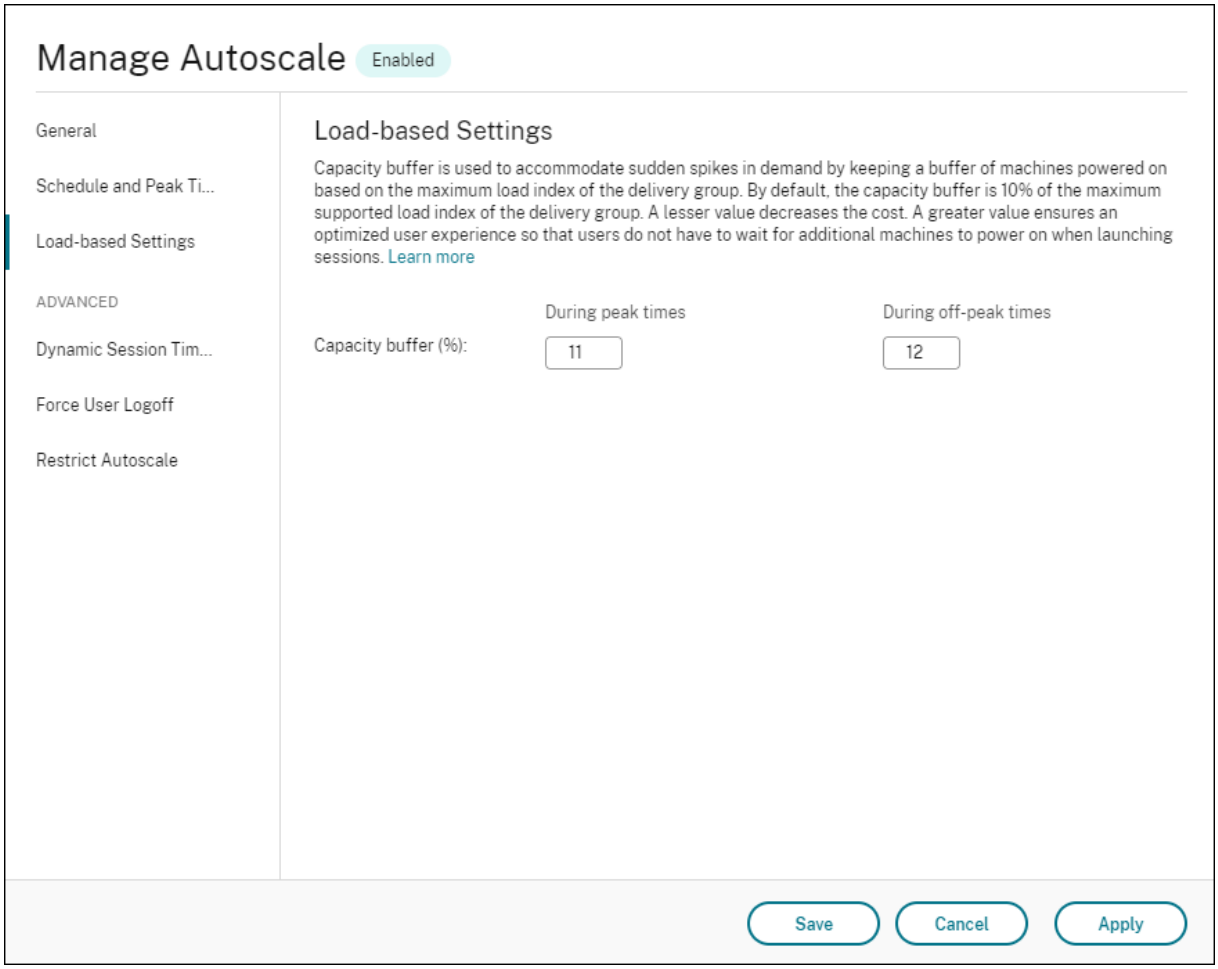
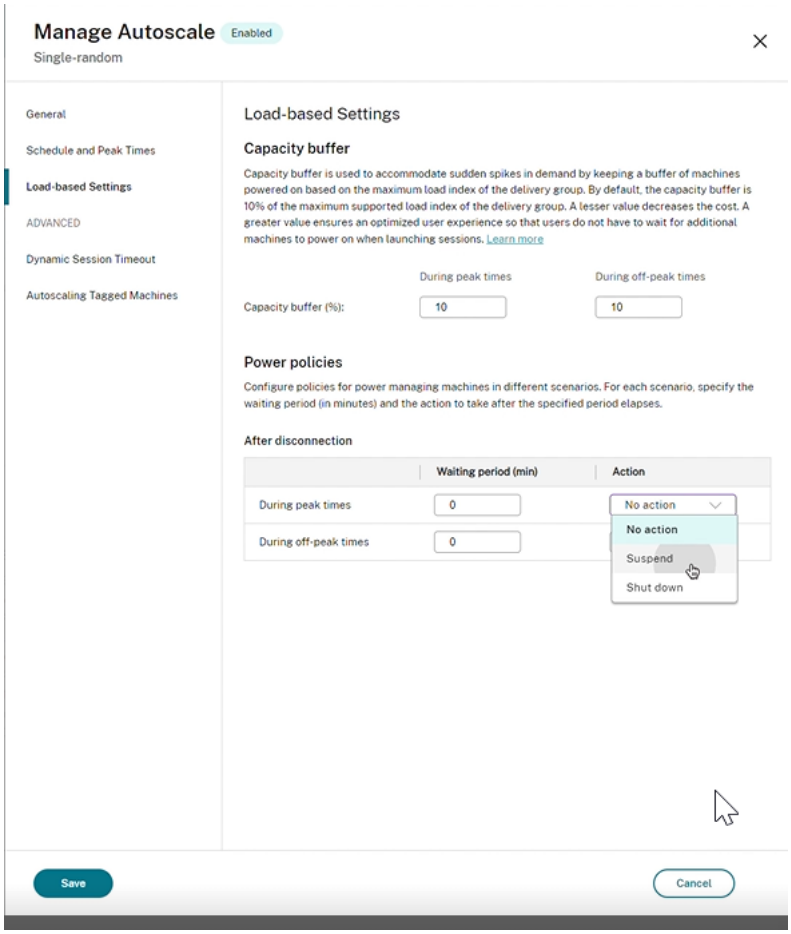
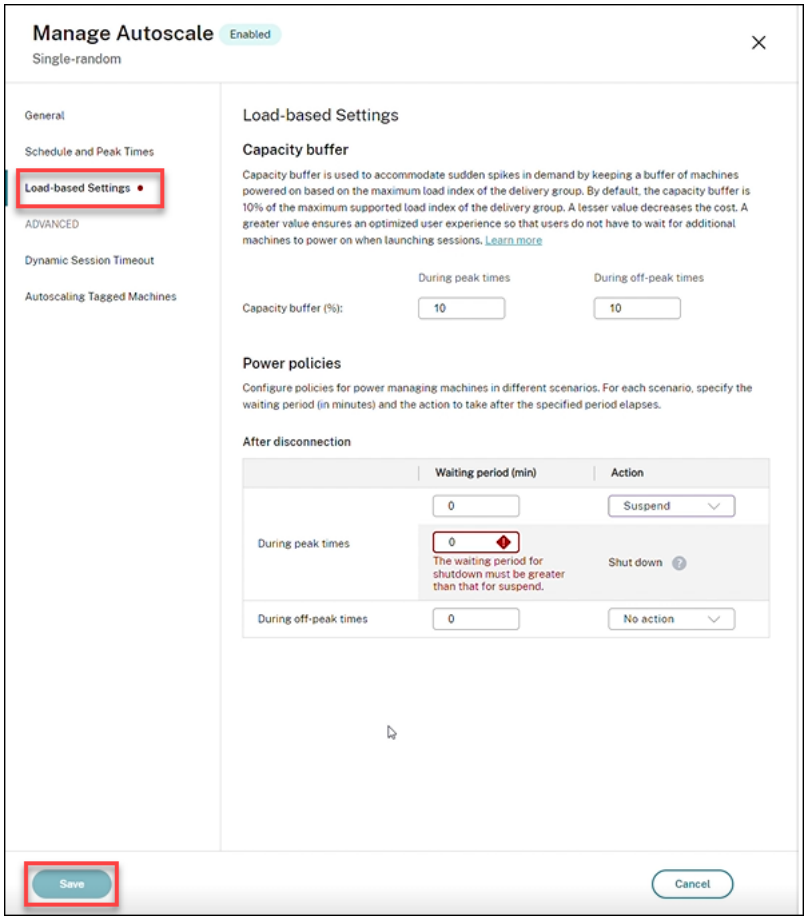
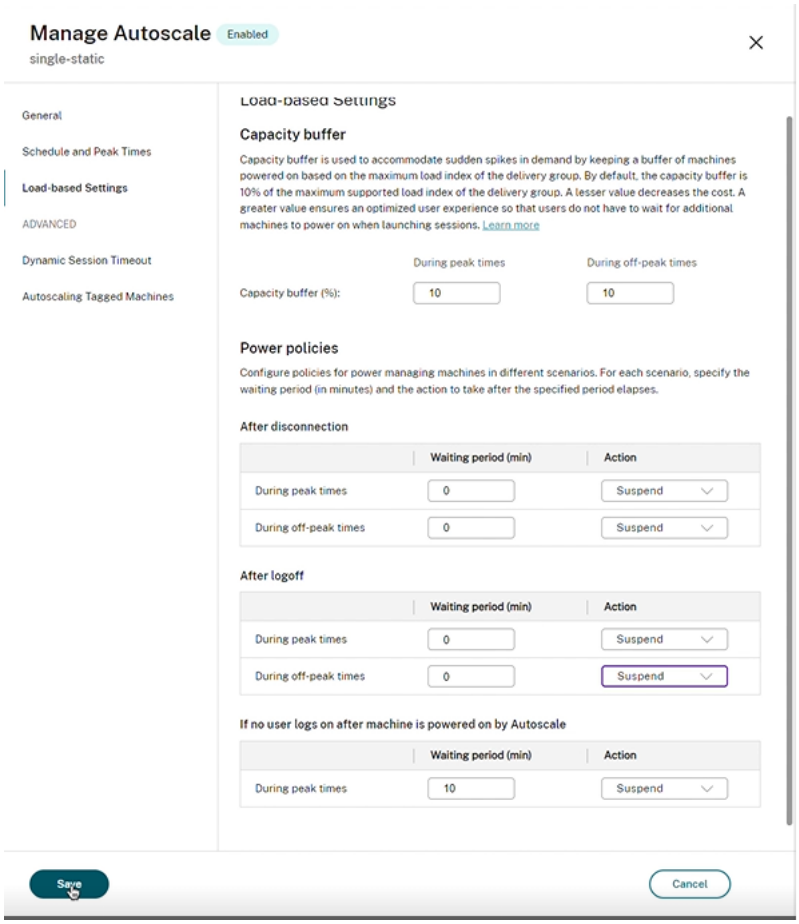
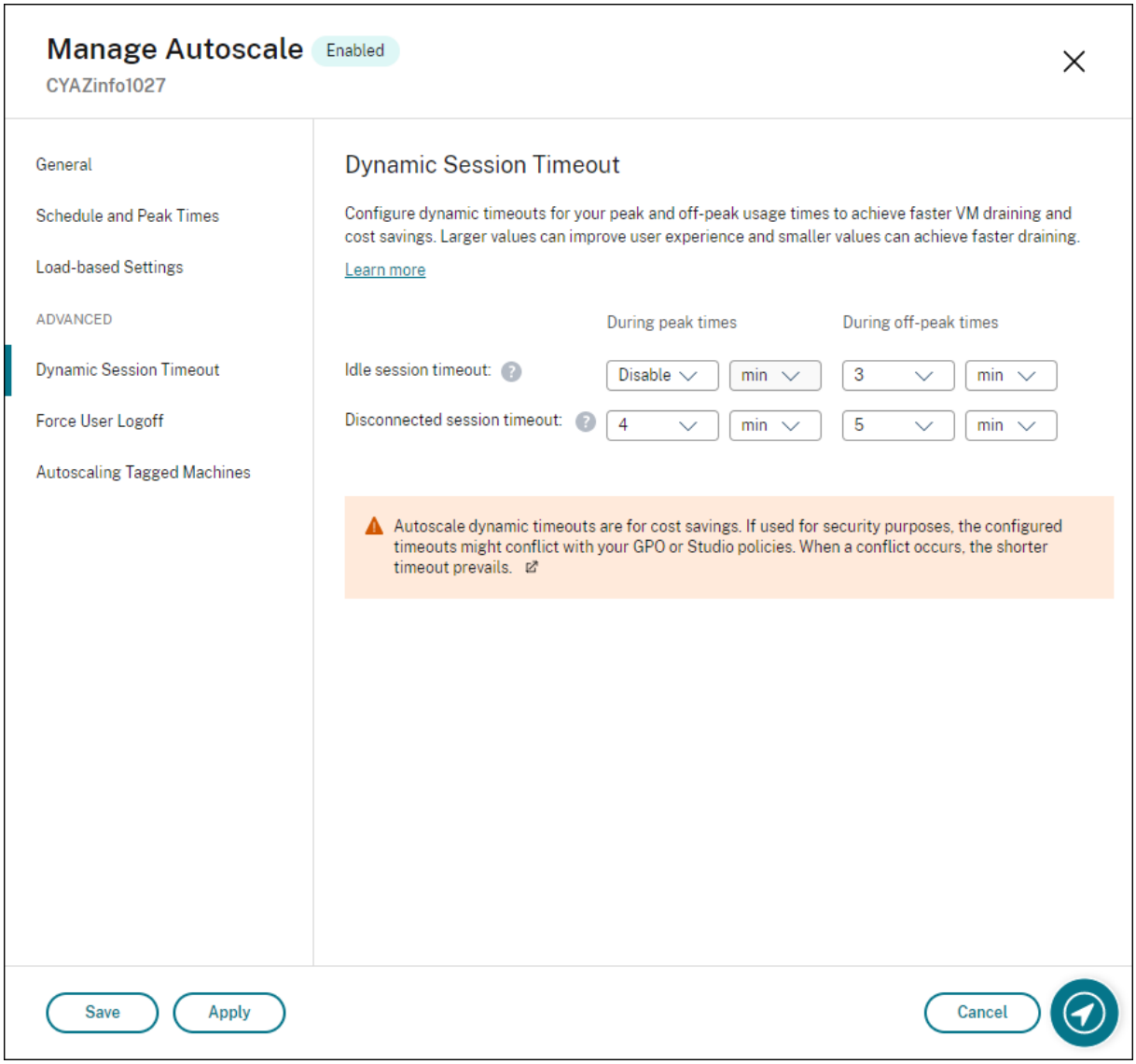
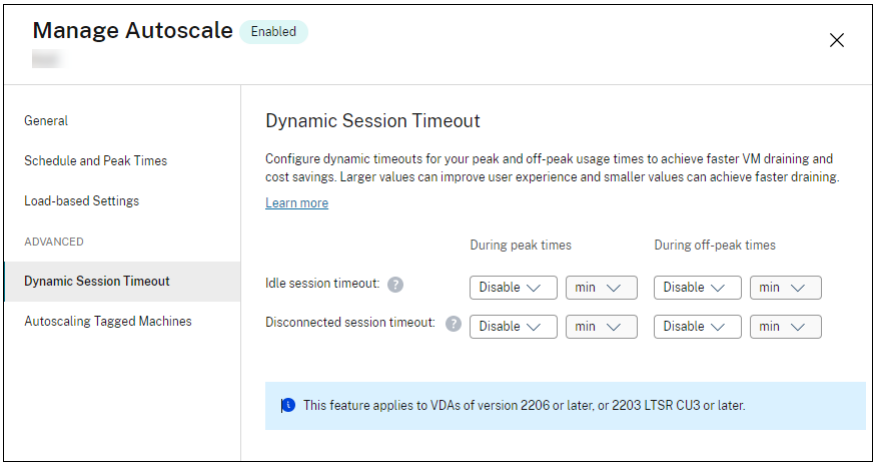
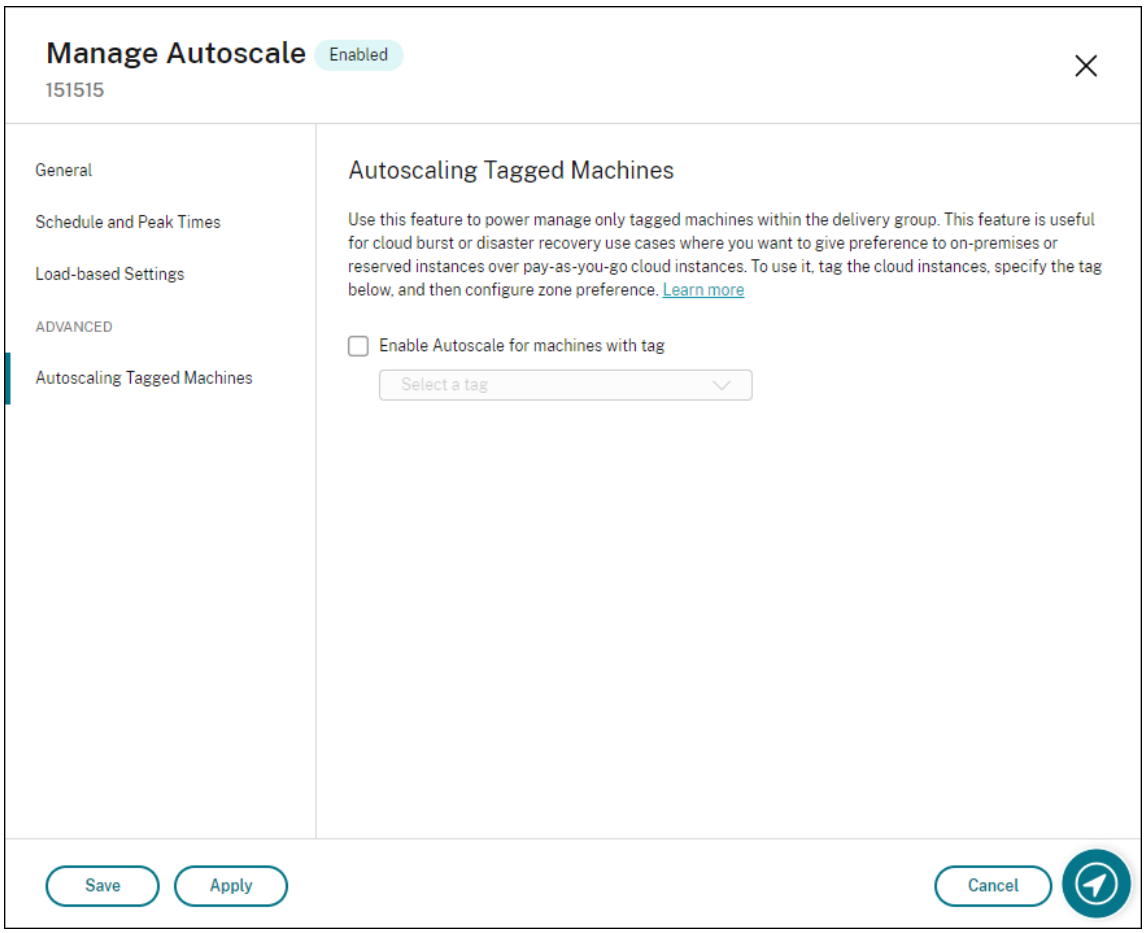
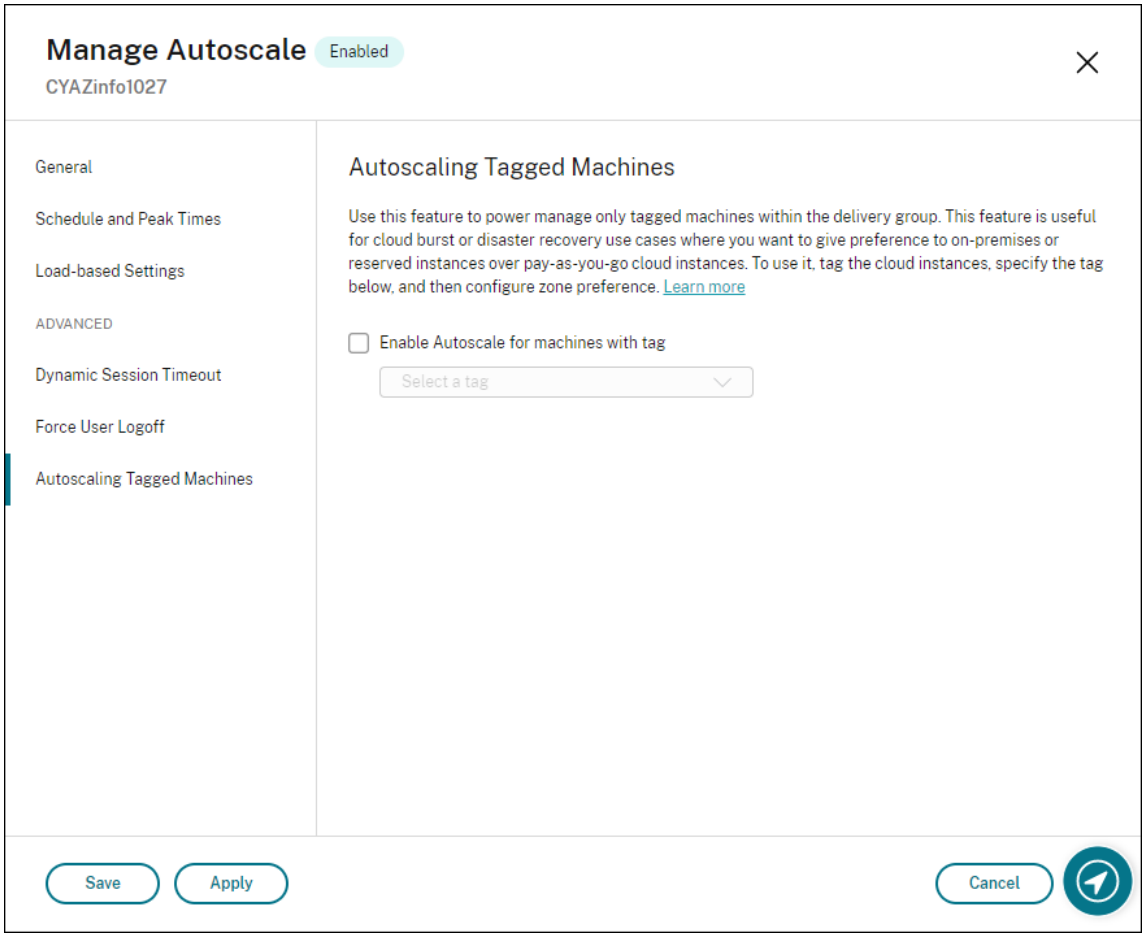
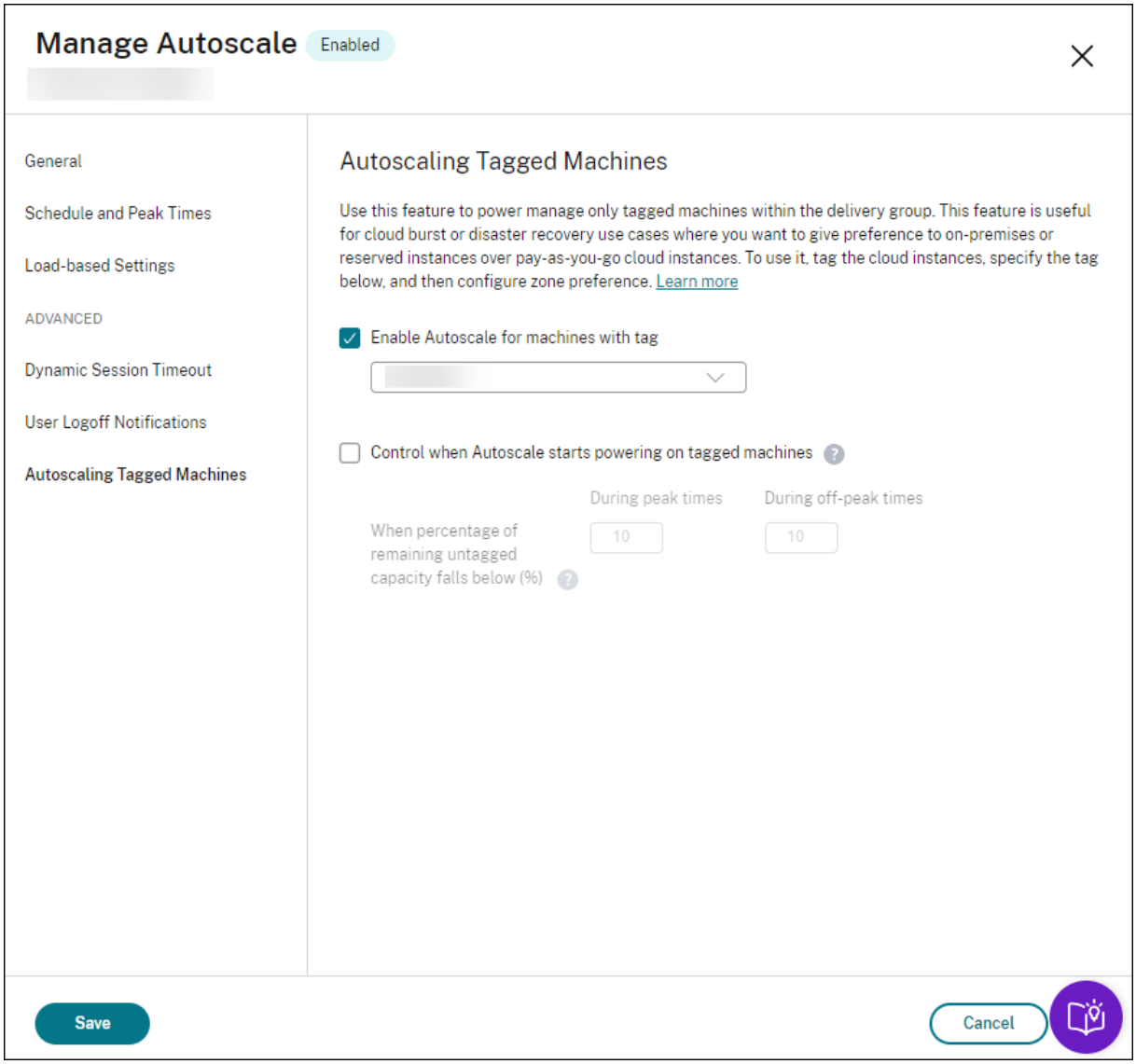
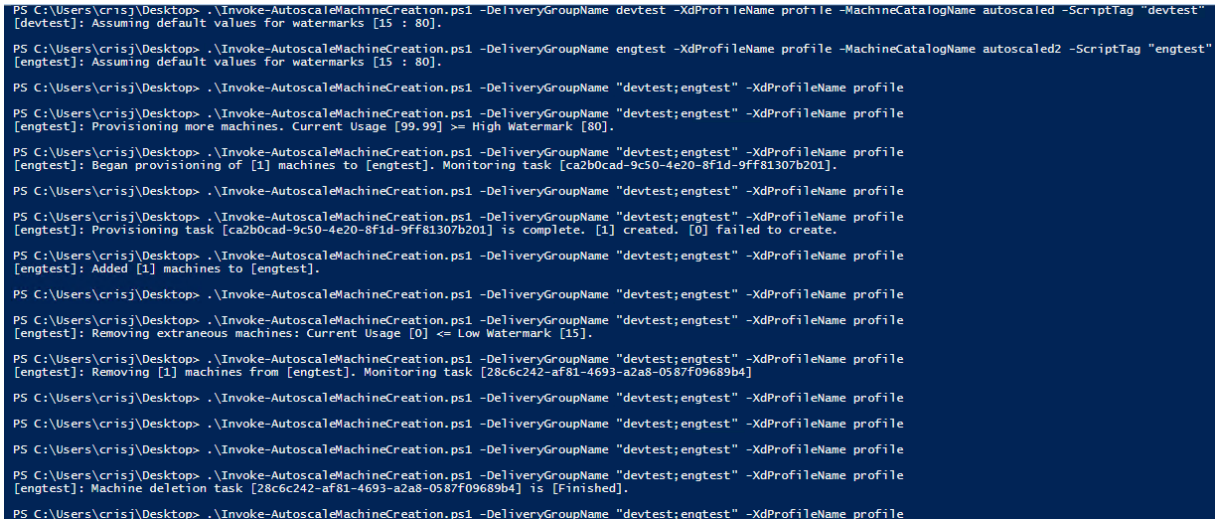
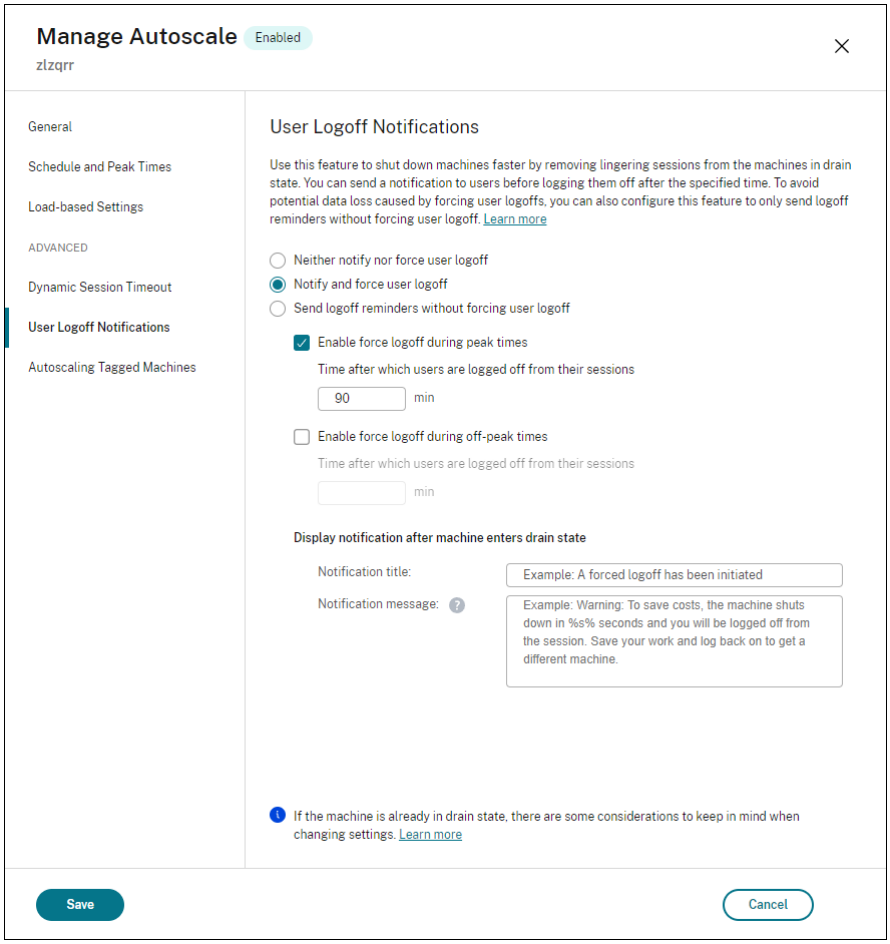
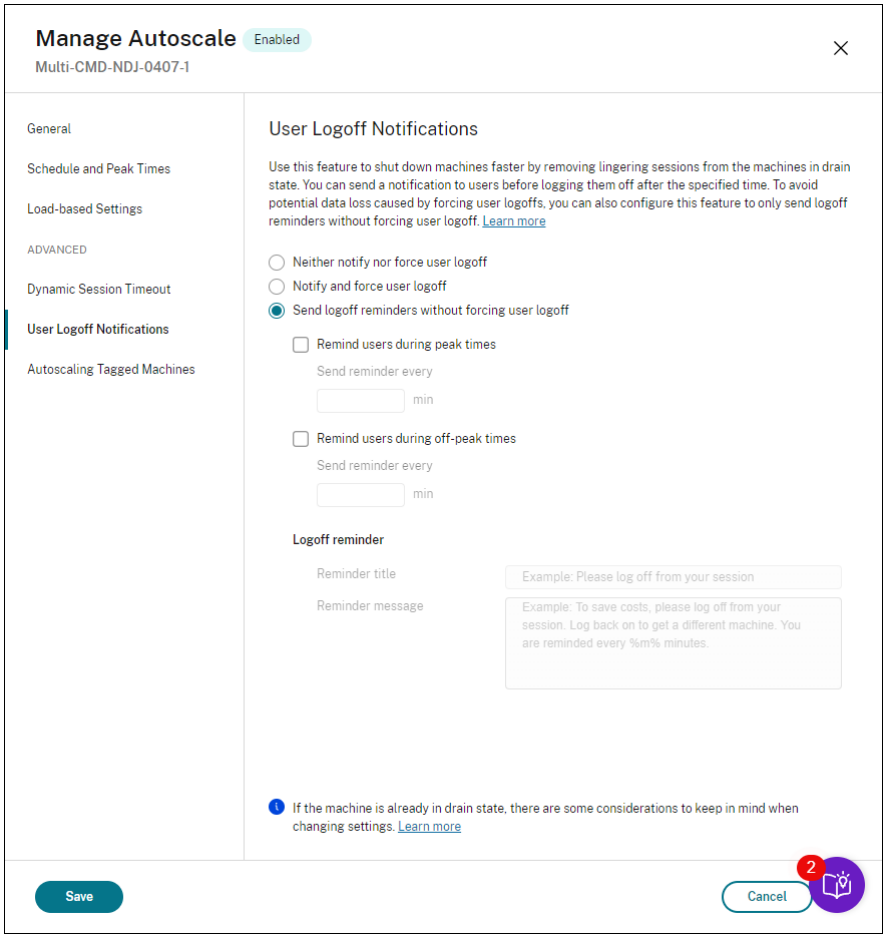
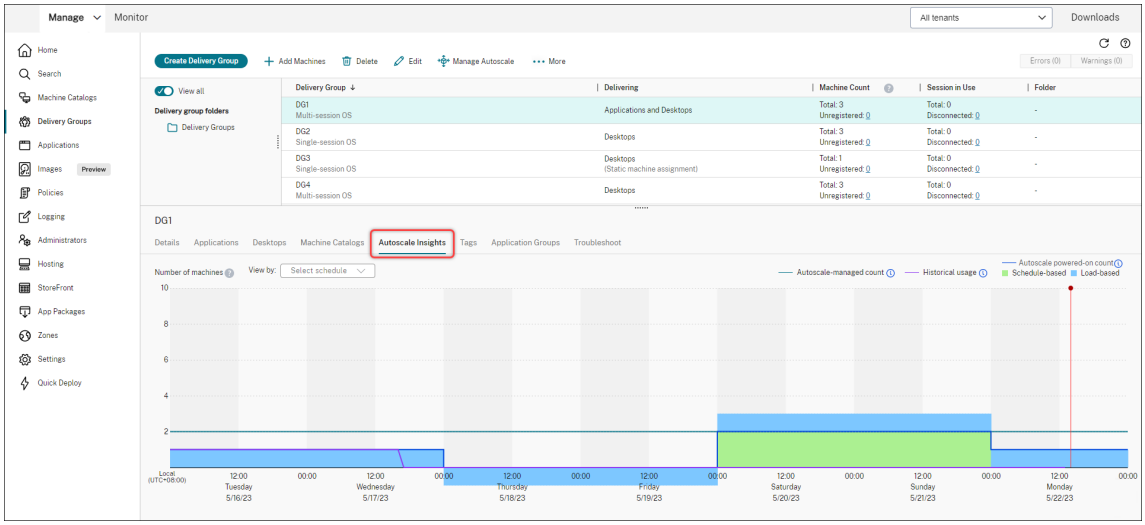
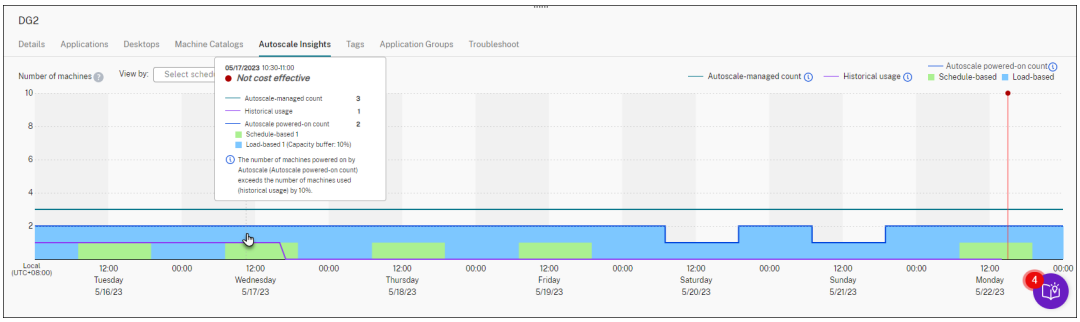
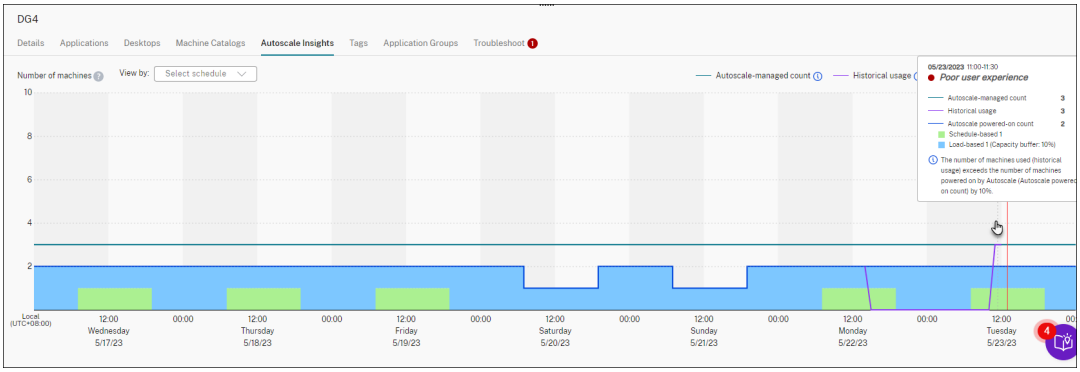
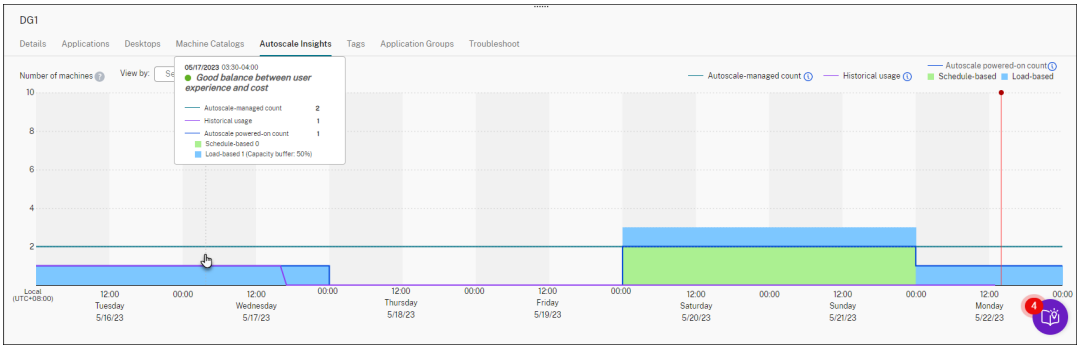
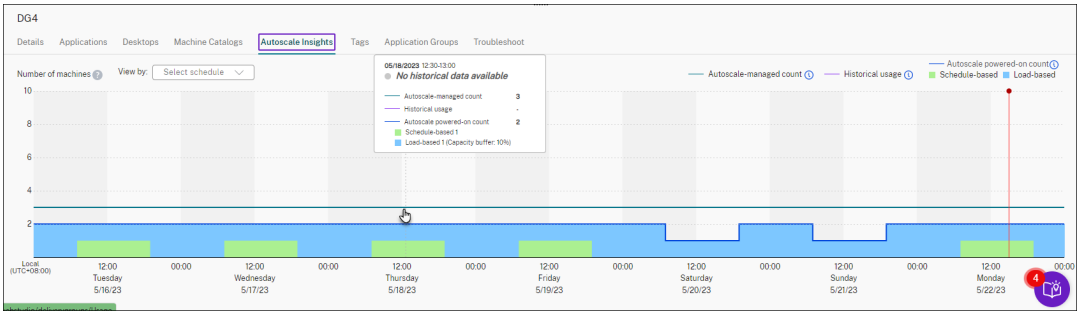
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer

<!--NeedCopy-->
```

If there are multiple ICE candidates, the order of preference is:

1. host
2. peer reflexive
3. server reflexive
4. transport relay

If you encounter an issue and can reproduce it consistently, we recommend that you click **Help > Report a problem** in Teams. Logs are shared between Citrix and Microsoft to resolve technical issues if you opened a case with Microsoft.
Capturing CDF traces before contacting Citrix Support is also beneficial. For more information, see the Knowledge Center article CDFcontrol.

For recommendations for collecting CDF Traces, see the Knowledge Center article Recommendations for Collecting the CDF Traces.

VDA side CDF traces - Enable the following CDF trace providers:



Workspace app side CDF traces - Enable the following CDF trace providers:



- IcaClient_DriversVd_TeamsRedir (optional)
- IcaClient_Multimedia_HdxTeams (requires Citrix Workspace app 2012 or later)

Windows Media redirection

March 23, 2022

Windows Media redirection controls and optimizes the way servers deliver streaming audio and video to users. By playing the media run-time files on the client device rather than the server, Windows Media redirection reduces the bandwidth requirements for playing multimedia files. Windows Media redirection improves the performance of Windows Media Player and compatible players running on virtual Windows desktops.

If the requirements for Windows Media client-side content fetching are not met, media delivery automatically uses server-side fetching. This method is transparent to users. You can use the Citrix Scout to perform a Citrix Diagnosis Facility (CDF) trace from HostMMTransport.dll to determine the method used. For more information see, Citrix Scout.

Windows Media redirection intercepts the media pipeline at the host server, captures the media data in its native compressed format, and redirects the content to the client device. The client device then recreates the media pipeline to decompress and render the media data received from the host server. Windows Media redirection works well on client devices running a Windows operating system. Those devices have the multimedia framework required to rebuild the media pipeline as it existed on the host server. Linux clients use similar open-source media frameworks to rebuild the media pipeline.

The policy setting **Windows Media Redirection** controls this feature and is **Allowed** by default. Usually, this setting increases audio and video quality rendered from the server to a level that is comparable to content played locally on a client device. In the rare cases, media playing using Windows Media redirection appears worse than media rendered using basic ICA compression and regular audio. You can disable this feature by adding the **Windows Media Redirection** setting to a policy and setting its value to **Prohibited**.

For more information about the policy settings, see Multimedia policy settings.

Limitation:

When you're using Windows Media Player and Remote Audio & Video Extensions (RAVE) enabled inside a session, a black screen might appear. This black screen might appear if you right-click on the video content and select **Always show Now Playing on top**.

General content redirection

March 18, 2022

Content redirection allows you to control whether users access information by using applications published on servers or by using applications running locally on user devices.

Client folder redirection

Client folder redirection changes the way client-side files are accessible on the host-side session.

- When you enable only client drive mapping on the server, client-side full volumes are automatically mapped to the sessions as Universal Naming Convention (UNC) links.
- When you enable client folder redirection on the server and the user configures it on the Windows desktop device, the portion of the local volume specified by the user is redirected.

Host to client redirection

Consider using host to client redirection for specific uncommon use cases. Normally, other forms of content redirection might be better. We support this type of redirection only on Multi-session OS VDAs and not on Single-session OS VDAs.

Local App Access and URL redirection

Local App Access seamlessly integrates locally installed Windows applications in to a hosted desktop environment. It does so without changing from one computer to another.

HDX technology provides **generic USB redirection** for specialty devices that don't have any optimized support or where it is unsuitable.

Client folder redirection

March 23, 2022

Client folder redirection changes the way client-side files are accessible on the host-side session. If you enable only client drive mapping on the server, client-side full volumes are automatically mapped as Universal Naming Convention (UNC) links to the sessions. When you enable client folder redirection on the server and the user configures it on the user device, the portion of the local volume specified by the user is redirected.

Only the user-specified folders appear as UNC links inside sessions. That is, instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session.

Client folder redirection is supported on Windows Single-session OS machines only.

Client folder redirection for an external USB drive is not saved on detaching and reattaching the device.

Enable client folder direction on the server. Then, on the client device, specify which folders to redirect. The application you use to specify the client folder options is included with the Citrix Workspace app supplied with this release.

Requirements:

For servers:

- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions

For clients:

- Windows 10, 32-bit and 64-bit editions (minimum version 1607)
- Windows 8.1, 32-bit and 64-bit editions (including Embedded edition)
- Windows 7, 32-bit and 64-bit editions (including Embedded edition)

To enable client folder redirection on the server, see Client folder redirection in the list of features managed through the registry.

On the user device, specify which folders to redirect:

1. Ensure that the latest version of Citrix Workspace app is installed.
2. From the Citrix Workspace app installation directory, start CtxCFRUI.exe.
3. Choose the **Custom** radio button and add, edit, or remove folders.
4. Disconnect and reconnect your sessions for the setting to take effect.

Bidirectional content redirection configuration

January 25, 2024

Bidirectional content redirection allows URLs to be redirected from client to server or server to client, depending on the configurations. This policy setting replaces the following three settings, which are deprecated:

- Allow bidirectional content redirection
- Allowed URLs to be redirected to VDA
- Allowed URLs to be redirected to Client

It also replaces the following three local GPO settings on Windows clients:

- Bidirectional content redirection
- Bidirectional content redirection overrides
- OAuth redirection

If this setting is configured, it takes precedence over the legacy settings in Studio and on the client. To configure the Bidirectional content redirection policy, do the following:

1. On the Citrix DaaS configuration page, click the **Manage** tab.
2. Click the **Policies** tab.

3. Click **Create Policy**. The **Create Policy** blade opens.
4. Search for `Bidirectional content redirection configuration` in the **Search** field, select the check box and click **Edit**.
5. In the **Edit Setting** blade, set this policy to **Enabled** and click **Manage URLs**.



6. In the **Manage URLs** blade, for **VDA-to-client redirection** specify the following:

   - **URL** (Required): Add the URL that should redirect from the VDA to open on the client. For OAuth redirection, set the authentication scheme and pattern on the client to redirect the session back to the host.
   - **Pattern** (Optional): URL regular expression that, when redirected to the client through VDA-to-Client URL redirection, is tracked as if an OAuth authentication flow has begun, and when the flow completes (detected by the resulting scheme or redirect URL pattern being opened), that resulting URL is redirected back into the Host VDA that initiated that flow.
   - **Scheme** (Optional): If a Scheme is specified, the terminating URL is expected to be of the form: `scheme://<something>`. If Scheme is not specified (empty), then the original resulting URL pattern is extracted from the Pattern via a regular expression capture group (must be specified in the Pattern), and the original URL is rewritten to use a `citrix-oauth-redir://` redirect URL. When the flow completes, the original redirect URL is then redirected back into the Host (VDA). Any OAuth Authorization server, in this case,

must be configured to allow `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` redirect URLs.

> **Note:**
>
> Though both **Pattern** and **Scheme** are optional, if **Pattern** is specified, you must also specify **Scheme**.

7. In the **Manage URLs** blade, for **Client-to-VDA redirection** specify the following:
   - **Type**: Choose **Desktop** or **Application**.
   - **Name**: Provide a name to the type.
   - **URL**: Provide the URL you want to redirect to the source. You can add multiple URLs and delete the ones that are not required
8. Click **Save**. The **Edit Setting** blade displays the number of items configured.
9. Click **Save**. The **Create Policy** blade displays the **Current Value** configured. Click **Next**.
10. In the **Assign Policy To** step, click **Next**.
11. In the **Summary** step, select the **Enable policy** check box and provide a name in the **Policy name** field.
12. Click **Finish**. The new policy is listed.
13. Select the new policy created to review the settings configured.

For legacy settings see Host-to-client redirection and Bidirectional content redirection.

Host-to-client redirection

January 25, 2024

> **Note:**
>
> This article describes the legacy host-to-client redirection settings. For the latest settings, see Bidirectional content redirection configuration. The new policy settings will take precedence over the legacy settings. Citrix recommends using only the new policy settings and deleting any legacy settings to avoid unexpected behavior.

Host-to-client redirection allows URLs, embedded as hyperlinks in applications running on a Citrix session, to open using the corresponding application on the user endpoint device. Some common use cases for host-to-client redirection include:

- Redirection of websites in cases where the Citrix server doesn't have Internet or network access to the source.
- Redirection of websites when running a web browser inside the Citrix session is not desired for security, performance, compatibility, or scalability reasons.
- Redirection of specific URL types in cases where the required applications to open the URL are not installed on the Citrix server.

Host-to-client redirection is not intended for URLs that you access on a webpage or type in the address bar of the web browser running in the Citrix session. For redirection of URLs in web browsers, see Bidirectional URL redirection or Browser content redirection.

System requirements

- Multi-session OS VDA
- Supported clients:
  - Citrix Workspace app for Windows
  - Citrix Workspace app for Mac
  - Citrix Workspace app for Linux
  - Citrix Workspace app for HTML5
  - Citrix Workspace app for Chrome

The client device must have an application installed and configured for handling the redirection of the URL types.

Configuration

Use the Host-to-client redirection Citrix policy to enable this functionality. **Host to client redirection** is disabled by default. After you enable the Host-to-client redirection policy, the Citrix Launcher application registers with the Windows server to ensure that it can intercept URLs and send them to the client device.

Then you must configure the Windows Group Policy to use Citrix Launcher as the default application for the required URL types. On the Citrix server VDA, create the ServerFTAdefaultPolicy.xml file and insert the following XML code.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

```



```
<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>
<!--NeedCopy-->
```

From the Group Policy management console, go to **Computer configuration > Administrative Templates > Windows Components > File Explorer > Set a default associations configuration file**, and save your ServerFTAdefaultPolicy.xml file.

> **Note:**
>
> If a Citrix server doesn't have the Group Policy settings, Windows prompts users to select an application for opening URLs.

By default, we support redirection of the following URL types:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

To include additional standard or custom URL types on the list for redirection, create a new **Association Identifier** line in the ServerFTAdefaultPolicy.xml file referenced earlier. For example:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>
```

```
<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

Adding URL types to the list also requires client configuration. Create the following registry key and values on the Windows client.

> **Note:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use

> of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Value name: ExtraURLProtocols
- Value type: REG_SZ
- Value data: Specify the required URL types separated by semicolon. Include everything before the authority portion of the URL. For example:
  `ftp://;mailto:;customtype1:///;custometype2://`

You can add URL types only for Windows clients. Clients missing the registry settings above reject redirection back to the Citrix session. Client must have an application installed and configured to handle the specified URL types.

To remove URL types from the default redirection list, create the following registry key and values on the server VDA.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Value name: DisableServerFTA
- Value type: DWORD
- Value data: 1
- Value name: NoRedirectClasses
- Value type: REG_MULTI_SZ
- Value data: Specify any combination of the values: `http`, `https`, `rtsp`, `rtspu`, `pnm`, or `mms`. Type multiple values on separate lines. For example:

```
http
https
rtsp
```

To enable host-to-client redirection for a specific set of websites, create a registry key and values on the server VDA.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Value name: ValidSites
- Value type: REG_MULTI_SZ
- Value data: Specify any combination of fully qualified domain names (FQDNs). Type multiple FQDNs on separate lines. Include the FQDN only, without protocols (`http://` or `https://`). An FQDN can include an asterisk (*) as a wildcard character in the leftmost position only. This wildcard matches a single level of domain, which is consistent with the rules in RFC 6125. For example:

`www.exmaple.com`

`*.example.com`

> **Note:**
>
> You cannot use the **ValidSites** key in combination with the **DisableServerFTA** and **NoRedirectClasses** keys.

Server VDA default browser configuration

Enabling host-to-client redirection as referenced in this section supersedes any previous default browser configuration on the server VDA. If a web URL is not redirected, the Citrix Launcher passes the URL to the browser configured in the `command_backup` registry key. The key points to Internet Explorer by default, but you can modify it to include the path to a different browser. For more information, see Server VDA default browser configuration in the list of features managed through the registry.

Bidirectional content redirection

January 25, 2024

> **Note:**
>
> This article describes the legacy bidirectional content redirection settings. For the latest policy settings, see Bidirectional content redirection configuration. The new policy settings will take precedence over the legacy settings. Citrix recommends using only the new policy settings and deleting any legacy settings to avoid unexpected behavior.

Bidirectional content redirection allows HTTP or HTTPS URLs in web browsers, or embedded into applications, to be forwarded between the Citrix VDA session and the client endpoint in both directions. A URL entered in a browser running in the Citrix session can be opened using the client's default browser. Conversely, a URL entered in a browser running on the client can be opened in a Citrix session, either with a published application or desktop. Some common use cases for bidirectional content redirection include:

- Redirection of web URLs in cases where the starting browser does not have network access to the source.
- Redirection of web URLs for browser compatibility and security reasons.
- Redirection of web URLs embedded in applications when running a web browser on the Citrix session or the client isn't wanted.

System requirements

- Single-session or multi-session OS VDAs
- Citrix Workspace app for Windows

Browsers:

- Google Chrome with Citrix Browser Redirection Extension (available on the Google Chrome Web Store)
- Microsoft Edge (Chromium) with Citrix Browser Redirection Extension (available on the Google Chrome Web Store)

Configuration

Bidirectional content redirection must be enabled using the Citrix policy on both the VDA and client for redirection to work. Bidirectional content redirection is disabled by default.

For VDA configuration, see Bidirectional content redirection in the ICA policy settings.

For client configuration, see Bidirectional content redirection in the Citrix Workspace app for Windows documentation.

Browser extensions must be registered using the commands shown. Run the commands as needed on the VDA and client based on the browser in use.

To register the browser extensions on the VDA, open a command prompt. Then, run `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` with the required browser option as shown in the examples shown:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

To register the extension on all available browsers run:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

To unregister a browser extension use the `/unreg<browser>` option as in the example shown:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

To register the browser extensions on the client open a command prompt and run `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` with the same options as the examples shown.

> **Note:**
>
> The register command causes Chrome and Edge browsers to prompt users to enable the Citrix Browser Redirection Extension during first launch. The browser extension can also be installed manually from the Google Chrome Web Store.

Wildcard redirection from Citrix VDA to client

Bidirectional content redirection supports the use of wildcards when defining the URLs to be redirected. To configure bidirectional content redirection, see the configuration instructions.

In Citrix Studio, set the wildcard URL in **Allowed URLs to be redirected to Client**. The asterisk (*) is the wildcard character.

> **NOTE:**
>
> - Don't set the **Allowed URLs to be redirected to VDA** in the client policy. Ensure that the sites set the **Allowed URLs to be redirected to VDA** to avoid infinite redirection loops.
> - Top-level domains are not supported. For example, `https://www.citrix.*` or `http://www.citrix.co*` is not redirected.

Custom protocol redirection from VDA to client

Bidirectional content redirection supports redirecting custom protocols from the Citrix VDA to the client. Protocols other than HTTP or HTTPS are supported. To configure bidirectional content redirection, see the configuration instructions.

In Citrix Studio, set the custom protocol in **Allowed URLs to be redirected to Client**.

> **NOTE:**
>
> - The client must have an application registered to handle the protocol. Otherwise, the URL redirects to the client and fails to launch.
> - Custom protocol URLs that you enter or launch in the Chrome and Edge browsers are not supported and not redirected.
> - The following protocols are not supported: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

Other considerations

- Browser requirements and configurations are only applicable to the browser starting the redirection. The destination browser, where the URL opens after redirection is successful, isn't con-

sidered for support. When redirecting URLs from the VDA to a client, a supported browser configuration is only required on the VDA. Conversely, when redirecting URLs from the client to a VDA, a supported browser configuration is only required on the client. Redirected URLs are handed off to the default browser configured on the destination machine, either the client or the VDA, depending on direction. Using the same browser type on the VDA and the client is NOT required.

- Check that redirection rules do not result in a looping configuration. For example, a VDA policy is set to redirect `https://www.citrix.com`, and the client policy is set to redirect the same URL, resulting in infinite looping.
- Only HTTP/HTTPS protocol URLs are supported. URL shorteners aren't supported.
- Client to VDA redirection requires the Windows client to be installed with administrator rights.
- If the destination browser is already open, the redirected URL opens in a new tab. Otherwise the URL opens in a new browser window.
- Bidirectional content redirection does not work when Local App Access (LAA) is enabled.

Local App Access and URL redirection

June 8, 2022

Introduction

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without switching from one desktop to another. With Local App Access, you can:

- Access applications installed locally on a physical laptop, PC, or other device directly from the virtual desktop.
- Provide a flexible application delivery solution. If users have local applications that you cannot virtualize or that IT does not maintain, those applications still behave as though they are installed on a virtual desktop.
- Eliminate the double-hop latency when applications are hosted separately from the virtual desktop. Do so by putting a shortcut to the published application on the user's Windows device.
- Use applications such as:
  - Video conferencing software such as GoToMeeting.
  - Specialty or niche applications that are not yet virtualized.
  - Applications and peripherals that would otherwise transfer large amounts of data from a user device to a server and back to the user device. For example, DVD burners and TV tuners.

In Citrix Virtual Apps and Desktops, hosted desktop sessions use URL redirection to start Local App Access applications. URL redirection makes the application available under more than one URL address. It launches a local browser (based on the browser's URL block list) by selecting embedded links within a browser in a desktop session. If you navigate to a URL that is not present in the block list, the URL is opened in the desktop session again.

URL redirection works only for desktop sessions, not application sessions. The only redirection feature you can use for application sessions is host-to-client content redirection, which is a type of server FTA (File Type Association) redirection. This FTA redirects certain protocols to the client, such as HTTP, HTTPS, RTSP, or MMS. For example, if you only open embedded links with HTTP, the links directly open with the client application. There is no URL block list or allow list support.

When Local App Access is enabled, URLs that are displayed to users as links from locally running applications, from user-hosted applications, or as shortcuts on the desktop are redirected in one of the following ways:

- From the user's computer to the hosted desktop
- From the Citrix Virtual Apps and Desktops server to the user's computer
- Rendered in the environment in which they are started (not redirected)

To specify the redirection path of content from specific websites, configure the URL allow list and URL block list on the Virtual Delivery Agent. Those lists contain multi-string registry keys that specify the URL redirection policy settings. For more information, see the Local App Access policy settings.

URLs can be rendered on the VDA with the following exceptions:

- Geo/Locale information —Websites that require locale information, such as msn.com or news.google.com (opens a country specific page based on the Geo). For example, if the VDA is provisioned from a data center in the UK and the client is connecting from India, the user expects to see in.msn.com. Instead, the user sees uk.msn.com.
- Multimedia content —Websites containing rich media content, when rendered on the client device, give the end users a native experience and also save bandwidth even in high latency networks. This feature redirects sites with other media types such as Silverlight. This process is in a secure environment. That is, the URLs that the administrator approves are run on the client while the rest of the URLs are redirected to the VDA.

In addition to URL redirection, you can use FTA redirection. FTA starts local applications when a file is encountered in the session. If the local app is started, the local app must have access to the file to open it. Therefore, you can only open files that reside on network shares or on client drives (using client drive mapping) using local applications. For example, when opening a PDF file, if a PDF reader is a local app, then the file opens using that PDF reader. Because the local app can access the file directly, there is no network transfer of the file through ICA to open the file.

Requirements, considerations, and limitations

We support Local App Access on the valid operating systems for VDAs for Windows Multi-session OS and for VDAs for Windows Single-session OS. Local App Access requires Citrix Workspace app for Windows version 4.1 (minimum). The following browsers are supported:

- Edge, latest version
- Firefox, latest version and extended support release
- Chrome, latest version

Review the following considerations and limitations when using Local App Access and URL redirection.

- Local App Access is designed for full-screen, virtual desktops spanning all monitors:
  - The user experience can be confusing if you use Local App Access with a virtual desktop that runs in windowed mode or does not cover all monitors.
  - Multiple monitors —When one monitor is maximized, it becomes the default desktop for all applications started in that session. This default occurs even if the subsequent applications typically start on another monitor.
  - The feature supports one VDA. There is no integration with multiple concurrent VDAs.
- Some applications can behave unexpectedly, affecting users:
  - The drive letters might confuse users, such as local C: rather than virtual desktop C: drive.
  - Available printers in the virtual desktop are not available to local applications.
  - Applications that require elevated permissions cannot be started as client-hosted applications.
  - There is no special handling for single-instance applications (such as Windows Media Player).
  - Local applications appear with the Windows theme of the local machine.
  - Full-screen applications are not supported. These applications include applications that open to a full screen, such as PowerPoint slide shows or photo viewers that cover the entire desktop.
  - Local App Access copies the properties of the local application (such as the shortcuts on the client's desktop and Start menu) on the VDA. However, it does not copy other properties such as shortcut keys and read-only attributes.
  - Applications that customize how overlapping window order is handled can have unpredictable results. For example, some windows might be hidden.
  - Shortcuts are not supported, including My Computer, Recycle Bin, Control Panel, Network Drive shortcuts, and folder shortcuts.
  - The following file types and files are not supported: custom file types, files with no associated programs, zip files, and hidden files.

  - Taskbar grouping is not supported for mixed 32-bit and 64-bit client-hosted or VDA applications. That is, grouping 32-bit local applications with 64-bit VDA applications.
  - Applications cannot be started using COM. For example, if you click an embedded Office document from within an Office application, the process start cannot be detected, and the local application integration fails.

- Double-hop scenarios, where a user is starting a virtual desktop from within another virtual desktop session, are not supported.
- URL redirection supports only explicit URLs (that is, URLs appearing in the browser's address bar or found using the in-browser navigation, depending on the browser).
- URL redirection works only with desktop sessions, not with application sessions.
- The local desktop folder in a VDA session does not allow users to create files.
- Multiple instances of a locally running application behave according to the taskbar settings established for the virtual desktop. However, shortcuts to locally running applications are not grouped with running instances of those applications. They are also not grouped with running instances of hosted applications or pinned shortcuts to hosted applications. Users can close only windows of locally running applications from the Taskbar. Although users can pin local application windows to the desktop Taskbar and Start menu, the applications might not start consistently when using these shortcuts.
- If you set the **Allow local app access** policy setting to **Enabled**, browser content redirection isn't supported.

Interaction with Windows

The Local App Access interaction with Windows includes the following behaviors.

- Windows 8 and Windows Server 2012 shortcut behavior
  - Windows Store applications installed on the client are not enumerated as part of Local App Access shortcuts.
  - Image and video files are opened by default using Windows store applications. However, Local App Access enumerates the Windows store applications and opens shortcuts with desktop applications.
- Local Programs
  - For Windows 7, the folder is available in the Start menu.
  - For Windows 8, Local Programs is available only when the user chooses **All Apps** as a category from the Start screen. Not all subfolders are displayed in Local Programs.
- Windows 8 graphics features for applications
  - Desktop applications are restricted to the desktop area and are covered by the Start screen and Windows 8 style applications.

  - Local App Access applications do not behave like desktop applications in multi-monitor mode. In multi-monitor mode, the Start screen and the desktop display on different monitors.

- Windows 8 and Local App Access URL Redirection
  - Because Windows 8 Internet Explorer has no add-ons enabled, use desktop Internet Explorer to enable URL redirection.
  - In Windows Server 2012, Internet Explorer disables add-ons by default. To implement URL Redirection, disable the Internet Explorer enhanced configuration. Then reset the Internet Explorer options and restart to ensure that add-ons are enabled for standard users.

Configure Local App Access and URL redirection

To use Local App Access and URL redirection with Citrix Workspace app:

- Install Citrix Workspace app on the local client machine. You can enable both features during the Citrix Workspace app installation or you can enable Local App Access template using the Group Policy editor.
- Set the **Allow local app access** policy setting to **Enabled**. You can also configure URL allow list and block list policy settings for URL redirection. For more information, see Local App Access policy settings.

Enable Local App Access and URL redirection

To enable Local App Access for all local applications, follow these steps:

1. From **Manage > Full Configuration**, select **Policies** in the left pane.
2. Select **Create Policy** in the action bar.
3. In the Create Policy window, type "Allow Local App Access"in the search box and then click **Select**.
4. In the Edit Setting window, select **Allowed**. By default, the **Allow local app access** policy is prohibited. When this setting is allowed, the VDA allows the end-user to decide whether published applications and Local App Access shortcuts are enabled in the session. (When this setting is prohibited, both published applications and Local App Access shortcuts do not work for the VDA.) This policy setting applies to the entire machine and the URL redirection policy.
5. In the Create Policy window, type "URL redirection allow list"in the search box and then click **Select**. The URL redirection allow list specifies URLs to open in the default browser of the remote session.
6. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.

7. In the Create Policy window, type "URL redirection block list"in the search box and then click **Select**. The URL redirection block list specifies URLs that are redirected to the default browser running on the endpoint.
8. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.
9. On the Settings page, click **Next**.
10. On the Users and Machines page, assign the policy to the applicable Delivery Groups and then click **Next**.
11. On the Summary page, review the settings and then click **Finish**.

To enable URL redirection for all local applications during Citrix Workspace app installation, follow the steps below:

1. Enable URL redirection when you install Citrix Workspace app for all users on a machine. Doing so also registers the browser add-ons required for URL redirection.
2. From the command prompt, run the appropriate command to install the Citrix Workspace app using one of the following options:
    - For CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
    - For CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Enable the Local App Access template using the Group Policy editor

> **Note:**
>
> - Before you enable the Local App Access template using the Group Policy editor, add the `receiver.admx/adml` template files to the local GPO. For more information, see Get started and search for *Group Policy Object administrative template*.
> - Citrix Workspace app for Windows template files are available in the local GPO in **Administrative Templates > Citrix Components > Citrix Workspace** folder only when you add the `CitrixBase.admx/CitrixBse.adml` to the %systemroot%\policyDefinitions folder.

To enable the Local App Access template using the Group Policy editor, follow these steps:

1. Run **gpedit.msc**.
2. Go to **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User Experience**.
3. Click **Local App Access settings**.
4. Select **Enabled** and then select **Allow URL Redirection**. For URL redirection, register browser add-ons using the command line described in the *Register browser add-ons* section further down in this article.

Provide access only to published applications

You can provide access to published applications using the Registry Editor or the PowerShell SDK.

To the Registry Editor, see The Local App Access for published applications in the list of features managed through the registry.

To use the PowerShell SDK:

1. Open PowerShell on the machine where the Delivery Controller is running.
2. Enter the following command: `set-configsitemetadata -name "studio_clientHostedApps "-value "true"`.

To have access to **Add Local App Access Application** in a Citrix DaaS deployment, use the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For more information, see Citrix Virtual Apps and Desktops Remote PowerShell SDK.

1. Download the installer:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Run these commands:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Enter the following command: `set-configsitemetadata -name “studio_clientHostedApps ” -value “true”`.

After you complete the applicable preceding steps, follow these steps to continue.

1. From **Manage > Full Configuration**, select **Applications** in the left pane.
2. In the upper middle pane, right-click the blank area and select **Add Local App Access Application** from the menu. You can also click **Add Local App Access Application** in the Actions pane. To display the Add Local App Access Application option in the Actions pane, click **Refresh**.
3. Publish Local App Access application.

   - The Local Application Access wizard launches with an Introduction page, which you can remove from future launches of the wizard.
   - The wizard guides you through the Groups, Location, Identification, Delivery, and Summary pages described below. When you are finished with each page, click **Next** until you reach the Summary page.
   - On the Groups page, select one or more Delivery Groups where the new applications will be added, and then click **Next**.

- On the Location page, type the full executable path of the application on the user's local machine, and type the path to the folder where the application is located. Citrix recommends that you use the system environment variable path; for example, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
- On the Identification page, accept the default values or type the information that you want and then click **Next**.
- On the Delivery page, configure how this application is delivered to users and then click **Next**. You can specify the icon for the selected application. You can also specify whether the shortcut to the local application on the virtual desktop will be visible on the Start menu, the desktop, or both.
- On the Summary page, review the settings and then click **Finish** to exit the Local Application Access wizard.

Register browser add-ons

> **Note:**
>
> The browser add-ons required for URL redirection are registered automatically when you install Citrix Workspace app from the command line using the `/ALLOW_CLIENTHOSTEDAPPSURL=1` option.

You can use the following commands to register and unregister one or all add-ons:

- To register add-ons on a client device: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- To unregister add-ons on a client device: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- To register add-ons on a VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- To unregister add-ons on a VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

Where <*browser*> is Internet Explorer, Firefox, Chrome, or All.

For example, the following command registers Internet Explorer add-ons on a device running Citrix Workspace app.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

The following command registers all add-ons on a Windows Multi-session OS VDA.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

URL interception across browsers

- By default, Internet Explorer redirects the specified URL. If the URL is not in the block list but the browser or website redirects it to another URL, the final URL is not redirected. It is not redirected

even if it is on the block list.

For URL redirection to work correctly, enable the add-on when prompted by the browser. If the add-ons that are using Internet options or the add-ons in the prompt are disabled, URL redirection does not work correctly.

- The Firefox add-ons always redirect the URLs.

When an add-on is installed, Firefox prompts to allow or prevent installing the add-on on a new tab page. Allow the add-on for the feature to work.

- The Chrome add-on always redirects the final URL that is navigated, and not the entered URLs.

The extensions have been installed externally. When you disable the extension, the URL redirection feature does not work in Chrome. If the URL redirection is required in Incognito mode, allow the extension to run in that mode in the browser settings.

Configure local application behavior on logoff and disconnect

> **Note:**
>
> If you do not follow these steps to configure the settings, by default, local applications continue to run when a user logs off or disconnects from the virtual desktop. After reconnection, local applications are reintegrated if they are available on the virtual desktop.

To configure local application behavior on logoff and disconnect, see Local application behavior on logoff and disconnect in the list of features managed through the registry.

Generic USB redirection and client drive considerations

August 3, 2023

HDX technology provides **optimized support** for most popular USB devices. Optimized support offers an improved user experience with better performance and bandwidth efficiency over a WAN. Optimized support is usually the best option, especially in high latency or security-sensitive environments.

HDX technology provides **generic USB redirection** for specialty devices that don't have optimized support or where it is unsuitable, for example:

- The USB device has more advanced features that are not part of optimized support, such as a mouse or webcam having more buttons.

- Users need functions which are not part of optimized support.
- The USB device is a specialized device, such as test and measurement equipment or an industrial controller.
- An application requires direct access to the device as a USB device.
- The USB device only has a Windows driver available. For example, a smart card reader might not have a driver available for Citrix Workspace app for Android.
- The version of Citrix Workspace app does not provide any optimized support for this type of USB device.

With generic USB redirection:

- Users do not need to install device drivers on the user device.
- USB client drivers are installed on the VDA machine.

> **Important:**
>
> - Generic USB redirection can be used together with optimized support. If you enable generic USB redirection, configure Citrix USB devices policy settings for both generic USB redirection and optimized support.
> - The Citrix policy setting in Client USB device optimization rules is a specific setting for generic USB redirection, for a particular USB device. It doesn't apply to optimized support as described here.
> - When brokering a session using Citrix software to an Azure Virtual Machine, Citrix provides best effort support for USB redirection to the Azure Virtual Machine. We support fixing a Citrix software problem, but we do not support the underlying Azure Virtual Machine.
> - CD/DVD devices with disc burning capabilities can be redirected, but the burning capabilities of these devices cannot be used. This is due to the buffer limits of a session.

Performance considerations for USB devices

Network latency and bandwidth can affect user experience and USB device operation when using generic USB redirection for some types of USB devices. For example, timing-sensitive devices might not operate correctly over high-latency low-bandwidth links. Use optimized support instead where possible.

Some USB devices require high bandwidth to be usable, for example a 3D mouse (used with 3D apps that also typically require high bandwidth). If bandwidth cannot be increased, you might be able to mitigate the issue by tuning bandwidth usage of other components using the bandwidth policy settings. For more information, see Bandwidth policy settings for Client USB device redirection, and Multi-stream connection policy settings.

Security considerations for USB devices

Some USB devices are security-sensitive by nature, for example, smart card readers, fingerprint readers, and signature pads. Other USB devices such as USB storage devices can be used to transmit data that might be sensitive.

USB devices are often used to distribute malware. Configuration of Citrix Workspace app and Citrix Virtual Apps and Desktops can reduce, but not eliminate, risk from these USB devices. This situation applies whether generic USB redirection or optimized support is used.

> **Important:**
>
> For security-sensitive devices and data, always secure the HDX connection using either TLS or IPsec.
>
> Only enable support for the USB devices that you need. Configure both generic USB redirection and optimized support to meet this need.
>
> Provide guidance to users for safe use of USB devices:
>
> - Use only USB devices that have been obtained from a trustworthy source.
> - Don't leave USB devices unattended in open environments - for example, a flash drive in an internet cafe.
> - Explain the risks of using a USB device on more than one computer.

Compatibility with generic USB redirection

Generic USB redirection is supported for USB 2.0 and earlier devices. Generic USB redirection is also supported for USB 3.0 devices connected to a USB 2.0 or USB 3.0 port. Generic USB redirection does not support USB features introduced in USB 3.0, such as super speed.

These Citrix Workspace apps support generic USB redirection:

- Citrix Workspace app for Windows, see Configuring application delivery.
- Citrix Workspace app for Mac, see Citrix Workspace app for Mac.
- Citrix Workspace app for Linux, see Optimize.
- Citrix Workspace app for Chrome OS, see Citrix Workspace app for Chrome.

For Citrix Workspace app versions, see the Citrix Workspace app feature matrix.

If you are using earlier versions of Citrix Workspace app, see the Citrix Workspace app documentation to confirm that generic USB redirection is supported. See Citrix Workspace app documentation for any restrictions on USB device types that are supported.

Generic USB redirection is supported for desktop sessions from VDA for Single-session OS version 7.6 through current.

Generic USB redirection is supported for desktop sessions from VDA for Multi-session OS version 7.6 through current, with these restrictions:

- The VDA must be running Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022.
- The USB device drivers must be fully compatible with Remote Desktop Session Host (RDSH) for the VDA OS (Windows 2012 R2), including full virtualization support.

Some types of USB devices are not supported for generic USB redirection because it would not be useful to redirect them:

- USB modems.
- USB network adapters.
- USB hubs. The USB devices connected to USB hubs are handled individually.
- USB virtual COM ports. Use COM port redirection rather than generic USB Redirection.

For information on USB devices that have been tested with generic USB redirection, see Citrix Ready Marketplace. Some USB devices do not operate correctly with generic USB redirection.

Configure generic USB redirection

You can control, and separately configure, which types of USB devices use generic USB redirection:

- On the VDA, using Citrix policy settings. For more information, see Redirection of client drives and user devices and USB devices policy settings in the Policy settings reference
- In Citrix Workspace app, using Citrix Workspace app-dependent mechanisms. For example, an Administrative Template controls registry settings that configure Citrix Workspace app for Windows. By default, USB redirection is allowed for certain classes of USB devices and denied for others. For more information, see Configure in the Citrix Workspace app for Windows documentation.

This separate configuration provides flexibility. For example:

- If two different organizations or departments are responsible for Citrix Workspace app and VDA, they can enforce control separately. This configuration applies when a user in one organization accesses an application in another organization.
- Citrix policy settings can control USB devices that are allowed only for certain users or for users connecting only over a LAN (rather than by using Citrix Gateway).

Enable generic USB redirection

To enable generic USB Redirection, and not require manual redirection by the user, configure both Citrix policy settings and Citrix Workspace app connections preferences.

In Citrix policy settings:

1. Add the Client USB device redirection to a policy and set its value to **Allowed**.



2. (Optional) To update the list of USB devices available for redirection, add the Client USB device redirection rules setting to a policy and specify the USB policy rules.

   In Citrix Workspace app:

3. Specify that devices are connected automatically without manual redirection. You can do this using an Administrative template or in Citrix Workspace app for Windows > Preferences > Connections.



If you specified USB policy rules for the VDA in the previous step, specify those same policy rules for Citrix Workspace app.

For thin clients, consult the manufacturer for details of USB support and any required configuration.

Configuring the types of USB devices available for generic USB redirection

USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to connect USB devices automatically. USB devices are also automatically redirected when the connection bar is not present.

Users can explicitly redirect devices that are not automatically redirected by selecting the devices from the USB device list. For more information, the Citrix Workspace app for Windows user help article, Display your devices in the Desktop Viewer.



To use generic USB redirection rather than optimized support, you can either:

- In Citrix Workspace app, manually select the USB device to use generic USB redirection, choose **Switch to generic** from the Devices tab of the Preferences dialog box.
- Automatically select the USB device to use generic USB redirection, by configuring auto-redirection for the USB device type (for example, AutoRedirectStorage=1) and set USB user preference settings to automatically connect USB devices. For more information, see Configure automatic redirection of USB devices.

> **Note:**
>
> Only configure generic USB redirection for use with a webcam if the webcam is found to be incompatible with HDX multimedia redirection.

To prevent USB devices from ever being listed or redirected, you can specify device rules for Citrix Workspace app and the VDA.

For generic USB redirection, you need to know at least the USB device class and subclass. Not all USB devices use their obvious USB device class and subclass. For example:

- Pens use the mouse device class.
- Smart card readers can use the vendor-defined or HID device class.

For more precise control, you need to know the Vendor ID, Product ID, and Release ID. You can get this information from the device vendor.

> **Important:**
>
> Malicious USB devices might present USB device characteristics that do not match their intended usage. Device rules are not intended to prevent this behavior.

You control the USB devices available for generic USB redirection by specifying USB device redirection rules for both VDA and Citrix Workspace app, to override the default USB policy rules.

For the VDA:

- Edit the administrator override rules for the Multi-session OS machines through group policy rules. The Group Policy Management Console is included on the installation media:
  - For x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - For x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

At Citrix Workspace app for Windows:

- Edit the user device registry. An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\icaclient_usb.adm

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default rules. Instead, use them as a guide for creating administrator override rules, which is explained later in this article. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format **{Allow: | Deny:}** followed by a set of *tag=value* expressions separated by white space.

The following tags are supported:

Tag	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor; see the USB website at http://www.usb.org/ for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating policy rules, note the following:

- Rules are case-insensitive.
- Rules can have an optional comment at the end, introduced by #. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator =. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

> **Note:**
>
> If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- The following example shows an administrator-defined USB policy rule for a defined class, subclass, and protocol:


```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

Use and remove USB devices

Users can connect a USB device before or after starting a virtual session.

When using Citrix Workspace app for Windows, the following apply:

- Devices connected after a session begins appear immediately in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, you can try to resolve the problem by waiting to connect the device until after the virtual session starts.
- To avoid data loss, use the Windows "Safely Remove Hardware"icon before removing the USB device.

Security controls for USB mass storage devices

Optimized support is provided for USB mass storage devices. This support is part of Citrix Virtual Apps and Desktops client drive mapping. Drives on the user device are automatically mapped to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders that have mapped drive letters. To configure client drive mapping, use the **Client removable drives** setting. This setting is in the File Redirection policy settings section of the ICA policy settings.

With USB mass storage devices you can use either Client drive mapping or generic USB redirection, or both. Control them using Citrix policies. The main differences are:

Feature	Client drive mapping	Generic USB redirection
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Encrypted device access	Yes, if encryption is unlocked before the device is accessed	Yes
BitLocker To Go devices	No	No
Safe to delete device during a session	No	Yes, provided users follow operating system recommendations for safe removal

If both generic USB redirection and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it is redirected using client drive mapping. When both generic USB redirection and the client drive mapping policies are enabled and a device is configured for automatic redirection and a mass storage device is inserted either before or after a session starts, it is redirected using generic USB redirection. For more information, see Knowledge Center article CTX123015.

> **Note:**
>
> USB redirection is supported over lower bandwidth connections, for example 50 Kbps. However, copying large files doesn't work.

Manage

March 23, 2022

Citrix manages Citrix Virtual Apps and Desktops service deployments by installing and maintaining the core components and features in Citrix Cloud.

You take care of the machines (VDAs) in resource locations that deliver apps and desktops. You also manage connections to those resource locations, plus the apps, desktops, and users.

- **Autoscale:** A consistent, high-performance solution to proactively power manage your machines.
- **Applications:** Manage applications in delivery groups.
- **Virtual IP and virtual loopback:** The Microsoft virtual IP address feature provides a published application with a unique dynamically assigned IP address for each session. With Citrix virtual loopback, you can configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).
- **VDA registration:** Before a VDA can facilitate delivery of apps and desktops, it must register (establish communication) with a Cloud Connector. You can specify Cloud Connector addresses using several methods, which are described in this article. As you add Cloud Connectors, VDAs must have current information.
- **Sessions:** Maintaining session activity is critical to providing the best user experience. Several features can optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity.
- **Using Search:** To view information about machines, sessions, machine catalogs, applications, or delivery groups in the Full Configuration management interface, use the flexible search feature.

- **IPv4/IPv6 support:** Citrix Virtual Apps and Desktops supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks. This article describes and illustrates these deployments. It also describes the Citrix policy settings that control the use of IPv4 or IPv6.
- **Profile management:** Citrix Profile Management can be installed when you install a VDA. If you use this user profile solution, review its documentation.
- **Citrix Insight Services:** Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation. Analytics and diagnostics are collected when you install a VDA.
- **Local Host Cache:** Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. Scale, size, and other configuration considerations are also provided.
- **Delegated administration:** With delegated administration, you can configure the access permissions that all of your administrators need, according to their role in your organization.
- **Configuration logging:** Configuration logging tracks configuration changes and administrative activities.
- **Event logs:** Services within Citrix Virtual Apps and Desktops log the events that occur. Event logs can be used to monitor and troubleshoot operations.
- **Licenses:** You can view Citrix license usage information for this service from the Citrix Cloud console.
- **Load balance machines:** You can control how to load balance machines.

Adaptive access

June 6, 2022

In today's ever changing situations, application security is vital for any businesses. Making context-aware security decisions and then enabling access to the applications reduces the associated risks while enabling access to users.

The Adaptive access feature offers a comprehensive zero-trust access approach that delivers secure access to the applications. Adaptive access enables admins to provide granular level access to the apps that users can access based on the context. The term "context"refers to:

- Users and groups (users and user groups)
- Devices (desktop or mobile devices)

- Location (geo-location or network location)
- Device posture (device posture check)
- Risk (user risk score)

Device Posture

January 5, 2024

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (Citrix Virtual Apps and Desktops) or Citrix Secure Private Access resources (SaaS and Web apps or TCP and UDP apps). Establishing device trust by checking the device's posture is critical to implement zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in.

For details, see Device Posture.

Adaptive Authentication service

June 6, 2022

Citrix Cloud customers can use Citrix Workspace to provide Adaptive Authentication to Citrix DaaS. Adaptive Authentication is a Citrix Cloud service that enables advanced authentication for customers and users logging in to Citrix Workspace. Adaptive Authentication service is a Citrix managed and Citrix Cloud hosted ADC that provides all the advanced authentication capabilities such as the following:

- Multifactor authentication using different auth methods like AD, RADIUS, certificate, multiple third-party IdPs using SAML 2.0, OAuth, OIDC, Google Captcha.
- Verify user identity and authorization levels based on factors such as location, device status, and user group.
- Enable contextual or smart access to DaaS (virtualized) and SPA (non-virtualized resources like Web and SaaS apps).
- Login page customization

For complete details about Adaptive Authentication, see Adaptive Authentication service.

Adaptive access based on the user's network location

May 9, 2024

The Citrix Workspace Adaptive Access feature uses advanced policy infrastructure to enable access to Citrix DaaS based on the user's network location. The location is defined using the IP address range or subnet addresses.

Admins can define policies to either enumerate or not enumerate virtual apps and desktops based on the user's network location. Admins can also control the user actions by enabling or disabling clipboard access, printers, client drive mapping and so on, based on the user's network location. For example, admins can set up policies such that users accessing the resources from home have limited access to applications and users accessing the resources from branch offices have full access.



An admin can implement the following policies for accessing the applications:

- Enumerate a few sensitive applications only from corporate location or from their branch offices.
- Do not enumerate sensitive applications if the employees are accessing the workspace from an outside network.
- Disable printer access from the branch offices.
- Disable clipboard access and printer access when the users are outside the corporate network.

Entitlements

The Adaptive Access feature is available for the customers with the any of the following licenses.

- DaaS Premium / Premium Plus
- Secure Private Access Advanced

Prerequisites

- Ensure that the **Adaptive Access** feature is enabled (**Citrix Workspace > Access > Adaptive Access**). For details, see Enable the Adaptive Access feature.

  When adaptive access is enabled, the DaaS access policies are updated to use the option **Connections through Citrix Gateway**.

  > **Note:**
  >
  > NetScaler Gateway is required to add smart access tags in DaaS access policies. However, because DaaS consumes tags from Device Posture, Adaptive Access, and Adaptive Authentication services, it isn't necessary have a configured NetScaler Gateway in your setup.

- Understanding of location tags. For details, see Network Location tags.

Points to note

The following points are only applicable if you want to restrict application enumeration based on the location. If you plan to use adaptive access to restrict user controls like disabling clipboard access, printer redirection, client drive mapping, based on the network location, you can ignore these guidelines.

- If you plan to selectively enumerate Citrix DaaS based on network location, then user management must be performed for those delivery groups using Citrix Studio policies instead of workspace. When creating a Delivery group, in **Users setting**, either choose **Restrict use of this Delivery Group** users or **Allow any authenticated users to use this Delivery Group**. This enables you to configure adaptive access in the **Access Policy** tab under **Delivery Group**.



- Changes to Direct Workload Connection when adaptive access is enabled.
  - The **Location tags** field is visible in **Citrix Cloud > Network Locations > Add a Network Location > Location tags**.
  - Existing Direct Workload Connection policies work as intended.
  - New policies must be created in the Network Locations service (without defining tags) and also on the delivery group. In addition, the network connectivity type must be **Internal**.
  - For new policies for Direct Workload Connection with tags, tags must be defined in the Network Locations service and also the same tags must be defined on the delivery group or access policy in DaaS Studio. In addition, the network connectivity type must be **Internal**. Location tags aren't relevant for Direct Workload Connection.
- The following is recommended testing your Citrix DaaS deployment.
  - Identify a test delivery group or create a delivery group to implement this capability.
  - Create a policy or identify a policy that can be used with a test delivery group.

Enable the Adaptive Access feature

1. Log in to Citrix Cloud.
2. Select **Workspace Configuration** from the hamburger menu.
3. **Adaptive Access** toggle is turned off, by default. Turn the **Adaptive Access** toggle on.
4. Click **Yes, enable adaptive access** on the confirmation message.





When adaptive access is enabled, you can define the location tags for adaptive access (**Citrix Cloud > Network Locations > Add a Network Location > Location tags**).



When Adaptive Access is disabled, you can't add a network location. Location tags aren't applicable in this case.



Important:

When you try to disable the Adaptive Access feature, the following message appears. Note that Workspace does not send the tags to the DaaS for adaptive access when the feature is disabled.



Configure adaptive access

Configuring adaptive access based on network locations involves the following high-level steps.

1. Define the network location policies

2. Define the tags in DaaS Studio

For configuration examples, two user types (**BranchOffice** users and **WorkFromHome** users) are selected to achieve the following use case.

- BranchOffice users must be able to access applications with all the access.
- WorkFromHome users must not have clipboard access.

In this configuration example, **Home** and **Office** are used as the tags in the examples.

Configure network location policies

1. Sign into Citrix Cloud.
2. Select **Network Locations** from the hamburger menu.
   Ensure that the Adaptive Access toggle is enabled. Else the user interface for the Direct Workload Connection is displayed.
3. Click **Add network location**.
   - **Location name:** Enter an appropriate name for the policy.

     Example: BranchOffice or WorkFromHome
   - **Public IP address range:** Define the public IP address range for your network.

     Example: 172.9.2.1-172.9.2.30
   - **Location Tags:** Define tags for your location. This can be a name referring to your location. These tags are used to configure the adaptive access policies in Citrix Studio. For details, see **Define tags in Citrix Studio**.

     Example: *BranchOffice* or *WorkFromHome*
   - **Connectivity type:** Define the application launch type.

   Internal - Bypass gateway for application launch.
   External - Use Citrix Gateway service or traditional gateway for application launch.
4. Click **Save**.

You can now use these tags on DaaS Studio to enable adaptive access.

> **Note:**
>
> While defining the location tags, ensure that you only enter the preferred tag name without the prefix "LOCATION_TAG", for example "BranchOffice". However, while defining tags in

> Citrix Studio, you must prefix the tag name with "LOCATION_TAG". For example, "LOCATION_TAG_BRANCHOFFICE".

Define tags in Citrix Studio by using the GUI

In this example, tags are defined in the delivery groups to restrict the application enumeration for users. Two delivery groups are created.

- Adaptive Access Delivery group –For the users from location **BranchOffice**. These users must see all applications from this delivery group.
- WFH Delivery Group –For the users from location **WorkfromHome**. These users must see applications from this delivery group.

1. Sign into Citrix Cloud.
2. On the **Citrix DaaS** tile, click **Manage**.
3. Create a delivery group. For details, see Create delivery groups.
4. Select the delivery group that you've created, and click **Edit Delivery Group**.
5. Click **Access Policy**.
6. For customers using adaptive access within the Citrix Workspace platform, perform the following steps to restrict access for a delivery group to internal networks only:
    a) Right-click the delivery group and select **Edit**.
    b) Select the access policy in the left pane.
    c) Click the edit icon to modify the default Citrix Gateway connections policy.



d) On the **Edit policy** page, select **Connections meeting the following criteria**, select **Match any**, and then add the criteria.



For WorkFromHome users, enter the following values in the respective delivery controller.

Farm: Workspace

Filter: LOCATION_TAG_WORKFROMHOME

For BranchOffice users, enter the following values in the respective delivery controller.

Filter: Workspace

Value: LOCATION_TAG_BRANCHOFFICE

You can now use these tags to restrict access to applications.

> **Note:**
>
> Ensure that in the **Value** field, you enter the correct location tag name as you have defined while creating network location policies prefixed by "LOCATION_TAG". For example, if you have defined the location tag as "BranchOffice", then you must enter "LOCATION_TAG_BRANCHOFFICE" in the **Value** field. For details on configuring location tags, see Configure network location policies.

Restrict access for the applications

In this example, client clipboard redirection is disabled for users from the WorkFromHome location.

1. Sign into Citrix DaaS.
2. Navigate to **Policies** and click **Create Policy**.
3. Select **Client clipboard redirection**, and then click **Prohibit**.
4. Click **Next**.



1. On the **Assign policy To** page, select **Access control**.
2. Define the following values for the policy:
   - Mode: **Allow**
   - Connection type : **With Citrix Gateway**
   - Gateway farm name: **Workspace**
   - Access Condition: **LOCATION_TAG_WORKFROMHOME** (all in upper case)



1. Click **Next**.
2. Enter a name for the policy and add a policy description.
3. Click **Finish**.

Users from the **WorkFromHome** location can't perform clipboard access to their launched resources.

Configure session recording policies based on tags

Session Recording allows organizations to record on-screen user activity in virtual sessions. You can specify tags including network location tags when creating a custom session recording policy, event detection policy, or event response policy. For an example, see Create a custom recording policy.

Network Location tags

The Network Locations service provides the following tags.

- **Default tags:** These tags are defined on the Network Locations service. The following default tags are available.
  - **Location_internal:** Tag sent by default when the network connectivity type is set as **INTERNAL**.
  - **Location_external:** Tag sent by default when the network connectivity type is set as **EXTERNAL**.
  - **Location_undefined:** Tag sent for an IP address that is not defined in the policy but is coming through the Network Locations service. Launch for these users are the same as what is defined in the resource group.
- **Custom tags:** Admins can define custom tag names in the policies. Example: office, home, branch

Examples:

Default tags: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

Custom tags: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

> **Note:**
>
> When defining tags for the Network Location service, ensure the following:
>
> - The default tags always start with the prefix "LOCATION_<tag name>. For example, LOCATION_INTERNAL.
> - The custom tags always start with the prefix "LOCATION_TAG<tag name>. For example, LOCATION_TAG_OFFICE.

Known issues

If you disable the Adaptive Access feature after it was enabled and the rules were set (tags and connectivity type), this does not remove the locations from the Network Locations page though the location tags and the connectivity type columns are hidden. But these locations are disabled in the back-end. This is a cosmetic issue.

App packages

May 15, 2024

There're several packaging technologies for delivering applications to users, including App-V, MSIX, MSIX app attach, and FlexApp. This article walks you through how to deploy and deliver these packaged applications in your Citrix DaaS environment:

- Deploy and deliver App-V applications
- Deploy and deliver MSIX and MSIX app attach applications
- Deploy and deliver FlexApp applications

Deploy and deliver App-V applications

This section covers the following information:

- Overview. Describes the management methods that Citrix DaaS uses to deliver and manage the App-V packages.
- Procedures. Provides procedures for deploying and delivering these packages.

Overview

This section describes the management methods that Citrix DaaS uses to deliver and manage the App-V packages. For more information about the components and concepts with which you interact when delivering App-V packaged applications, see the Microsoft documentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Citrix DaaS delivers and manages App-V packages using the following methods:

- **Dual Admin**. Application packages are configured and managed on App-V servers. Citrix DaaS and App-V servers work together to deliver and manage packages.

  This method requires Citrix DaaS to periodically refresh the snapshot view of the App-V server's state. It incurs hardware, infrastructure, and administration overhead. Citrix DaaS and App-V servers must stay synchronized, particularly for user permissions.

  Dual Admin works best in deployments where App-V and Citrix Cloud are closely coupled:

  - **App-V management server**. Publishes and manages the lifecycle of App-V Packages and the Dynamic Configuration Files.
  - **Citrix Personalization component** installed on VDA machines. Manage the registration of the appropriate App-V publishing server required for application launches.

  This method ensures that the App-V publishing server is synchronized for the user at the appropriate time. The publishing server maintains other aspects of the package life cycle, such as refresh on logon and connection groups.

- **Single Admin**. Application packages are stored on network shares. Citrix DaaS delivers and manages packages independently.

  This method reduces overhead because the App-V servers and database infrastructure aren't needed in the deployment.

  In this method, you store App-V packages on a network share and upload their metadata from that location to Citrix Cloud. The Citrix Personalization component installed on VDA machines then manages and delivers applications as follows:

  - Process the Deployment Configuration Files and User Configuration Files when an application is launched.
  - Manage all aspects of the life cycles for packages on the host machine.

You can use both management methods simultaneously. In other words, when you add applications to delivery groups, the applications can come from App-V packages present on App-V servers or on network shares.

> **Note:**
>
> If you're using both management methods simultaneously and the App-V package has a Dynamic Configuration File in both locations, the file on the App-V server (Dual Admin) is used.

Procedures

To support the delivery of App-V applications, you must install the Citrix Personalization component on VDA machines. See Install the Citrix Personalization component on VDA machines for details.

To deliver App-V packaged applications to your users, follow these steps:

1. Store application packages on network shares.
2. Upload application packages into Citrix Cloud.
3. Add applications to delivery groups.
4. To enable automatic delivery of interdependent App-V packages, create isolation groups.

To have Citrix DaaS recognize and apply App-V Dynamic Configuration Files in the Single Admin method, see this Citrix blog.

Deploy and deliver MSIX and MSIX app attach applications

This section covers the following information:

- Overview. Describes how Citrix DaaS delivers and manages the MSIX and MSIX app attach packages.
- Procedures. Provides procedures for deploying and delivering these packages.

Overview

Citrix DaaS delivers MSIX and MSIX app attach applications to users through the Citrix Personalization component installed on VDA machines. This component manages all aspects of the life cycles for packages on the host machine.

For more information about MSIX and MSIX app attach, see the Microsoft documentation: https://docs.microsoft.com/en-us/windows/msix/ and https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach respectively.

Procedures

To support the delivery of MSIX and MSIX app attach packages, you must install the Citrix Personalization component on VDA machines. See Install the Citrix Personalization component on VDA machines

for details.

To deliver MSIX and MSIX app attach packaged applications to your users, follow these steps:

1. Store application packages on network shares.
2. Upload application packages into Citrix Cloud.
3. Add applications to delivery groups.

Deploy and deliver FlexApp applications

This section covers the following information:

- Overview. Describes how Citrix DaaS delivers and manages the FlexApp packages.
- Procedures. Provides procedures for deploying and delivering these packages.

Overview

Citrix DaaS delivers FlexApp applications to users through the Citrix Personalization component and FlexApp delivery agent installed on VDA machines. These two components manage all aspects of the life cycles for packages on the host machine.

Procedures

To support the delivery of FlexApp applications, you must install the following components on the VDA machines:

- The Citrix Personalization component on VDA machines. See Install the Citrix Personalization component on VDA machines for details.
- The FlexApp Agent on VDAs. See Install the FlexApp Agent for details.

Deliver FlexApp packaged applications to your users by following these steps:

1. Store application packages on network shares.
2. Upload application packages into Citrix Cloud.
3. Add applications to delivery groups.

Install the Citrix Personalization component on VDA machines

The Citrix Personalization component manages the publishing process for application packages in App-V, MSIX, MSIX app attach, and FlexApp formats. This component isn't installed by default when you install a VDA. You can install the component during or after VDA installation.

To install the component during VDA installation, use either of the following ways:

- In the installation wizard, go to the **Additional Components** page and then select the **Citrix Personalization for App-V - VDA** check box.
- In the command line interface, use the **/includeadditional "Citrix Personalization for App-V –VDA"** option.

To install the component after VDA installation, follow these steps:

1. On the VDA machine, go to **Control Panel > Programs > Programs and Features**, right-click **Citrix Virtual Delivery Agent**, and then select **Change**.
2. In the wizard that appears, proceed to the **Additional Components** page and then enable the **Citrix Personalization for App-V - VDA** check box.

> **Note:**
>
> Microsoft App-V Desktop Client is the component that runs virtual applications from App-V packages on user devices. Windows 10 (1607 or later), Windows Server 2016, and Windows Server 2019 already include this App-V client software. You only need to enable it on VDA machines. For more information, see this Microsoft documentation article: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

Store application packages on network shares

After you set up the infrastructure, generate the application packages and store them in a network location, such as a UNC or SMB network share, or on an Azure File Share.

Detailed steps are as follows:

1. Generate application packages. See the Microsoft documentation for details.
2. Store application packages in a network location:
    - For **App-V Single Admin**: Store the packages and the corresponding Dynamic Configuration Files (App-V) on a UNC or SMB network share or on an Azure File Share.
    - For **App-V Dual Admin**: Publish the packages onto the App-V management server from a UNC path. (Publishing from HTTP URLs isn't supported.)
    - For **MSIX or MSIX app attach**: Store the packages on a UNC or SMB network share or an Azure File Share.
    - For **FlexApp**: Store the packages on a UNC or SMB network share or an Azure File Share.
3. Make sure that the VDA has read permission on the package storage path:
    - If you store packages on a UNC or SMB network share in your AD domain, grant the VDA machine read permission to the storage path. To do so, you can give the machine's AD

account read permission to the share explicitly, or include the account in an AD group that has that permission.

- If you store packages on an Azure File Share, first grant a user account read permission to the storage path in Azure. Next, configure `ctxAppVService` running on the VDA machine to use that user account to access the package storage path. See the following section for detailed steps.

Change the user logon account

The VDA calls `ctxAppVService` to access package storage paths. By default, `ctxAppVService` accesses package storage paths using the machine's **Local System account**. This type of machine authentication works in AD domains. However, it doesn't work in the AD and Azure AD integration scenarios, which require user account-based authentication.

If you store packages on an Azure File Share, change the logon account for `ctxAppVService` to a user account that has read permission on the package storage path. Detailed steps are as follows:

1. Start **Services**, right-click **ctxAppVService**, and then select **Properties**.
2. On the **Log on** tab, select **This account**, enter a user account that has read permission to the package storage path, and then enter the user's password twice.
3. Click **OK**.

Upload application packages into Citrix Cloud

After you store application packages to a network location as needed, upload them to Citrix Cloud for delivery. Use either of the following methods as needed:

- Upload in bulk
- Upload one by one

Preparations

Citrix DaaS uses a VDA machine to set up the connection to the network location for package discovery. Therefore, create a delivery group beforehand and make sure that at least one VDA in the group meets the following requirements:

- VDA version:
  - To discover App-V packages: 2203 or later
  - To discover MSIX and MSIX app attach packages: 2209 or later

  - To discover FlexApp packages: 2311 or later

- Citrix Personalization for App-V component: Installed
- Permission on the package location: Read (See Step 2: Store application packages on network shares for details.)
- Power: On
- State: Registered

Required roles

By default, if you have the Cloud Administrator or Full Administrator role, you can upload application packages to Citrix Cloud. You can also create custom roles to perform the upload actions. The following table lists the permissions required by the App packages actions.

Action	Required permission
Add package (upload one by one)	Create Application Discovery Sessions
Add source (upload in bulk)	Create Application Discovery Profiles
Check for package updates	Create Application Discovery Sessions
Remove source	Remove Application Discovery Profiles

Upload application packages in bulk

Upload packages in a network location to Citrix Cloud. Make sure that you have the following items ready before the upload:

- A delivery group that meets the Preparation requirements
- The network location path

To upload packages in bulk, follow these steps:

1. From **Manage > Full Configuration**, select **App Packages** in the left pane.
2. On the **Sources** tab, click the **Add Source** button. The **Add Source** page appears.
3. In the **Name** field, enter a descriptive name for the package source.
4. In the **Delivery group** field, click **Select a delivery group**. Next, select a delivery group that meets the requirements stated in Preparation and then click **OK**.
5. In the **Location type** field, select **Microsoft App-V server** or **Network share** based on where you store the packages, and then complete the corresponding settings:

- If you select **Microsoft App-V server**, enter the following information:
  - URL of the Management server. Example: `http://appv-server.example.com`
  - Login credentials of the management server administrator.
  - URL and port number of the publishing server. Example: `http://appv-server.example.com:3330`
- If you selected **Network share**, specify the following information:
  - Enter the UNC path of the network share. Example: `\\Package-Server\apps\`
  - Select the package types that you want to upload. Options include App-V, MSIX, MSIX app attach, and FlexApp.
  - Specify whether to search subfolders for packages.

6. Click **Add Source**.

   The Add Source page closes and the newly added source appears in the source list. Citrix DaaS uploads the packages to Citrix Cloud using a VDA in the delivery group. After the upload completes, the Status field shows *Import successful*. The corresponding packages appear on the **Packages** tab.

   > **Note:**
   >
   > To check for package updates in a source location and import them to Citrix Cloud, select the location in the source list and click **Check for Package Updates**.

Upload application packages one by one

Upload an application package from a network share to Citrix Cloud. Before the upload, make sure that you have the following items ready:

- A delivery group that meets the requirements stated in Preparation
- The network location path.

To upload a package to Citrix Cloud, follow these steps:

1. From **Manage > Full Configuration**, select **App Packages** in the left pane.
2. On the **Packages** tab, click the **Add Package** button. The **Add Package** page appears.
3. In the **Delivery group** field, click **Select a delivery group**. Next, select a delivery group that meets the requirements stated in Preparation, and then click **OK**.
4. In the **Package full path** field, enter a path as needed:
   - To upload several packages at a time, enter their full paths, separated by semicolons (`;`). Example: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`

- To upload all packages present on a network share, enter the storage path. Example: \package-Server\apps\

5. Click **Add Package**.

   The application package appears on the **Packages** tab.

Add applications to delivery groups

After an application package is fully uploaded, add its applications to one or more delivery groups as needed. As a result, users associated with those delivery groups can access the applications.

> **Note:**
>
> - You can deliver packaged applications to single-session VDAs and mult-session VDAs through delivery groups.
> - By default, end users have access to all packaged applications assigned to the delivery groups associated with their *single-session* (or called *Desktop*) VDAs. To limit visibility of a packaged application on *desktop* VDAs to specific users or groups, go to the **Applications** node, select the application, and then select **Edit Application Properties > Limit Visibility** to make changes.

To add one or more applications in a package to several delivery groups, follow these steps:

1. From **Manage > Full Configuration**, select **App Packages** in the left pane.
2. On the **Packages** tab, select a package as needed.
3. In the action bar, click **Assign Applications to Delivery Groups**. The Assign Applications to Delivery Groups page appears.
4. Select one or more applications in the package as needed, and then click **Next**.
5. In the delivery groups list, select the groups to which you want to assign the applications, and then click **Next**.

   > **Note:**
   >
   > - If you selected an *MSIX* or *MSIX app attach* package, only delivery groups whose functional level is 2106 or later are shown in the list.
   > - If you selected a *FlexApp* package, only delivery groups whose functional level is 2206 or later appear in the list.

6. Click **Finish**.

To add applications in various packages to multiple delivery groups, follow these steps:

1. From **Manage > Full Configuration**, select **Applications** in the left pane.
2. On the **Applications** tab, select **Add Applications**.
3. On the **Groups** page, select one or more delivery groups as needed.
4. On the **Applications** page, select one or more application packages as follows:

    a) Click **Add** and then select **Application packages**.
    b) Select the type of package source needed (for example, App-V Single Admin). All packages of this type appear.
    c) Select one or more packages as needed.
    d) Click **OK** and then **Next**.
    e) To add more applications of a different package type, repeat steps a through d.

5. Click **Finish**.

You can also add packaged applications to a delivery group when:

- Creating a delivery group. For more information, see Create delivery groups.
- Editing existing delivery groups or application groups. For more information, see Add applications.

(Optional) Create isolation groups for App-V packages

You can create isolation groups to enable the automatic delivery of interdependent App-V packages.

> **Note:**
>
> Isolation groups are supported for the App-V Single Admin method. If you're using the App-V Dual Admin method, you can achieve the same goal by creating *connection groups* in the Microsoft App-V infrastructure. For more information, see this Microsoft documentation article: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

About isolation groups

An isolation group is a collection of interdependent application packages that must run in the same Windows Sandbox to create a virtual environment. Citrix App-V isolation groups are similar but not identical to App-V connection groups. An isolation group includes two types of packages:

- **Explicit** application packages. Applications with specific licensing requirements. You can restrict those applications to a specific range of users by adding them to delivery groups.
- **Automatic** application packages. Applications that are always available to all users regardless of whether they are added to delivery groups.

For example, the application app-a requires JRE 1.7 to run. You can create an isolation group that contains app-a (marked as *Explicit*) and JRE 1.7 (marked as *Automatic*). Next, add the App-V package for app-a to one or more delivery groups. When a user launches app-a, JRE 1.7 is automatically deployed with it.

When a user starts an App-V application marked as *Explicit* in an isolation group, Citrix DaaS checks the user's access permission to the application in delivery groups. If the user has permission to access the application, any *Automatic* application packages in the same isolation group are made available to the user.

You do not need to add the *Automatic* packages to any delivery group. If there's another *Explicit* application package in the isolation group, that package is made available to the user only if it is in the same delivery group.

For more information about isolated groups, see this Citrix blog.

Create an App-V isolation group Create an isolation group and add interdependent application packages to it. Detailed steps are as follows:

1. On the **Isolation Groups** tab, click **Add Isolation Group**.
2. Enter a name and description for the isolation group. All application packages in Citrix Cloud appear in the **Available Packages** list.
3. From the **Available Packages** list, select an application as needed, and then click the right arrow. The selected application appears in the **Packages in Isolation Group** list.
4. In the **Deployment** field, select **Explicit** or **Automatic** for the application.
5. Repeat steps 2–3 to add more packages.
6. To adjust the order of packages in the list, click the up or down arrow.
7. Click **Save**.

> **Note:**
>
> Isolation Group configurations result in the creation of an App-V Connection Groups on the VDA. Deployment scenarios can become complex and the App-V client supports packages that are only in one active Connection Group at a time. We recommend that you avoid adding the same package to two different isolation groups that are added to the same delivery group.

Autoscale

February 21, 2024

Autoscale provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience. Autoscale incorporates the deprecated Smart Scale technology into the **Manage** console's power management solution.

Autoscale enables proactive power management of all registered single-session and multi-session OS machines in a delivery group.

Autoscale features include:

- Schedule-based and load-based settings
- Dynamic session timeouts
- Autoscale tagged machines (cloud burst)
- Dynamic machine provisioning
- User logoff notifications

Supported VDA hosting platforms

Autoscale supports all the platforms that Citrix DaaS supports. This includes various infrastructure platforms including XenServer (formerly Citrix Hypervisor), Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere, and many more. For a complete list of supported platforms, see System requirements for Citrix DaaS.

Supported workloads

Autoscale supports both multi-session OS and single-session OS delivery groups. There are three user interfaces to be aware of:

- Autoscale user interface for multi-session OS delivery groups (formerly RDS delivery groups)
- Autoscale user interface for single-session OS random (pooled) delivery groups (formerly pooled VDI delivery groups)
- Autoscale user interface for single-session OS static delivery groups (formerly static VDI delivery groups)

For more information about the user interfaces for different delivery groups, see Autoscale user interfaces.

Benefits

The Autoscale feature delivers the following benefits:

- Provide you with a single, consistent mechanism to power manage machines in a delivery group.

- Ensure availability and control costs by powering machines with load-based or schedule-based power management, or a combination of both.
- To monitor metrics such as cost savings and capacity utilization, and to enable notifications, use Director, available on the **Monitor** tab.

Watch a 2-minute video

The following video provides a quick tour of Autoscale.

This is an embedded video. Click the link to watch the video

Get started with Autoscale

September 22, 2023

Autoscale works at a delivery group level. It proactively power manages machines in a delivery group based on the schedules that you set.

Autoscale applies to all types of delivery groups:

- Single-session static OS
- Single-session random OS
- Multi-session random OS

This article describes basic Autoscale-related concepts and provides guidance on how to enable and configure Autoscale for a delivery group.

Basic concepts

Before you start, learn about the following basic concepts in Autoscale:

- Schedules
- Capacity buffer
- Load index

Schedules

Autoscale powers on and off machines in a delivery group based on a schedule that you set.

A schedule includes the number of active machines for each time slot, with peak and off-peak times defined.

Schedule settings vary with the type of delivery group. For more information, see:

- Multi-session OS delivery groups
- Single-session OS random delivery groups
- Single-session OS static delivery groups

Capacity buffer

Capacity buffer is used to add spare capacity to the current demand to account for dynamic load increases. There are two scenarios to be aware of:

- For multi-session OS delivery groups, the capacity buffer is defined as a percentage of the total capacity of the delivery group in terms of load index.
- For single-session OS delivery groups, the capacity buffer is defined as a percentage of the total number of machines in the delivery group.

Load index

> **IMPORTANT:**
>
> Load index applies only to multi-session delivery groups.

The load index metric determines how likely a machine is to receive user logon requests. It's calculated using the **Citrix Load Management policy** settings configured for concurrent logon, session, CPU, disk, and memory use.

The load index ranges from 0 to 10,000. By default, a machine is considered at full load when it's hosting 250 sessions:

- The digit "0"indicates an unloaded machine. A machine with a load index value of 0 is at a baseline load.
- The digit "10,000"indicates a fully loaded machine that can't run any more sessions.

Enable Autoscale for a delivery group

Autoscale is disabled by default when you create a delivery group. To enable and configure Autoscale for a delivery group using the Full Configuration interface, follow these steps:

You can also use PowerShell commands to enable and configure Autoscale for a delivery group. For more information, see Broker PowerShell SDK commands.

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane.

2. Select the delivery group that you want to manage and then click **Manage Autoscale**.



3. On the **Manage Autoscale** page, select the **Enable Autoscale** check box to enable Autoscale. After you enable Autoscale, the options on the page are enabled.



4. To change the default settings based on your organization's needs, complete the following settings:

   - Set up schedules
   - To power off inactive machines more efficiently, use Dynamic session timeouts and User logoff notifications

- To power manage a subset of machines in the delivery group, use Autoscaling tagged machines

To disable Autoscale, clear the **Autoscale** check box. The options on the page turn gray to indicate that Autoscale is disabled for the selected delivery group.

> **Important:**
>
> - If you disable Autoscale, all machines managed by Autoscale remain in their states at the time of disabling.
> - After you disable Autoscale, the machines in drain state are taken out of drain state. For more information about drain state, see Drain state.

You can dynamically provision machines for the group using a PowerShell script. For more information, see Dynamic machine provisioning.

Monitor metrics

After you enable Autoscale for a delivery group, you can monitor the following metrics of Autoscale-managed machines from the **Monitor** tab.

- Machine usage
- Estimated savings
- Alert notifications for machines and sessions
- Machine status
- Load evaluation trends

> **Note:**
>
> When you initially enable Autoscale for a delivery group, it might take a few minutes to display monitoring data for that delivery group.
> Monitoring data remains available if Autoscale is enabled and then disabled for the delivery group. Autoscale collects monitoring data at 5-minute intervals.

For more information about the metrics, see Monitor Autoscale-managed machines.

Good to know

Autoscale works at a delivery group level. It's configured on a per-delivery group basis. It power manages only the machines in the selected delivery group.

Capacity and machine registration

Autoscale includes only machines that are registered with the site when determining the capacity. Powered-on machines that are unregistered can't accept session requests. As a result, they aren't included in the overall capacity of the delivery group.

Scaling across multiple machine catalogs

In some sites, multiple machine catalogs might be associated with a single delivery group. Autoscale randomly powers on machines from each catalog to meet schedule or session demand requirements.

For example, a delivery group has two machine catalogs: Catalog A has three machines powered on and Catalog B has one machine powered on. If Autoscale needs to power on an extra machine, it might power on a machine from either Catalog A or Catalog B.

Machine provisioning and session demand

The machine catalog associated with the delivery group must have enough machines to power on and off as demand increases and decreases. If session demand exceeds the total number of registered machines in the delivery group, Autoscale ensures that all registered machines are powered on. However, **Autoscale does not provision additional machines**.

To overcome this bottleneck, you can use a PowerShell script to create machines and delete them dynamically. For more information, see Dynamically provision machines

Instance size considerations

You can optimize your costs if you appropriately size your instances in public clouds. We recommend that you provision smaller instances as long as they match your workload performance and capacity requirements.

Smaller instances host fewer user sessions than larger instances. Therefore, Autoscale puts machines into drain state much faster because it takes less time for the last user session to be logged off. As a result, Autoscale powers off smaller instances sooner, thereby reducing costs.

Drain state

Autoscale attempts to scale down the number of powered-on machines in the delivery group to the configured pool size and capacity buffer.

To achieve this goal, Autoscale puts the excess machines with the fewest sessions into "drain state" and powers them off when all sessions are logged off. This behavior occurs when session demand lessens and the schedule requires fewer machines than are powered on.

Autoscale puts excess machines into "drain state"one by one:

- If two or more machines have the same number of active sessions, Autoscale drains the machine that has been powered on for the specified power-off delay.

  Doing so avoids putting recently powered-on machines into drain state because those machines are more likely to have the fewest sessions.

- If two or more machines have been powered on for the specified power-off delay, Autoscale drains those machines one by one at random.

Machines in drain state no longer host new session launches and are waiting for the existing sessions to be logged off. A machine becomes a candidate for shutdown only when all sessions are logged off. However, if there are no machines immediately available for session launches, Autoscale prefers directing the session launches to a machine in drain state over powering on a machine.

A machine is taken out of drain state when one of the following conditions is met:

- The machine is powered off.
- Autoscale is disabled for the delivery group to which the machine belongs.
- Autoscale uses the machine to meet schedule or load demand requirements. This case occurs when the schedule (schedule-based scaling) or the current demand (load-based scaling) requires more machines than the number of machines that are currently powered on.

> **Important:**
>
> If no machines are immediately available for session launches, Autoscale prefers directing session launches to a machine in drain state over powering on a machine. A machine in drain state that hosts a session launch remains in drain state.

To find out which machines are in drain state, use the `Get-BrokerMachine` PowerShell command. For example: `Get-BrokerMachine -DrainingUntilShutdown $true`. Alternatively, you can use the Manage console. See Display machines in drain state.

Display machines in drain state

> **Note:**
>
> This feature applies only to multi-session machines.

In **Manage > Full Configuration**, you can display machines that are in drain state, letting you know which machines are about to shut down. Complete the following steps:

1. Navigate to the **Search** node and then click **Columns to Display**.
2. In the **Columns to Display** window, select the check box next to **Drain State**.
3. Click **Save** to exit the **Columns to Display** window.

The **Drain State** column can display the following information:

- **Draining until shutdown.** Appears when machines are in drain state until they're shut down.
- **Not draining.** Appears when machines aren't yet in drain state.



More information

For more information on Autoscale, see Citrix Autoscale in Tech Zone.

Schedule-based and load-based settings

October 16, 2023

How Autoscale power manages machines

Autoscale powers machines on and off based on the selected schedule. Autoscale lets you set multiple schedules that include specific days of the week and adjust the number of machines available during those times. If you expect a set of users to consume the machine resources at a specific time on specific days, Autoscale helps provide an optimized experience. Note that those machines will be powered on during the schedule, whether or not there are sessions running on them.

> **Note:**
>
> Autoscale supports any power-managed machine.

The schedule is based on the **time zone** of the delivery group. To change the time zone, you can change user settings in a delivery group. For more information, see Manage Delivery Groups.

Autoscale has two default schedules: *Weekdays* (Monday through Friday) and *Weekend* (Saturday and Sunday). By default, the **Weekdays** schedule keeps one machine powered on from 07:00 AM to 06:30 PM during peak times and none during off-peak times. The default capacity buffer is set to 10% during peak and off-peak times. By default, the **Weekend** schedule keeps no machines powered on.

> **Note:**
>
> Autoscale treats only those machines that are registered with the site as part of the available capacity in the calculations it makes. "Registered"means that the machine is available for use or already in use. Doing so ensures that only machines that can accept user sessions are included in the capacity for the delivery group.

User interfaces

There are three types of user interfaces to be aware of.

User interface for *single-session OS static delivery groups*:





Autoscale user interface for *single-session OS random delivery groups*:





Autoscale user interface for *multi-session OS delivery groups*:





Schedule-based settings

Autoscale schedule. Lets you add, edit, select, and delete schedules.

Days applied. Highlights the days you applied to the selected schedule. The remaining days are grayed out.

Edit. Lets you assign the machines against each hour or each half hour. You can assign the machines by numbers and by percentages.

> **Note:**
>
> - This option is available only in the Autoscale user interfaces for multi-session OS and single-session OS random delivery groups.
> - The histogram next to **Edit** plots the number or percentage of machines that are running in different time slots.
> - You can **assign machines** against each time slot by clicking **Edit** above **Peak times**. Depending on the option you selected from the menu in the **Machines to start** window, you

> can assign the machines by numbers or by percentages.
> - For multi-session OS delivery groups, you can set the minimum number of running machines separately in granular increments of 30 minutes during each day. For single-session OS random delivery groups, you can set the minimum number of running machines separately in granular increments of 60 minutes during each day.

To define your own schedules, follow these steps:

1. On the **Schedule and Peak Times** page of the **Manage Autoscale** window, click **Set schedules**.
2. In the **Edit Autoscale Schedules** window, select the days you want to apply to each schedule. You can also delete schedules as applicable.
3. Click **Done** to save the schedules and to return to the **Schedule and Peak Times** page.
4. Select the applicable schedule and configure it as needed.
5. Click **Apply** to exit the **Manage Autoscale** window or configure settings on other pages.

> **Important:**
>
> - Autoscale does not allow the same day to overlap in different schedules. For example, if you select Monday in schedule2 after selecting Monday in schedule1, Monday is automatically cleared in schedule1.
> - A schedule name is not case sensitive.
> - A schedule name must not be blank or contain only spaces.
> - Autoscale allows blank spaces between characters.
> - A schedule name must not contain the following characters: \ / ; : # . * ? = < > | [ ] ( ) { } ‘“‘.
> - Autoscale does not support duplicate schedule names. Enter a different name for each schedule.
> - Autoscale does not support empty schedules. This means that schedules without days selected are not saved.
>
> **Note:**
>
> The days included in the selected schedule are highlighted, while those not included are grayed out.

Load-based settings

Peak times. Lets you define the peak times for the days you applied in the selected schedule. You can do so by right-clicking the horizontal bar graph. After you define the peak times, the remaining, undefined times default to off-peak times. By **default**, the 7:00 AM to 7:00 PM time slot is defined as peak times for the days included in the selected schedule.

> **Important:**
>
> - For multi-session OS delivery groups, the peak times bar graph is used for the capacity buffer.
> - For single-session OS delivery groups, the peak times bar graph is used for the capacity buffer and controls the actions to be triggered after logoff and/or disconnection.
> - You can define the peak times for the days included in a schedule at a granular level of 30 minutes for both multi-session OS and single-session OS delivery groups. Alternatively, you can use the `New-BrokerPowerTimeScheme PowerShell` command instead. For more information, see Broker PowerShell SDK commands.

Capacity buffer. Lets you keep a buffer of powered-on machines. A lesser value decreases the cost. A greater value ensures an optimized user experience so that when launching sessions, users do not have to wait for additional machines to power on. By default, the capacity buffer is 10% for peak and off-peak times. If you set the capacity buffer to 0 (zero), users might have to wait for additional machines to power on when launching sessions. Autoscale lets you determine the capacity buffer separately for peak and off-peak times.

Miscellaneous settings

> **Tip:**
>
> - You can choose to configure the miscellaneous settings using the Broker PowerShell SDK. For more information, see Broker PowerShell SDK commands.
> - To understand the SDK commands associated with the when disconnected and when logged off settings, see `https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy`.

When disconnected. Lets you specify how long a disconnected, locked machine remains powered on after session disconnection before it is suspended or shut down. If a time value is specified, the machine is suspended or shut down when the specified disconnection time elapses, depending on the action you configured. By default, no action is assigned to disconnected machines. You can define actions separately for peak and off-peak times. To do so, click the down arrow and then select one of the following options from the menu:

- **No action**. If selected, the machine after session disconnection remains powered on. Autoscale does not act on it.
- **Suspend**. If selected, Autoscale pauses the machine without shutting it down when the specified disconnection time elapses. The following option becomes available after you select **Suspend**.

  - **When no reconnection in (minutes)**. Suspended machines remain available to disconnected users when they reconnect but are not available for new users. To make the machines available again to handle all workloads, shut them down. Specify the timeout, in minutes, after which Autoscale shuts them down.

- **Shut down**. If selected, Autoscale shuts down the machine when the specified disconnection time elapses.

> **Note:**
>
> This option is available only in the Autoscale user interfaces for single-session OS random and static delivery groups.

When logged off. Lets you specify how long a machine remains powered on after session logoff before it is suspended or shut down. If a time value is specified, the machine is suspended or shut down when the specified logoff time elapses, depending on the actions you configured. By default, no action is assigned to logged-off machines. You can define actions separately for peak and off-peak times. To do so, click the down arrow and then select one of the following options from the menu:

- **No action**. If selected, the machine after session logoff remains powered on. Autoscale does not act on it.
- **Suspend**. If selected, Autoscale pauses the machine without shutting it down when the specified logoff time elapses.
- **Shut down**. If selected, Autoscale shuts down the machine when the specified logoff time elapses.

> **Note:**
>
> This option is available only in the Autoscale user interface for single-session OS static delivery groups.

Power manage single-session OS machines transitioning to a different time period with disconnected sessions

> **Important:**
>
> - This enhancement applies only to single-session OS machines with disconnected sessions. It does not apply to single-session OS machines with logged off sessions.
> - For this enhancement to take effect, you need to enable Autoscale for the applicable delivery group. Otherwise, disconnect power policy actions are not triggered on period transition.

In earlier releases, a single-session OS machine transitioning to a time period where an action (disconnect action=”**Suspend**”or “**Shutdown**”) was required remained powered on. This scenario occurred

if the machine disconnected during a time period (peak or off-peak times) where no action (disconnect action="**Nothing**") was required.

Starting with this release, Autoscale suspends or powers off the machine when the specified disconnection time elapses, depending on the disconnect action configured for the destination time period.

For example, you configure the following power policies for a single-session OS delivery group:

- Set `PeakDisconnectAction` to "Nothing"
- Set `OffPeakDisconnectAction` to "Shutdown"
- Set 'OffPeakDisconnectTimeout'to "10"

> **Note:**
>
> For more information about the disconnect action power policy, see https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy and https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

In earlier releases, a single-session OS machine with a session disconnected during peak times remained powered on when it transitioned from peak to off-peak. Starting with this release, the `OffPeakDisconnectAction` and the `OffPeakDisconnectTimeout` policy actions are applied to the single-session OS machine on period transition. As a result, the machine is powered off 10 minutes after it transitions to off-peak.

In case you want to revert to the previous behavior (that is, take no action on machines that transition from peak to off-peak or off-peak to peak with disconnected sessions), do one of the following:

- Set the "LegacyPeakTransitionDisconnectedBehaviour"registry value to 1 (true; enables the previous behavior). By default, the value is 0 (false; triggers disconnect power policy actions on period transition).
  - Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Name: LegacyPeakTransitionDisconnectedBehaviour
  - Type: REG_DWORD
  - Data: 0x00000001 (1)
- Configure the setting by using the `Set-BrokerServiceConfigurationData` PowerShell command. For example:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

A machine must meet the following criteria before power policy actions can be applied to it on period transition:

- Has a disconnected session.
- Has no pending power actions.
- Belongs to a single-session OS delivery group that transitions to a different time period.
- Has a session that disconnects during a certain time period (peak or off-peak times) and transitions to a period where a power action is assigned.

How capacity buffer works

Capacity buffer is used to add spare capacity to the current demand to account for dynamic load increases. There are two scenarios to be aware of:

- For multi-session OS delivery groups, the capacity buffer is defined as a percentage of the total capacity of the delivery group in terms of load index. For more information about load index, see Load index.
- For single-session OS delivery groups, the capacity buffer is defined as a percentage of the total capacity of the delivery group in terms of the number of machines.

> **Note:**
>
> In scenarios where you restrict Autoscale to tagged machines, the capacity buffer is defined as a percentage of the total capacity of the tagged machines in the delivery group in terms of load index.

Autoscale lets you set the capacity buffer separately for peak and off-peak times. A lesser value in the capacity buffer field decreases the cost because Autoscale powers on less spare capacity. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. By default, the capacity buffer is 10%.

> **Important:**
>
> The capacity buffer results in machines being powered on when the total spare capacity drops to a level below "X"percent of the total capacity of the delivery group. Doing so reserves the required percentage of spare capacity.

Multi-session OS delivery groups

When are machines powered on?

> **Important:**
>
> If a schedule is selected, Autoscale powers on all machines configured to be powered on in the schedule. Autoscale keeps this specified number of machines powered on during the schedule,

> regardless of the load.

When the number of powered-on machines in the delivery group can no longer meet the buffer needed for honoring the buffer capacity in terms of load index, Autoscale powers on extra machines. For example, let's say your delivery group has 20 machines and 3 machines are scheduled to be powered on as part of schedule-based scaling with a capacity buffer of 20%. Eventually, 4 machines will be powered on when there is no load. This is because a 4 x 10k load index is needed as a buffer; therefore at least 4 machines need to be powered on. This case might occur during peak times, increased load on machines, new session launches, and when you add new machines to the delivery group. Note that Autoscale powers on only the machines that meet the following criteria:

- The machines are not in maintenance mode.
- The hypervisor on which the machines are running is not in maintenance mode.
- The machines are currently powered off.
- The machines have no pending power actions.

When are machines powered off?

> **Important:**
>
> - If a schedule is selected, Autoscale powers off the machines based on the schedule.
> - Autoscale does not power off the machines configured in the schedule to be powered on during the schedule.

When there are more than enough machines to support the targeted number of powered-on machines (including the buffer) for the delivery group, Autoscale powers off extra machines. This case might occur during off-peak times, decreased load on machines, and session logoffs, and when you remove machines from the delivery group. Autoscale powers off only the machines that meet the following criteria:

- The machines and the hypervisor on which the machines are running are not in maintenance mode.
- The machines are currently powered on.
- The machines are registered as available or waiting to register after start-up.
- The machines have no active sessions.
- The machines have no pending power actions.
- The machines satisfy the specified power-off delay. This means that the machines have been powered on for at least "X"minutes, where "X"is the power-off delay specified for the delivery group.

Example scenario

Suppose you have the following scenario:

- **Delivery group configuration**. The delivery group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Capacity buffer is set to 10%.
  - No machine is included in the selected schedule.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. More user sessions start.
4. User session load decreases because of session termination.
5. User session load decreases further until the session load is handled only by on-premises resources.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)
  - One machine (for example, M1) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10,000 (load index) x 10% (configured capacity buffer) equals 10,000. Therefore, one machine is powered on.
  - The load index value of the powered-on machine (M1) is at a baseline load (load index equals 0).
- The first user logs on
  - The session is directed to be hosted on machine M1.
  - The load index of the powered-on machine M1 increases and machine M1 is no longer at a baseline load.
  - Autoscale starts to power on an additional machine (M2) to meet the demand because of the configured capacity buffer.
  - The load index value of machine M2 is at a baseline load.
- Users increase load
  - The sessions are load-balanced across machines M1 and M2. As a result, the load index of the powered-on machines (M1 and M2) increases.
  - The total spare capacity is still at a level above 10,000 in terms of load index.

  - The load index value of machine M2 is no longer at a baseline load.

- More user sessions start

  - The sessions are load-balanced across machines (M1 and M2). As a result, the load index of the powered-on machines (M1 and M2) increases further.
  - When the total spare capacity drops to a level below 10,000 in terms of load index, Autoscale starts to power on an additional machine (M3) to meet the demand because of the configured capacity buffer.
  - The load index value of machine M3 is at a baseline load.

- Even more user sessions start

  - The sessions are load-balanced across machines (M1 to M3). As a result, the load index of the powered-on machines (M1 to M3) increases.
  - The total spare capacity is at a level above 10,000 in terms of load index.
  - The load index value of machine M3 is no longer at a baseline load.

- User session load decreases because of session termination

  - After users log off from their sessions or idle sessions time out, the freed-up capacity on machines M1 to M3 is reused to host sessions started by other users.
  - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the machines (for example, M3) into drain state. As a result, sessions started by other users are no longer directed to that machine unless new changes occur. For example, end-user load increases again or other machines become least loaded.

- User session load continues to decrease

  - After all sessions on machine M3 are terminated and the specified power-off delay times out, Autoscale powers off machine M3.
  - After more users terminate their sessions, the freed-up capacity on powered-on machines (M1 and M2) is reused to host sessions started by other users.
  - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the machines (for example, M2) into drain state. As a result, sessions started by other users are no longer directed to that machine.

- User session load continues to decrease until there are no sessions

  - After all sessions on machine M2 are terminated and the specified power-off delay times out, Autoscale powers off machine M2.
  - The load index value of the powered-on machine (M1) is at a baseline load. Autoscale does not put machine M1 into drain state because of the configured capacity buffer.

> **Note:**
>
> For multi-session OS delivery groups, all changes to the desktop are lost when users log off sessions. However, if configured, user-specific settings are roamed along with the user profile.

Single-session OS random delivery groups

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the total number of machines in the delivery group. By default, the capacity buffer is 10% of the total number of machines in the delivery group.

If the number of machines (including the capacity buffer) exceeds the total number of currently powered-on machines, additional machines are powered on to meet the demand. If the number of machines (including the capacity buffer) is less than the total number of currently powered-on machines, the excess machines are shut down or suspended, depending on the actions you configured.

Power policies

Configure policies to manage the power of the machines for different scenarios. For each scenario, you can specify the wait time (in minutes) and the action to take after the specified time ends. Power policies are applicable for Single-session OS random delivery groups and Single-session OS static delivery groups.



After disconnection, the following settings are applicable for both during peak times and during off-peak times:

- You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down.
- If you select the suspend action, configure an additional wait time to shut down the machine.

> **Note:**
>
> - During peak and off-peak times, the wait time for shutdown action must be greater than the wait time of suspend.
> - Suspended machines are accessible only to disconnected users when they reconnect. To make the suspended machines available for new users, shut them down.
> - If the time settings are incorrectly configured for suspend and shut down fields, the **Save** option is disabled and a red dot also appears next to the navigation items indicating setting errors.



For example

- If you set the wait time to 12 minutes and choose the first action to be no action, then after the end of 12 minutes, the machine will continue to be in powered on state.
- If you set the wait time to 15 minutes and choose the first action to be suspend and the second wait time to be 20 minutes, after the end of 15 minutes, the machine will be suspended. After the end of the second wait time, the machine will be shut down.
- If you set the wait time to 18 minutes and choose the first action to be shut down, then after the end of 18 minutes, the machine will be shut down.

Example scenario

Suppose you have the following scenario:

- **Delivery group configuration**. The delivery group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Capacity buffer is set to 10%.

  - No machine is included in the selected schedule.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. More user sessions start.
4. User session load decreases because of session termination.
5. User session load decreases further until the session load is handled only by on-premises resources.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)
  - One machine (M1) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10% (configured capacity buffer) equals 1. Therefore, one machine is powered on.
- A first user logs on
  - The first time a user logs on to use a desktop, the user is assigned a desktop from a pool of desktops hosted on powered-on machines. In this case, the user is assigned a desktop from machine M1.
  - Autoscale starts to power on an additional machine (M2) to meet the demand because of the configured capacity buffer.
- A second user logs on
  - The user is assigned a desktop from machine M2.
  - Autoscale starts to power on an additional machine (M3) to meet the demand because of the configured capacity buffer.
- A third user logs on
  - The user is assigned a desktop from machine M3.
  - Autoscale starts to power on an additional machine (M4) to meet the demand because of the configured capacity buffer.
- A user logs off
  - After a user logs off or the user's desktop times out, the freed-up capacity (for example, M3) is available as buffer. As a result, Autoscale starts to power off machine M4 because the capacity buffer is configured as 10%.
- More users log off until there are no users

- After more users log off, Autoscale powers off machines (for example, M2 or M3).
- Even though there are no users left, Autoscale does not power off the remaining one machine (for example, M1) because that machine is reserved as a spare capacity.

> **Note:**
>
> For single-session OS random delivery groups, all changes to the desktop are lost when users log off sessions. However, if configured, user-specific settings are roamed along with the user profile.

Single-session OS static delivery groups

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of unassigned machines powered on based on the total number of unassigned machines in the delivery group. By default, the capacity buffer is 10% of the total number of unassigned machines in the delivery group.

> **Important:**
>
> After all machines in the delivery group are assigned, the capacity buffer does not play a role in powering machines on or off.

If the number of machines (including the capacity buffer) exceeds the total number of currently powered-on machines, additional, unassigned machines are powered on to meet the demand. If the number of machines (including the capacity buffer) is less than the total number of currently powered-on machines, excess machines are powered off or suspended, depending on the actions you configured.

For single-session OS static delivery groups, Autoscale:

- Powers assigned machines on during peak times and off during off-peak times only when the `AutomaticPowerOnForAssigned` property of the applicable single-session OS delivery group is set to true.
- Automatically powers on a machine during peak times if it is powered off and the `AutomaticPowerOnForAssignedDuringPeak` property of the delivery group to which it belongs is set to true.

To understand how capacity buffer works with assigned machines, consider the following:

- The capacity buffer works only when the delivery group has one or more unassigned machines.
- If the delivery group has no unassigned machines (all machines in the delivery group are assigned), the capacity buffer does not play a role in powering machines on or off.
- The `AutomaticPowerOnForAssignedDuringPeak` property determines whether assigned machines are powered on during peak times. If it is set to true, Autoscale keeps the

machines powered on during peak times. Autoscale will also power them on even if they are powered off.

Power policies

Configure policies to manage the power of the machines for different scenarios. For each scenario, you can specify the wait time (in minutes) and the action to take after the specified time ends. Power policies is applicable for Single-session OS random delivery groups and Single-session OS static delivery groups.



For **After disconnection** and **After logoff**, the following settings are applicable for both, during peak times and during off-peak times:
You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down.

If no user logs on after machine is powered on by Autoscale, the following settings are applicable only during peak times:
You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down during peak times.

Example scenario

Suppose you have the following scenario:

- **Delivery group configuration**. The delivery group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Machines M1 to M3 are assigned, and machines M4 to M10 are unassigned.
  - Capacity buffer set to 10% for peak and off-peak times.
  - According to the selected schedule, Autoscale power manages machines between 09:00 AM and 06:00 PM.

See below for details about how Autoscale works in the scenario above.

- Start of schedule –09:00 AM
  - Autoscale powers on machines M1 to M3.
  - Autoscale powers on an additional machine (for example, M4) because of the configured capacity buffer. Machine M4 is unassigned.
- A first user logs on
  - The first time a user logs on to use a desktop, the user is assigned a desktop from a pool of desktops hosted on unassigned powered-on machines. In this case, the user is assigned a desktop from machine M4. Subsequent logons from that user connect to the same desktop that was assigned on first use.
  - Autoscale starts to power on an additional machine (for example, M5) to meet the demand because of the configured capacity buffer.
- A second user logs on
  - The user is assigned a desktop from the unassigned powered-on machines. In this case, the user is assigned a desktop from machine M5. Subsequent logons from that user connect to the same desktop that was assigned on first use.
  - Autoscale starts to power on an additional machine (for example, M6) to meet the demand because of the configured capacity buffer.
- Users log off
  - As users log off from their desktops or the desktops time out, Autoscale keeps the machines M1 to M5 powered on during 09:00 AM –06:00 PM. When those users log on the next time, they connect to the same desktop that was assigned on first use.
  - The unassigned machine M6 is waiting to serve a desktop to an incoming, unassigned user.
- End of schedule –06:00 PM

- At 06:00 PM, Autoscale powers off machines M1 to M5.
- Autoscale keeps the unassigned machine M6 powered on because of the configured capacity buffer. That machine is waiting to serve a desktop to an incoming, unassigned user.
- In the delivery group, machines M6 to M10 are unassigned machines.

Dynamic session timeouts

June 9, 2023

This feature lets you configure disconnected and idle session timeouts for your peak and off-peak usage times to achieve faster machine draining and cost savings. This feature applies to single-session and multi-session OS machines. A VDA reports idle times for sessions that have been idle for more than 10 minutes, so dynamic session timeouts will not be able to disconnect idle sessions within 10 minutes of being idle. A lesser value removes lingering sessions sooner, thus reducing costs.



Note:

- This feature is always available for multi-session OS delivery groups.
- For single-session OS delivery groups, this feature applies to VDAs of version 2206 CR or later, or 2203 LTSR CU3 or later. Ensure that those VDAs have registered with Citrix Cloud at least once. When unavailable, the following user interface appears:



- Autoscale dynamic timeouts are for cost savings. If used for security purposes, the configured timeouts might conflict with your GPO or Manage console policies. When a conflict occurs, the shorter timeout prevails.

Idle session timeout. Enables or disables a timer that specifies how long an uninterrupted user connection is maintained if there is no user input. When the timer expires, the session is placed in the disconnected state and the **Disconnected session timeout** applies. If the **Disconnected session timeout** is disabled, the session is not logged off.

Important:

- If you specify a value less than or equal to 10 minutes (600 seconds), Autoscale disconnects the relevant sessions after they have been idle for 10 minutes. This is because Autoscale relies on session idle times that VDAs report. VDAs report idle times only for sessions that have been idle for more than 10 minutes.
- An idle session will still be placed into a disconnected state if the user interacts with it within the last 5 minutes of reaching the idle session timeout.

Disconnected session timeout. Enables or disables a timer that specifies how long a disconnected desktop remains locked before the session is logged off. If enabled, the disconnected session is logged off when the timer expires.

Autoscaling tagged machines (cloud burst)

February 20, 2023

Note:

> This feature was formerly Restrict Autoscale.

Introduction

Autoscale provides the flexibility to power manage only a subset of machines in a delivery group. To achieve this, apply a tag to one or more machines and then configure Autoscale to power manage only tagged machines.

This feature can be useful in cloud bursting use cases, where you want to use on-premises resources (or reserved public cloud instances) to handle workloads before cloud-based resources address additional demand (that is, burst workloads). To let on-premises machines (or reserved instances) address workloads first, you must use tag restriction along with zone preference.

Tag restriction specifies machines to be power managed by Autoscale. Zone preference specifies machines in the preferred zone to handle user launch requests. For more information, see Tags and Zone preference.

To autoscale certain tagged machines, you can use the Manage console or PowerShell.

Use the Manage console to autoscale certain tagged machines

To autoscale certain tagged machines, complete the following steps:

1. Create a tag and apply that tag to the applicable machines in the delivery group. For more information, see Manage tags and tag restrictions.
2. Select the delivery group and then open the **Manage Autoscale** wizard.
3. On the **Autoscaling Tagged Machines** page, select **Enable Autoscale for machines with tag**, select a tag from the list, and then click **Apply** to save your changes.

   User interface for single-session OS *static* and *random* delivery groups:



User interface for *multi-session OS delivery groups*:



> **Warning:**
>
> - Autoscaling machines with a specific tag might cause the histogram to update automatically to reflect the number of machines per the tag. On the **Schedule and Peak Times** page, you can manually assign machines against each time slot if needed.
> - You cannot delete a tag that is being used on tagged machines. To delete the tag, you must first remove the tag restriction.

After you apply the tag restriction, you might want to remove it from the delivery group later. To do so, go to the **Manage Autoscale > Autoscaling Tagged Machines** page and then clear **Enable Autoscale for machines with tag**.

> **Warning:**
>
> - If you remove the tag from the applicable machines without clearing **Enable Autoscale for machines with tag**, you might receive a warning when you open the **Manage Autoscale** wizard. Removing the tag from the machines can leave no machines for Autoscale to manage because the tag you specified in Autoscale has become invalid. To resolve the warning,

> go to the **Autoscaling Tagged Machines** page, remove the invalid tag, and then click **Apply** to save your changes.

Control when Autoscale powers on resources

You can also control when Autoscale starts powering on tagged machines based on the usage of untagged machines. This helps you further optimize the consumption of your tagged or public cloud workloads.

To do this, complete the following steps:

1. On the **Autoscaling Tagged Machines** page, select **Control when Autoscale starts powering on tagged machines**.
2. Enter the percentage amount of untagged machine usage you want to reach for both peak times and off-peak times and then click **Apply**. Supported values: 0–100.



Tip:

The percentage controls when Autoscale starts powering on tagged machines. When the percentage falls below the threshold (default, 10%), Autoscale starts powering on tagged machines. When the percentage exceeds the threshold, Autoscale goes into power-off mode. When entering the percentage, consider two scenarios:

- For single-session OS delivery groups: The value is defined as a percentage of the total number of untagged machines in idle state. Example: You have 10 untagged single-session OS machines. When only one is left without a session, Autoscale starts powering on a tagged machine.
- For multi-session OS delivery groups: The value is defined as a percentage of the total capacity (in terms of load index) of available untagged machines. Example: You have 10 un-

> tagged multi-session OS machines. When they are 90% loaded, Autoscale starts powering on a tagged machine.

Use PowerShell to autoscale certain tagged machines

To use the PowerShell SDK directly, complete the following steps:

1. **Create a tag.** Use the New-Brokertag PowerShell command to create a tag.
   - For example: `$managed = New-BrokerTag Managed`. In this case, the tag is named "Managed."For more information about the New-Brokertag PowerShell command, see https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Apply the tag to machines**. Use the Get-Brokermachine PowerShell command to apply the tag to machines in a catalog that you want Autoscale to power manage.
   - For example: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. In this case, the catalog is named "cloud."
   - For more information about the Get-Brokermachine PowerShell command, see https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Note:**
   >
   > You might add new machines to the catalog after applying the tag. The tag is *NOT* automatically applied to those new machines.

3. **Add tagged machines to the delivery group that you want Autoscale to power manage.** Use the Get-BrokerDesktopGroup PowerShell command to add a tag restriction to the delivery group that contains the machines (in other words, "restrict launches to machines with tag X").
   - For example: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In this case, the UID of the Delivery Group is 1.
   - For more information about the Get-BrokerDesktopGroup PowerShell command, see https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

After you apply the tag restriction, you might want to remove it from the delivery group later. To do so, use the Get-BrokerDesktopGroup PowerShell command.

Example: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscal $null`. In this case, the UID of the delivery group is 1.

> **Note:**
>
> Untagged machines restart automatically after users power them off. This behavior ensures that they become available to handle workloads sooner. This can be enabled or disabled on a per desktop group using the `Set-BrokerDesktopGroup`'s `AutomaticRestartForUntaggedMachines` property. For more information, see https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

Example scenario

Suppose you have the following scenario:

- **Machine catalog configuration**. There are two machine catalogs (C1 and C2).
  - Catalog C1 contains 5 machines (M1 to M5) that are local in the on-premises deployments.
  - Catalog C2 contains 5 machines (M6 to M10) that are remote in the cloud deployments.
- **Tag restriction**. A tag named "Cloud"is created and applied to machines M6 to M10 in catalog C2.
- **Zone configuration**. Two zones (Z1 and Z2) are created.
  - Zone Z1 containing catalog C1 corresponds to the on-premises deployments.
  - Zone Z2 containing catalog C2 corresponds to the cloud deployments.
- **Delivery group configuration**
  - The delivery group contains 10 machines (M1 to M10), 5 machines from catalogs C1 (M1 to M5) and 5 from catalog C2 (M6 to M10).
  - Machines M1 to M5 are powered on manually and remain powered on throughout the schedule.
- **Autoscale configuration**
  - Capacity buffer is set to 10%.
  - Autoscale power manages only machines with the tag "Cloud."In this case, Autoscale power manages cloud machines M6 to M10.
- **Published application or desktop configuration**. Zone preferences are configured for the published desktops (for example), where Zone Z1 is preferred over Zone Z2 for a user launch request.
  - Zone Z1 is configured as the preferred zone (home zone) for the published desktops.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. User sessions increase further until all available on-premises machines are consumed.
4. More user sessions start.
5. User session decreases because of session termination.
6. User session decreases further until the session load is handled only by on-premises machines.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)
  - The on-premises machines M1 to M5 are all powered on.
  - One machine in the cloud (for example, M6) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10,000 (load index) x 10% (configured capacity buffer) equals 10,000. Therefore, one machine is powered on.
  - The load index value of all the powered-on machines (M1 to M6) is at a baseline load (load index equals 0).
- Users log on
  - The sessions are directed to be hosted on machines M1 to M5 through the configured zone preference and are load-balanced across these on-premises machines.
  - The load index value of the powered-on machines (M1 to M5) increases.
  - The load index value of the powered-on machine M6 is at a baseline load.
- Users increase load, consuming all on-premises resources
  - The sessions are directed to be hosted on machine M1 to M5 through the configured zone preference and are load-balanced across these on-premises machines.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of the powered-on machine M6 remains at a baseline load.
- One more user logs on
  - The session overflows the zone preference and is directed to be hosted on cloud machine M6.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of the powered-on machine M6 increases and is no longer at a baseline load. When the total spare capacity drops to a level below 10,000 in terms of load index, Autoscale starts to power on an additional machine (M7) to meet the demand because of the configured capacity buffer. Note that it might take some time to power on machine M7. So there might be a delay until machine M7 is ready.
- More users log on

  - The sessions are directed to be hosted on machine M6.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of the powered-on machine M6 increases further, but the total spare capacity is at a level above 10,000 in terms of load index.
  - The load index value of the powered-on machine M7 remains at a baseline load.

- Even more users log on
  - After machine M7 is ready, the sessions are directed to be hosted on machines M6 and M7 and are load-balanced across these machines.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of machine M7 is no longer at a baseline load.
  - The load index value of the powered-on machines (M6 and M7) increases.
  - The total spare capacity is still at a level above 10,000 in terms of load index.
- User session load decreases because of session termination
  - After users log off from their sessions or idle sessions time out, the freed-up capacity on machines M1 to M7 is reused to host sessions started by other users.
  - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the cloud machines (M6 to M7) into drain state. As a result, sessions started by other users are no longer directed to that machine (for example, M7) unless new changes occur; for example, user load increases again or other cloud machines become least loaded.
- User session load decreases further until one or more cloud machines are no longer needed
  - After all sessions on machine M7 are terminated and the specified power-off delay times out, Autoscale powers off machine M7.
  - The load index value of all the powered-on machines (M1 to M5) might drop to a level below 10,000.
  - The load index value of the powered-on machine (M6) decreases.
- User session decreases further until no cloud machines are needed.
  - Even though there are no user sessions on machine M6, Autoscale does not power it off because it is reserved as a spare capacity.
  - Autoscale keeps the remaining cloud machine M6 powered on because of the configured capacity buffer. That machine is waiting to serve a desktop to an incoming user.
  - Sessions are not directed to be hosted on machine M6 as long as the on-premises machines have available capacity.

Dynamically provision machines

November 1, 2022

Autoscale provides the capability to create machines and delete them dynamically. You can leverage the capability by using a PowerShell script. The script helps you dynamically scale up or down the number of machines in the delivery group based on the current load conditions.

The script offers the following benefits (and more):

- **Reducing storage costs**. Different from Autoscale, which helps reduce your computing costs, the script provides a more cost-effective solution to provision machines.
- **Effectively handling load changes**. The script helps you handle load changes by automatically scaling up or down the number of machines based on the current delivery group load.

Download the script

The PowerShell script is available at https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs.

How the script works

> **Important:**
>
> - You cannot specify a machine catalog in more than one delivery group that is to be managed by the script. In other words, if multiple delivery groups share the same machine catalog, the script does not work with any of those delivery groups.
> - You cannot concurrently run the script for the same delivery group from multiple locations.

The script works at a delivery group level. It measures the load (in terms of load index) and then determines whether to create or delete machines.

Machines created through this script are uniquely tagged (through the `ScriptTag` parameter) so that they can be identified later. Creating or deleting machines is based on:

- **Maximum percentage load of a delivery group**. Specifies the maximum level at which to create machines for Autoscale to address extra loads. When this threshold is exceeded, machines are created in batches to ensure that the current load decreases to or below the threshold.
- **Minimum percentage load of a delivery group**. Specifies the minimum level at which to delete machines created through this script that have no active sessions. When this threshold is exceeded, machines created through this script that have no active sessions are deleted.

This script is intended to monitor across a delivery group and to create or delete machines when the trigger criterion is met. It executes on a per-run basis. This means that you need to run the script on a regular basis so that it can function as intended. We recommend that you run the script at a minimum interval of five minutes. Doing so improves overall responsiveness.

The script relies on the following parameters to work:

Parameter	Type	Default value	Description
DeliveryGroupName	String	X	Name of the delivery group to be monitored to determine the current load. You can provide a semicolon-separated list of names. For example: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`.
XdProfileName	String	X	Name of the profile to use for authenticating to remote servers. For details about authenticating to remote servers using this parameter, see Authentication API.
HighWatermark	Integer	80	Maximum percentage load (in terms of load index) at which to create machines for Autoscale to address extra loads.

Parameter	Type	Default value	Description
LowWatermark	Integer	15	Minimum percentage load (in terms of load index) at which to delete machines created through this script that have no active sessions.
MachineCatalogName	String	X	Name of the machine catalog where machines are to be created.
MaximumCreatedMachines	Integer	-1	Maximum amount of machines that can be created in a specified delivery group. If the value is equal to or less than 0, the script does not process this parameter.
ScriptTag	String	AutoscaledScripted	Tag that applies to machines created through the script.
EventLogSource	String	X	Source name that appears in Windows Event Viewer.

> **Note:**
>
> An "X"indicates that no default value is specified for that parameter.

By default, the script requires all parameters (except the `ScriptTag` parameter) the first time it runs. On subsequent runs, only the `DeliveryGroupName` and the `XdProfileName` parameters are required. Optionally, you can choose to update the minimum and maximum percentage loads.

Note that you must specify a single delivery group the first time you run the script. For example, the script does *not* work if you use the following PowerShell command to specify two delivery groups the first time you run the script:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;`


```
dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -
MachineCatalogName 'cat1'\
```

Instead, first specify a single delivery group (in this example, dg1) using the following command:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1 '-XdProfileName profile -LowWatermark 20 -HighWatermark 70 - MachineCatalogName 'cat1'\`

Then, use the following command to run the script for the second delivery group (in this example, dg 2):

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

Prerequisites

To run the script, make sure that these prerequisites are met:

- The machine resides within the same domain where machines are being created.
- Remote PowerShell SDK is installed on that machine. For more information about the Remote PowerShell SDK, see SDKs and APIs.
- Other prerequisites:
  - A delivery group to monitor
  - A machine catalog created through Machine Creation Services (MCS) that has an associated provisioning scheme (template)
  - An identity pool that is associated with the provisioning scheme
  - An event log source to be created so that the script can write information to the Windows Event Log
  - A secure client that allows you to authenticate to remote servers

Permissions, recommendations, and notices

When you run the script, keep the following in mind:

- To authenticate to remote servers using the `XdProfileName` parameter, you need to define an authentication profile by using an API access secure client, created in the Citrix Cloud console. For details, see Authentication API.
- You must have permissions to create and delete machine accounts in Active Directory.
- We recommend that you automate the PowerShell script with Windows Task Scheduler. For details, see Create an automated task using Windows Task Scheduler.

- If you want the script to write information (for example, failures and actions) to the Windows Event Log, you need to first specify a source name using the `New-EventLog` cmdlet. For example, `New-EventLog -LogName Application –Source <sourceName>`. You can then view the events in the **Application** pane of Windows Event Viewer.
- If errors occurred during execution of the script, execute the script manually and then troubleshoot problems by performing script checks.

Authentication API

Before you run the script, you need to define an authentication profile by using an API access secure client. You must create a secure client using the same account under which the script will run.

The secure client must have the following permissions:

- Create and delete machines using MCS.
- Edit machine catalogs (to add and remove machines).
- Edit delivery groups (to add and remove machines).

When you create a secure client, make sure that your account has the permissions above because the secure client automatically inherits the permissions from your current account.

To create a secure client, complete these steps:

1. Sign in to Citrix Cloud and then navigate to **Identity and Access Management > API Access**.
2. Type the name for your secure client and then click **Create Client**.

To authenticate to remote servers, use the `Set-XDCredentials` PowerShell command. For example:

- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

Create an automated task using Windows Task Scheduler

You can automate the PowerShell script with Windows Task Scheduler. Doing so lets the script run automatically at certain intervals or when certain conditions are met. To execute this script with Windows Task Scheduler, make sure to select **Do not start a new instance** on the **Create Task > Settings** tab. Doing so prevents the Windows Task Scheduler from running a new instance of the script if the script is already running.

Script execution example

See below for an example of executing the script. Note that the script file is invoked multiple times. In this example, to simulate the load, one session is launched and then terminated.



Troubleshooting checklist for the script

The script writes information (for example, errors and actions) to the Windows Event Log. The information helps you troubleshoot issues you experience when executing the script. It might be helpful to keep the following troubleshooting checklist in mind:

- Failure to communicate with remote servers. Possible actions:
  - Verify your connection to the server.
  - Verify that the API key you use is valid.
- Failure to create machines. Possible actions:
  - Verify that the user account running the script has sufficient permissions to create user accounts in the domain.
  - Verify that the user who created the API key has sufficient permissions to use MCS to provision machines.
  - Verify the validity of the machine catalog (that is, its image still exists and is in good state).
- Failure to add machines to a machine catalog or a delivery group. Possible action:
  - Verify that the user who created the API key has sufficient permissions to add and remove machines to and from machine catalogs and delivery groups.

User logoff notifications (formerly force user logoff)

May 17, 2023

> **Important:**
>
> This feature is available only in the Autoscale user interface for multi-session app-based delivery groups.

To better achieve cost savings, Autoscale lets you force log off lingering sessions. It does so by letting you send a custom notification to the users and specify a grace period after which the sessions are force logged off. This is done only for machines in drain state and not for all powered-on machines. To avoid potential data loss caused by forcing user logoffs, you can instead configure this feature to only send logoff reminders without forcing user logoff.

You have the following options:

- **Notify and force user logoff**
- **Send logoff reminders without forcing user logoff**
- **Neither notify nor force user logoff**

Notify and force user logoff

If selected, Autoscale logs off users from their sessions after the times specified below.



Enable force logoff during peak times. If selected, Autoscale logs off those users from their sessions during peak times when the specified time elapses.

Enable force logoff during off-peak times. If selected, Autoscale logs off those users from their sessions during off-peak times when the specified time elapses.

Display notification after machine enters drain state. Lets you send notifications to users after their machine enters drain state.

- **Notification title**. Lets you specify a title of the notification to be sent to users. Example: `A forced logoff has been initiated`.
- **Notification message**. Lets you specify the content of the notification to be sent to users. You can use %s% or %m% as variables to indicate the specified time in the message. To express the time in seconds, use %s%. To express the time in minutes, use %m%. Example: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine`.

Send logoff reminders without forcing user logoff

If selected, users will receive a reminder to log off from their machine after it has entered drain state. This reminder can be configured to be sent at the interval specified below.



Remind users during peak times. If selected, users receive a reminder to log off from their sessions during peak times every X minutes (X denotes the specified time).

Remind users during off-peak times. If selected, users receive a reminder to log off from their sessions during off-peak times every X minutes (X denotes the specified time).

Logoff reminder. Lets you configure the reminder sent to users after their machine enters drain state.

- **Reminder title**. Lets you specify a title for the reminder to be sent to users. Example: `Please log off from your session`.
- **Reminder message**. Lets you specify a message to be sent to users. Example: `Please log off from your session and log back on to save costs`.

Neither notify nor force user logoff

If selected, Autoscale neither forces users to log off from machines in drain state nor notifies users to manually switch to a different machine.

Considerations

If the machine is already in drain state, consider the following when changing settings:

- If you change the setting from **Send logoff reminders without forcing user logoff** to **Notify and force user logoff**, the new setting takes effect immediately.
- If you change the setting from **Notify and force user logoff** to **Send logoff reminders without forcing user logoff**, the new setting does not take effect until the next time the machine enters drain state. The user is still forced to log off.

Analyze the effectiveness of Autoscale settings

February 7, 2024

To use this feature, enable the toggle **Autoscale Insights** in **DaaS > Home > Preview features**. It might take about 15 minutes for **Autoscale Insights** to show up after enabling it.

You can analyze the effectiveness of the Autoscale settings based on machine usage from the previous week. Through the analysis, you can gain these insights into the effectiveness of Autoscale settings:

- Identify financial waste resulting from over-provisioning.
- Determine whether the user experience is negatively impacted due to under-provisioning.
- Ensure that the capacity provisioned is properly aligned with the machine usage.

To achieve this goal, follow these steps:

1. Select an Autoscale-enabled delivery group.
2. In the bottom pane, click the **Autoscale Insights** tab.

   The following graph appears, showing the comparison between machine usage data from the previous week and the number of machines to be powered on based on Autoscale settings.



* The red vertical line identifies the current time.

The following table provides descriptions of the metrics shown in this graph.

Metric	Description
Autoscale-managed count	Total number of machines managed by Autoscale. Autoscale-managed count = Total number of machines in the delivery group – Number of machines in maintenance mode – Number of machines not tagged for Autoscale (If tagged Autoscale feature is enabled).
Autoscale powered-on count	Total number of machines powered on by Autoscale. Autoscale powered-on count = Schedule-based machine count + Load-based machine count.
Historical usage	Number of machines that were delivered to users.
Schedule-based	Number of machines that are powered on based on the Autoscale schedule-based settings (**Note:** Schedule-based settings don't apply to delivery groups of the static single-session OS type).
Load-based	Number of machines that are powered on based on the Autoscale load-based settings.

3. To check the effectiveness of Autoscale settings at a specific time slot, hover your mouse over that slot on the graph. An information box appears, showing the comparison results and detailed machine counts:

- **Not cost effective**. The historical usage is less than 90% of the Autoscale settings (Autoscale powered-on count). As a result, wasted capacity might exist.



- **Poor user experience**. The historical usage is more than 110% of the Autoscale settings (Autoscale powered-on count). As a result, users might experience longer wait times for machines to power on.



- **Good balance between user experience and cost**. The difference between the historical usage and the Autoscale settings (Autoscale powered-on count) is less than 10%. The Autoscale settings are aligned with the historical usage.



- **No historical data available**. No historical data is available. Possible causes include that Autoscale was enabled for the delivery group less than a week ago.



4. To highlight a date range based on an Autoscale schedule, select the schedule from the **View by** field.
5. Based on your analysis, adjust the Autoscale settings. For more information, see Schedule-based and load-based settings.

Broker PowerShell SDK commands

November 22, 2022

You can configure Autoscale for delivery groups using the Broker PowerShell SDK. To configure Autoscale using PowerShell commands, you must use Remote PowerShell SDK version 7.21.0.12 or later. For more information about the Remote PowerShell SDK, see SDKs and APIs.

Set-BrokerDesktopGroup

Disables or enables an existing BrokerDesktopGroup or alters its settings. For more information about this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

Examples

See the following examples for details about how to use the PowerShell cmdlets.

Enable Autoscale

- Suppose you want to enable Autoscale for the delivery group whose name is “MyDesktop.”Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled $true
  ```

Configure the capacity buffer separately for peak and off-peak times

- Suppose you want to set the capacity buffer to 20% for peak times and 10% for off-peak times for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

Configure the **when disconnected timeout** setting

- Suppose you want to set the **when disconnected timeout** value to 60 minutes for peak times and 30 minutes for off-peak times for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

Configure the **when logged off timeout** setting

- Suppose you want to set the **when logged off timeout** value to 60 minutes for peak times and 30 minutes for off-peak times for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

Configure the **power-off delay** setting

- Suppose you want to set the power-off delay to 15 minutes for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15`

Configure a time period during which the power-off delay does not take effect

- Suppose you want the power-off delay to take effect until 30 minutes have elapsed for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh 30.`

Configure the **machine instance cost** setting

- Suppose you want to set the machine instance cost per hour to 0.2 dollars for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2`

New-BrokerPowerTimeScheme

Creates a BrokerPowerTimeScheme for a delivery group. For more information, see https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

Example

Suppose you want to create a power time scheme for a delivery group whose UID value is 3. The new scheme covers the weekend, Monday, and Tuesday. The 8:00 AM to 6:30 PM time slot is defined as peak times for the days included in the scheme. For peak times, the pool size (the number of machines kept powered on) is 20. For off-peak times, it is 5. You can use the `Set-BrokerDesktopGroup` PowerShell command. For example:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

Parameters for dynamic session timeouts

The following Broker PowerShell SDK cmdlets have been extended for dynamic session timeouts by supporting multiple new parameters:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Those parameters include:

- **DisconnectPeakIdleSessionAfterSeconds** –Represents the time in seconds after which an idle session is disconnected during peak time. This property has a default value of 0, which indicates the disablement of its associated behavior during peak time. A value greater than 0 enables its behavior for the delivery group during peak time only.
- **DisconnectOffPeakIdleSessionAfterSeconds** - Represents the time in seconds after which an idle session is disconnected during off-peak hours. The default value of this property is 0, which indicates the disablement of its associated behavior during off-peak. A value greater than 0 enables its associated behavior for the delivery group during off-peak hours only.

- **LogoffPeakDisconnectedSessionAfterSeconds** - Represents the time in seconds after which a disconnected session is terminated during peak time. The default value of this property is 0, which indicates the disablement of its associated behavior during peak time. A value greater than 0 enables its associated behavior for the delivery group during peak time only.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - Represents the time in seconds after which a disconnected session is terminated during off-peak hours. The default value of this property is 0, which indicates the disablement of its associated behavior during off-peak. A value greater than 0 enables its associated behavior for the delivery group during off-peak hours only.

Example

Suppose you want to set the idle session timeout to 3,600 seconds during peak times for a delivery group whose name is "MyDesktop."Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

- ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte
  3600
  ```

Doing that disconnects sessions that have been idle for more than 1 hour in off-peak for the desktop group whose name is "MyDesktop."

Cloud Health Check

June 12, 2024

> **Note:**
>
> Cloud Health Check is integrated into Citrix DaaS. The integration is available as the Run Health Check action in the Full Configuration management interface. For more information, see Troubleshoot VDA registration and session launch issues.

Cloud Health Check allows you to run checks that gauge the health and availability of the site and its components. You can run health checks for Virtual Delivery Agents (VDAs), StoreFront servers, and Profile Management. VDA health checks identify possible causes for common VDA registration and session launch issues.

If issues are present during the checks, Cloud Health Check provides a detailed report and the actions to fix the issues. Each time Cloud Health Check starts, it checks for the latest version of scripts on the Content Delivery Network (CDN) and automatically downloads the scripts if they do not exist on the


  ```

local machine. Cloud Health Check always chooses the latest local version of scripts to run health checks.

> **Note:**
>
> Cloud Health Check does not update every time it runs.

In a Citrix Cloud environment, run Cloud Health Check from a domain-joined machine to run checks on one or more VDAs or StoreFront servers.

> **Note:**
>
> You cannot install or run Cloud Health Check on a Cloud Connector.

The log for the Cloud Health Check application is stored in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. You can use this file for troubleshooting.

View an introduction to Cloud Health Check.


View when to use Cloud Health Check.

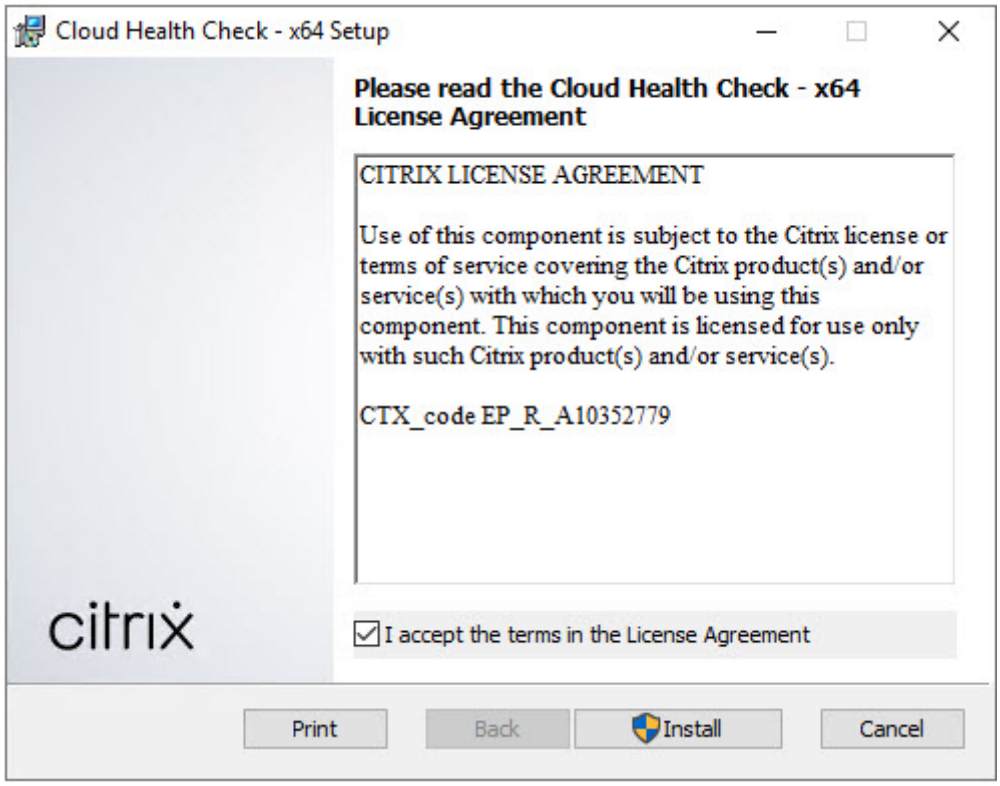
### Installation

To prepare your environment for installation of Cloud Health Check, you must have a domain-joined Windows machine.

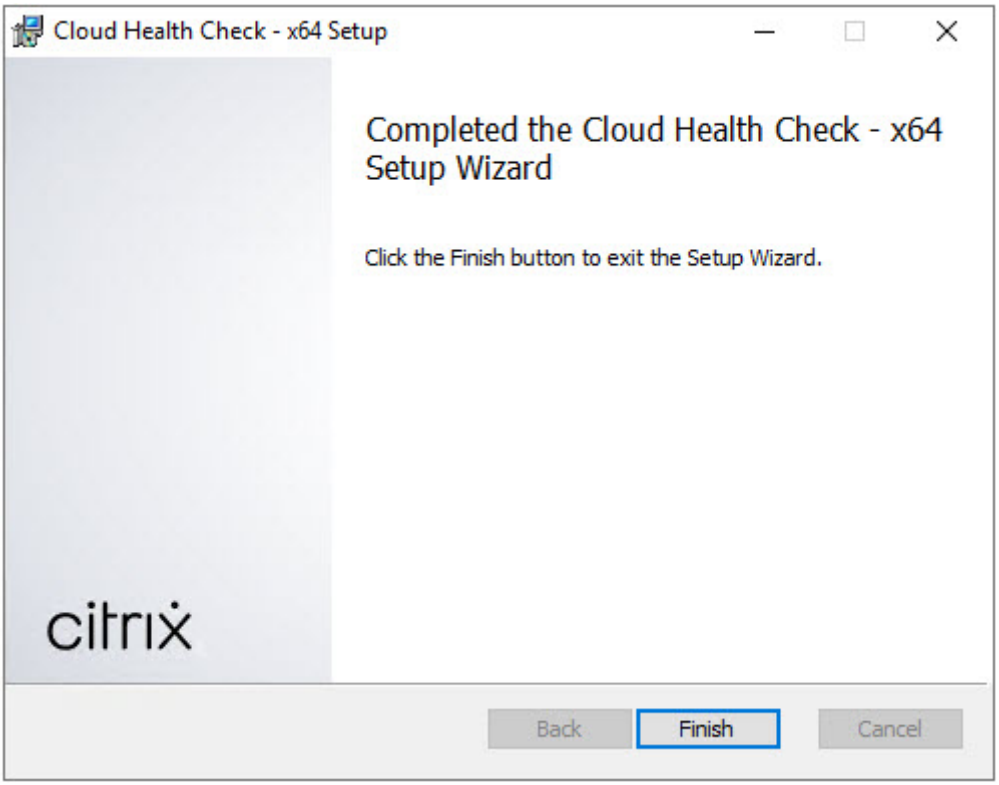
> **Note:**
>
> You cannot install or run Cloud Health Check on Cloud Connector.

1. On the domain-joined machine, download the Cloud Health Check installer.
2. Double-click the CloudHealthCheckInstaller_x64.msi file.
3. Click the box to accept the terms.
4. Click Install.




5. After installation has completed, click **Finish**.



### Permissions and requirements

Permissions:

- To run health checks:
  - You must be a member of the domain users group.
  - You must be a full administrator or have a custom role with read-only and **Run Environment Tests** permissions for the site.
  - Set the script execution policy to at least `RemoteSigned` to allow the scripts to run. For example: `Set-ExecutionPolicy RemoteSigned`. **Note:** other script execution permissions can work as well.
- Use **Run as administrator** when launching Cloud Health Check.

For each VDA or StoreFront machine that you run health checks on:

- The OS must be 64-bit.
- Cloud Health Check must be able to communicate with the machine.
- File and printer sharing must be turned on.
- PSRemoting and WinRM must be enabled. The machine must also be running PowerShell 3.0 or later.
- Windows Management Infrastructure (WMI) access must be enabled on the machine.

### About health checks

Health check data is stored in folders under `C:\ProgramData\Citrix\TelemetryService\` .

#### VDA health checks

For registration on the VDA, Cloud Health Check checks:

- VDA software installation
- VDA machine domain membership
- VDA communication port availability
- VDA service status
- Windows firewall configuration
- Communication with Controller
- Time sync with Controller
- VDA registration status

For session launches on VDAs, Cloud Health Check checks:

- Session launch communication port availability
- Session launch services status
- Session launch Windows firewall configuration
- VDA Remote Desktop Services Client Access Licenses
- VDA application launch path
- Session launch registry settings
- Citrix Universal Injection Driver (CTXUVI) status

For Profile Management on VDAs, Cloud Health Check checks:

- Hypervisor detection
- Provisioning detection
- Citrix Virtual Apps and Desktops
- Personal vDisk configuration
- User store
- Profile Management Service status detection
- Winlogon.exe hooking test

To run checks on Profile Management, you must install and enable Profile Management on the VDA. For more information on Profile Management configuration checks, see Knowledge Center article CTX132805.

#### StoreFront health checks

StoreFront checks verify whether:

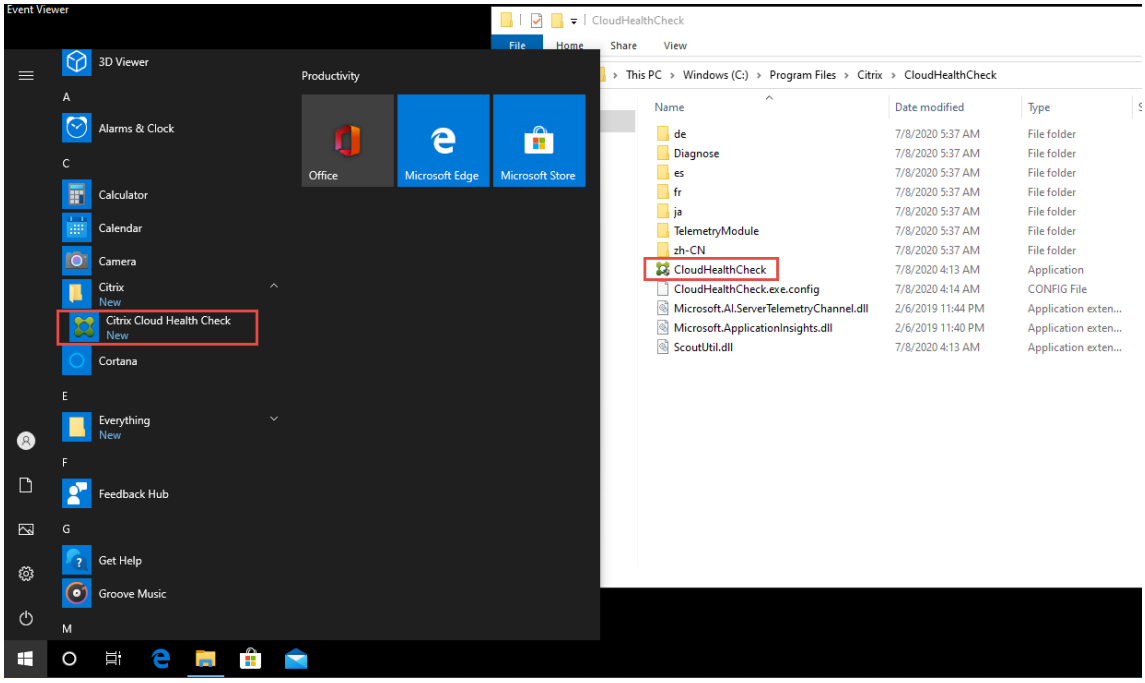
- Citrix Default Domain service is running
- Citrix Credential Wallet service is running
- The connection from the StoreFront server to Active Directory is port 88
- The connection from the StoreFront server to Active Directory is port 389
- The connection from the StoreFront server to Active Directory is port 464
- The base URL has a valid FQDN
- The correct IP address from the base URL can be retrieved
- The IIS application pool is using .NET 4.0
- The certificate is bound to the SSL port for the host URL
- The certificate chain is complete
- The certificates have expired
- A certificate is expiring within 30 days

### Running Cloud Health Check

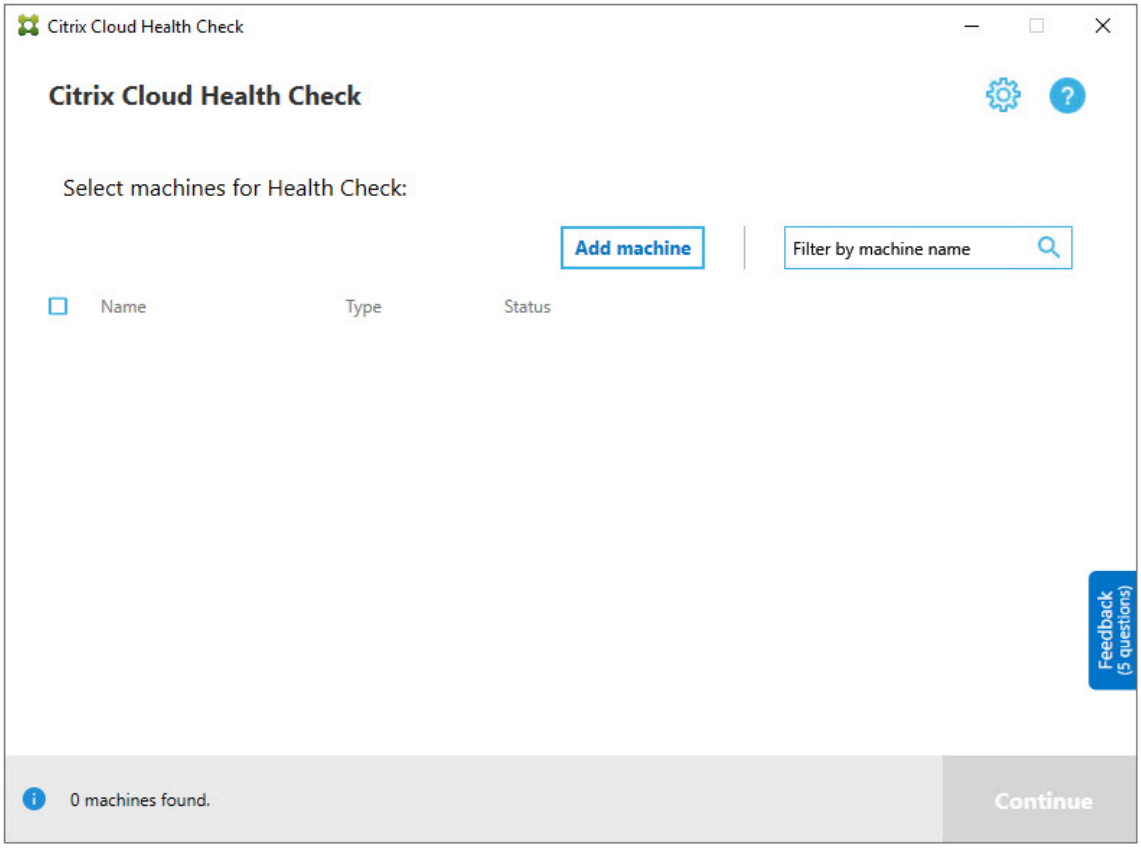
To run Citrix Cloud Health Check:

1. Select **Citrix > Citrix Cloud Health Check** from the machine's Start menu, or run `CloudHealthCheck.exe` in `C:\Program Files\Citrix\CloudHealthCheck`.



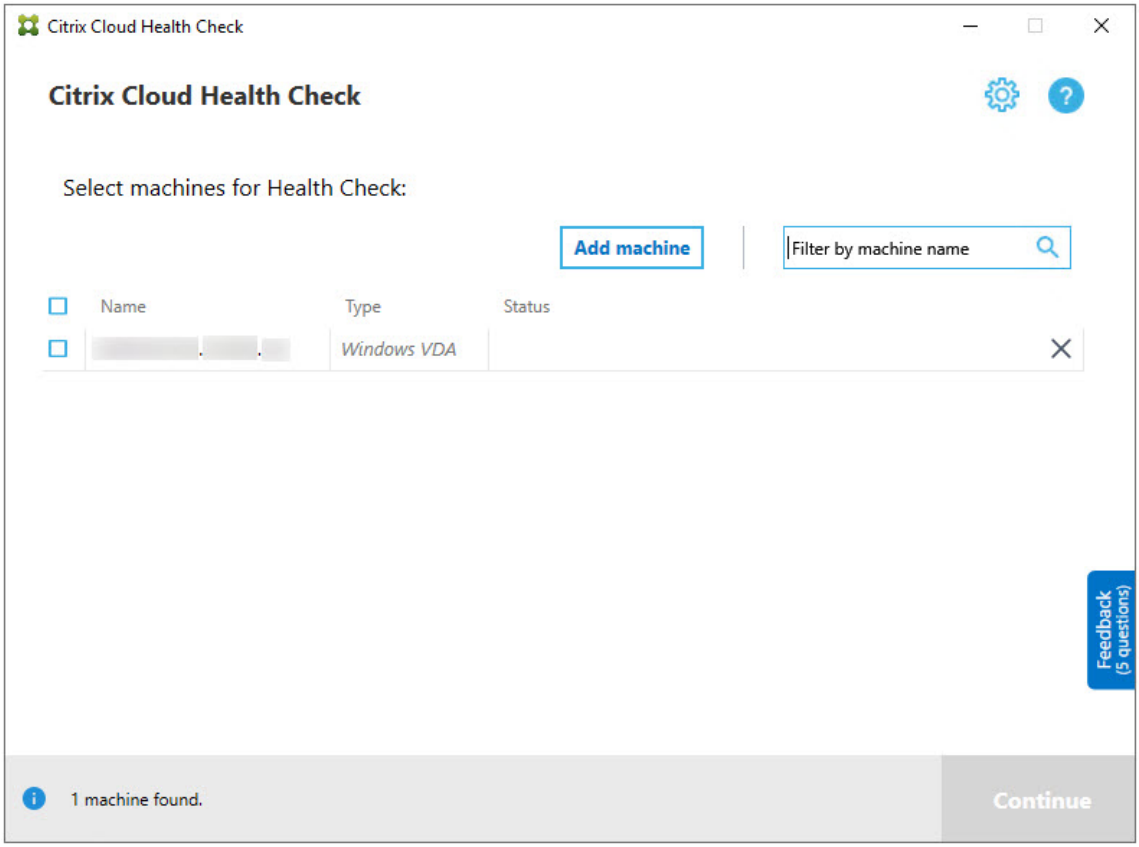

2. On the main Cloud Health Check screen, click **Add machine**.




3. Type the FQDN of the machine you want to add. **Note:** Although entering a DNS alias instead of an FQDN can appear valid, the health checks might fail.
4. Click **Continue**.
5. Repeat to add other machines as needed.




6. To remove a manually added machine, click the **X** on the right end of the row and confirm the deletion. Repeat to delete other manually added machines.

Cloud Health Check remembers manually added machines until you remove them. When you close and then reopen Cloud Health Check, the manually added machines are still listed at the top of the list.

### Import VDA machines

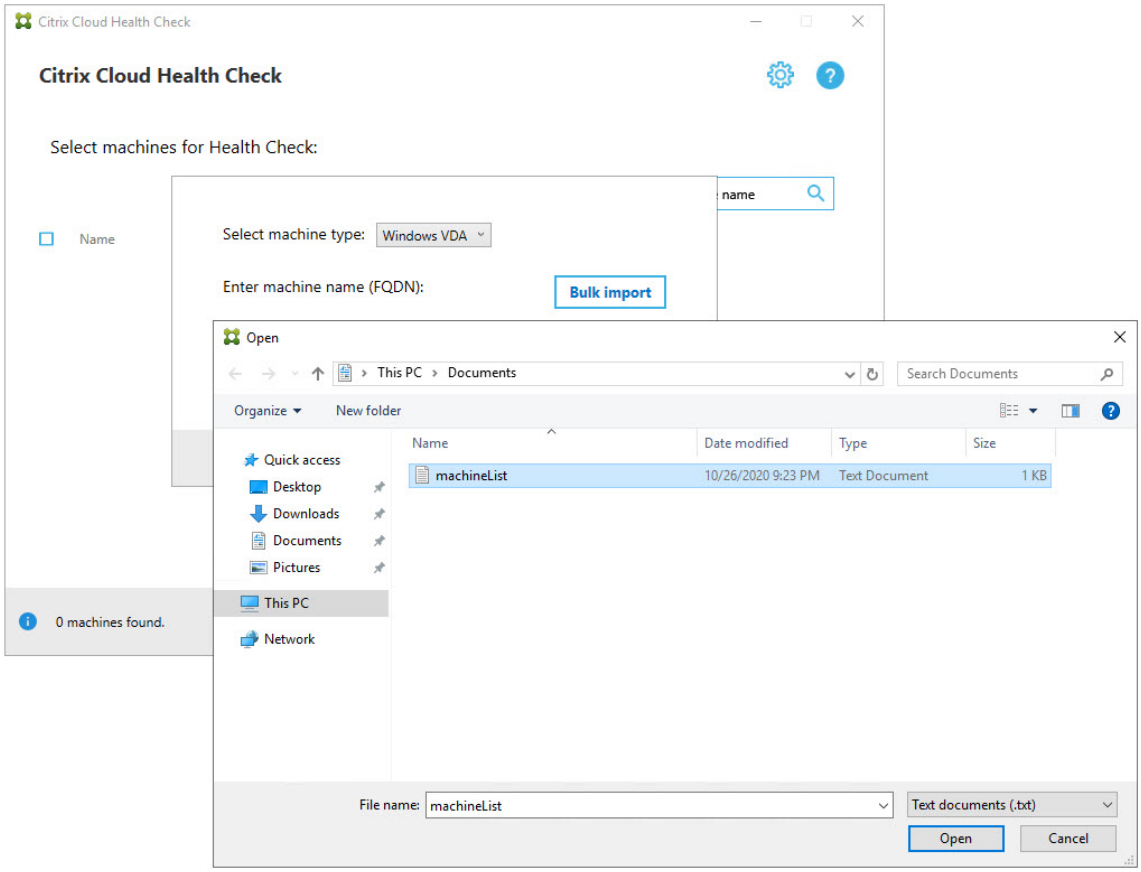
You can import VDA machines in the deployment when running health checks.

1. On Connector, generate the machine list file with the following PowerShell command. On Connector, you must input Citrix credentials and select the customer in the pop-up dialog.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
```

1. Copy the machineList.txt file to the domain-joined machine you want to run Cloud Health Check on.
2. On the Cloud Health Check page, click **Add Machine**.
3. Select the Windows VDA machine type.

4. Click **Import VDA machines**.
5. Select the machineList.txt file.
6. Click **Open**.



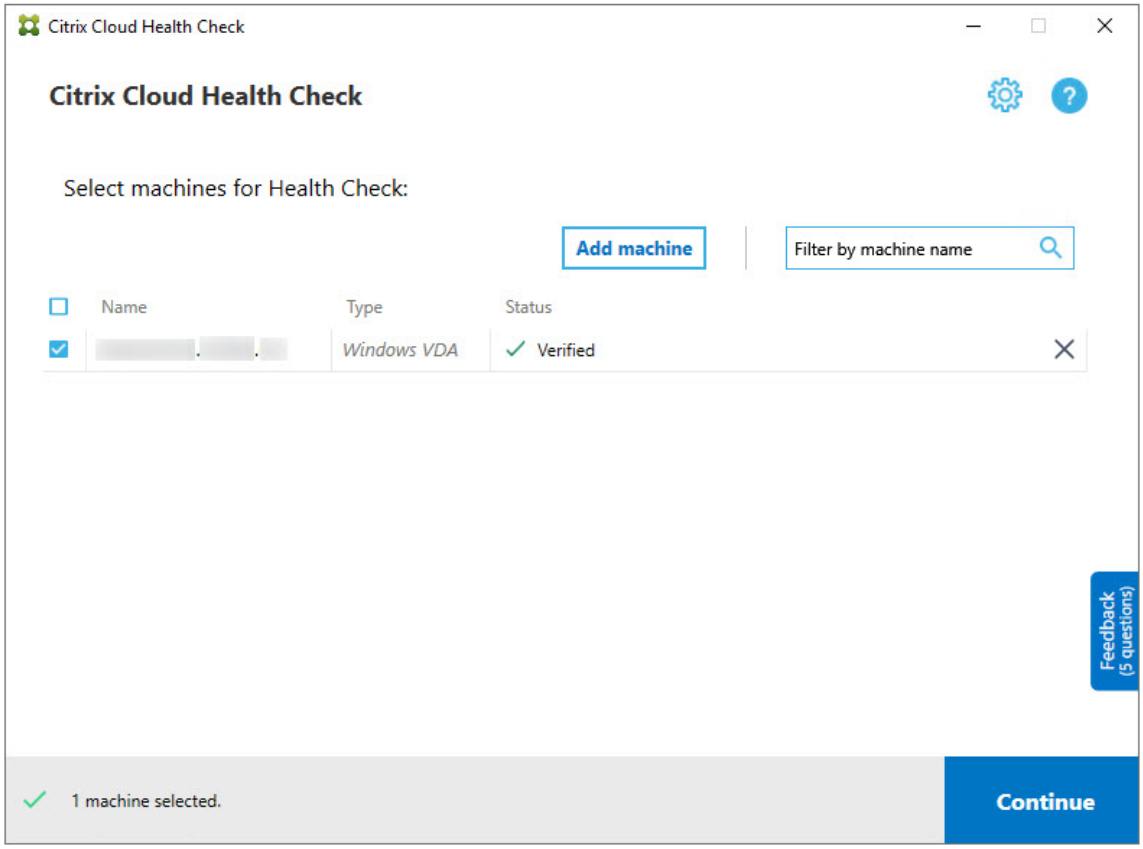
The imported VDA machines are listed on the Cloud Health Check page.

7. Select the check box next to each machine you want to run health checks on.

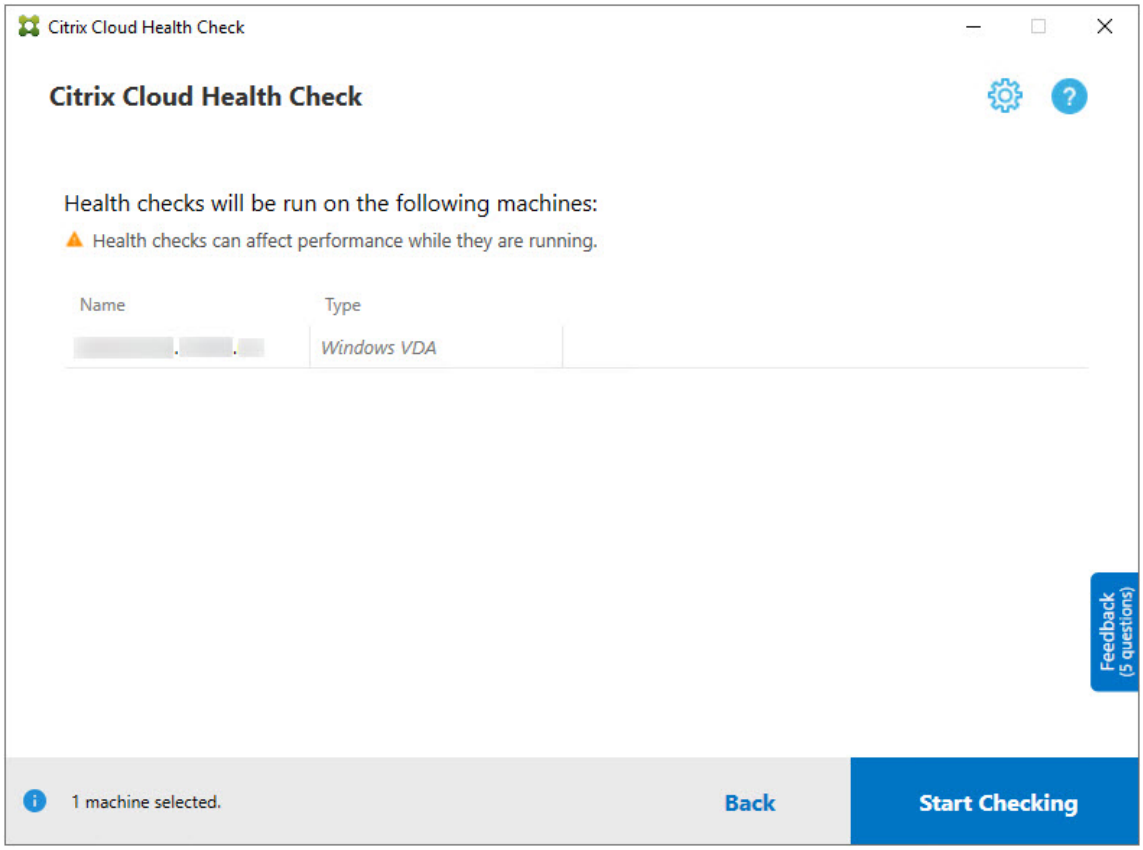
   Cloud Health Check automatically launches verification tests on each selected machine, making sure it meets the criteria listed in verification tests. If verification fails, a message appears in the **Status** column, and that machine's check box is cleared. You can then:

   - Resolve the issue and then select the machine's check box again. This triggers a retry of the verification tests.
   - Skip that machine by leaving its check box unselected. Health checks are not run for that machine.

8. When the verification tests are complete, click **Continue**.

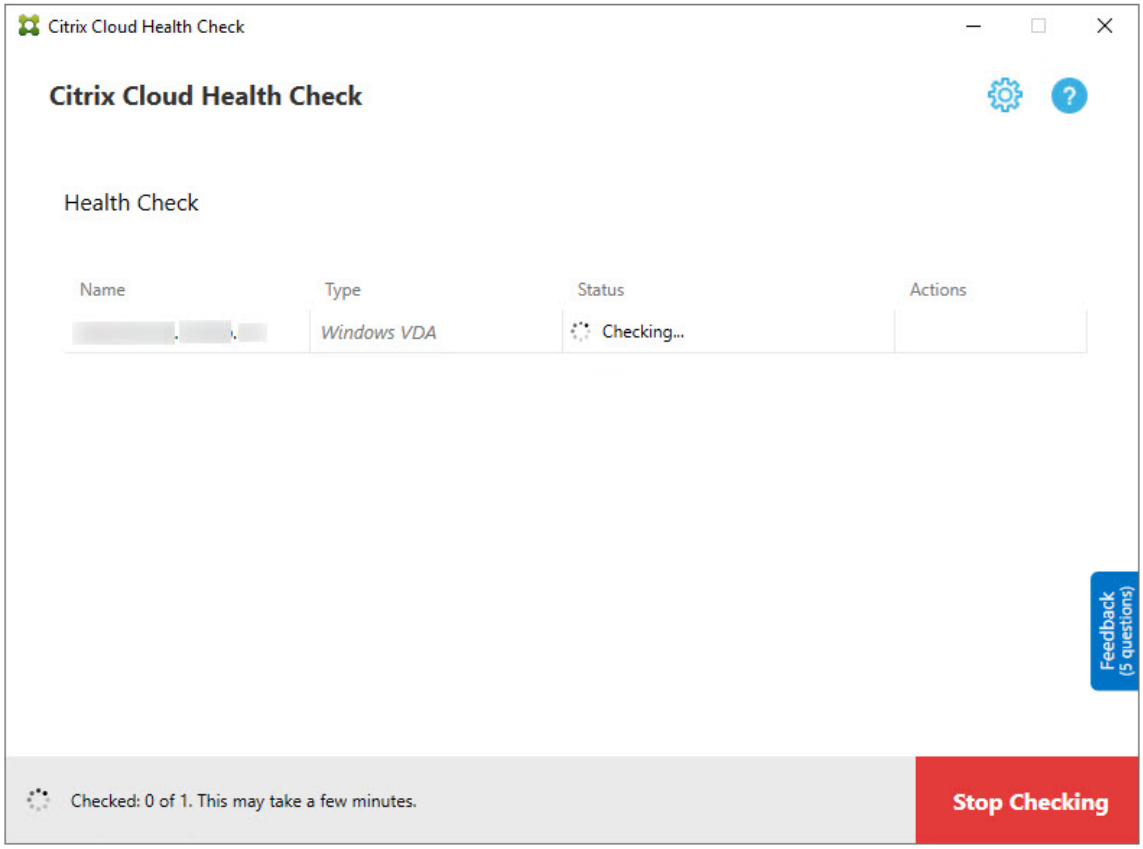


9. Run the health checks on the selected machines. The summary lists the machines where the tests run (the machines you selected that passed the verification tests).
10. Click **Start Checking**.

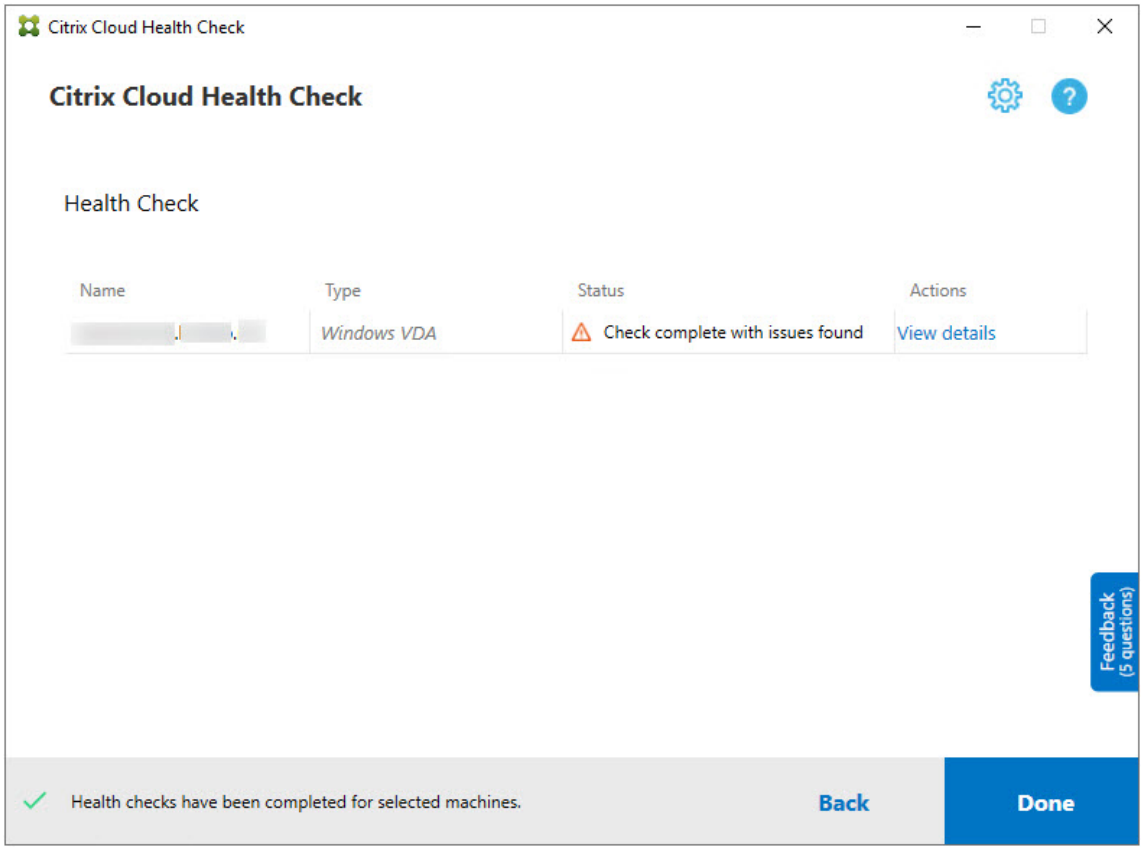


During and after checking, the **Status** column indicates the current checking state for a machine.

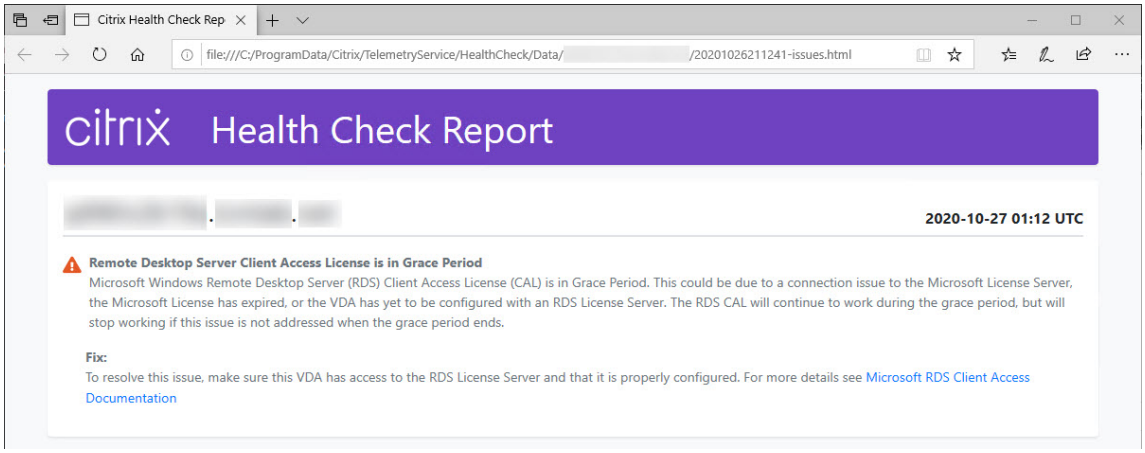
11. To stop all in-progress checks, click **Stop Checking** in the lower right corner of the page. You can't cancel a single machine's health check, you can only cancel the check for all selected machines.



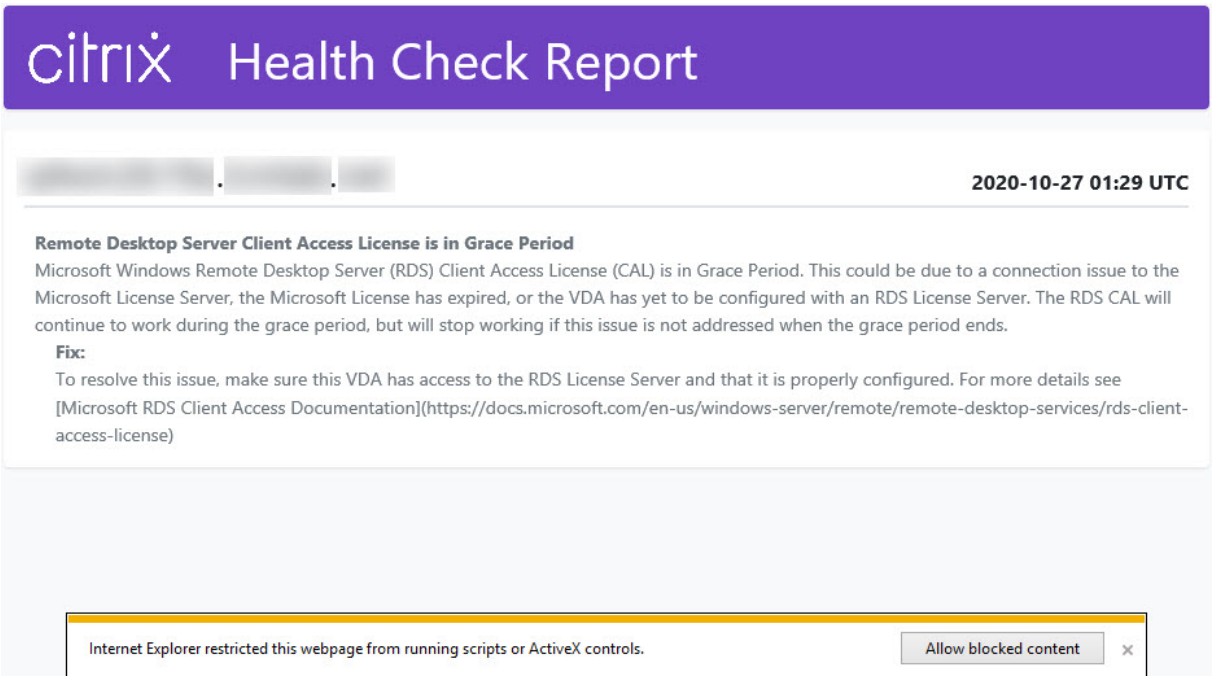
12. When the checks are complete for all selected machines, the **Stop Checking** button in the lower right corner changes to **Done**.



- If a check fails, you can click **Retry** in the **Action** column.
- If a check completes with no issues found, the **Action** column is empty.
- If a check finds issues, click **View Details** to view the results.



If you use Internet Explorer to view the report, you must click **Allow blocked content** to display the hyperlink.



After the check completes for all selected machines, clicking **Back** causes you to lose your check results.

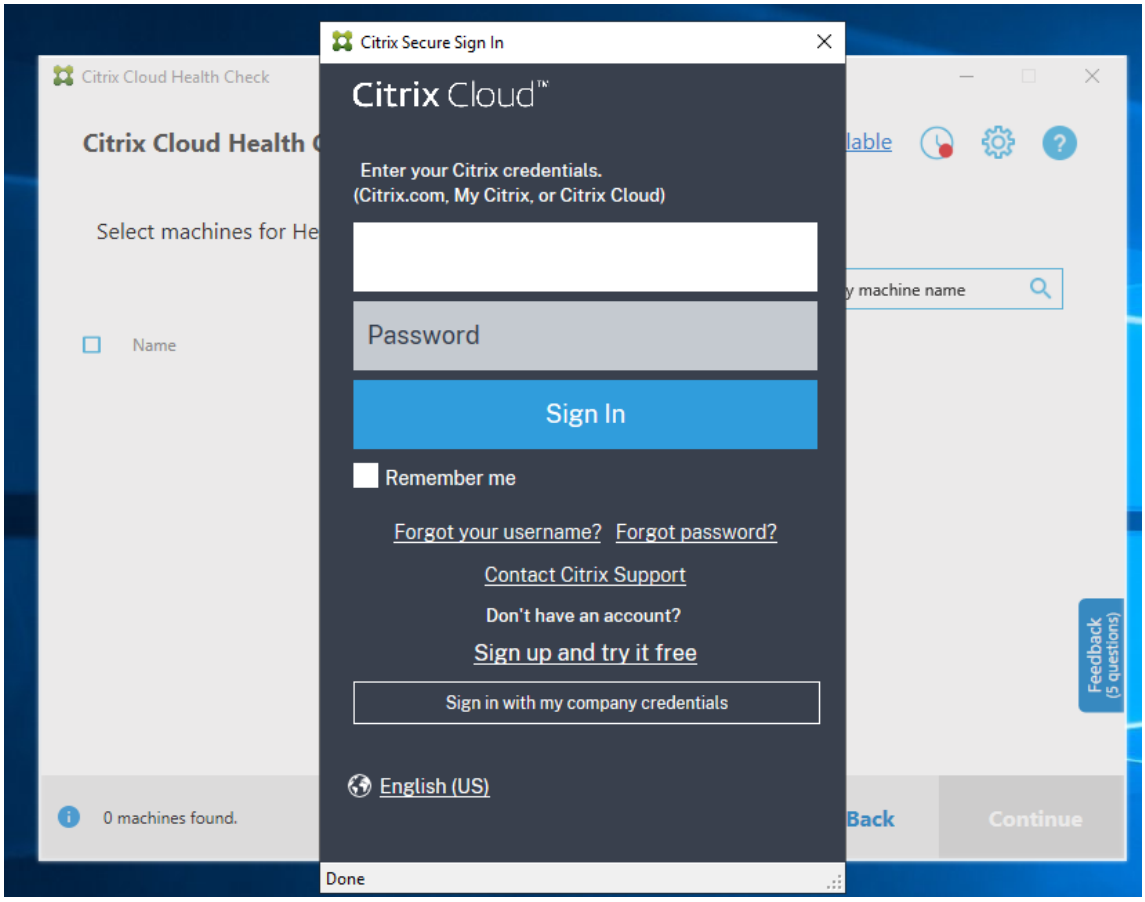
When the checks complete, click **Done** to return to the Cloud Health Check main screen.

Retrieve VDA machines

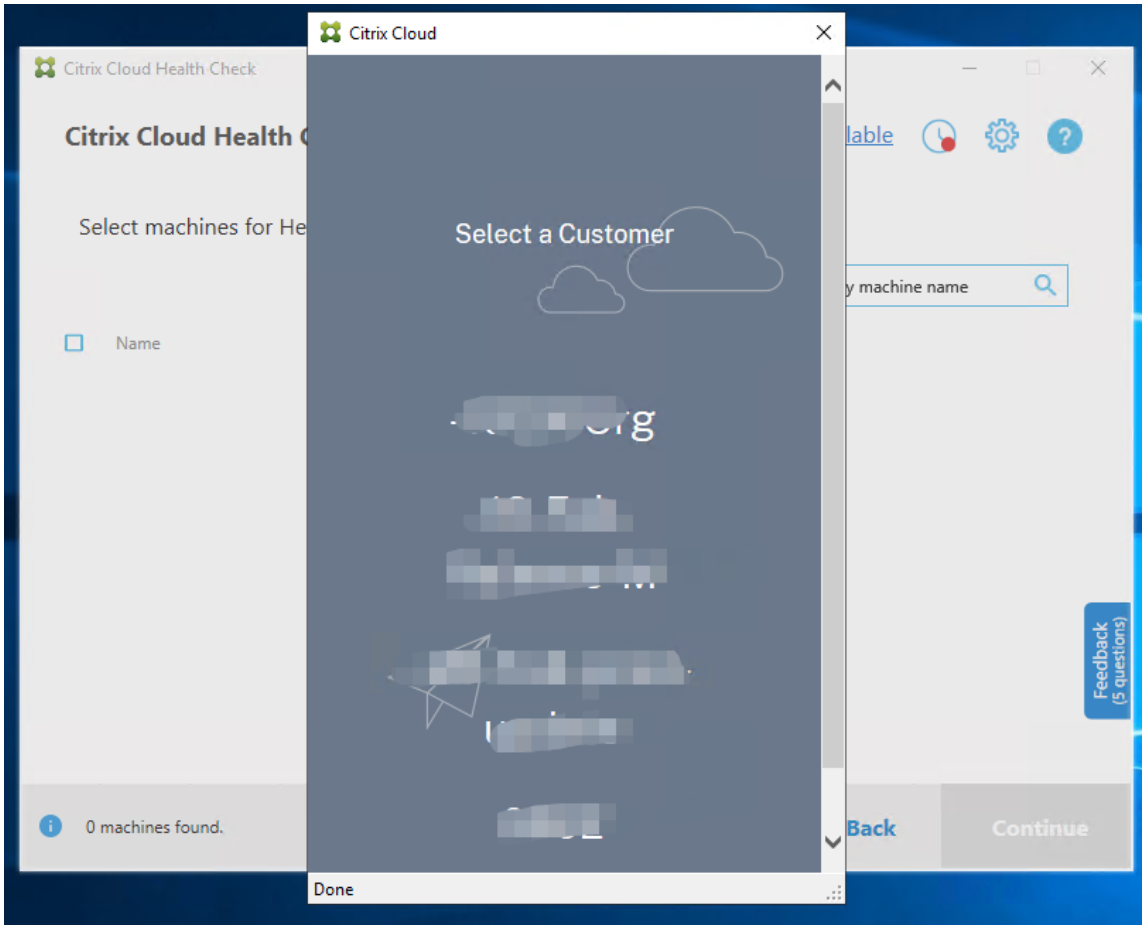
Cloud Health Check can automatically detect and retrieve VDAs from your Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments.

To retrieve your VDAs:

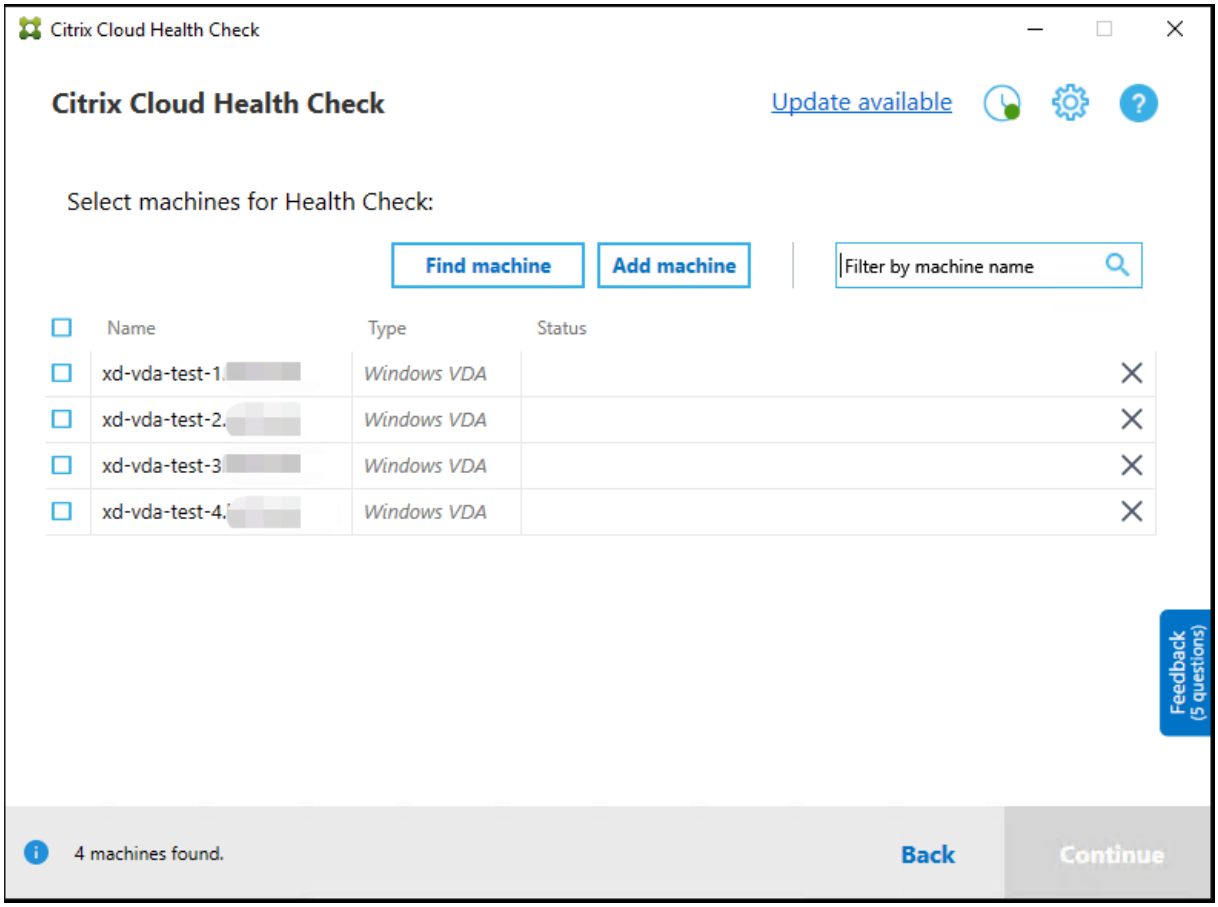
1. Prepare a new machine that is joined to the same domain forest as the machine Cloud Health Check runs on.
2. Open Cloud Health Check and click **Find machine** to sign in to Citrix Cloud.



3. Select the customer with the cloud site you want to retrieve.

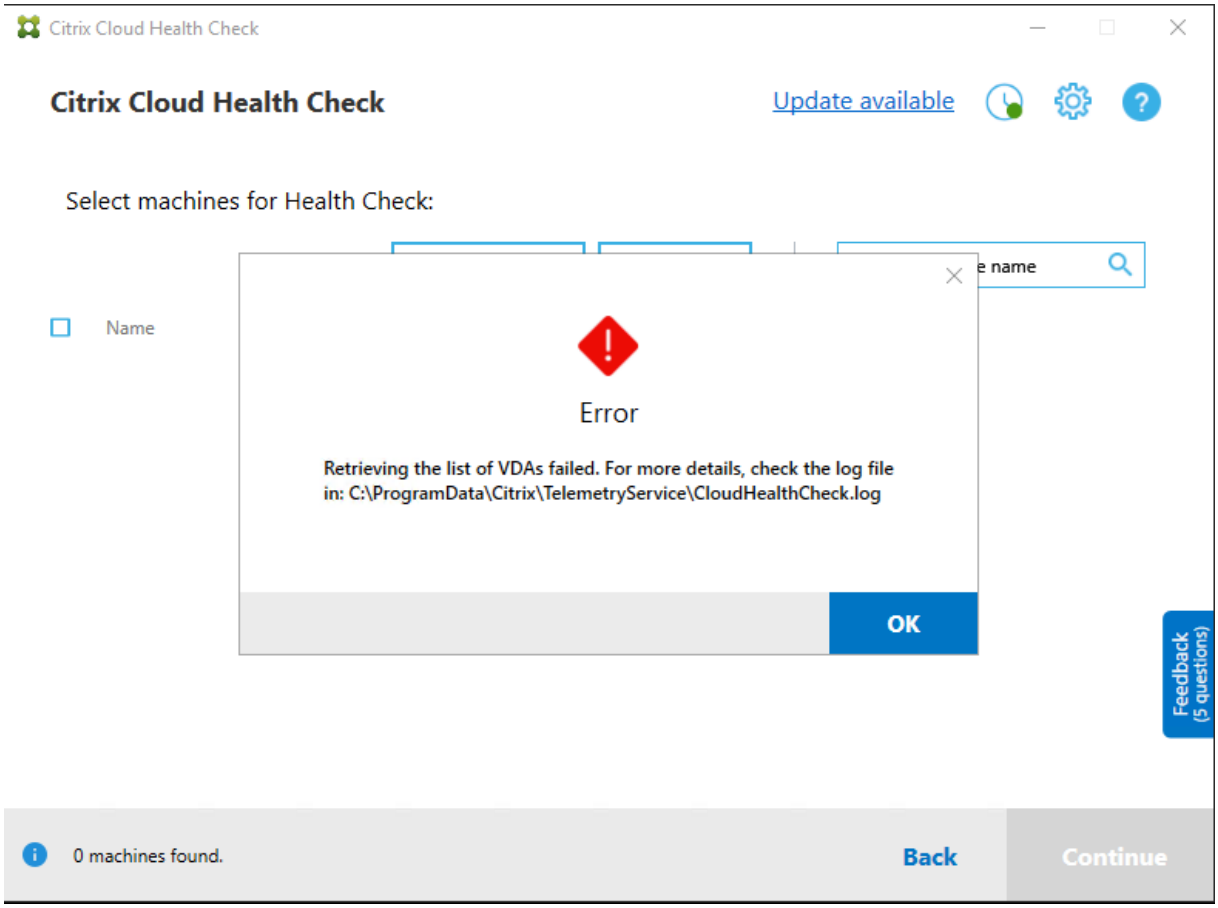


The VDA list displays in Cloud Health Check. The list is also saved in a local file located at `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.



Your machine list loads the local cache when you open Cloud Health Check again. If you have made any updates in your deployment, you must click **Find machine** to refresh the machine list.

> **Note:**
>
> - Cloud Health Check finds machines only in the same domain forest as the machine Cloud Health Check runs on.
> - Citrix Cloud sessions expire in one hour. After one hour, you must click **Find machine** again to get the latest VDA list.
> - An error message pops up if retrieving the VDA list fails. You can check the details in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.



Heath check results

Health checks that generate reports contain the following elements:

- Time and date when the results report was generated
- FQDNs of the machines that were checked
- Conditions checked on the target machines

Running Cloud Health Check on the command line

Cloud Health Check can be run on the command line to help customers to perform health checks. To use Cloud Health Check on the command line, you must be an administrator on the machine Cloud Health Check is running on.

> **Note:**
>
> When using Cloud Health Check on the command line, only one machine can be checked at a time. Only one instance of `CloudHealthCheck.exe` can be run at the same time on the target

> machine. If you want to check multiple machines, the machines must be checked one by one, by wrapping the cmdlets in a loop in cmdlet/PowerShell scripts. Any opened UI instance of Cloud Health Check must also be closed.

Cmdlets

The supported command line cmdlets are:

- `MachineFQDN` - This cmdlet is **mandatory**. This is the fully qualified domain name of the target machine.
- `MachineType` - This cmdlet is optional. The cmdlet value can be the Windows VDA (default value) or StoreFront.
- `ReportName` - This cmdlet is optional. The cmdlet value must be a valid file name on Windows. The default value is `HealthCheckReport`.
- `SkipAdminCheck` - This cmdlet is optional. This can be added to skip the checks that require administrator permissions.
- `UpdateScripts` - This cmdlet is optional. This can be added to update the check scripts from CDN server.
- `DisableCeip` - This cmdlet is optional if CEIP is enabled on the UI, add it to disable CEIP.
- `Help` - Show help information about parameters.

Examples:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

> **Note:**
>
> Parameter names are not case sensitive.

By default, the console output is not shown in the command line console window. You can manually display the output by appending `|more` to the cmdlet.

Example: `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

The command line default needs administrator permissions to run. Add the parameter –SkipAdminCheck to override the need for administrator permissions.

Exit codes

Exit codes explain the result of Cloud Health Check checks within the command line. To get the exit code, you must add `start /wait` before the cmdlet.

Example: `start /wait HealthCheckCLI.exe –MachineFQDN machine.domain.local`

Exit codes are:

- 0 - Normal, check completed and passed.
- 1 - Failure, check completed with issues.
- 2 - Error, check not completed with errors.

You can also use the cmdlet `echo %errorlevel%` to get the exit code for the last ran command.

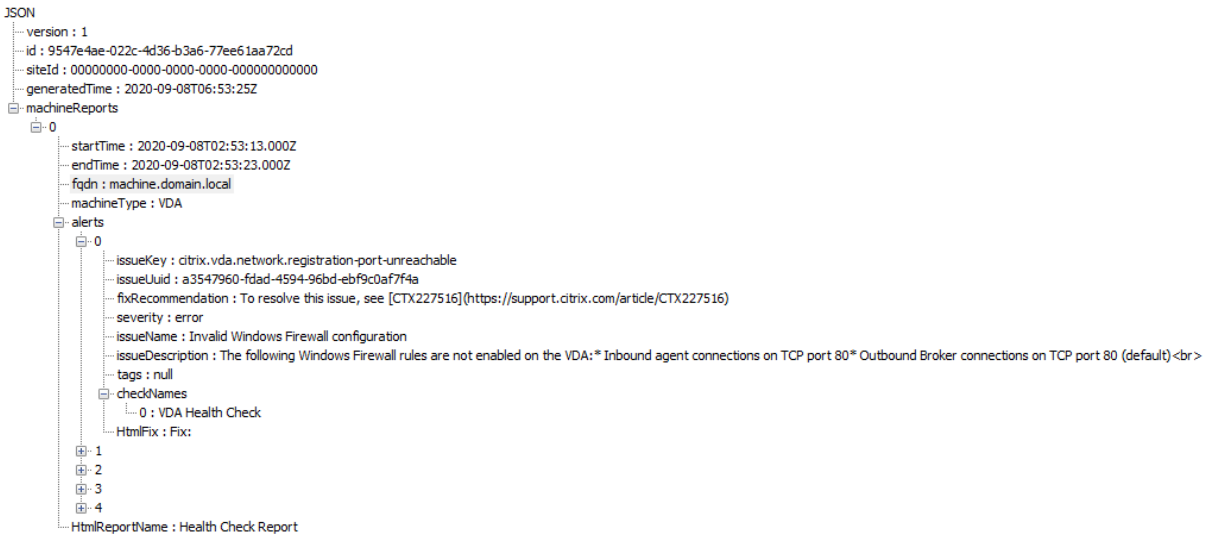
Reports

Cloud Health Check creates folders with the name of the machine in `HealthCheckDataFolder` for the target machine. An .html file and a .json file are created on the machine Cloud Health Check is installed on. Health check reports are located in the `HealthCheckDataFolder` in `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Reports are only created when issues exist on the target machine.

> **Note:**
>
> The report files are overwritten if the specified report name exists.

Alerts and basic information are stored in the .json report.

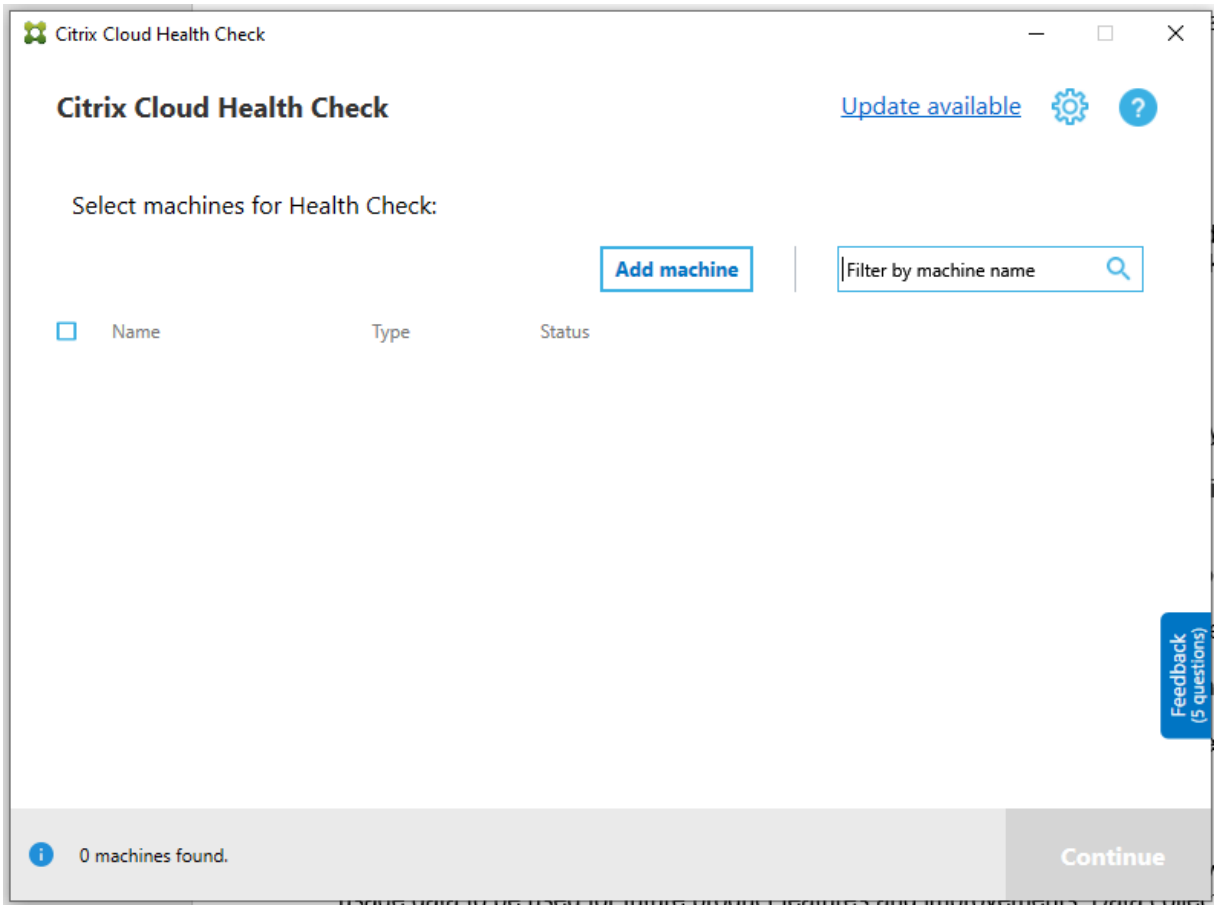


Report codes are:

- **issueKey**: a plain text description of the issue.
- **issueUuid**: a unique identifying string for the issue.
- **fixRecommendation**: the fix recommendation for the issue.
- **severity**: indicates if the issue must be fixed. An error can indicate that the component (VDA or StoreFront) malfunctioned, and a warning indicates that the component can work but might have some potential issues.
- **issueName**: the title of the issue.
- **issueDescription**: a detailed description of the issue.

Updating Cloud Health Check

If there is a new version of Cloud Health Check available, an Update available link displays on the top right of the Cloud Health Check window. Click the link to go to Citrix Downloads to get the new version.

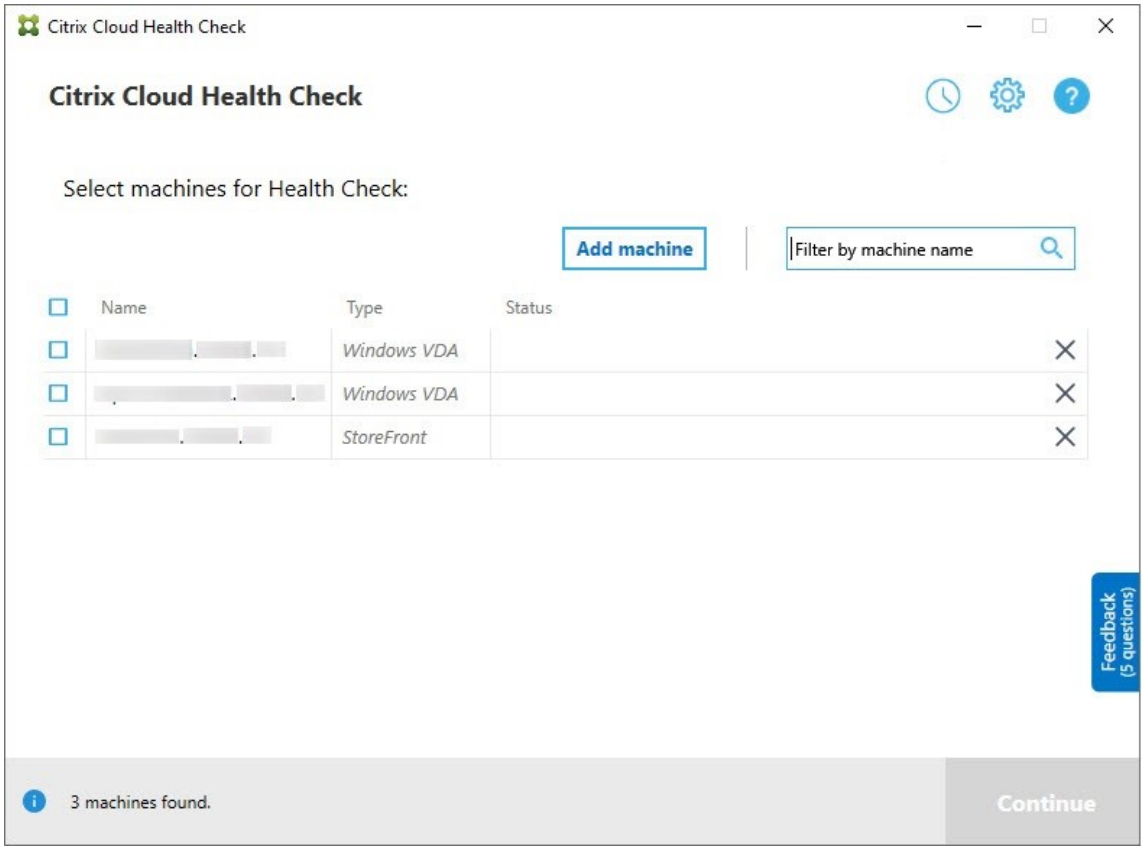


Cloud Health Check scheduler

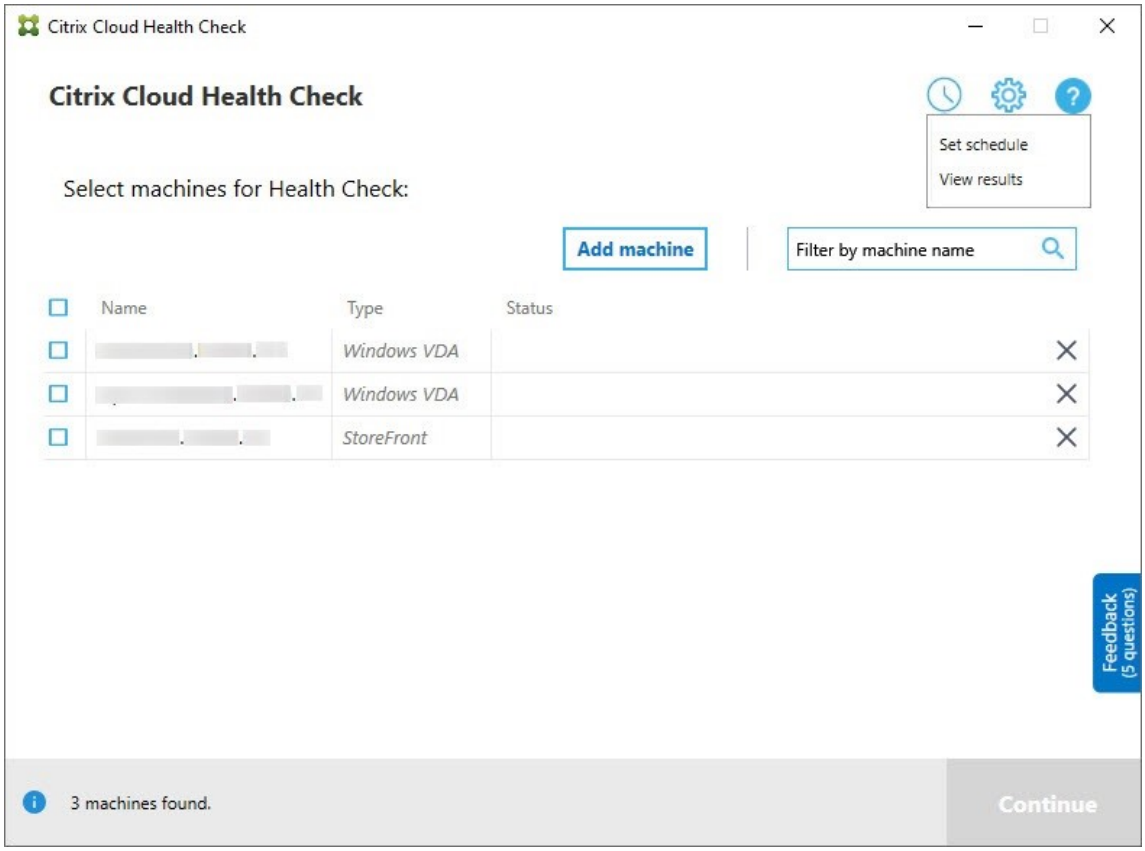
Use the Cloud Health Check scheduler to perform periodic health checks.

Set up the schedule

1. Click **Add machine** in the Cloud Health Check main window to add machines that you want to run periodic checks on.



2. Click the clock icon, then click **Set schedule**.



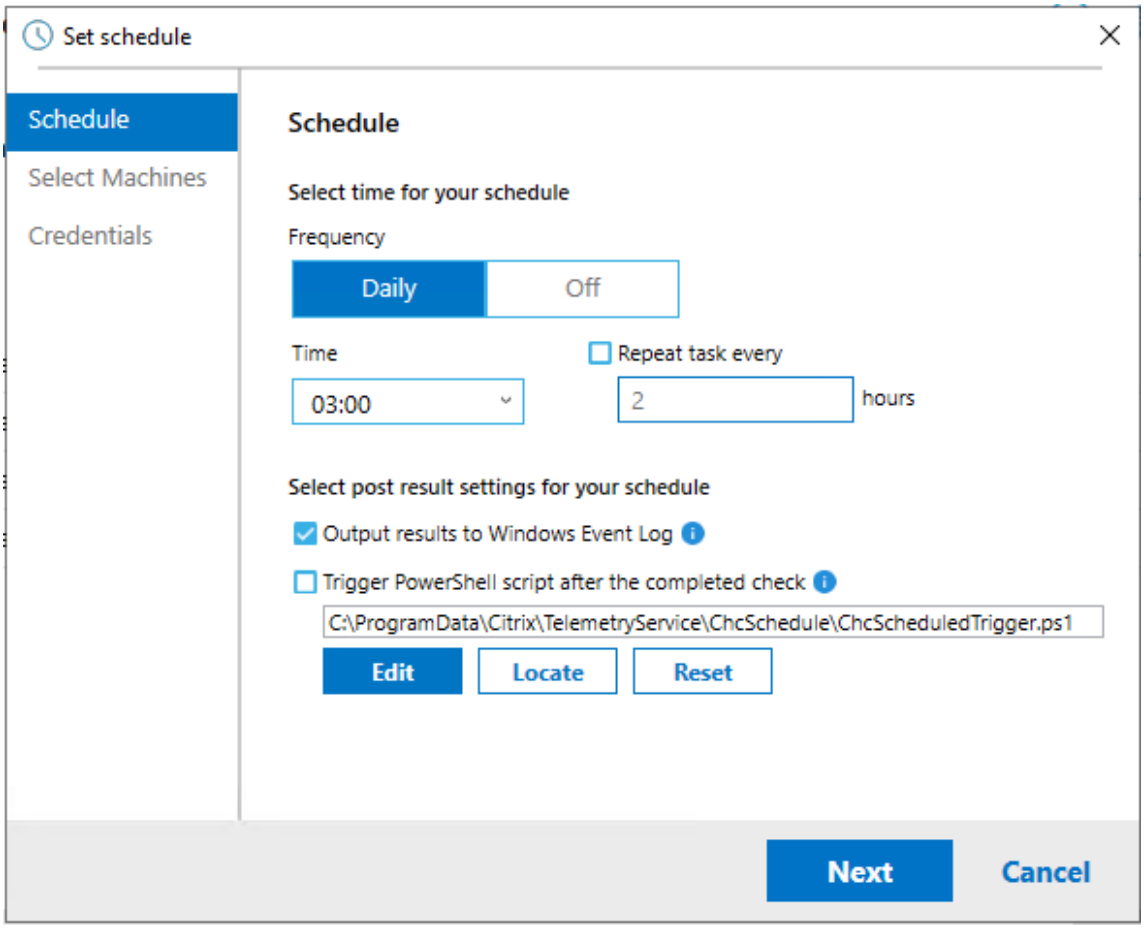
3. Select a time for your schedule, then click **Next**. The task can be set to repeat by selecting the **Repeat task every** check box.
4. Choose to output results to Windows Event Log. The task can be set to write the results to Windows Event Log.
5. Choose to trigger a custom PowerShell script after the scheduled check finishes, and then click **Next**.

    - Click **Edit** to edit the script content in Windows PowerShell ISE if needed.
    - Click **Locate** to open the file location and to use a different editor to open the file to edit the script.
    - Click **Reset** to reset the script to its original setting.

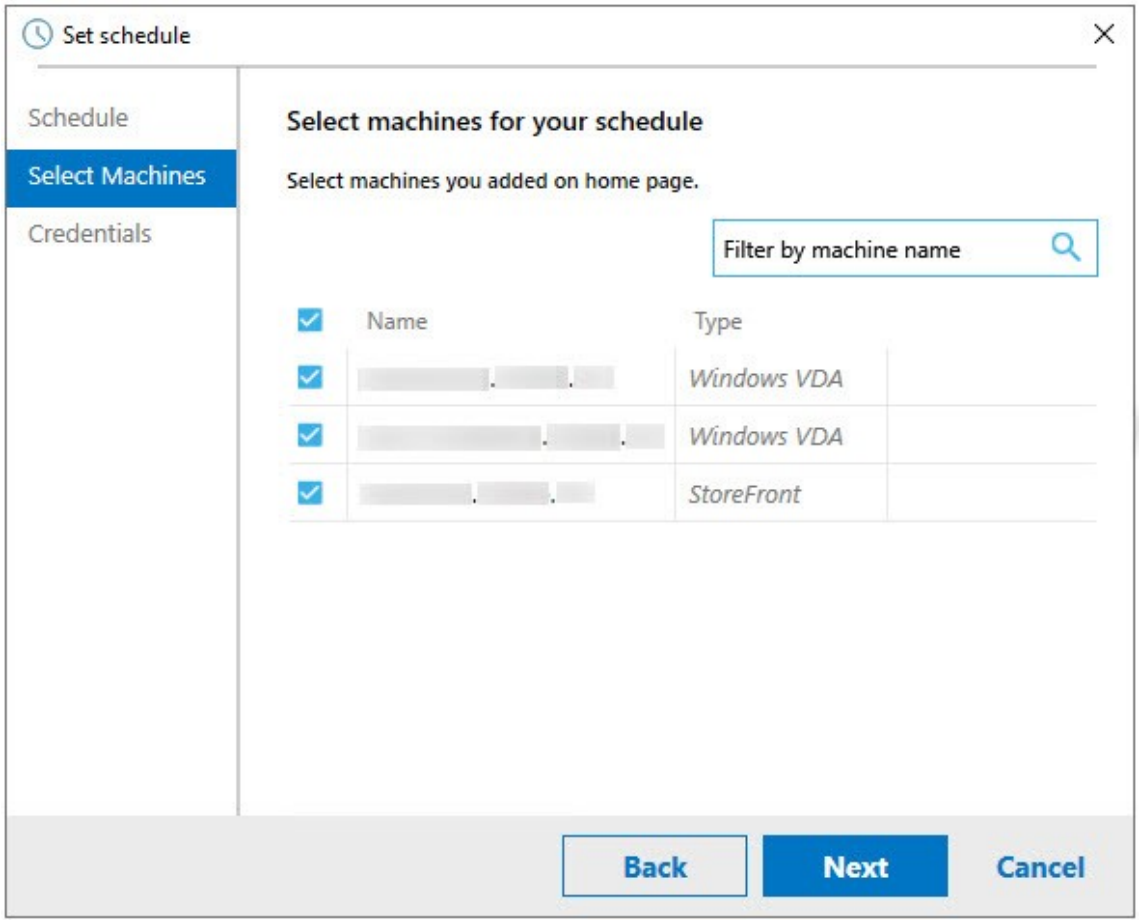
    > **Note:**
    >
    > – You cannot change the script name and path for the script.
    > – You can implement custom actions using the ChcShceduledTrigger.ps1 script, such as sending an email after the scheduled check report is ready. Add the following code to the end of the script. Customize the code to add the correct email accounts and the SMTP server address. An email notification is sent using the

> credentials of the account that the scheduled task runs.

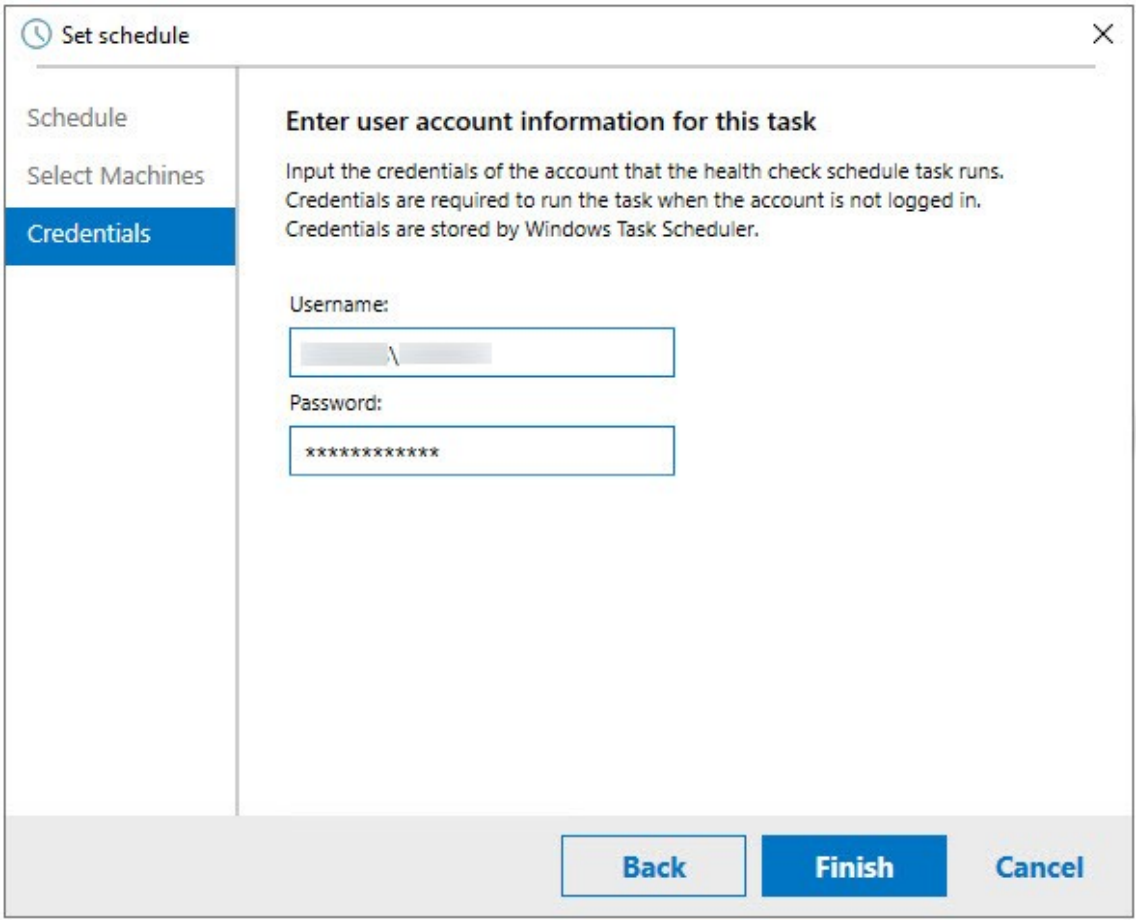
```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
   Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



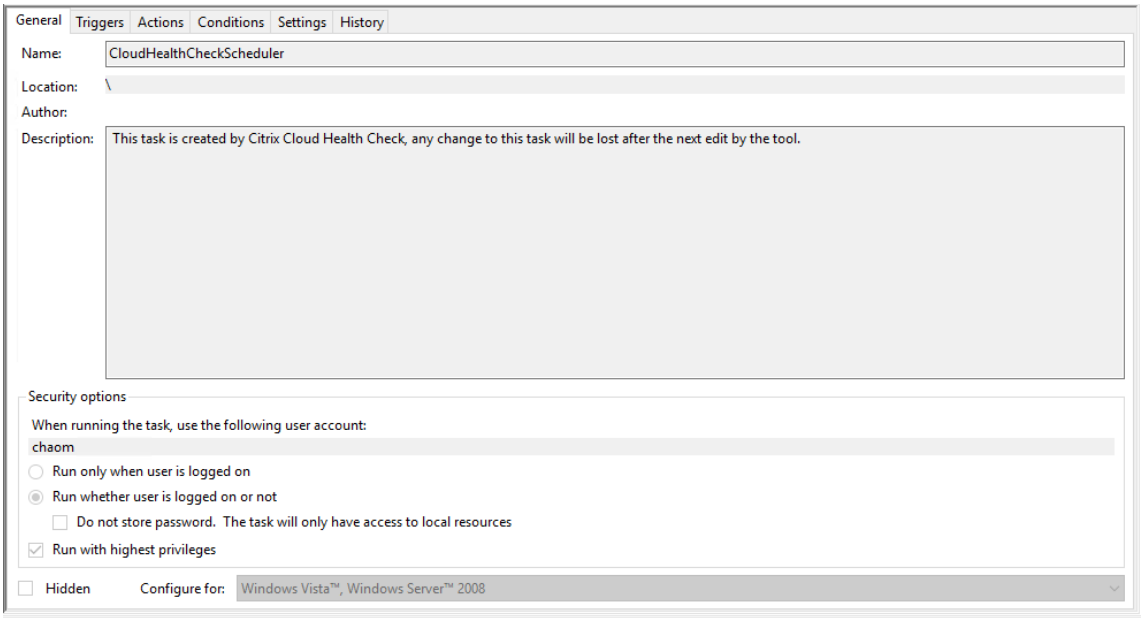
6. Select the machines for your schedule, then click **Next**.



7. Input the credentials of the account that the task runs on, then click **Finish**.

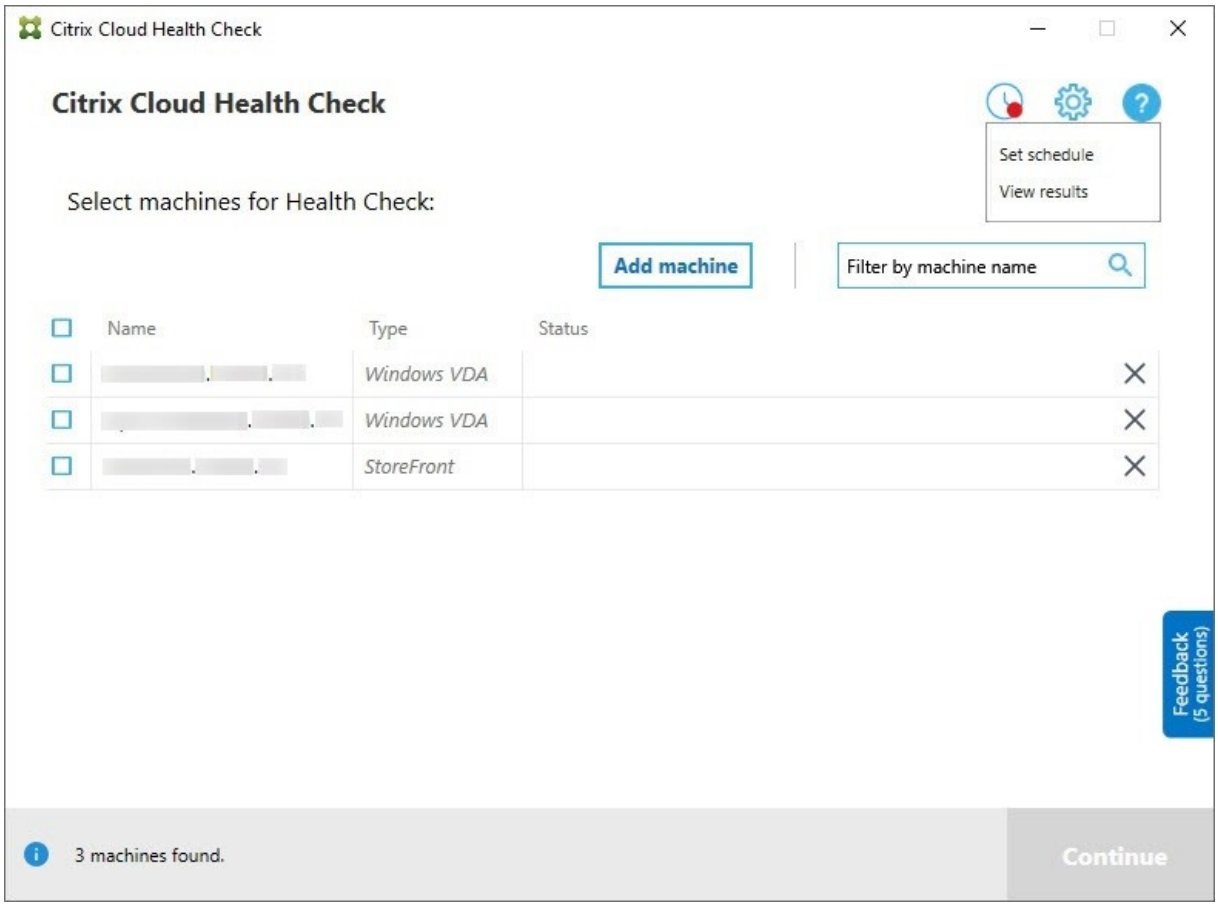


8. A CloudHealthCheckScheduler task is created in Windows Task Scheduler.

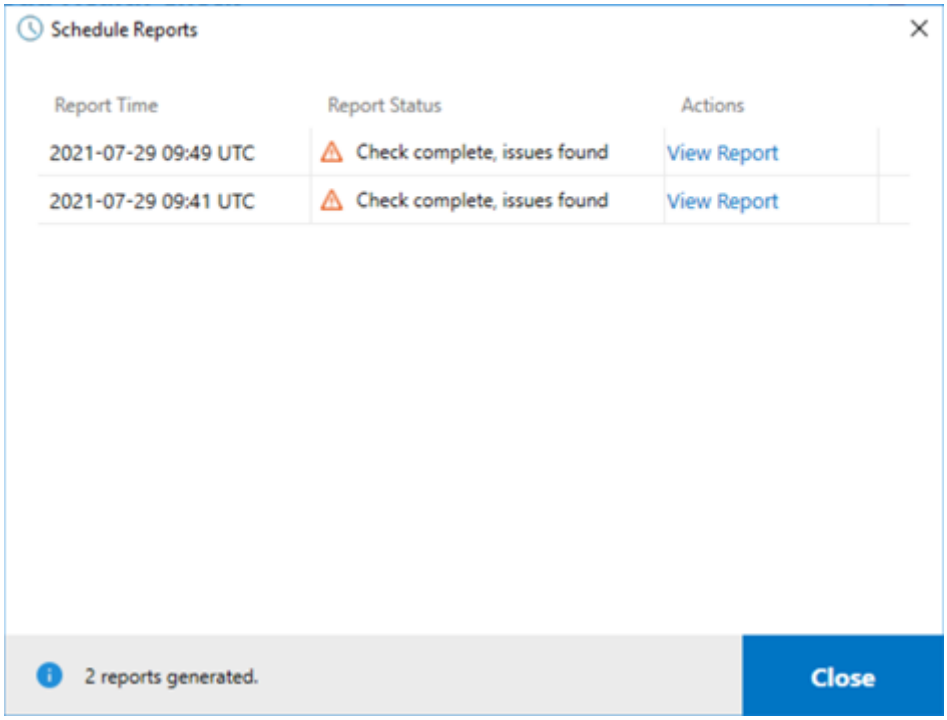


View schedule results

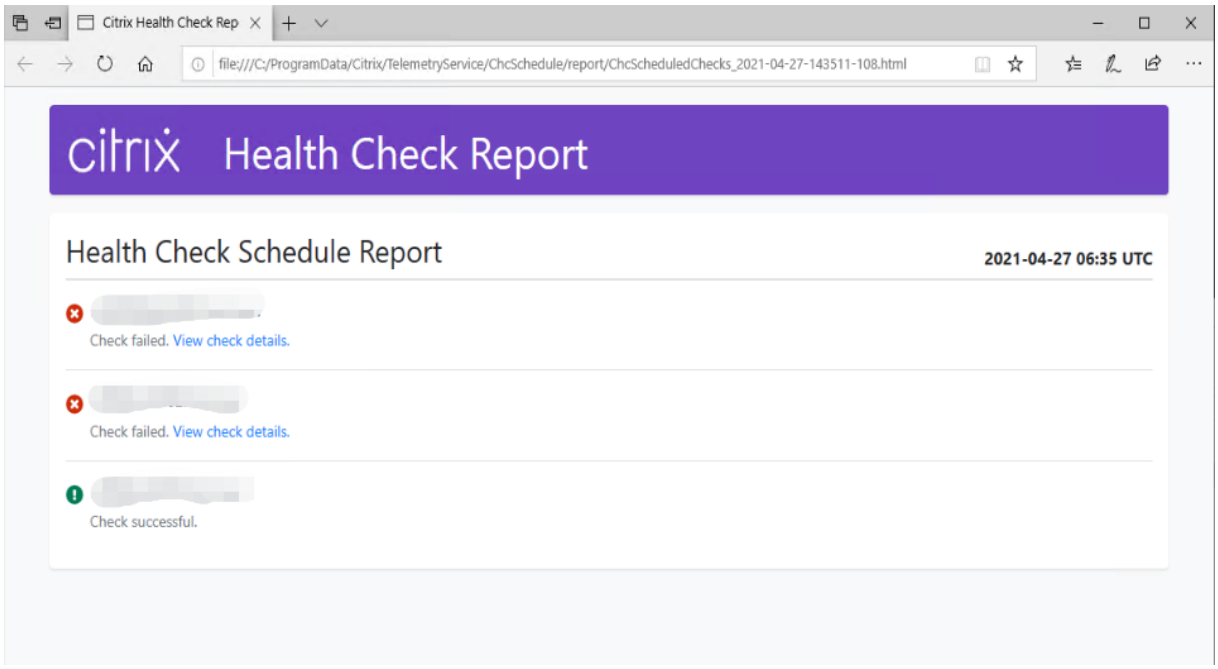
The clock icon with a red dot indicates that issues were found in the last check. To view the results, click the clock icon, then click **View results**.



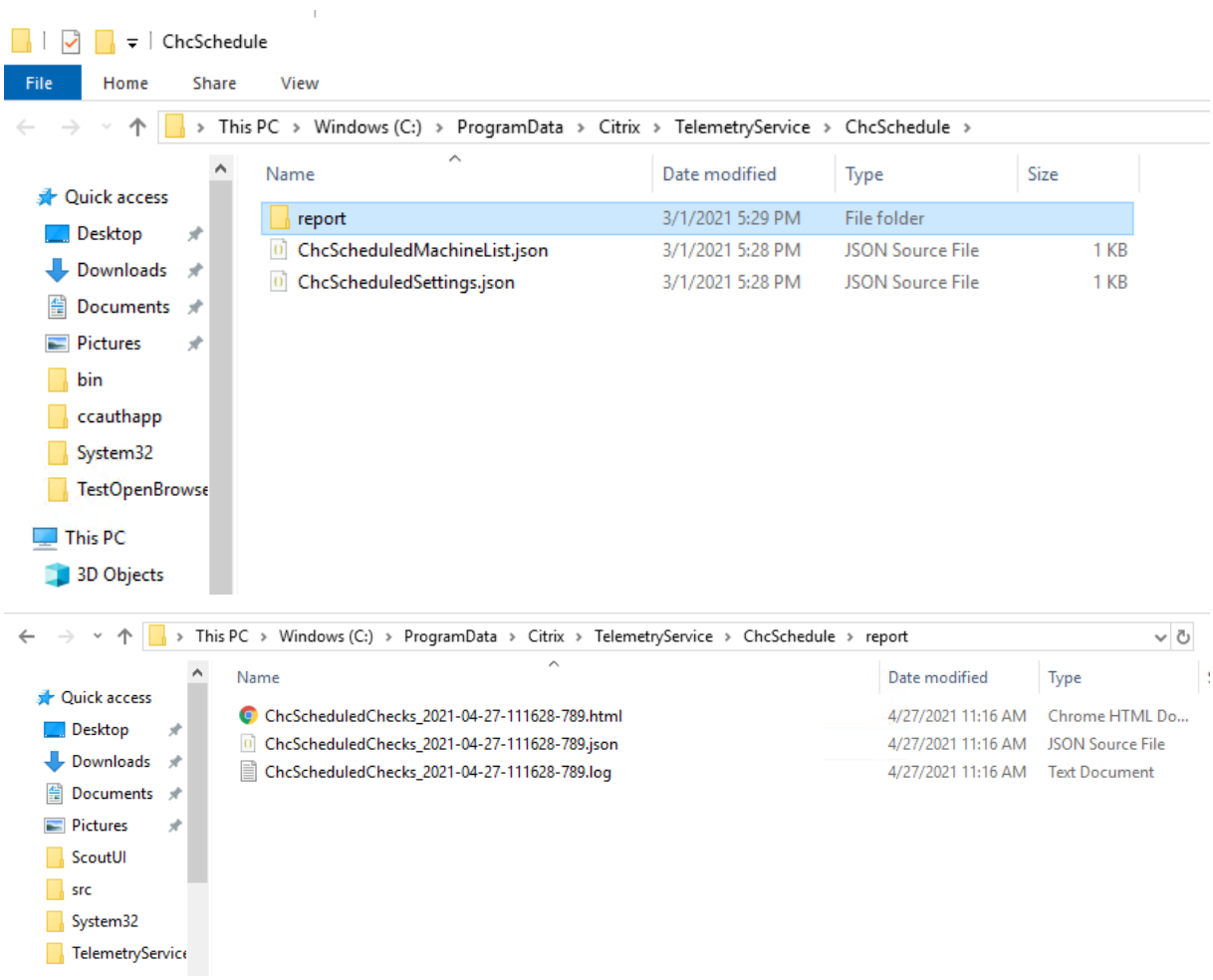
The Schedule Reports page shows the results for all the scheduled health check tasks. Click **View Report** to check the report for each schedule.



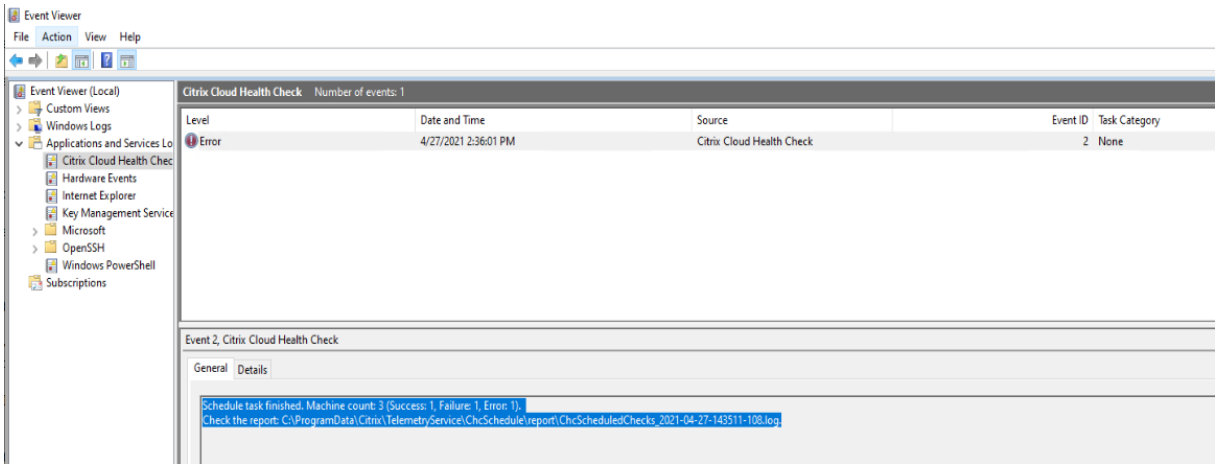
The html report lists the overall report for each schedules. An example of the report is below:



All health check results are stored in a folder called ChcSchedule. Cloud Health Check creates three files during each check run. Up to 500 iteration logs are kept.

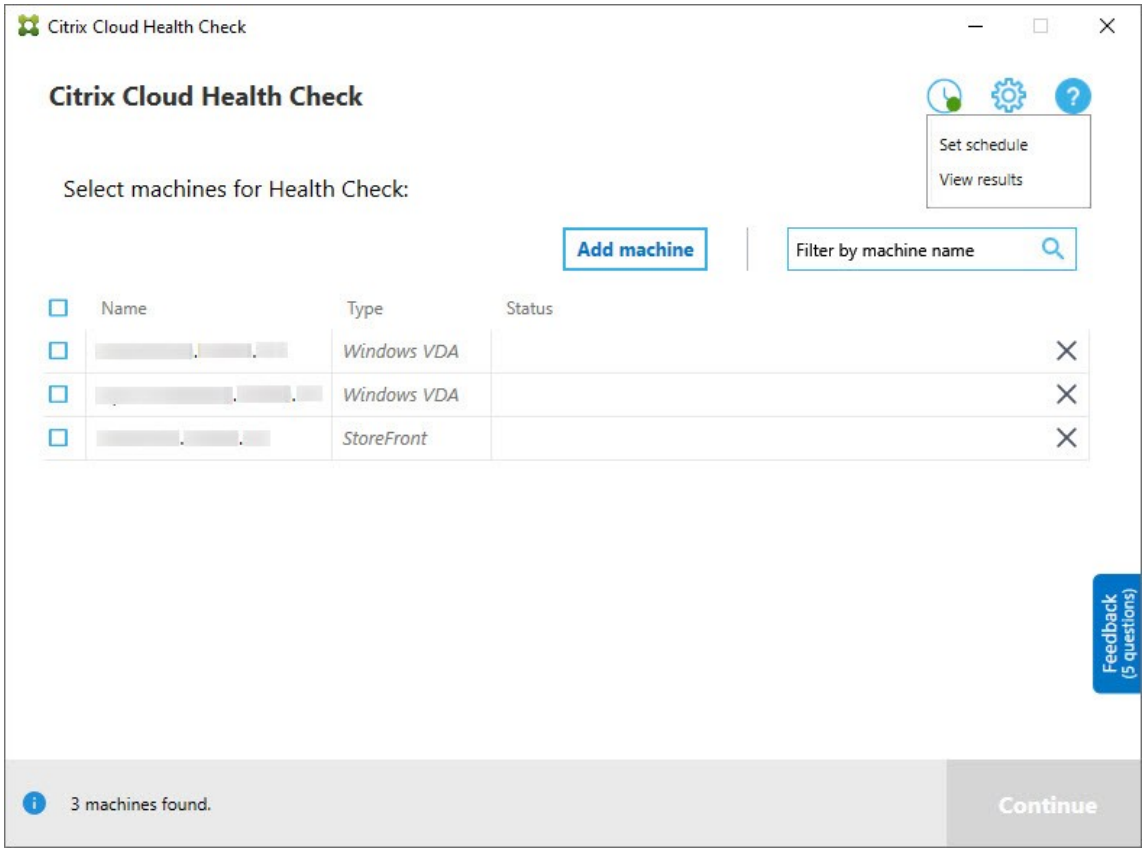


If the **Output results to Windows Event Log** checkbox is selected, the check result is also sent to Window Event Log.

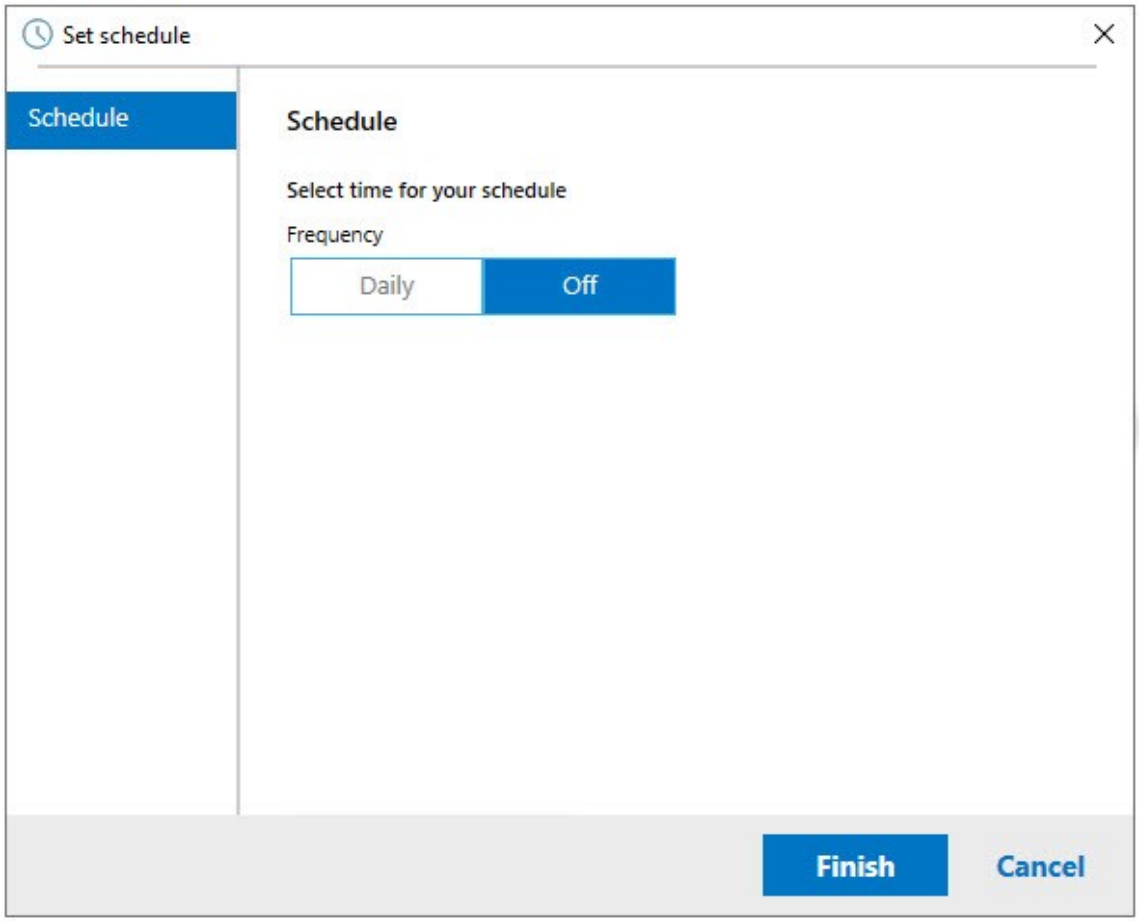


Disable schedules

1. Click the clock icon, then click **Set schedule**.



2. Click **Off**, then click **Finish** to disable the scheduler.



More information

- You must add or import VDAs to Cloud Health Check first. For more information, see Import VDA Machines.
- The Cloud Health Check scheduler can only schedule one task at a time on a domain-joined machine. If you set the schedule multiple times, only the latest one takes effect.

Verification tests

Before a health check starts, verification tests run automatically for each selected machine. These tests make sure that the requirements are met for a health check to run. If a test fails for a machine, Cloud Health Check displays a message with suggested corrective actions.

- **Cloud Health Check cannot reach this machine** - Ensure that:
  - The machine is powered on.
  - The network connection is working properly. (This can include verifying that your firewall is properly configured.)

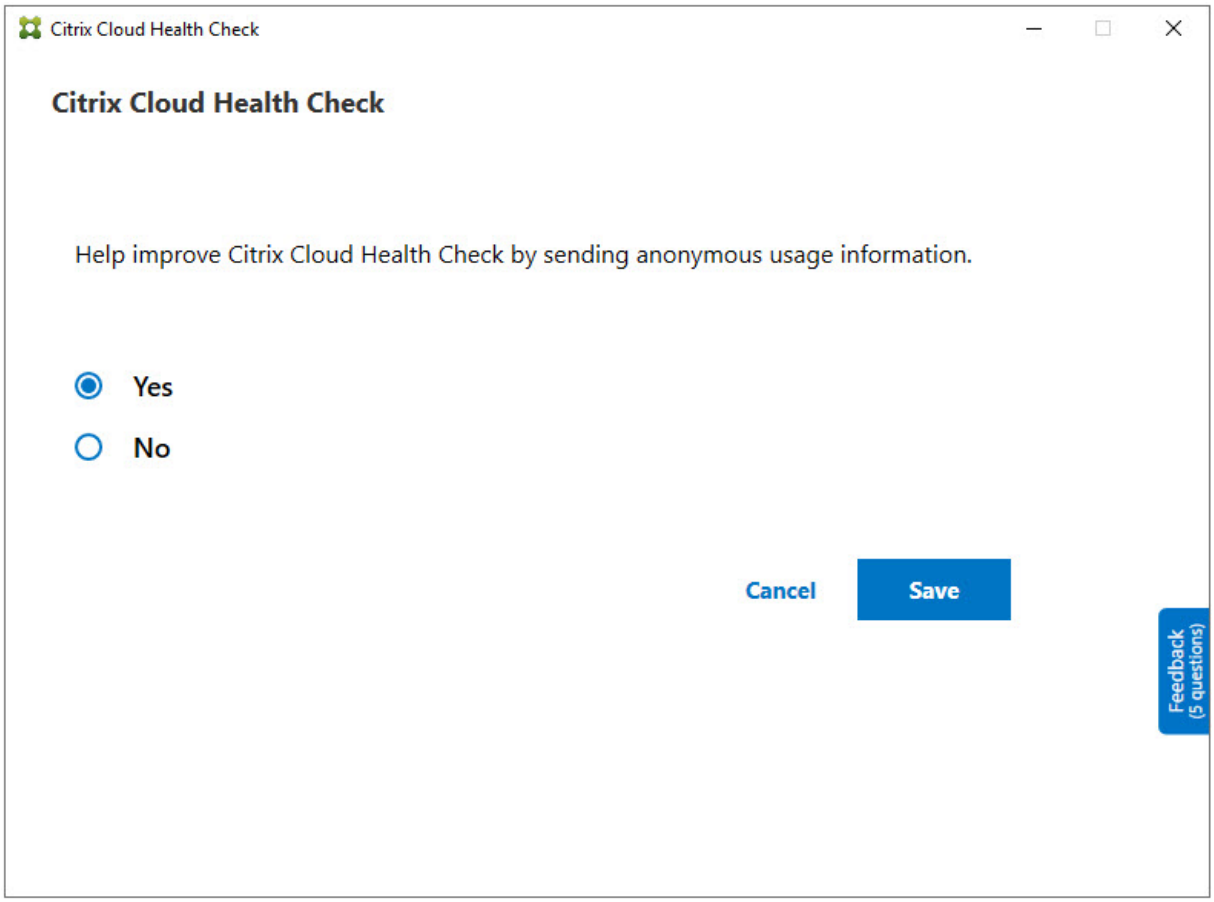
  - File and printer sharing is turned on. See the Microsoft documentation for instructions.

- **Enable PSRemoting and WinRM** - You can enable PowerShell remoting and WinRM by running PowerShell as an administrator, then running the Enable-PSRemoting cmdlet. For details, see the Microsoft help for the cmdlet.
- **Cloud Health Check requires PowerShell 3.0 or later** - Install PowerShell 3.0 or later on the machine, and then enable PowerShell remoting.
- **WMI is not running on the machine** - Ensure that Windows Management Instrumentation (WMI) access is enabled.
- **WMI connections blocked** - Enable WMI in the Windows Firewall service.

Usage data collection

When you use Cloud Health Check, Citrix uses Google Analytics to collect anonymous usage data to be used for future product features and improvements. Data collection is enabled by default.

To change usage data collection and upload, click the **Settings** gear in the Cloud Health Check UI. You can then choose whether to send the information by selecting **Yes** or **No** and then clicking **Save**.



Automatic fix

Automatic fix allows Cloud Health Check to automatically detect and fix certain issues by changing the settings or restarting the services.

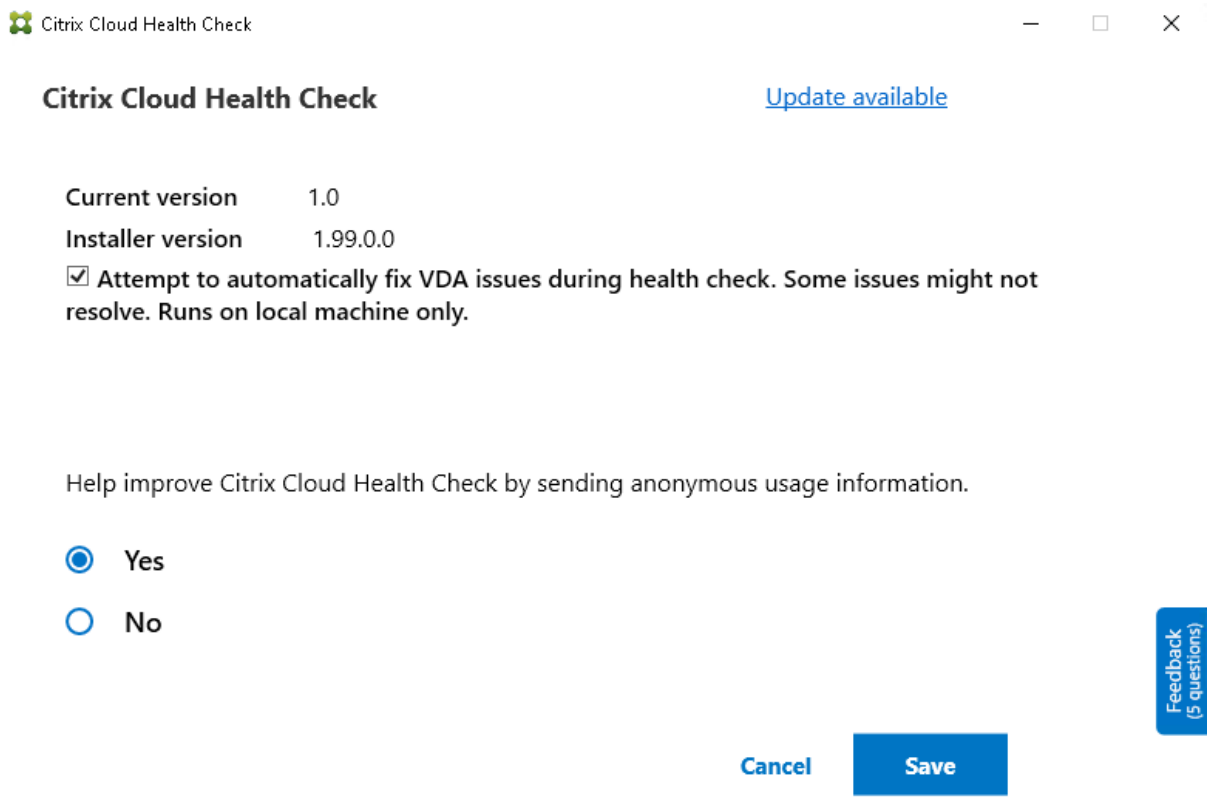
Automatic fix checks the following VDA registration items, with the recommended fixes:

- VDA machine domain membership
  - Fix: Test connection security channel with a "repair"model to fix
- VDA services status
  - Fix: Restart BrokerAgent service
- Communication with Controller
  - Fix: Restart BrokerAgent service
- Time sync with Controller
  - Fix: Run W32tm command

For session launches, automatic fix checks the following item, with the recommended fix:

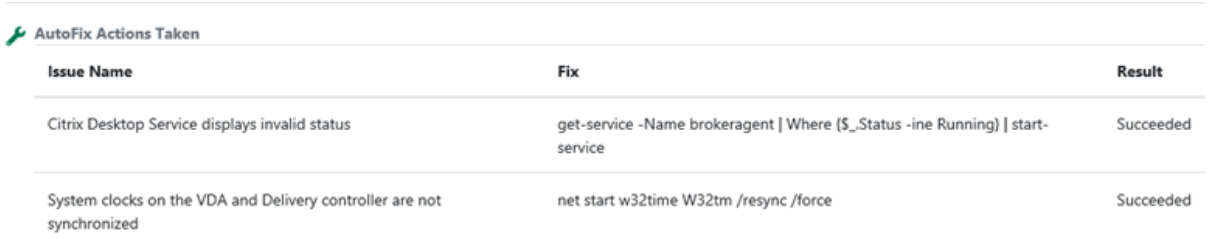
- Session launch service status
  - Fix: Restart BrokerAgent service

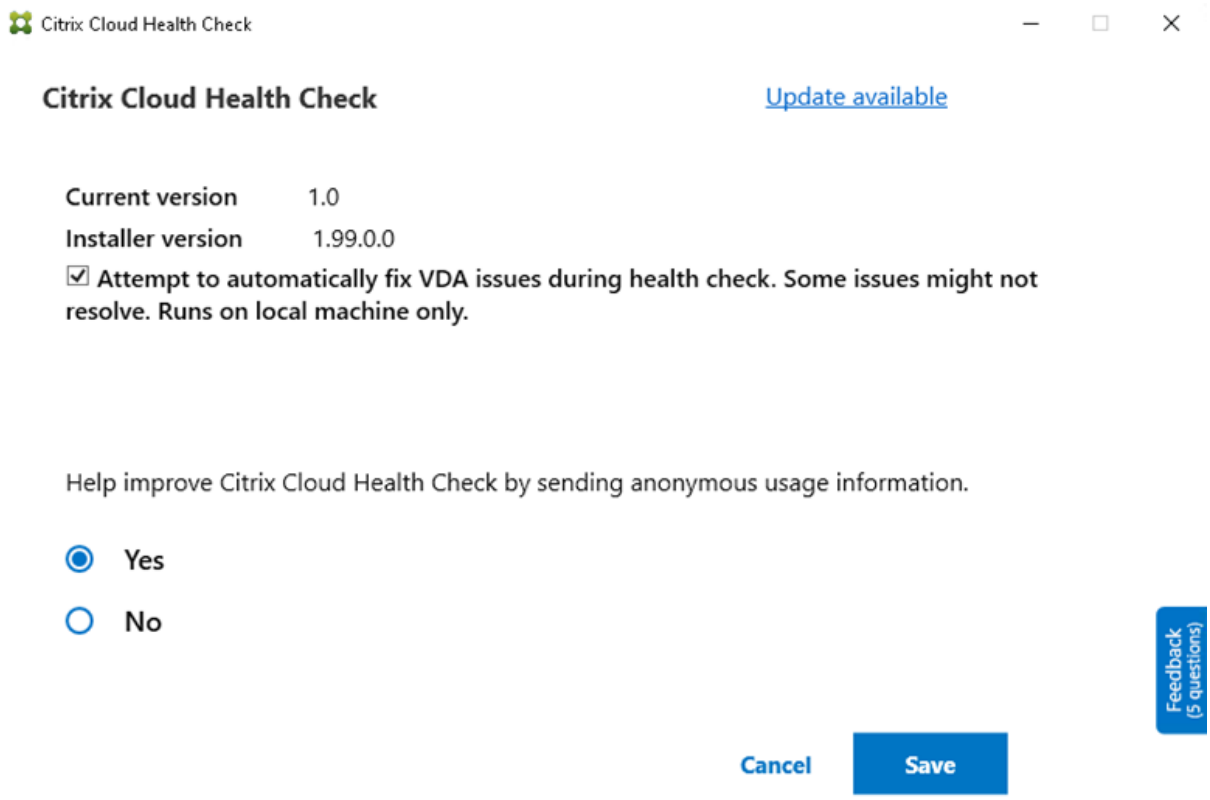
This feature is enabled by default. To disable it, click the gear icon in the upper right corner of the Cloud Health Check main window and then clear **Attempt to automatically fix VDA issues during health check**.



Result report

After running automatic fix, there is a section in the check results report to show all the details:





Troubleshooting

When Cloud Health Check fails to run or any exception occurs, check the Cloud Health Check log in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

The Cloud Health Check log for each target machine is in `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

To enable the debug log:

Edit `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, update `<add name="TraceLevelSwitch"value="3"/>` to `<add name="TraceLevelSwitch"value="4"/>`, save the file and reopen Cloud Health Check.

Feedback

To leave feedback on Cloud Health Check, fill out the Citrix survey.

Configuration logging

June 25, 2024

> **Note:**
>
> Configuration log records appear only in English, regardless of which language you select for your Citrix Cloud account. Dates and times associated with those records are in MM/DD/YY format, expressed in Coordinated Universal Time (UTC).

Configuration logging is a feature that captures Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment configuration changes and administrative activities to a logging database in Citrix Cloud. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes are made. The log provides a breadcrumb trail.
- Assist change management and track configurations.
- Report administrative activities.

In this Citrix DaaS, configuration logging is always enabled. You cannot disable it.

From the Full Configuration management interface, you can view configuration log content, filtered by date ranges or by full text search. You can also generate a CSV report using PowerShell. From this console, you cannot edit or delete log content. You can use the Remote PowerShell SDK to schedule periodic data deletion from the log.

Update the retention of DaaS configuration logs

To maintain the performance of DaaS tenants, starting September 9th, 2024 configuration log retention will be set to 180 days.

Logs older than 180 days on September 9th, 2024 will be deleted. As we keep growing our DaaS Limits for a single DaaS tenant, this implementation ensures the best performance and resilience for our customers.

As a best practice, we advise customers to have a quarterly export mechanism. This can be done through PowerShell, see Generate reports. We also recommend customers schedule periodic date deletion, see Schedule periodic data deletion.

Permissions required (see Delegated administration):

- Full Administrators in Citrix Cloud, plus Citrix DaaS Cloud Administrators and Read Only Administrators can view configuration logs in the **Manage** console.

- Full Administrators and Cloud Administrators can also download a CSV report of logging activity, using PowerShell.

What is logged

The following operations are logged:

- Configuration changes and administrative activities initiated from the **Manage** and **Monitor** tabs
- PowerShell scripts
- REST API requests

> **Note:**
>
> You cannot see log entries for Citrix Cloud platform internal operations, such as database setup and management.

Examples of logged configuration changes include working with (creating, editing, deleting, assigning):

- Machine catalogs
- Delivery groups (including changing power management settings)
- Administrator roles and scopes
- Host resources and connections
- Citrix policies through the **Manage** console

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Manage or monitor functions sending a message to a user

The following operations are not logged. (Many of them are not available to customer administrators.)

- Automatic operations such as pool management power-on of virtual machines.
- Policy actions implemented through the Group Policy Management Console (GPMC). Use Microsoft tools to view logs of those actions.
- Changes made through the registry or from sources other than the Full Configuration management interface, Monitor, or PowerShell.

View configuration log content

To view configuration log content, follow these steps:

1. Sign in to Citrix Cloud. Select **My Services > DaaS** in the upper left menu.
2. From **Manage > Full Configuration**, select **Logging > Events** in the left pane.

By default, the display in the center pane lists the log content chronologically (newest entries first), separated by date. You can:

- Sort the display by column header.
- Filter the display by specifying a day interval or a custom time period, or by entering text in the Search box. To return to the standard display after using search, clear the text in the Search box.
- Choose which columns appear in the display by selecting the **Columns to Display** icon in the top right corner of the table. For example, to view the IP address that the administrator uses to access DaaS, click the icon and add the **Client IP** column.

Display characteristics:

- High-level operations created during management and monitoring are listed in the upper middle pane. A high-level operation results in one or more services and PowerShell SDK calls, which are low-level operations. When you select a high-level operation in the upper middle pane, the lower pane displays the low-level operations.
- If you create a low-level operation in PowerShell without specifying a parent high-level operation, configuration logging creates a surrogate high-level operation.
- If an operation fails before completion, the log operation might not be completed in the database. For example, a start record has no corresponding stop record. In such cases, the log indicates that there is missing information. When you display logs based on time ranges, incomplete logs are shown if the data in the logs matches the criteria. For example, if you request logs for the last five days, and a log with a start time in the last five days has no end time, it is included.
- Remember: You cannot see log entries for Citrix Cloud platform internal operations, such as database setup and management.

View tasks related to machine catalog operations

To view tasks related to machine catalog operations, navigate to **Manage > Full Configuration > Logging > Tasks**. The **Tasks** tab displays only tasks related to catalogs created through Machine Creation Services (MCS) or Provisioning Services (PVS). Specifically, tasks associated with the following machine catalog operations appear:

- Create catalogs
- Clone catalogs
- Add machines
- Remove machines
- Update a catalog (update images or machines)

- Roll back machine updates

> **Tip:**
>
> The **Tasks** tab displays only tasks related to provisioning scheme changes (creating or modifying a provisioning scheme).

A task can be in the following state:

- Completed
- Not started
- Running
- Canceled
- Failed
- Unknown

To cancel a running task, select the task and then click **Cancel**. The cancelation takes some time to complete.

Examples of logged tasks include:

- Image update completed for a certain catalog
- Error while updating the image for a certain catalog
- Canceled image update for a certain catalog
- Provisioning VMs to a certain catalog
- Removing VMs from a certain catalog
- Created a certain catalog

By default, the display in the center pane lists logged tasks chronologically (newest entries first), separated by date. You can sort the display by column header. To clear completed tasks, click **Clear Completed Tasks** under the **Tasks** tab. To choose which columns to appear in the display, select the **Columns to Display** icon in the top right corner of the table.

View API logs

To view REST API logs, navigate to **Manage > Full Configuration > Logging > APIs**. The **APIs** tab displays REST API requests made during a certain time period.

Be aware of the following considerations:

- REST API logs are cleared after you sign out of the console. (They are also cleared if you refresh your browser window.)
- Any operations in the console that result in API calls have their corresponding API requests displayed on the **APIs** tab.

- The display lists the API requests chronologically (newest entries first), separated by date. The maximum number of API requests in the display is 1,000.

View PowerShell logs

To view PowerShell commands corresponding to UI actions you've taken during the day, navigate to the **Manage > Full Configuration > Logging > PowerShell** tab.

Associate metadata with configuration logs

You can attach metadata to configuration logs by associating a `name-value` pair called `MetadataMap` with the log records.

> **Note:**
>
> - You can only attach metadata to high-level operation objects.
> - Metadata is associated with the existing records at the time of execution.

Set the metadata

Run the PowerShell command `Set-LogHighLevelOperationMetadata` to associate a log record with the `MetadataMap`.
`Set-LogHighLevelOperationMetadata` takes the following parameters:

- **Id**:ID of the high-level operation.
- **InputObject**:The high-level operations to which you add the metadata. This is an alternative to the `Id` parameter where a high-level operation object or list of objects is passed to the PowerShell command.
- **Name**:Property name of the metadata to be added. The property must be unique for the high-level operation specified. The property cannot contain any of the following characters: `()\/;:#.*?=<>|[]"'`
- **Value**:Value for the property.
- **Map**:Dictionary of (name, value) pairs for the properties. This is an alternative to setting the metadata using the `-Name` and `-Value` parameters.

For example, to attach the metadata to all the high-level log records with Id 40, run the following PowerShell command:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```


To attach the metadata to the high-level record with the user `abc@example.com`, run the following PowerShell command:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

Retrieve using the metadata

Run the following PowerShell commands to use the associated metadata to retrieve the log records:

- Search by key and value:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Search by value and any key:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Search by key and any value:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

Remove the metadata

Run the PowerShell command `Remove-LogHighLevelOperationMetadata` to remove the associated metadata.
`Remove-LogHighLevelOperationMetadata` takes the following parameters:

- **Id**:ID of the high-level operation.
- **InputObject**:The high-level operations to which you add the metadata. This is an alternative to the `Id`‘ parameter where a high-level operation object or list of objects is passed to the PowerShell command.
- **Name**:Property name of the metadata to be removed. Set to $null to remove all the metadata for the specified object.
- **Map**:Dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{“name1”=“val1”; “name2”=“val2”}) or a string dictionary (created with new-object “System.Collections.Generic.Dictionary[String, String]”). The properties whose names match the keys in the map are removed.

Generate reports

To generate a CSV or HTML report containing configuration log data, use PowerShell cmdlets for the ConfigLogging Service in the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For details, see:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

Schedule periodic data deletion

Use the Remote PowerShell SDK to specify how long data is retained in the configuration logging database. (This feature is not available in the Full Configuration management interface.) In Citrix DaaS, you must have Full access.

In the `Set-LogSite` cmdlet, the `-LoggingDBPurgeDurationDays` parameter specifies how many days data is retained in the configuration logging database before it's deleted automatically.

- By default, the value of this parameter is 0. A zero value means that data in the configuration logging database is never deleted automatically.
- When you set a non-zero value, the database is checked once every 120 minutes. Data older than the retention period is deleted.

Use `Get-LogSite` to view the current value of the parameter.

Differences from on-premises Citrix Virtual Apps and Desktops

If you're familiar with configuration logging in the on-premises Virtual Apps and Desktops product, the Citrix Cloud version has several differences. In Citrix Cloud:

- Configuration logging is always enabled. You cannot disable it. Mandatory logging is not available.
- You cannot change the location of the configuration logging database, because the database is managed in the Citrix Cloud platform.
- Configuration log displays do not include operations and activities that are performed within the Citrix Cloud platform.
- PowerShell is your only choice to create a CSV or HTML report of logged operations. In the on-premises product, reports can be generated from Citrix Studio or PowerShell.
- You cannot delete configuration log content.

Delegated administration

March 13, 2024

Overview

With delegated administration in Citrix Cloud, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization.

By default, administrators have full access. This setting enables access to all available customer administration and management functions in Citrix Cloud, plus all subscribed services. To tailor an administrator's access:

- Configure custom access for an administrator's general management permissions in Citrix Cloud.
- Configure custom access for subscribed services. In Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), you can configure custom access when you invite a new administrator. You can change an administrator's access later.

For information about displaying the list of administrators and defining access permissions, see Manage administrator access to Citrix Cloud.

This article describes how to configure custom access in Citrix DaaS.

Administrators, roles, and scopes

Delegated administration uses three concepts for custom access: administrators, roles, and scopes.

- **Administrators:** An administrator represents a person identified by their Citrix Cloud sign-in, which is typically an email address. Each administrator is associated with one or more role and scope pairs.
- **Roles:** A role represents a job function, and has permissions associated with it. These permissions allow certain tasks that are unique to Citrix DaaS. For example, the Delivery Group Administrator role has permission to create a delivery group and remove a desktop from a delivery group, plus other associated permissions. An administrator can have multiple roles. An administrator might be a Delivery Group Administrator and a Machine Catalog Administrator.

  Citrix DaaS offers several built-in custom access roles. You cannot change the permissions within these built-in roles, or delete those roles.

  You can create your own custom access roles to meet your organization's requirements, and delegate permissions with more detail. Use custom roles to allocate permissions at the granularity of an action or task. You can delete a customized role only if it is not assigned to an administrator.

  You can change which roles an administrator has.

  A role is always paired with a scope.

- **Scopes:** A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your organization. Objects can be in more than one scope.

  There is one built-in scope: All, which contains all objects. Citrix Cloud and Help Desk administrators are always paired with the All scope. That scope cannot be changed for those administrators.

  When you invite (add) an administrator for this service, a role is always paired with a scope (by default, the All scope).

  You create and delete scopes in the **Manage > Full Configuration** interface. You assign role/scope pairs in the Citrix Cloud console.

  A scope is not shown for Full access administrators. By definition, those administrators can access all customer-managed Citrix Cloud and subscribed services objects.

Built-in roles and scopes

Citrix DaaS has the following built-in roles.

- **Cloud Administrator:** Can perform all tasks that can be initiated from Citrix DaaS.

  Can see the **Manage** and **Monitor** tabs in the console. This role is always combined with the All scope. You cannot change the scope.

  Do not be confused by this role's name. A custom access Cloud Administrator cannot perform Citrix Cloud-level tasks (Citrix Cloud tasks require Full access).

- **Read Only Administrator:** Can see all objects in the specified scopes (in addition to global information), but cannot change anything. For example, a Read Only Administrator with a scope of London can see all global objects and any objects in the London scope (for example, London Delivery Groups). However, that administrator cannot see objects in the New York scope (assuming that the London and New York scopes do not overlap).

  Can see the **Manage** and **Monitor** tabs in the console.

- **Help Desk Administrator:** Can view delivery groups, and manage the sessions and machines associated with those groups. Can see the machine catalog and host information for the delivery groups being monitored. Can also perform session management and machine power management operations for the machines in those delivery groups.

  Can see the **Monitor** tab in the console. Cannot see the **Manage** tab. This role is always combined with the All scope. You cannot change the scope.

- **Machine Catalog Administrator:** Can create and manage machine catalogs and provision the machines into them. Can manage base images and install software, but cannot assign applications or desktops to users.

Can see the **Monitor** and **Manage** tabs in the console. Cannot see the **Monitor** tab. You can change the scope.

- **Delivery Group Administrator:** Can deliver applications, desktops, and machines. Can also manage the associated sessions. Can manage application and desktop configurations such as policies and power management settings.

  Can see the **Monitor** and **Manage** tabs in the console. You can change the scope.

  > **Note:**
  >
  > To change a desktop's display name as a Delivery Group Administrator, you need the **Perform Machine Update** permission. This permission is necessary because changing the display name involves updating the machine property.

- **Host Administrator:** Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

  Can see the **Manage** tab in the console. Cannot see the **Monitor** tab. You can change the scope.

- **Session Administrator:** Can view delivery groups being monitored and manage their associated sessions and machines.

  Can see the **Monitor** tab in the console. Cannot see the **Manage** tab. You cannot change the scope.

- **Full Administrator:** Can perform all tasks and operations. A full administrator is always combined with **All scope**.

  Can see the **Manage** and **Monitor** tabs in the console. This role is always combined with **All scope**. You cannot change the scope.

- **Full Monitor Administrator:** Has full access to all views and commands on the **Monitor** tab.

  Can see the **Monitor** tab in the console. Cannot see the **Manage** tab. You cannot change the scope.

- **Probe Agent Administrator:** Has access to Probe Agent APIs.

  Can see the **Monitor** and **Manage** tabs in the console. Has read-only access to the **Applications** page but cannot access any other views.

The following table summarizes which console tabs are visible for each custom access role in Citrix DaaS, and whether the role can be used with custom scopes.

Custom access administrator role	Can see **Manage** tab in console?	Can see **Monitor** tab in console?	Can role be used with custom scopes?
Cloud Administrator	Yes	Yes	No
Read Only Administrator	Yes	Yes	Yes
Help Desk Administrator	No	Yes	No
Machine Catalog Administrator	Yes	Yes	Yes
Delivery Group Administrator	Yes	Yes	Yes
Host Administrator	Yes	No	Yes
Session Administrator	No	Yes	No
Full Administrator	Yes	Yes	No
Full Monitor Administrator	No	Yes	No
Probe Agent Administrator	Yes	Yes	No

> **Note:**
>
> Custom access administrator roles (except Cloud Administrator and Help Desk Administrator) are not available for Citrix Virtual Apps and Desktops Standard for Azure, Virtual Apps Essentials, and Virtual Desktops Essentials.

To view the permissions associated with a role:

1. Sign in to Citrix Cloud. Select **My Services > DaaS** in the upper left menu.
2. From **Manage > Full Configuration**, select **Administrators** in the left pane.
3. Select the **Roles** tab.
4. Select a role in the upper middle pane. The **Role definition** tab in the lower pane lists the categories and permissions. Select a category to see the specific permissions. The **Administrators** tab lists the administrators who have been assigned the selected role.

   Known issue: A Full Administrator entry does not display the correct set of permissions for a full access Citrix DaaS administrator.

How many administrators you need

The number of administrators and the granularity of their permissions generally depend on the size and complexity of the deployment.

- In small or proof of concept deployments, one or a few administrators do everything. There is no custom access delegation. In this case, each administrator has Full access, which always has the All scope.
- In larger deployments with more machines, applications, and desktops, more delegation is needed. Several administrators might have more specific functional responsibilities (roles). For example, two have Full access, and others are Help Desk Administrators. Also, an administrator might manage only certain groups of objects (scopes), such as machine catalogs in a particular department. In this case, create new scopes, plus administrators with the appropriate custom access role and scopes.

Administrator management summary

Setting up administrators for Citrix DaaS follows this sequence:

1. If you want the administrator to have a role other than a Full administrator (which covers all subscribed services in Citrix Cloud) or a built-in role, create a custom role.
2. If you want the administrator to have a scope other than All (and a different scope is allowed for the intended role, and has not already been created), create scopes.
3. From Citrix Cloud, invite an administrator. If you want the new administrator to have anything other than the default Full access, specify a custom access role and scope pair.

Later, if you want to change an administrator's access (roles and scope), see Configure custom access.

Add an administrator

To add (invite) administrators, follow the guidance in Add administrators to a Citrix Cloud account. A subset of that information is repeated here.

> **Important:**
>
> Do not confuse how "custom" and "custom access" are used.
>
> - When creating administrators and assigning roles for Citrix DaaS in the Citrix Cloud console, the term "custom access" includes both the built-in roles and any additional custom roles that were created in the service's **Manage > Full Configuration** interface.

> - In the service's **Manage > Full Configuration** interface, "custom"simply differentiates that role from a built-in role.

The general workflow for adding administrators is as follows:

1. Sign in to Citrix Cloud and then select **Identity and Access Management** in the upper left menu.
2. On the **Identity and Access Management** page, select **Administrators**. The **Administrators** tab lists all current administrators for the account.
3. On the **Administrators** tab, select your identity type, enter the administrator's email address, and then click **Invite**.

- Select **Full access** if you want the administrator to have full access. In that way, the administrator can access all customer administrator functions in Citrix Cloud and in all subscribed services.
- Select **Custom access** if you want the administrator to have limited access. You can then select a custom access role and scope pair. In that way, the administrator has the intended permissions when signing in to Citrix Cloud.

1. Click **Send Invite**. Citrix Cloud sends an invitation to the email address and adds the administrator to the list after the administrator completes onboarding.

When receiving the email, the administrator clicks the **Sign In** link to accept the invitation.

For more information about adding administrators, see Manage Citrix Cloud administrators.

Alternatively, go to **Manage > Full Configuration > Administrators > Administrators** and click **Add Administrator**. You are directly taken to **Identity and Access Management > Administrators**, which opens in a new browser tab. After you are finished adding administrators there, close the tab and return to the console to continue with your other configuration tasks.

Create and manage roles

When administrators create or edit a role, they can enable only the permissions that they themselves have. This control prevents administrators from creating a role with more permissions than they currently have and then assigning it to themselves (or editing a role that they are already assigned).

Custom role names can contain up to 64 Unicode characters. Names cannot contain: backslash, forward slash, semicolon, colon, pound sign, comma, asterisk, question mark, equal sign, left arrow, right arrow, pipe, left or right bracket, left or right parenthesis, quotation marks, and apostrophe.

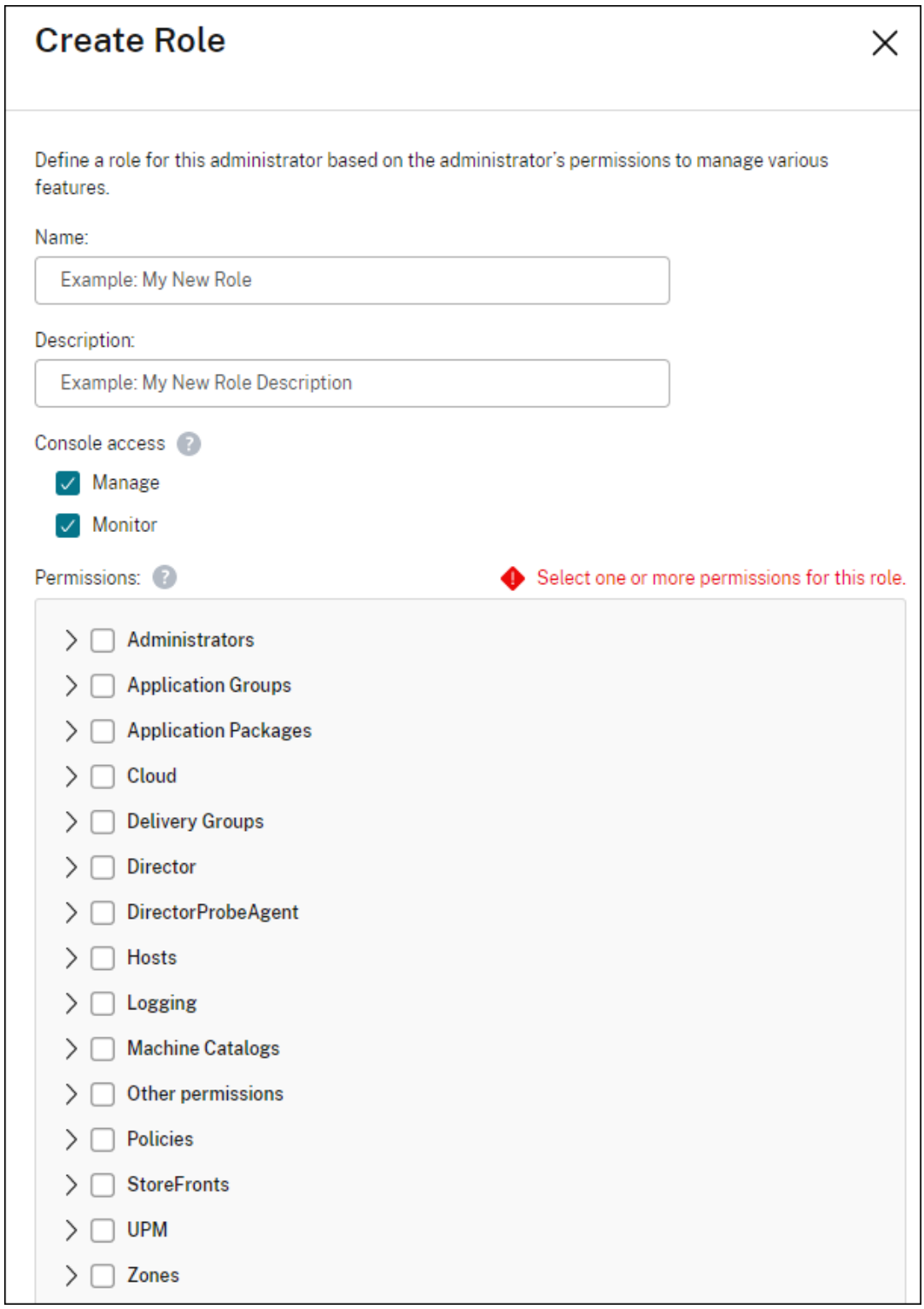
Role descriptions can contain up to 256 Unicode characters.

1. Sign in to Citrix Cloud if you haven't already. Select **My Services > DaaS** in the upper left menu.
2. From **Manage > Full Configuration**, select **Administrators** in the left pane.

3. Select the **Roles** tab.
4. Follow the instructions for the task you want to complete:

    - **View role details:** Select the role in the middle pane. The lower portion of the middle pane lists the object types and associated permissions for the role. Select the **Administrators** tab in the lower pane to display a list of administrators who currently have this role.
    - **Create a custom role:** Select **Create Role** in the action bar. Configure settings as follows:

        – Enter a name and description.
        – Configure console access. Determine which consoles are visible to the administrators. You can proceed without selecting any console. In that case, administrators with the role cannot access **Manage** and **Monitor** but can access, view, or manage objects through SDKs and APIs.
        – Select the object types and permissions. To grant full access permission to an object type, select its check box. To grant permission at a granular level, expand the object type and then select **Read Only** or individual objects under **Manage** within the type.



- **Copy a role:** Select the role in the middle pane and then select **Copy Role** in the action bar. Change the name, description, object types, and permissions, as needed. When you're done, select **Save**.

- **Edit a custom role:** Select the role in the middle pane and then select **Edit Role** in the action bar. Change the name, description, object types, and permissions, as needed. You cannot edit a built-in role. When you're done, select **Save**.
- **Delete a custom role:** Select the role in the middle pane and then select **Delete Role** in the action bar. When prompted, confirm the deletion. You cannot delete a built-in role. You cannot delete a custom role if it is assigned to an administrator.

Create and manage scopes

By default, all roles have the All scope for their relevant objects. For example, a Delivery Group Administrator can manage all Delivery Groups. For some administrator roles, you can create a scope that allows that administrator role to access a subset of the relevant objects. For example, you might want a give a Machine Catalog Administrator access to only catalogs that contain a certain type of machines, rather than all catalogs.

- Full access administrators or custom access Cloud Administrators can create scopes for the Read Only Administrator, Machine Catalog Administrator, Delivery Group Administrator, and Host Administrator roles.
- Scopes cannot be created for Full access administrators, nor can they be created for Cloud Administrators or Help Desk Administrators. Those administrators always have the All scope.

Rules for creating and managing scopes:

- Scope names can contain up to 64 Unicode characters. Names cannot include: backslash, forward slash, semicolon, colon, pound sign, comma, asterisk, question mark, equal sign, left or right arrow, pipe, left or right bracket, left or right parenthesis, quotation marks, and apostrophe.
- Scope descriptions can contain up to 256 Unicode characters.
- When you copy or edit a scope, keep in mind that removing objects from the scope can make those objects inaccessible to an administrator. If the edited scope is paired with one or more roles, ensure that your scope updates do not make any role/scope pair unusable.

To create and manage scopes:

1. Sign in to Citrix Cloud. Select **My Services > DaaS** in the upper left menu.
2. From **Manage > Full Configuration**, select **Administrators** in the left pane.
3. Select the **Scopes** tab.
4. Follow the instructions for the task you want to complete:

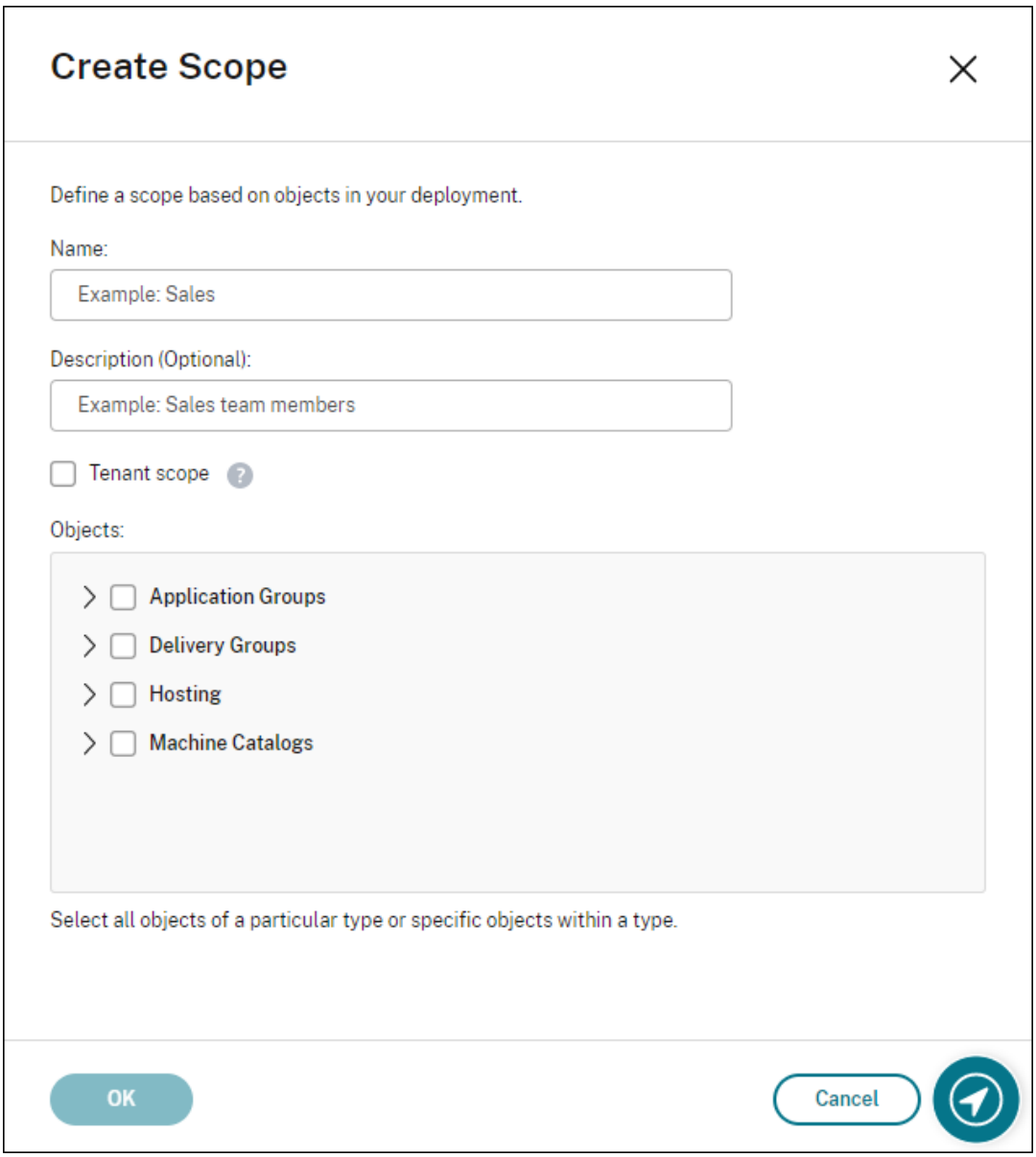
    - **View scope details:** Select the scope. The lower portion of the pane lists the objects and administrators that have that scope.

- **Create a scope:** Select **Create Scope** in the action bar. Enter a name and description. The objects are listed by type, such as delivery group and machine catalog.
  - To include all objects of a particular type (for example, all delivery groups), select the check box for the object type.
  - To include individual objects within a type, expand the type and then select the check boxes for the objects (for example, specific delivery groups).

    > **Note:**
    >
    > Application groups, delivery groups, or machine catalogs are displayed in folder structures that align with their management in DaaS. You can select a folder to select all its objects or expand a folder to select specific objects.

  - To create a tenant customer, select the **Tenant scope** check box. If selected, the name you entered for the scope is the tenant name. For more information about the tenant scope, see Tenant management.

When you're done, select **OK**.



- **Copy a scope:** Select the scope in the middle pane and then select **Copy Scope** in the action bar. Change the name, description. Change the object types and objects, as needed. When you're done, select **Save**.
- **Edit a scope:** Select the scope in the middle pane and then select **Edit Scope** in the action bar. Change the name, description, object types, and objects, as needed. When you're done, select **Save**.
- **Delete a scope:** Select the scope in the middle pane and then select **Delete Scope** in the action bar. When prompted, confirm the deletion.

  You cannot delete a scope if it is assigned to a role. If you attempt to do this, an error message indicates that you do not have permission. In fact, the error occurs because the role/s-

cope pair that uses this scope is assigned to an administrator. First, remove the role/scope pair assignment for all administrators who use it. Then delete the scope in the **Manage** console.

After you create a scope, it appears in the **Custom access** list in the Citrix Cloud console. You can then select it when you assign a role to an administrator.

For example, let's say you create a scope named CAD, and select the catalogs that contain machines suitable for CAD applications. When you return to the Citrix Cloud console and select **Edit scopes** for a role, the list of available scopes displays the CAD scope you created earlier.

The Cloud Administrator and Help Desk Administrator always have the All scope, so the CAD scope does not apply to them.

Tenant management

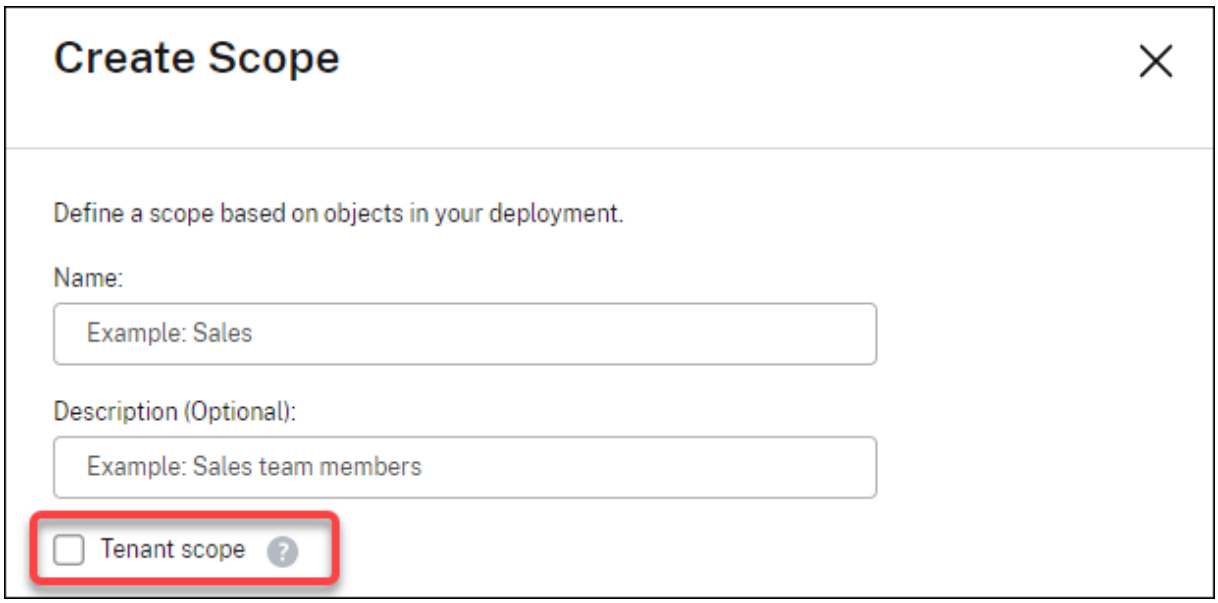
Using the Full Configuration management interface, you can create mutually exclusive tenants under a single Citrix DaaS. You achieve that by creating tenant scopes in **Administrators > Scopes** and associating related configuration objects, such as machine catalogs and delivery groups, with those tenants. As a result, administrators with access to a tenant can manage only objects that are associated with the tenant.

This feature is useful, for example, if your organization:

- Has different business silos (independent divisions or separate IT management teams) or
- Has multiple on-premises sites and wants to maintain the same setup in a single Citrix DaaS instance.

The interface lets you filter tenant customers by name. By default, the interface displays information about all tenant customers. To display information about a specific tenant, select that tenant from the list in the upper-right corner.

Create a tenant customer To create a tenant customer, select **Tenant scope** when creating a scope. By selecting the option, you create a unique scope type that applies to objects in scenarios where you share a Citrix DaaS instance between different business units—each of those business units are independent of the others. After you create a tenant scope, you cannot change the scope type.



The **Scopes** tab displays all scope items. The only difference between regular scopes and tenant scopes is in the **Type** column. A blank column field indicates a regular scope. You can click the **Type** column to sort scope items if needed.

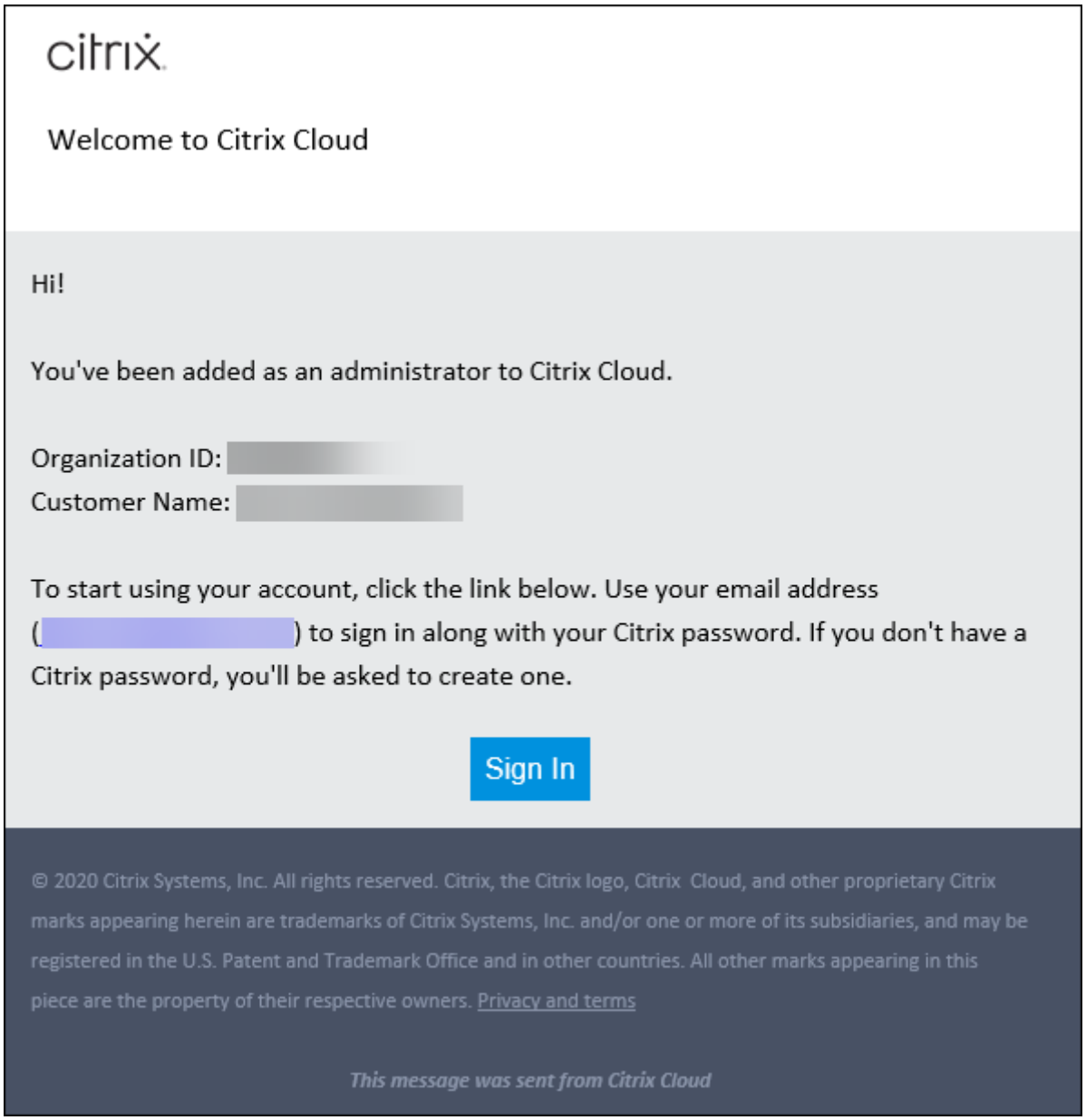
To see the resources (objects) attached to a scope, select **Administrators** in the left pane. On the **Scopes** tab, select the scope and then select **Edit Scope** in the action bar.

> **Tip:**
>
> The tenant property is assigned at a scope level. Machine catalogs, delivery groups, applications, and connections inherit the tenant property from the applicable scope.

When using a tenant scope, be aware of the following considerations:

- The tenant property is assigned in the following order: **Hosting > Machine Catalogs > Delivery Groups > Applications**. Lower-level objects rely on higher-level objects to inherit the tenant property from. For example, when selecting a delivery group, you must select the associated hosting and machine catalog. Otherwise, the delivery group cannot inherit the tenant property.
- After creating a tenant scope, you can edit tenant assignments by modifying objects. When a tenant assignment is changed, it is still subject to the constraint that it must be assigned to the same tenants or to a subset of those tenants. However, lower-level objects are not reevaluated when tenant assignments change. Make sure that objects are properly restricted when you change tenant assignments. For example, if a machine catalog is available for `TenantA` and `TenantB`, you can create a delivery group for `TenantA` and one for `TenantB`. (`TenantA` and `TenantB` are both associated with that machine catalog.) You can then change the machine catalog to be associated only with `TenantA`. As a result, the delivery group associated with `TenantB` becomes invalid.

Configure custom access for administrators After creating tenant scopes, configure custom access for respective administrators. For more information, see Configure custom access for an administrator. Citrix Cloud sends an invitation to those customer administrators you specified and adds them to the list. When they receive the email, they click **Sign In** to accept the invitation. When they log on to the **Full Configuration** management interface, they see resources that the assigned role and scope pairs contain.



Administrators with access to a tenant can manage only objects (for example, machine catalog, delivery group) that are associated with the tenant.

Configure custom access for an administrator

This feature lets you define access permissions of existing administrators or administrators you invite in a way that aligns with their role in your organization.

Changes you made to access permissions take 5 minutes to take effect. Logging out of the Full Configuration management interface and logging back on makes the changes take effect immediately. In scenarios where administrators still use the management interface after the changes take effect without reconnecting to it, a warning appears when they attempt to access items to which they no longer have permissions.

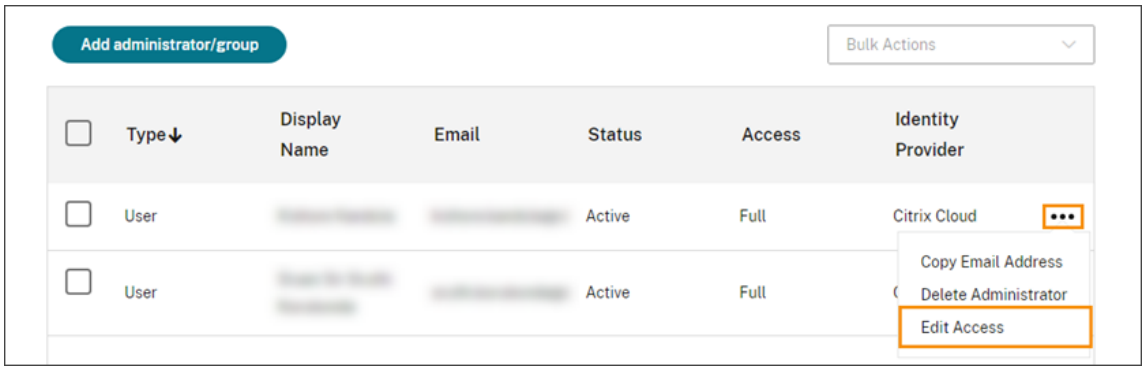
By default, when you invite administrators, they have Full access. Full access allows the administrator to manage all subscribed services and all Citrix Cloud operations (such as inviting more administrators). A Citrix Cloud deployment needs at least one administrator with Full access.

You can also grant custom access when you invite an administrator. Custom access allows the administrator to manage only the services and operations that you specify.

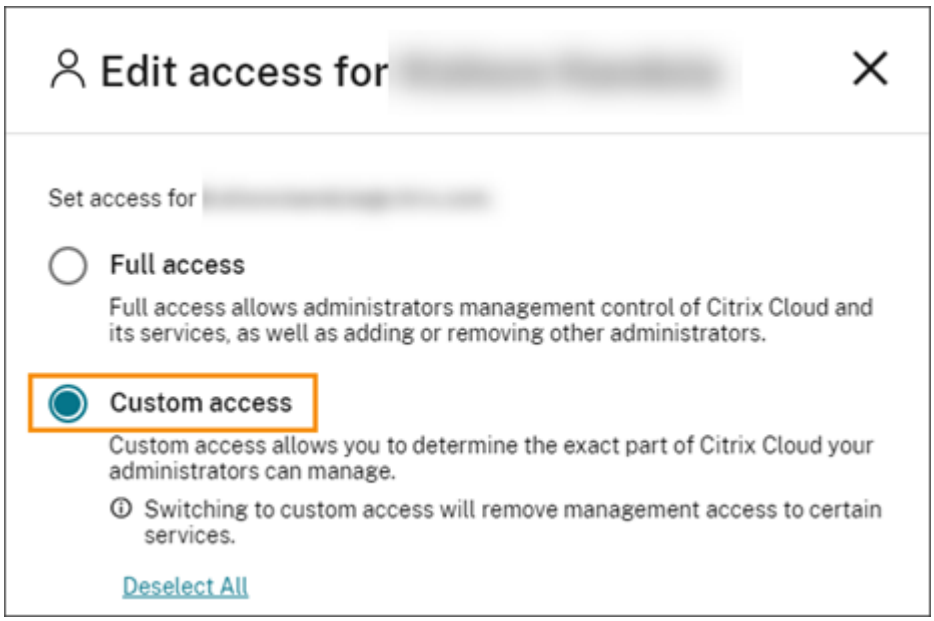
When you create a role or scope in Citrix DaaS, it appears in the custom access list and can be selected. When you select a role for an administrator, you can modify the scopes as needed to reflect the administrator's role in your organization.

To configure custom access for an administrator:

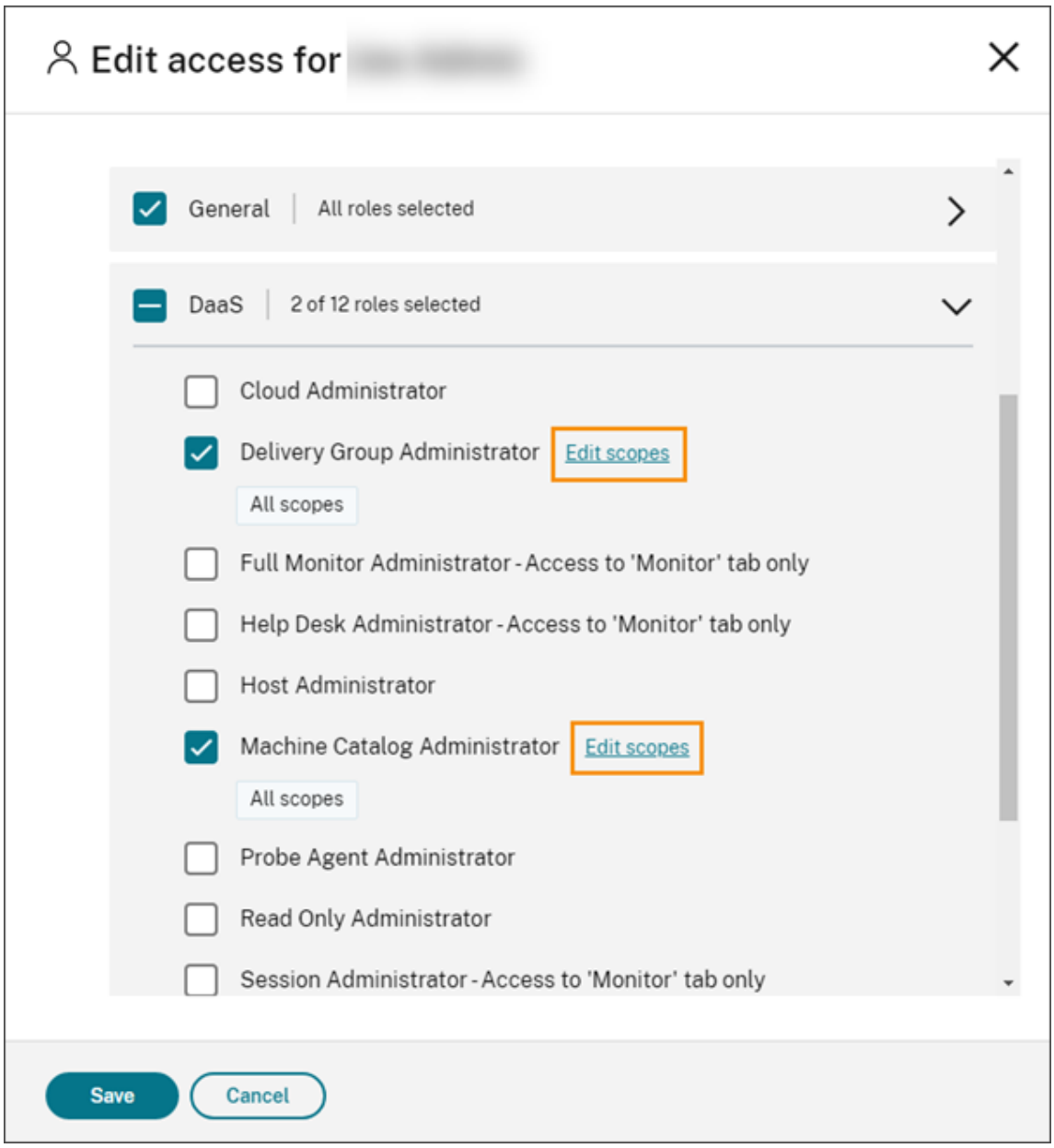
1. Sign in to Citrix Cloud. Select **Identity and Access Management** > **Administrators** in the upper left menu.
2. Locate the administrator you want to manage, select the ellipsis menu, and select **Edit access**.



3. Select **Custom access**.

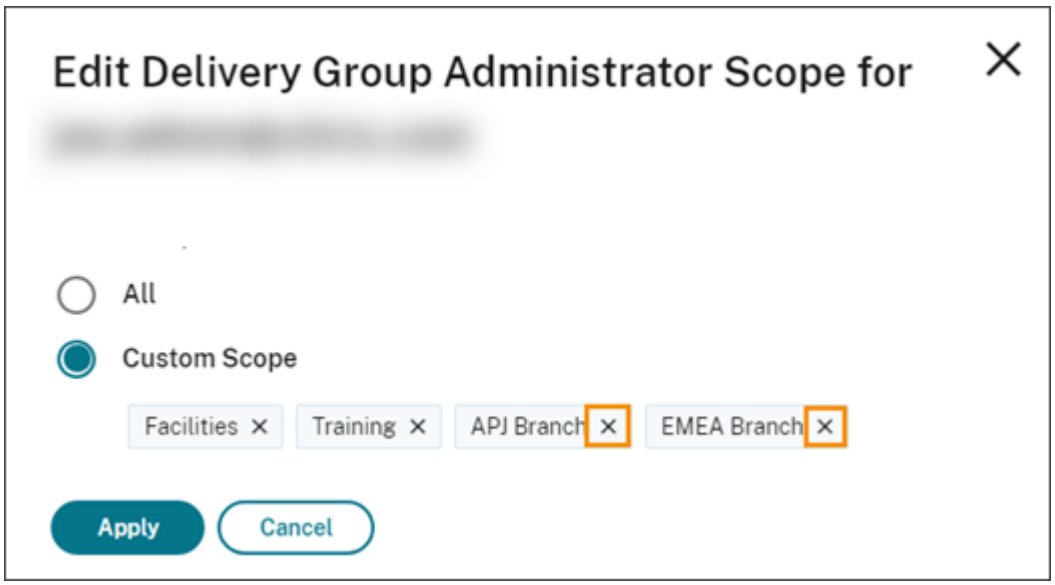


4. Under **DaaS**, select or clear the check marks next to one or more roles. To modify the scopes associated with an assigned role, select **Edit scopes**.

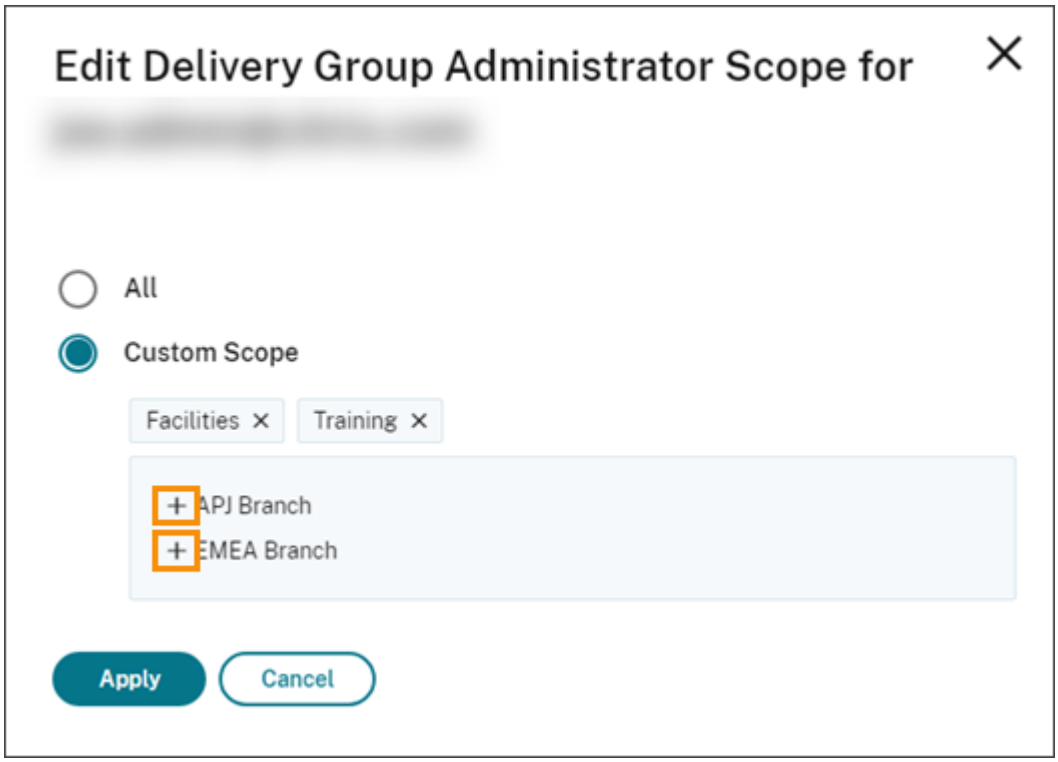


By default, each selected role has all scopes selected, as noted by the **All scopes** label.

5. To specify the scopes for a selected role, select **Custom Scope** and then add or remove the appropriate scopes. By default, all custom scopes are added to a role. To remove a scope, click the X icon on the scope.



Scopes that have been removed and are available to add to the role appear in a list below the scopes that are already added. To add a scope to the role, select the plus icon for the scope.



6. When you're finished selecting scopes, select **Apply**.
7. Select **Save** to save the selected roles for the administrator.

Differences from on-premises Citrix Virtual Apps and Desktops

If you're familiar with delegated administration in the on-premises Citrix Virtual Apps and Desktops product, Citrix DaaS version has several differences.

In Citrix Cloud:

- Administrators are identified by their Citrix Cloud login, rather than their Active Directory account. You can create role/scope pairs for Active Directory individuals, but not groups.
- Administrators are created, configured, and deleted in the Citrix Cloud console, rather than Citrix DaaS.
- Role/scope pairs are assigned to administrators in the Citrix Cloud console, rather than Citrix DaaS.
- Reports are not available. You can view administrator, role, and scope information in the service's **Manage > Full Configuration** interface.
- The custom access Cloud Administrator is similar to a Full Administrator in the on-premises version. Both have full management and monitoring permissions for the Citrix Virtual Apps and Desktops version being used.

  However, in Citrix DaaS, there is no named Full Administrator role. Do not equate "Full access" in Citrix Cloud with the "Full administrator"in on-premises Citrix Virtual Apps and Desktops. Full access in Citrix Cloud spans the platform-level domains, library, notifications, and resource locations, plus all subscribed services.

Differences from earlier Citrix DaaS releases

Before the release of the expanded custom access feature (September 2018), there were two custom access administrator roles: Full Administrator and Help Desk Administrator. When your deployment has delegated administration enabled (which is a platform setting), those roles are mapped automatically.

- An administrator who was formerly configured as a custom access **Virtual Apps and Desktops (or XenApp and XenDesktop) Service: Full Administrator** is now a custom access **Cloud Administrator**.
- An administrator who was formerly configured as a custom access **Virtual Apps and Desktops (or XenApp and XenDesktop) Service: Help Desk Administrator** is now a custom access **Help Desk Administrator**.

More information

See Delegated administration and monitoring for information about administrators, roles, and scopes used in the service's **Monitor** console.

Home page for the Full Configuration interface

August 31, 2023

Provides an overview of your Citrix DaaS deployment and workloads along with information that helps you get the most from your subscription. The page comprises the following parts:

- Service overview
- Service health alerts
- Recommendations
- What's new
- Preview features
- Get started

To access the home page, follow these steps:

1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage**.
3. Select **Manage > Full Configuration**. The home page appears.

Service overview

Provides an overview of your Citrix DaaS deployment and workloads:

- **Resources**. Shows the numbers of deployed resources and their counts by category.

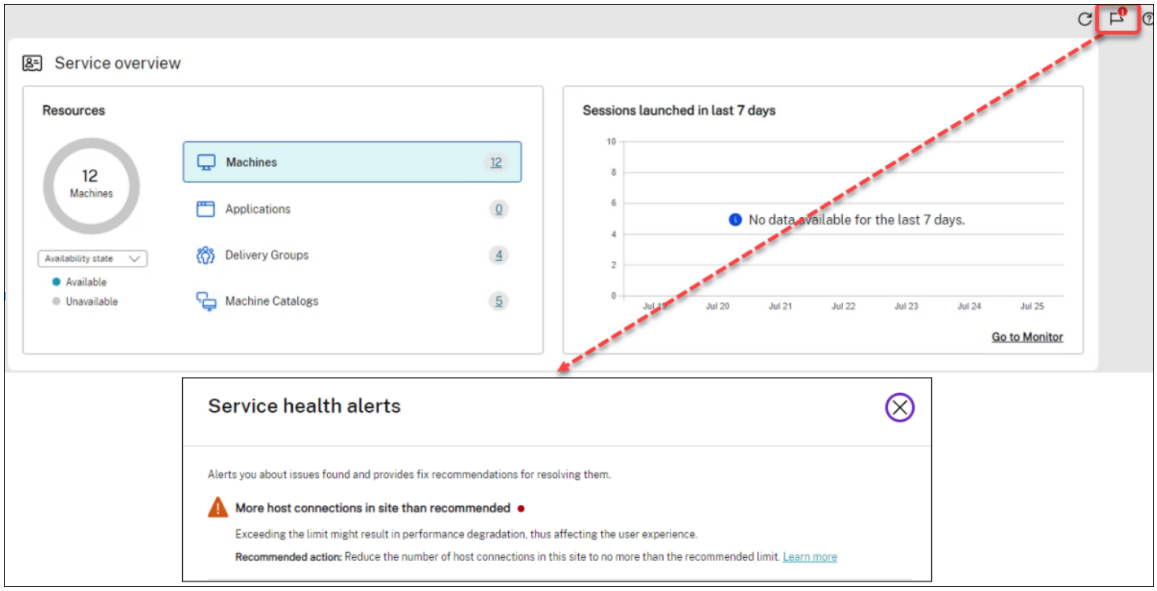
Resource	To view counts by category
Machines	Click **Machines**, select a state, and then hover over the donut chart for details. Available options: **Availability state** (Available, In use, Off, and Unavailable), **Registration state** (Registered and Unregistered), and **Maintenance state** (In maintenance and Not in maintenance). When viewing machine counts by availability state, you can click a state to view the corresponding machine details.
Applications	Click **Applications** and hover over the donut chart for details.
Delivery Groups	Click **Delivery Groups** and hover over the donut chart for details.
Machine Catalogs	Click **Machine Catalogs** and hover over the donut chart for details.

- **Sessions launched in last 7 days**. Shows the number of desktop and app sessions launched each day for the last seven days. To drill down for more details, click **Go to Monitor**.

Service health alerts

Alerts you about issues found and provides recommendations for resolving them. Alerts appear with warning and error symbols.

> **Note:**
>
> Diagnostics are updated on an hourly basis.
>
> Alert example:



Recommendations

Recommends features that are available with your subscription, such as Workspace Environment Management and Autoscale. To engage with us, like or dislike a recommendation and leave your feedback.

> **Note:**
>
> If you dislike a recommendation, the recommendation disappears. If you dislike all recommendations or the recommendation widget, the recommendation widget disappears.

What's new

Shows a select list of the latest Citrix DaaS features that are most valuable to your business. Using those features helps you get the most from your subscription. For a complete list of new features, see What's new.

Preview features

Shows features that are currently in preview. As a Citrix Cloud administrator with full access, you can turn preview features on or off without contacting Citrix. It takes up to 15 minutes for the changes to take effect.

Preview features are recommended for use in non-production environments. Issues found with preview features are not supported by Citrix Technical Support.

Get started

Shows steps that guide you through the initial setup of apps and desktops.

Setup steps are as follows:

1. Create resource locations

   Resource locations refer to locations that contain applications and desktops that you want to deliver to your users. This step lets you add your resource locations to DaaS and install Cloud Connectors in them. Cloud Connectors serve as channels that authenticate and encrypt all communication between Citrix Cloud and your resources.

2. Create a host connection

   Hosts are hypervisors or cloud services that are in use in your resource locations. This step lets you specify information that DaaS uses to communicate with VMs on a host. Detailed information includes the resource location, host type, access credentials, storage method to use, and which networks the VMs on the host can use.

3. Prepare a master image

   A master image includes the operating system, all required applications, and the Virtual Delivery Agent (VDA). VDAs establish and maintain connections between VMs and user devices.

4. Create a machine catalog

   A machine catalog is a collection of identical single- or multi-session OS VMs that you assign to users. This step lets you create a machine catalog by specifying the provisioning technology, master image, and VM size.

5. Assign users

   A delivery group is a collection of machines selected from one or more machine catalogs. This step lets you create delivery groups to specify which teams, departments, or types of users can use which machines.

6. Configure Workspace

   Share the Workspace URL from **Workspace Configuration > Access** with your users.

Licenses

March 23, 2022

This article covers tasks and resources for Microsoft licenses and Citrix licenses.

Configure a Microsoft RDS License Server for Windows Server workloads

This information applies when you are delivering Windows Server workloads.

This service accesses Windows Server remote session capabilities when delivering a Windows Server workload, such as Windows 2019. This typically requires a Remote Desktop Services client access license (RDS CAL). The VDA must be able to contact an RDS license server to request RDS CALs.

Install and activate the license server. For more information, see the Microsoft document Activate the Remote Desktop Services License Server. For proof of concept environments, you can use the grace period provided by Microsoft.

With this method, you can have this service apply the license server settings. You can configure the license server and per user mode in the RDS console on the image. You can also configure the license server using Microsoft Group Policy settings. For more information, see the Microsoft document License your RDS deployment with client access licenses (CALs).

To configure the RDS license server using Microsoft Group Policy settings:

1. Install a Remote Desktop Services License Server on an available VM. The VM must always be available. The Citrix service workloads must be able to reach this license server.
2. Specify the license server address and per-user license mode using Microsoft Group Policy. For details, see the Microsoft document Specify the Remote Desktop Licensing Model for an RD Session Host Server.

Windows 10 workloads require appropriate Windows 10 license activation. We recommend that you follow Microsoft documentation to activate Windows 10 workloads.

Citrix license usage

For information about Citrix license usage, see:

- Monitor license and active usage for cloud services
- Monitor license and active usage for Citrix DaaS

Multi-type licensing

August 3, 2023

Multi-type licensing supports consumption of different license entitlements in a single Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment. This article applies to you if you have more than one Citrix license entitlement. A Citrix entitlement is a combination of the following:

- Product, which in the current context of DaaS is always Citrix DaaS
- Service edition (for example: Advanced, Advanced Plus, Premium, or Premium Plus)
- License model (for example: User/Device or Concurrent)

Rules for mixing entitlements

The rules for mixing the service editions are the following:

- Only mixing of DaaS Advanced and Advanced Plus is allowed
- Only mixing of DaaS Premium and Premium Plus is allowed
- DaaS Standard can't be mixed with any other editions

You can mix the licenses models when the preceding service edition rules are followed.

Entitlement at site and delivery group level

You can configure and use License entitlements at the following two levels:

- Site (your deployment of Citrix DaaS product)
- Delivery group

If you have not yet configured site or delivery group entitlements, be aware of the following default behavior:

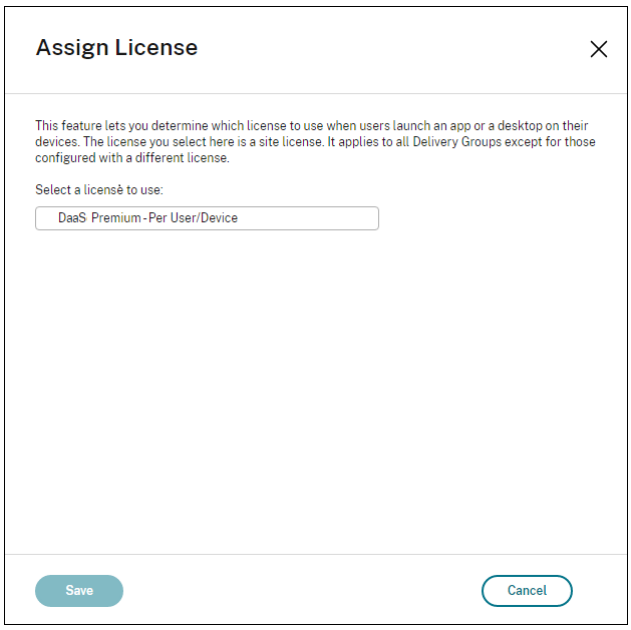
- If you have more than one entitlement, the most capable of the available entitlements is selected as site-wide entitlement provided they were ordered at the same time. Else the first one that came up becomes the site-wide default unless explicitly changed later.
- The site entitlement is used unless a delivery group entitlement is configured.

> **Note:**
>
> Configuring entitlements for a site or delivery group affects how license consumption is counted in the license usage displays in Citrix Cloud.

View and update the site-level entitlement

To specify which license entitlement to use site wide, navigate to **Full Configuration > Settings > Assign license** and click **Edit**. The **Assign License** blade appears. For information on how to get to **Full Configuration** page, see the Citrix DaaS documentation.

In the **Assign License** blade, select a license that you want the site to use. The selected license applies to all delivery groups on the site, except those delivery groups configured with a different license.



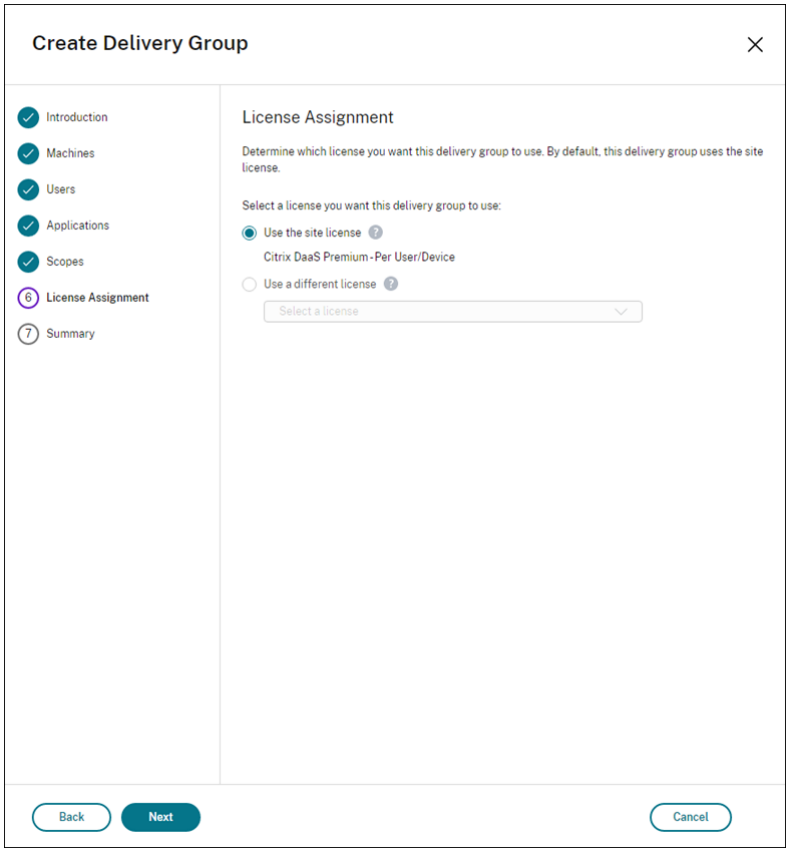
Possible licenses available for you to select are as follows:

- Citrix DaaS Premium –Per User/Device
- Citrix DaaS Premium –Concurrent
- Citrix DaaS Premium for Google Cloud - Per User/Device
- Citrix DaaS Premium for Google Cloud –Concurrent
- Citrix DaaS Advanced –Per User/Device
- Citrix DaaS Advanced –Concurrent
- Citrix DaaS Advanced Plus –Per User/Device
- Citrix DaaS Advanced Plus –Concurrent
- Citrix DaaS Standard for Azure - Per User/Device
- Citrix DaaS Standard for Azure –Concurrent
- Citrix DaaS Standard for Google Cloud - Per User/Device
- Citrix DaaS Standard for Google Cloud –Concurrent

If you have an expired license, contact your Citrix sales representative to renew it or to purchase new licenses.

View and update a delivery group level entitlement

You can specify which license you want a delivery group to use when creating or editing a delivery group. On the **License Assignment** page, select an option.



Options:

- **Use the site license**. A site license applies to all delivery groups except for those delivery groups configured with a different license. The license that appears under this option is the site license in use. To configure the site license, go to **Manage > Full Configuration**, select the **Settings** node, and then edit **Assign license**.
- **Use a different license**. This option lets you configure this delivery group to use a license different from the site license. Remember that a license entitlement is a combination of product code, edition, and license model. The delivery group must use the same license edition (Standard, Premium, or Advanced) as the site. If configured, the delivery group consumes only the selected license. Though the selected license is fully consumed or has become invalid, the delivery group doesn't fall back to the site license.

By default, the delivery group uses the site license.

When a delivery group license expires and is no longer valid, use a different license.

> **Note:**
>
> If you later configure a delivery group to use a different license, connected users consuming the current license might temporarily lose access to their desktops and applications.

An example for mixing of entitlements

For example, consider that Customer A has initially purchased the Advanced edition and later bought the Advanced Plus edition. In this case, Customer A still has site-wide license of Advanced edition only. Citrix does not modify the setting that is initially set at the site level by the Customer A. It is the responsibility of Customer A to modify the license edition to Advanced Plus at the site level.

Similarly, Customer A can update the license edition to Advanced Plus in the delivery group also. If this setting isn't configured, the delivery group inherits the license edition set at the site level.

Customer A's administrator can update the license edition using the following ways:

- Update site-level license edition - Go to **Manage > Full Configuration**, select the **Settings** node, and then edit **Assign license**.
- Update delivery group-level license edition - Go to **Manage > Full Configuration**, select the **Delivery groups** node. Edit the target delivery group to make changes.

Update delivery group using PowerShell command

The PowerShell command to update the delivery group is the following:

```
Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
    code> -LicenseModel <The type of license model>
<!--NeedCopy-->
```

Update the preceding command, based on your details.

For example, see the following:

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null` (Set the delivery group level configuration to the configuration set at the site level)
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

Consider that the license model and product code are not set at the delivery group level. In this scenario, these two properties set at the site level are used for the delivery group.

For more information on the Citrix DaaS Remote PowerShell SDK, see SDKs and API documentation.

More information

- Licenses
- Create delivery groups

- Manage delivery groups

Load balance machines

November 16, 2023

> **Note:**
>
> This feature applies to all your catalogs —single-session OS or multi-session OS catalogs. Vertical load balancing applies only to multi-session OS machines.

Load balancing can be configured at the site level and at the delivery group level. You have two options: vertical and horizontal. By default, horizontal load balancing is enabled.

Load balancing settings at site level

- **Vertical load balancing**. Assigns an incoming user session to the most loaded machine that has not yet reached the maximum load. This saturates existing machines before moving on to new machines. Users disconnecting from existing machines free up capacity on those machines. Incoming loads are then assigned to those machines. Vertical load balancing degrades the user experience but reduces costs (sessions maximize powered-on machine capacity).

  Example: You have two machines configured for 10 sessions each. The first machine handles the first 10 concurrent sessions. The second machine handles the eleventh session.

  > **Tip:**
  >
  > To specify the maximum number of sessions a machine can host, use the Maximum number of sessions policy setting.

  Alternatively, you can use PowerShell to enable or disable vertical load balancing site-wide. Use the `UseVerticalScalingForRdsLaunches` setting in the `Set-BrokerSite` cmdlet. Use `Get-BrokerSite` to display the value of the `UseVerticalScalingForRdsLaunches` setting. See the cmdlet help for details.

- **Horizontal load balancing**. Assigns an incoming user session to the least-loaded, powered-on machine available. Horizontal load balancing improves the user experience but increases costs (because more machines are kept powered on). By default, horizontal load balancing is enabled.

  Example: You have two machines configured for 10 sessions each. The first machine handles five concurrent sessions. The second machine also handles five.

To configure this feature, from **Manage > Full Configuration**, select **Settings** in the left pane. Select an option under **Load balance multi-session catalogs**.

Load balancing settings at delivery group level

Configuring load balancing at the delivery group level allows you to override the load balancing settings inherited from the site level. You can achieve maximum utilization for each machine when you select vertical load balancing at the delivery group level. This will help reduce costs in public clouds. This configuration can be done during the creation of a new delivery group or editing an existing delivery group.

Horizontal load balancing. Sessions are distributed among powered-on machines. For example, if you have two machines configured for 10 sessions each, the first machine handles five concurrent sessions and the second machine also handles five.

Vertical load balancing. Sessions maximize powered-on machine capacity and save machine costs. For example, if you have two machines configured for 10 sessions each, the first machine handles the first 10 concurrent sessions. The second machine handles the eleventh session.

Local Host Cache

May 22, 2024

> **Tip:**
>
> In **Full Configuration > Home**, the service health alerts feature gives you proactive alerts to make sure that your Local Host Cache and zones are configured correctly. So, when an outage happens, Local Host Cache works and your users are not impacted. Alerts come at two levels —site-wide alerts shown in Home (flag icon) and zone-related alerts shown on the Troubleshoot tab of each zone. For more information, see Zones.

Local Host Cache (LHC) enables connection brokering operations in a Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment to continue when a Cloud Connector cannot communicate with Citrix Cloud. Local Host Cache engages when the network connection is lost for 60 seconds.

With Local Host Cache, users who are connected when an outage occurs can continue working uninterrupted. Reconnections and new connections experience minimal connection delays.

> **Important:**
>
> If using an on-premises StoreFront deployment, you must add all Cloud Connectors that have (or can have) VDAs registered with them to the StoreFront as Delivery Controllers. A Cloud Connector that is not added to the StoreFront cannot transition to outage mode, which might result in user launch failures.
>
> For deployments with no on-premises StoreFront, use the service continuity Citrix Workspace platform feature to allow users to connect to resources during outages. For more information, see Service continuity.

Data content

Local Host Cache includes the following information, which is a subset of the information in the main database:

- Identities of users and groups who are assigned rights to resources published from the site.
- Identities of users who are currently using, or who have recently used, published resources from the site.
- Identities of VDA machines (including Remote PC Access machines) configured in the site.
- Identities (names and IP addresses) of client Citrix Workspace app machines being actively used to connect to published resources.

It also contains information for currently active connections that were established while the main database was unavailable:

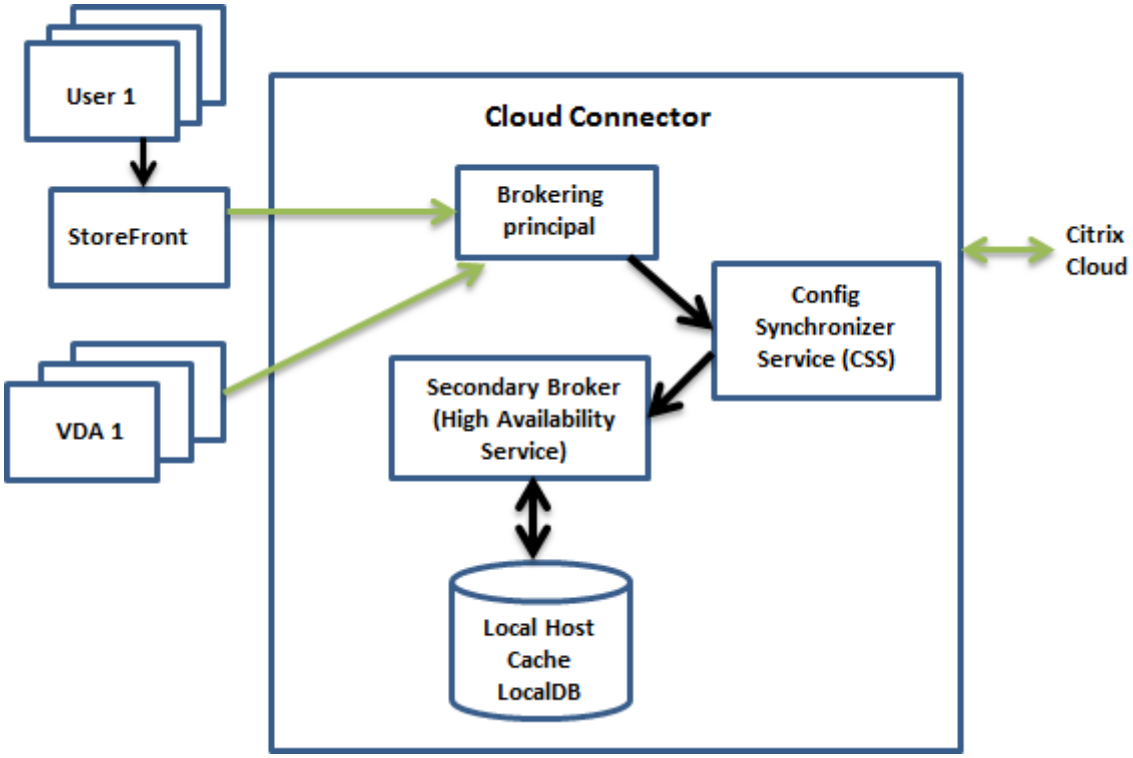
- Results of any client machine endpoint analysis performed by Citrix Workspace app.
- Identities of infrastructure machines (such as Citrix Gateway and StoreFront servers) involved with the site.
- Dates, times, and types of recent activity by users.

How it works

View how Local Host Cache interacts with Citrix Cloud.

This is an embedded video. Click the link to watch the video

During normal operations



- The Brokering Principal (also known as the Citrix Remote Broker Provider Service) on a Cloud Connector accepts connection requests from StoreFront. The Brokering Principal communicates with Citrix Cloud to connect users with VDAs that are registered with the Cloud Connector.
- The Citrix Config Synchronizer Service (CSS) checks with the broker in Citrix Cloud approximately every 5 minutes to see if any configuration changes were made. Those changes can be administrator-initiated (such as changing a delivery group property) or system actions (such as machine assignments).
- If a configuration change occurred since the previous check, the CSS synchronizes (copies) information to a secondary broker on the Cloud Connector. (The secondary broker is also known as the High Availability Service, or HA broker, as shown in the preceding figure.)

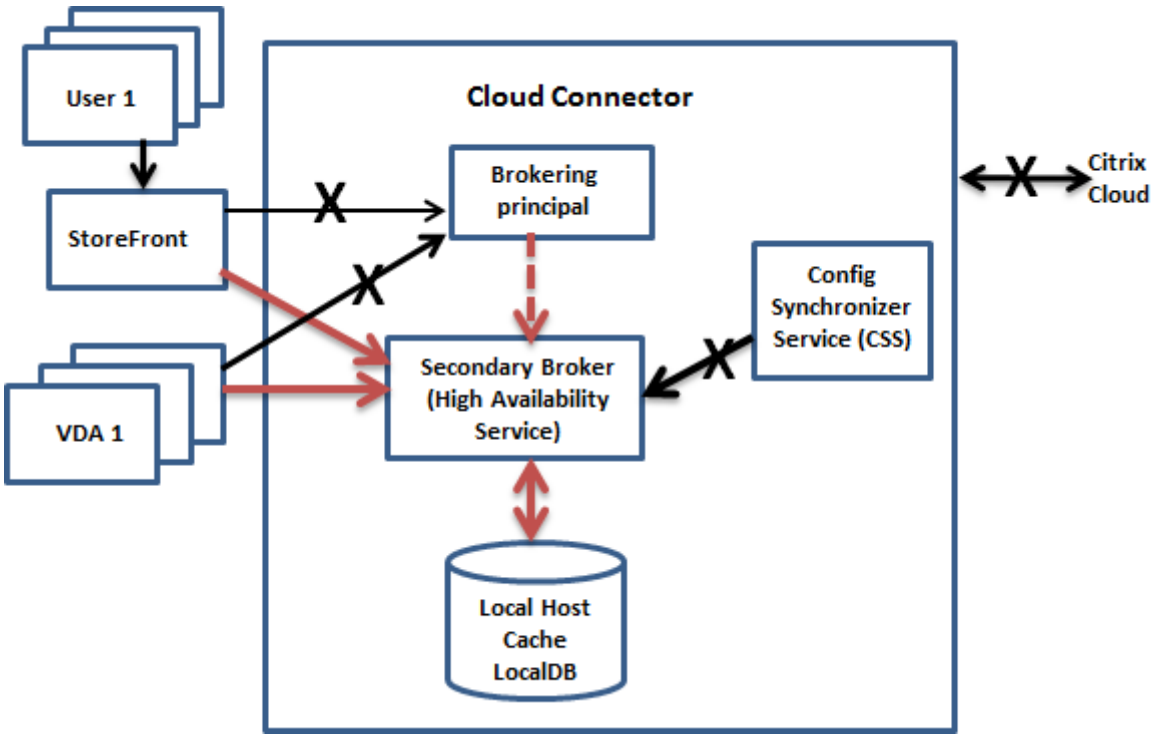
  All configuration data is copied, not just items that changed since the previous check. The CSS imports the configuration data into a Microsoft SQL Server Express LocalDB database on the Cloud Connector. This database is referred to as the Local Host Cache database. The CSS ensures that the information in the Local Host Cache database matches the information in the site database in Citrix Cloud. The Local Host Cache database is re-created each time synchronization occurs.

  Microsoft SQL Server Express LocalDB (used by the Local Host Cache database) is installed automatically when you install a Cloud Connector. The Local Host Cache database cannot be shared

across Cloud Connectors. You do not need to back up the Local Host Cache database. It is recreated every time a configuration change is detected.

- If no changes occurred since the last check, the configuration data is not copied.

During an outage



When an outage begins:

- The secondary broker starts listening for and processing connection requests.
- When the outage begins, the secondary broker does not have current VDA registration data, but when a VDA communicates with it, a registration process is triggered. During that process, the secondary broker also gets current session information about that VDA.
- While the secondary broker is handling connections, the Brokering Principal continues to monitor the connection to Citrix Cloud. When the connection is restored, the Brokering Principal instructs the secondary broker to stop listening for connection information, and the Brokering Principal resumes brokering operations. The next time a VDA communicates with the Brokering Principal, a registration process is triggered. The secondary broker removes any remaining VDA registrations from the previous outage. The CSS resumes synchronizing information when it learns that configuration changes have occurred in Citrix Cloud.

In the unlikely event that an outage begins during a synchronization, the current import is discarded and the last known configuration is used.

The event log indicates when synchronizations and outages occur.

There is no time limit imposed for operating in outage mode.

You can also intentionally trigger an outage. See Force an outage for details about why and how to do this.

Resource locations with multiple Cloud Connectors

Among its other tasks, the CSS routinely provides the secondary broker with information about all Cloud Connectors in the resource location. Having that information, each secondary broker knows about all peer secondary brokers running on other Cloud Connectors in the resource location.

The secondary brokers communicate with each other on a separate channel. Those brokers use an alphabetical list of FQDN names of the machines they're running on to determine (elect) which secondary broker will broker operations in the zone if an outage occurs. During the outage, all VDAs re-register with the elected secondary broker. The non-elected secondary brokers in the zone actively reject incoming connection and VDA registration requests.

> **Important:**
>
> Connectors within a resource location must be able to reach each other at `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. If Connectors cannot communicate at this address, multiple brokers may be elected and intermittent launch failures may occur during a Local Host Cache event.

If an elected secondary broker fails during an outage, another secondary broker is elected to take over, and VDAs register with the newly elected secondary broker.

During an outage, if a Cloud Connector is restarted:

- If that Cloud Connector is not the elected broker, the restart has no impact.
- If that Cloud Connector is the elected broker, a different Cloud Connector is elected, causing VDAs to register. After the restarted Cloud Connector powers on, it automatically takes over brokering, which causes VDAs to register again. In this scenario, performance can be affected during the registrations.

The event log provides information about elections.

What is unavailable during an outage, and other differences

There is no time limit imposed for operating in outage mode. However, if the outage is due to loss of Citrix Cloud connectivity from their resource location, Citrix recommends restoring connectivity from the resource location as quickly as possible.

During an outage:

- During a Local Host Cache event, the Full Configuration interface might be temporarily inaccessible. If the Full Configuration interface is accessible, VDAs in resource locations operating in HA mode display as unregistered in the Full Configuration interface. These VDAs remain accessible through Local Host Cache.
- You have limited access to the Remote PowerShell SDK.
  - You must first:
    * Add a registry key `EnableCssTestMode` with a value of 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Set the SDK auth to `OnPrem` so that the SDK proxy does not try to redirect the cmdlet calls: `$XDSDKAuth="OnPrem"`
    * Use port 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - After running those commands, you can access:
    * All `Get-Broker*` cmdlets.
- Monitoring data is not sent to Citrix Cloud during an outage. So, the **Monitor** functions do not show activity from an outage interval.
- Hypervisor credentials cannot be obtained from the Host Service. All machines are in the unknown power state, and no power operations can be issued. However, VMs on the host that are powered-on can be used for connection requests.
- An assigned machine can be used only if the assignment occurred during normal operations. New assignments cannot be made during an outage.
- Automatic enrollment and configuration of Remote PC Access machines is not possible. However, machines that were enrolled and configured during normal operation are usable.
- Server-hosted applications and desktop users might use more sessions than their configured session limits, if the resources are in different zones.
- Each zone acts independently during an LHC event. Launches across zones (from a broker in one zone to a VDA in a different zone) are not supported during an outage. Use the StoreFront advanced health check feature to route launch requests to the appropriate zone during an LHC event.
- If a site database outage occurs before a scheduled restart begins for VDAs in a delivery group, the restarts begin when the outage ends. This scenario can have unintended results. For more information, see Scheduled restarts delayed due to database outage.

- Zone preference cannot be configured. If configured, preferences are not considered for session launch.
- Tag restrictions where tags are used to designate resource locations are not supported for session launches. When such tag restrictions are configured, and a StoreFront store's advanced health check option is enabled, sessions might intermittently fail to launch.

StoreFront requirement

If using an on-premises StoreFront deployment, you must add all Cloud Connectors that have (or can have) VDAs registered with them to the StoreFront as Delivery Controllers. A Cloud Connector that is not added to the StoreFront cannot transition to outage mode, which might result in user launch failures.

Resource availability

You can ensure the availability of resources (apps and desktops) during an outage in two ways:

- Publish the resources in every resource location in your deployment.
- If you are using StoreFront 1912 CU4 or later, publish the resources to at least one resource location and turn on advanced health check on all StoreFront servers. For versions earlier than StoreFront 2308, the advanced health check is off by default, and must be enabled by an administrator. For StoreFront version 2308 and later, this feature is enabled by default. For more information and instructions on turning on the advanced health check, see advanced health check.

Application and desktop support

LHC supports the following types of VDAs and delivery models:

VDA type	Delivery model	VDA availability during LHC events
Multi-session OS	Applications and desktops	Always available.
Single-session OS static (assigned)	Desktops	Always available.
Power-managed single-session OS random (pooled)	Desktops	Not available by default. All session launch attempts to power-managed VDAs in pooled delivery groups will fail by default. You can make them available for new connections during LHC events. For more information, see Enable using Full Configuration and Enable using PowerShell.

> **Note:**
>
> Enabling access to power-managed desktop VDAs in pooled delivery groups doesn't affect how the configured `ShutdownDesktopsAfterUse` property works during normal operations. When access to these desktops during LHC is enabled, VDAs don't automatically restart after the LHC event is complete. Power-managed desktop VDAs in pooled delivery groups can retain data from previous sessions until the VDAs restart. A VDA restart can occur when a user logs off the VDA during non-LHC operations or when administrators restart the VDA.

Enable LHC for power-managed single-session OS pooled VDAs using Full Configuration

Using Full configuration, you can make those machines available for new connections during LHC events on a per-delivery group basis:

- To enable this feature during delivery group creation, see Create delivery groups.
- To enable this feature for an existing delivery group, see Manage delivery groups

> **Note:**
>
> This setting is available in Full Configuration only for pooled desktop delivery groups that deliver power-managed VDAs.

Enable LHC for power-managed single-session OS pooled VDAs using PowerShell

To enable LHC for VDAs in a specific delivery group, follow these steps:

1. Enable this feature at the site level by running this command:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. Enable LHC for a delivery group by running this command with the delivery group name specified:

   ```
   Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
    $true
   ```

To change the default LHC availability for newly created pooled delivery groups with power managed VDAs, run the following command:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

Verify that Local Host Cache is working

View how to verify that Local Host Cache is configured correctly.

This is an embedded video. Click the link to watch the video

To verify that Local Host Cache is set up and working correctly:

- If using StoreFront, verify that the local StoreFront deployment points to all of the Cloud Connectors in that resource location.
- Ensure that synchronization imports complete successfully. Check the event logs.
- Ensure that the Local Host Cache database was created on each Cloud Connector. This confirms that the High Availability Service can take over, if needed.
  - On the Cloud Connector server, browse to `c:\Windows\ServiceProfiles\NetworkService`.
  - Verify that `HaDatabaseName.mdf` and `HaDatabaseName_log.ldf` are created.
- Force an outage on all Cloud Connectors in the resource location. After you've verified that Local Host Cache works, remember to place all the Cloud Connectors back into normal mode. This can take approximately 15 minutes.

Event logs

Event logs indicate when synchronizations and outages occur. In event viewer logs, outage mode is referred to as *HA mode*.

Config Synchronizer Service

During normal operations, the following events can occur when the CSS imports the configuration data into the Local Host Cache database using the Local Host Cache broker.

- 503: The Citrix Config Sync Service received an updated configuration. This event occurs each time an updated configuration is received from Citrix Cloud. It indicates the start of the synchronization process.
- 504: The Citrix Config Sync Service imported an updated configuration. The configuration import completed successfully.
- 505: The Citrix Config Sync Service failed an import. The configuration import did not complete successfully. If a previous successful configuration is available, it is used if an outage occurs. However, it will be out-of-date from the current configuration. If there is no previous configuration available, the service cannot participate in session brokering during an outage. In this case, see the Troubleshoot section, and contact Citrix Support.
- 507: The Citrix Config Sync Service abandoned an import because the system is in outage mode and the Local Host Cache broker is being used for brokering. The service received a new configuration, but the import was abandoned because an outage occurred. This is expected behavior.
- 510: No Configuration Service configuration data received from primary Configuration Service.

- 517: There was a problem communicating with the primary Broker.
- 518: Config Sync script aborted because the secondary Broker (High Availability Service) is not running.

High Availability Service

This service is also known as the Local Host Cache broker.

- 3502: An outage occurred and the Local Host Cache broker is performing broker operations.
- 3503: An outage was resolved and normal operations have resumed.
- 3504: Indicates which Local Host Cache broker is elected, plus other Local Host Cache brokers involved in the election.
- 3507: Provides a status update of Local Host Cache every 2 minutes which indicates that Local Host Cache mode is active on the elected broker. Contains a summary of the outage including outage duration, VDA registration, and session information.
- 3508: Announces Local Host Cache is no longer active on the elected broker and normal operations have been restored. Contains a summary of the outage including outage duration, number of machines that registered during the Local Host Cache event, and number of successful launches during the LHC event.
- 3509: Notifies that Local Host Cache is active on the non-elected broker(s). Contains an outage duration every 2 minutes and indicates the elected broker.
- 3510: Announces Local Host Cache is no longer active on the non-elected broker(s). Contains the outage duration and indicates the elected broker.

Remote Broker Provider

This service acts as a proxy between Citrix Cloud, and your VDAs and Cloud Connectors.

- 3001: Checks if Cloud Connectors must enter HA mode. This event occurs after a single failed health check of the Cloud Connector. If an additional health check fails after 60 seconds, the Cloud Connector transitions into HA mode.
- 3002: Notifies that the Cloud Connector cannot enter HA mode. The reason for not entering HA mode is included in the event information.
- 3003: Notifies that the Cloud Connector is transitioning through various HA mode states. This diagram describes the states for entering and exiting HA mode. The event provides details about:
  - the state from which the Cloud Connector is transitioning.
  - the state to which the Cloud Connector is transitioning.
  - duration of the previous state.

> **Note:**
>
> You can frequently see 3001 events on your Cloud Connectors. These events might be due to network blips and aren't a cause for concern.

Force an outage

You might want to deliberately force an outage.

- If your network is going up and down repeatedly. Forcing an outage until the network issues are resolved prevents continuous transition between normal and outage modes (and the resulting frequent VDA registration storms).
- To test a disaster recovery plan.
- To help ensure that Local Host Cache is working correctly.

Although a Cloud Connector can be updated during a forced outage, unforeseen issues can occur. We recommend you set a schedule for Cloud Connector updates that avoids forced outage mode intervals.

To force an outage, edit the registry of each Cloud Connector server. In `HKLM\Software\Citrix\DesktopServer\LHC`, create and set `OutageModeForced` as `REG_DWORD` to `1`. This setting instructs the Local Host Cache broker to enter outage mode, regardless of the state of the connection to Citrix Cloud. Setting the value to `0` takes the Local Host Cache broker out of outage mode.

To verify events, monitor the `Current_HighAvailabilityService` log file in `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityService`.

Troubleshoot

Several troubleshooting tools are available when a synchronization import to the Local Host Cache database fails and a 505 event is posted.

CDF tracing: Contains options for the ConfigSyncServer and BrokerLHC modules. Those options, along with other broker modules, can identify the problem.

Report: If a synchronization import fails, you can generate a report. This report stops at the object causing the error. This report feature affects synchronization speed, so Citrix recommends disabling it when not in use.

To enable and produce a CSS trace report, enter the following command:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```


The HTML report is posted at: `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`

After the report is generated, enter the following command to disable the reporting feature:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

Local Host Cache PowerShell commands

You can manage Local Host Cache on your Cloud Connectors using PowerShell commands.

The PowerShell module is at the following location on the Cloud Connectors:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Important:**
>
> Run this module only on the Cloud Connectors.

Import PowerShell module To import the module, run the following on your Cloud Connector:

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

PowerShell commands to manage LHC The following cmdlets help you to activate and manage the LHC mode on the Cloud Connectors.

Cmdlets	Function
`Enable-LhcForcedOutageMode`	Place the Broker in LHC mode. Local Host Cache database files must have been successfully created by the ConfigSync Service for `Enable-LhcForcedOutageMode` to function properly. This cmdlet only forces LHC on the Cloud Connector that it was run on. For LHC to become active, this cmdlet must be run on all Cloud Connectors within the resource location.

Cmdlets	Function
`Disable-LhcForcedOutageMode`	Takes the Broker out of the LHC mode. This cmdlet only disables LHC mode on the Cloud Connector that it was run on. `Disable-LhcForcedOutageMode` must be run on all Cloud Connectors within the resource location.
`Set-LhcConfigSyncIntervalOverride`	Sets the interval at which the Citrix Config Synchronizer Service (CSS) checks for configuration changes within the Citrix DaaS site. The time interval can range from 60 seconds(one minute) to 3600 seconds(one hour). This setting only applies to the Cloud Connector on which it was run. For consistency across the Cloud Connectors, consider running this cmdlet on each Cloud Connector. For example: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Sets the interval at which the Citrix Config Synchronizer Service (CSS) checks for configuration changes within the Citrix DaaS site to the default value of 300 seconds (five minutes). This setting only applies to the Cloud Connector on which it was run. For consistency across the Cloud Connectors, consider running this cmdlet on each Cloud Connector.
`Enable-LhcHighAvailabilitySDK`	Enables access to all the `Get-Broker*` cmdlet within the Cloud Connector that it was run.
`Disable-LhcHighAvailabilitySDK`	Disables access to the Broker PowerShell commands within the Cloud Connector that it was run.

> **Note:**
>
> - Use port 89 when running the `Get-Broker*` cmdlets on the Cloud Connector. For example:
>
>   ```
>   - Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - When not in LHC mode, the LHC Broker on the Cloud Connector only holds configuration

> information.
> - During LHC mode, the LHC Broker on the elected Cloud Connector holds the following information:
>   - Resource states
>   - Session details
>   - VDA registrations
>   - Configuration information

More information

See Scale and size considerations for Local Host Cache for information about:

- Testing methodologies and results
- RAM size considerations
- CPU core and socket configuration considerations
- Storage considerations

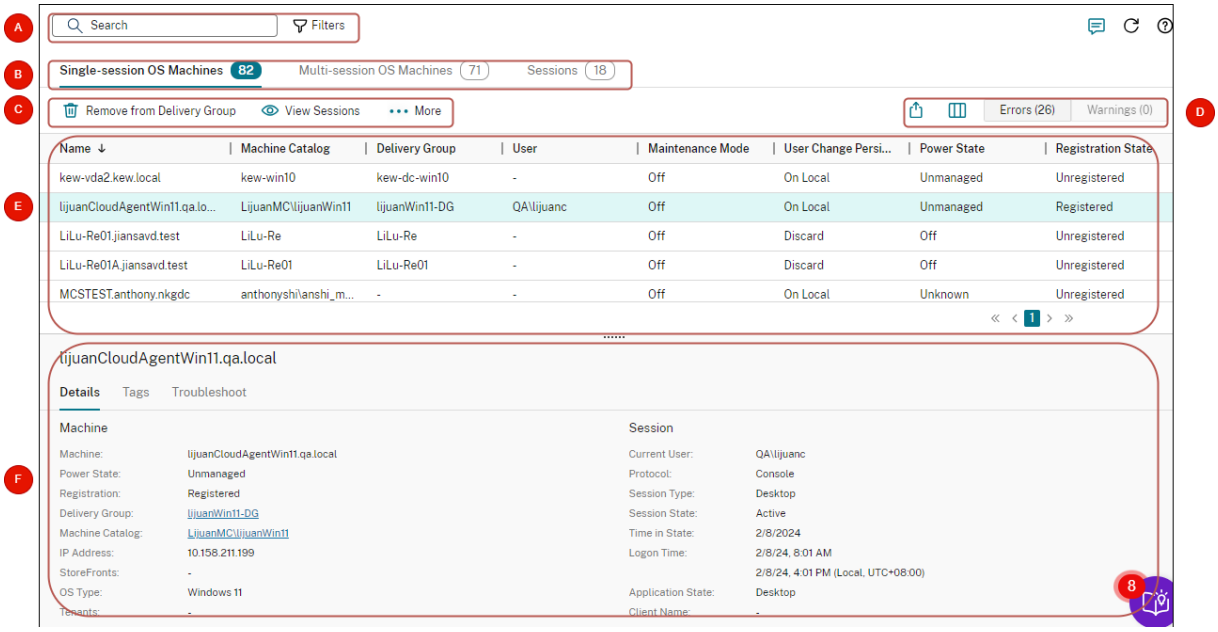
Monitor and manage machines and sessions using Search

May 11, 2024

This article guides you through how to monitor and manage machines and sessions using the **Full Configuration > Search** node.

Learn about the node

The **Search** node provides a central place for monitoring and managing machines and user sessions.



Callout	Area	Description
A	Search bar	Provides a quick search and a filter-based search that allows you to define complex search criteria. For more information, see Search for instances.
B	Type tabs	Displays tabs to list machines by type or list all sessions. Instance counts appear in the tab names.
C	Instance-level actions	Displays actions that you can perform on the *selected instances* (machines or sessions). For more information, see Machine actions and Session actions.
D	List-level actions	Displays actions that you can perform on the current *list*: **Export** icon: Export the list of instances displayed in the main view to a CSV file. **Column to display** icon: Customize the main view for the list. **Errors** label: Enable this label to display only unregistered machines with errors in the main view. To view issue details, go to the **Troubleshoot** tab in the **Details** pane.

Callout	Area	Description
E	Main view	Displays the instances and their properties. You can customize the main view by selecting the **Column to display** icon. For more information about available columns, see Machine columns and Session columns.
F	Details pane	Displays the following details: Details of the selected instance (machine or session) Tags applied to the selected machine Details of errors or warnings with the selected machine, including problems, possible causes, and suggested solutions

Search for instances

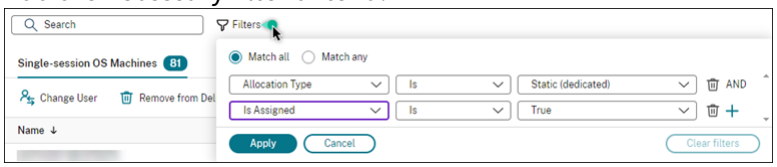
Use the search function to locate specific machines and sessions:

- Search using filters
- Save the current filter set for a quick search
- Pin a filter field in the search bar
- Search using the quick search box
- Tips to enhance a search

Search using filters

For example, to locate all single-session OS machines that are *static* and *assigned to users*, follow these steps:

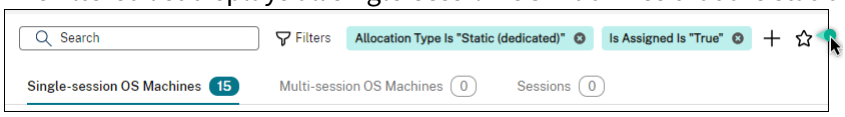
1. On the **Single-session OS machines** tab, click the **Filters** icon. The Filters panel appears.
2. Add the necessary filter criteria.



3. Select **Match all** (AND operator) if you want the search to return results that match all filter criteria. Select **Match any** (OR operator) if you want the search to return results that match any of the filter criteria.

4. Click **Apply**.

   The filtered list displays all single-session OS machines that are static and assigned to users.

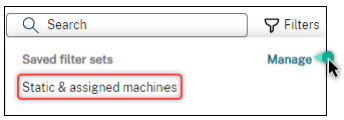


Save the current filter set for a quick search

For example, to save the filter set for single-session OS machines that are static and assigned to users for future use, follow these steps:

1. After you conduct a filter-based search, click the **Star** icon in the search bar, as shown in the preceding figure.
2. On the page that appears, enter a name for this filter set (for example, *Static & assigned machines*).
3. Click **Save**.

   The saved filter set appears in the search history list when you click the search box.

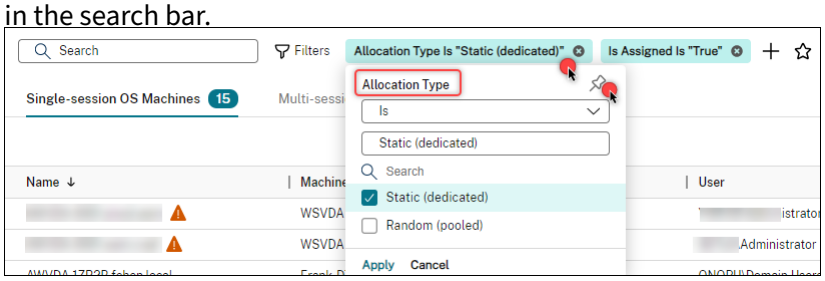


> **Note:**
>
> Filter sets are saved on a per user account basis. To manage saved filter sets, select **Manage**.

Pin a filter field in the search bar

Pin frequently used filter *fields* in the search bar for easy access. For example, after conducting a filter-based search, you want to pin **Allocate Type** in the search bar. Follow these steps:

1. Click the *filter setting* in the search bar.
2. In the panel that appears, click the **Pin** icon to pin the filter field (*Allocation Type* for this example) in the search bar.



Search using the quick search box

The quick search box provides a convenient way to search for instances based on name-related properties or saved filter sets. Detailed steps are as follows:

1. Click the search box. Your recent searches and saved filter sets appear in the drop-down list. You can click a previous search or filter set for a quick search.
2. To start a new search, enter a complete or partial name from the following options:
    - Machine name or DNS name
    - Machine catalog name
    - Delivery group name
    - Session user name
    - Session client name
    - Friendly name of the VM hosting the session, as used by its hypervisor
    - Hosting server name

Tips to enhance a search

Consider the following tips when using the Search feature:

- On the **Search** node, select any column to sort items.
- To show more characteristics to include in the display where you can search and sort, select **Columns to Display** or click any column and select **Columns to Display**. In the **Columns to Display** window, select the checkbox next to the items you want to display and select **Save** to exit.

  > **Note:**
  >
  > Columns that degrade performance are marked with the **Degrades performance** label.

- To locate a user device connected to a machine, use **Client (IP)** and **Is**, and enter the device IP address.
- To locate active sessions, use **Session State**, **Is**, and **Connected**.
- To list all machines in a delivery group, select **Delivery Groups** in the left pane. Select the group, and then select **View Machines** from the action bar or the context menu.

Keep the following considerations in mind when performing sorting operations:

- As long as the number of items does not exceed 5,000, you can click any column to sort the items in it. When the number exceeds 5,000, you can sort only by name or by current user (depending on which tab you are on). To enable sorting, use filters to reduce the number of items to 5,000 or fewer.

- When the number of items is greater than 500 but no more than 5,000:
  - We cache all data locally to improve sort performance. On the **Single-session OS Machines** and **Multi-session OS Machines** tabs, we cache the data the first time you click a column (any column except the **Name** column) to sort. On the **Sessions** tab, we cache the data the first time you click a column (any column except the **Current User** column) to sort. As a result, the sort takes longer to complete. For faster performance, sort by name or current user, or use filters to reduce the number of items.
  - The following message under the table indicates that the data is cached: Last refreshed: <the time when you refreshed the table>. In that case, sort operations are based on items that were loaded previously. Those items might not be up to date. To bring them up to date, click the refresh icon.

Customize columns to display

Create a personalized main view to display the properties and statuses crucial for your daily operations. Detailed steps are as follows:

1. In the **Search** node, select the **Multi-session OS Machines**, **Single-session OS Machines**, or **Sessions** tab as necessary.
2. Click the **Columns to display** icon in the action bar and select the columns.

   For more information about the available columns and their descriptions, see Machine columns and Session columns.

When choosing columns, you can see columns marked with the **Degrades performance** label. Selecting those columns might degrade the performance of the console. Keep these considerations in mind:

- After you complete your customization, the table refreshes to display the columns you select. Their presence might result in delays when you refresh the table.
- After you refresh the browser or sign out of the console and then sign in, a message appears asking whether to preserve those columns. If you choose to preserve them, you're restricted to refreshing the table more than once a minute for optimal console performance. For more frequent refreshes, remove any columns that degrade performance.

Manage machines and sessions

Use actions in the Search node to troubleshoot machines and session issues or process user requests.

Good to know

You can manage machines at different levels:

- At the individual machine level. Use the **Search** node to locate target machines and perform actions.
- At the machine catalog level, such as changing master images for a catalog, deleting machines from a catalog, and adding machines to a catalog. For more information, see Manage machine catalogs.
- At the delivery group level, such as turning on or off maintenance mode for machines in a group. For more information, see Manage delivery groups.

In addition to the individual session level, You can also manage sessions at the delivery group level, such as configuring session prelaunch and linger for a delivery group. For more information, see Manage Delivery Groups.

Perform actions on machines or sessions

To manage machines or sessions at the individual instance level, follow these steps:

1. In the **Search** node, select the **Multi-session OS Machines**, **Single-session OS Machines**, or **Sessions** tab.
2. Select one or more instances as necessary.
3. From the action bar or right-click menu, select an action based on the issues that you encounter with those instances or user requests.

   For more information about the available actions and their descriptions, see Machine actions and Session actions.

> **Note:**
>
> If you select two or more instances, only actions that apply to all of them are available.

Export machine or session data to CSV files

Export the list of instances (machines or sessions) displayed on a tab (up to 30,000 items) to a CSV file. Detailed steps are as follows:

1. In the **Search** node, select the **Multi-session OS Machines**, **Single-session OS Machines**, or **Sessions** tab as necessary.
2. Click the **Export** icon in the upper right corner.

3. In the dialog box that appears, click **Continue**.

   The export might take several minutes to complete. You can find the file in the default download folder of your browser.

> **Note:**
>
> On each tab of the **Search** node, you cannot perform another export while an export is in progress.

Machine actions and columns

May 11, 2024

This article lists machine actions and columns with descriptions for your reference.

Actions

View the actions you can perform on machines and their descriptions.

Action	Description	Applies to
Run Health Check	Available only for registered Windows VDAs, version 2019 or later. Run a health check on a machine. For more information about the checking contents, see About health checks.	Single-session and multi-session
Remove from Delivery Group	Remove a machine from the delivery group.	Single-session and multi-session
Add to Delivery Group	Add a machine to a delivery group.	Single-session and multi-session
View Sessions	View the sessions running on a machine	Single-session and multi-session
Manage Tags	Add and manage tags for a machine. For more information about typical use cases of tags, see Tags.	Single-session and multi-session

Action	Description	Applies to
Turn On Maintenance Mode	Place a machine in maintenance mode before applying patches, or for troubleshooting. This mode prevents new connections from being made to that machine. Users can connect to existing sessions on that machine, but they can't start new sessions on that machine.	Single-session and multi-session
Turn Off Maintenance Mode	Turn off maintenance mode for a machine.	Single-session and multi-session
Upgrade VDA	Upgrade VDA for a machine.	Single- or multi-session OS machines that meet certain requirements: Learn more.
Log Off	Force log off a machine	Single-session and multi-session
Delete	Delete a VM from a machine catalog while leaving it intact on the hypervisor or cloud service.	Single-session and multi-session
Change User	Assign a machine to a specific user.	single-session *static* machines.
Start	Start a machine.	Single-session and multi-session
Shut Down	Shut down a machine.	Single-session and multi-session
Restart	Restart a machine	Single-session and multi-session
Suspend	Place a machine in a hibernation or suspension state. When you suspend a machine, DaaS stores the memory contents of the machine in a file and then shuts down the machine.	Single-session OS machines

Action	Description	Applies to
Resume	Resume a suspended machine. When you resume a suspended machine, the DaaS starts the machine and restores it to the previous state.	Single-session OS machines
Force Restart	Force restart a machine.	Single-session OS machines
Force Shut Down	Force shut down a machine.	Single-session OS machines

Columns

View all machine columns and their descriptions by type:

- Machine
- Machine details
- Applications
- Hosting
- Connection
- Registration
- Session Details
- Session

Machine

Columns in the **Machine** category.

Column	Description	Applies to
Name	The DNS host name of the machine.	Single-session and multi-session
Machine Catalog	The name of the catalog the machine belongs to.	Single-session and multi-session
Delivery Group	The name of the delivery group the machine belongs to.	Single-session and multi-session

Column	Description	Applies to
User Display Name	The full names of the users associated with the machine (usually in the form `Firstname Lastname`). Associated users are the current users for shared machines and the assigned users for dedicated machines.	Single-session and multi-session
User	The user names of the users associated with the machine (in the form "domain\user"). Associated users are the current users for shared machines and the assigned users for dedicated machines.	Single-session and multi-session
User Principal Name	The User Principal Names of the users associated with the machine (in the form "user@domain"). Associated users are the current users for shared machines and the assigned users for dedicated machines.	Single-session and multi-session
Desktop Display Name	The published name of the machine originally used to launch the session. It's the name displayed on the Citrix Workspace app or StoreFront. **Note:** To change a desktop's display, you need the **Perform Machine Update** permission because changing the display name involves updating the machine property.	Single-session only

Column	Description	Applies to
Desktop Conditions	The list of outstanding desktop conditions for the machine. Possible values: Unknown, CPU, ICALatency, and UPMLogonTime.	Single-session and multi-session
Allocation Type	The allocation type of the machine: **Permanent**, when allocated to a user permanently. **Random**, when allocated randomly.	Single-session and multi-session
Maintenance Mode	Indicates whether the machine is in maintenance mode.	Single-session and multi-session
Windows Connection Setting	Logon mode reported by Windows. Possible values: LogonEnabled, Draining, DrainingUntilRestart, and LogonDisabled.	Multi-session only
Is Assigned	Indicates whether a dedicated desktop has been assigned to a user or a client (name/address). Users can be assigned explicitly or by assigning-on-first-use-of-the-machine.	Single-session and multi-session
Is Physical	Indicates whether the machine is physical or not. `True` indicates that the machine is physical, meaning it isn't power-managed by DaaS. `False` indicates otherwise.	Single-session and multi-session
Provisioning Type	How the machine was provisioned. Possible values: Manual: Not provisioned using PVS or MCS. PVS: Provisioned using PVS (physical, blade, and virtual machines) MCS: Provisioned using MCS (VMs only)	Single-session and multi-session
Scheduled Restart	The state of any scheduled reboot operation for the machine. Possible values: None: No reboot is scheduled. Pending: Awaiting reboot but is available for use. Draining: Awaiting reboot and is unavailable for new sessions. Reconnections to existing connections are still allowed,	Single-session and multi-session

Column	Description	Applies to
Zone	The name of the zone where the machine is located.	Single-session and multi-session
State	The overall state of the desktop associated with the machine, derived from various specific states such as session state, registration state, and power state. Possible states: Off, Unregistered, Available, Disconnected, InUse, and Preparing.	Single-session and multi-session
Tags	The list of tags associated with the machine.	Single-session and multi-session
VDA Upgrade	The machine state for VDA package upgrade actions. Possible values: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate, and Unknown.	Single-session and multi-session
Suspend Capable	Indicates whether the machine supports power actions (Suspend and Resume).	Single-session and multi-session
Load Index	The current load index. For more information, see Learn more.	Multi-session only
Drain State	Indicates whether the machine is draining and will shut down after all sessions on the machine end. True appears only for power-managed, multi-session machines.	Multi-session only

Column	Description	Applies to
	Note: The machine doesn't shut down if it's in maintenance mode. It shuts down only after it's off maintenance mode.	

Machine details

Columns in the **Machine details** category.

Column	Description	Applies to
Agent Version	The version of the Citrix Virtual Delivery Agent (VDA) installed on the machine.	Single-session and multi-session
IP Address	The IP address of the machine.	Single-session and multi-session
Is Assigned	Indicates whether a dedicated desktop has been assigned to a user or a client (name/address). Users can be assigned explicitly or by assigning-on-first-use-of-the-machine.	Single-session and multi-session
OS Type	The type of the operating system running on the machine.	Single-session only

Applications

Columns in the **Applications** category.

Column	Description	Applies to
Application in Use	The list of applications in use on the machine (displayed as browser names).	Single-session and multi-session

Column	Description	Applies to
Published Applications	The list of applications published by the machine (displayed as browser names).	Single-session and multi-session

Connections

Columns in the **Connections** category.

Column	Description	Applies to
Client (IP)	The IP address of the client connected to the machine.	Single-session only
Client	The host name of the client connected to the machine.	Single-session only
Plug-In Version	The version of the Citrix Workspace app on the connected client.	Single-session only
Connected Through	The host name of the incoming connection, typically a gateway, router, or client.	Single-session only
Connected Through (IP)	The IP address of the incoming connection, typically a gateway, router, or client.	Single-session only
Connection Type	The protocol used for the session. Possible values: HDX, RDP, and Console. Note: The field is left blank for console sessions on XenDesktop 5 VDAs.	Single-session only
Last Connection Time (UTC)	The time of the last detected connection attempt that either failed or succeeded.	Single-session and multi-session

Column	Description	Applies to
Last Connection User	The SAM name (in the form "DOMAIN\user") of the user that last attempted a connection with the machine. If the SAM name is not available, the SID is used.	Single-session and multi-session
Secure ICA Active	Indicates whether SecureICA is active on the current session. Always null for multi-session machines.	Single-session and multi-session

Hosting

Columns in the **Hosting** category.

Column	Description	Applies to
VM	The friendly name of a hosted machine running the session, as used by its hypervisor. It doesn't necessarily match either the DNS or AD name of the machine.	Single-session and multi-session
Hosting Server Name	The DNS name of the hypervisor that is hosting the machine if managed.	Single-session and multi-session
Connection	The name of the host connection assigned to the machine hosting the session.	Single-session and multi-session
Pending Update	Indicates whether the VM image for a hosted machine is out of date and due to be updated to a new image at the machine's next reboot.	Single-session and multi-session
User Change Persistence	How user changes are handled, indicating whether the changes are persistent: OnLocal: Persistent. User changes are saved locally. Discard: Non-persistent. User changes are discarded.	Single-session and multi-session

Column	Description	Applies to
Pending Power Action	Indicates whether there are any pending power actions for the machine.	Single-session and multi-session
Power State	The power state of the machine. Possible values: Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.	Single-session and multi-session
Will Shut Down After Use	Applicable only to power-managed, single-session machines. Indicates whether the machine is tainted and will shut down after all sessions end. **Note:** The machine won't shut down if it's in maintenance mode. It will shut down only after it is taken out of maintenance mode.	Single-session only

Registration

Columns in the **Registration** category.

Column	Description	Applies to
Last Registration Failure	The reason for the last deregistration of the machine with the broker.	Single-session and multi-session

Column	Description	Applies to
	Possible values are: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError, and BrokerRegistrationLimitReached.	
Last Registration Failure Time (UTC)	The time of the last deregistration of the machine.	Single-session and multi-session
Registration State	The registration state of the machine. Possible values: Unregistered, Initializing, Registered, and AgentError.	Single-session and multi-session

Column	Description	Applies to
Fault State	The summary state of any current fault state of the machine. Possible values: None: No fault. The machine is healthy. FailedToStart: The last power-on operation for the machine failed. StuckOnBoot: The machine failed to start after being powered on. Unregistered. The machine failed to register within the expected period or its registration has been rejected. MaxCapacity. The machine is reporting itself at maximum capacity.	Single-session and multi-session

Session details

Columns in the **Session details** category.

Column	Description	Applies to
Launched Over	The host name of the StoreFront server used to launch the current brokered session. Always null for multi-session machines.	Single-session and multi-session
Launched Over (IP)	The IP address of the StoreFront server used to launch the current brokered session. Always null for multi-session machines.	Single-session and multi-session
Session Change Time (UTC)	The time of the last state change of the current session.	Single-session only
SmartAccess Filters	Smart Access tags for the current session. Always null for multi-session machines.	Single-session and multi-session

Session

Columns in the **Session** category.

Column	Description	Applies to
Session State	The state of the current session. Possible values: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.	Single-session only
Current User	The name of the current session's user (in the form "DOMAIN\user").	Single-session only
Start Time (UTC)	The start time of the current session.	Single-session only
Session Count	The number of sessions on the machine.	Multi-session only

Session actions and columns

May 11, 2024

This article lists machine actions and columns with descriptions for your reference.

Actions

View the actions you can perform on sessions and their descriptions.

Action	Description	Applies to sessions on
Log off	Log a user off a session.	Single-session OS machines or multi-session OS machines
Send Message	Send a message to the user of a session.	Single-session OS machines or multi-session OS machines
View machines	View the hosting machine for a session.	Single-session OS machines or multi-session OS machines

Action	Description	Applies to sessions on
Disconnect	Disconnect a session. If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the DaaS.	Single-session OS machines or multi-session OS machines
Shut Down Machine	Shut down the machine associated with a session.	Single-session OS machines
Restart Machine	Restart the machine associated with a session.	Single-session OS machines

Columns

View session columns and their descriptions.

Column	Description
Current user	The name of the user; the User Principal Name (UPN) of the user.
Name	The DNS host name of the machine hosting the session.
Delivery Group	The name of the delivery group containing the session's hosting machine.
Machine Catalog	The name of the machine catalog containing the session's hosting machine.
Agent Version	The version of the Citrix Virtual Delivery Agent (VDA) installed on the machine hosting the session.
Application in Use	The list of applications in use in the session, identified by their administrative names.
Autonomously Brokered	Whether this is an HDX session established by a direct connection without being brokered.
Brokering Time (UTC)	The time at which the session was brokered.
Brokering User Name	The name of the brokering user.
Client (IP)	The IP address of the client connected to the session.

Column	Description
Client	The host name of the client connected to the session.
Plug-In Version	The version of Citrix Workspace app running on the client connected to the session.
Connected Through	The host name of the incoming connections, typically a gateway, router, or client.
Connected Through (IP)	The IP address of the incoming connection, typically a gateway, router, or client.
Allocation Type	Whether the session is shared or dedicated.
Hidden	Whether the session is hidden from the user and not to be reconnected to.
VM	The friendly name of the VM hosting the session, as used by its hypervisor. It doesn't necessarily match either the DNS or AD name of the machine.
Hosting Server Name	The DNS name of the hypervisor that is hosting the session's hosting machine.
Connection	The name of the host connection assigned to the machine hosting the session.
Pending Update	Whether the VM image for a hosted machine is out of date and due to be updated to a new image at the machine's next reboot.
Maintenance Mode	Whether the machine hosting the session is in maintenance mode.
IP Address	The IP address of the machine hosting the session.
Is Physical	Whether the machine hosting the session is physical or not. `True` indicates that the machine is physical, meaning it isn't power-managed by DaaS. `False` indicates otherwise.
Launched Over	The host name of the StoreFront server used to launch the session. Blank if the session was launched via Workspace.
Launched Over (IP)	The IP address of the StoreFront server used to launch the session. Blank if the session was launched via Workspace.

Column	Description
OS Type	The identification string of the operating system hosting the session.
User Change Persistence	How user changes are handled, indicating whether the changes are persistent: OnLocal: Persistent. User changes are saved locally. Discard: Non-persistent. User changes are discarded.
Connection Type	The protocol used for the session, such as HDX, RDP, or Console. **Note:** The field is blank for console sessions on XenDesktop 5 VDAs.
Provisioning Type	How the machine hosting the session was provisioned: Manual: Not provisioned using PVS or MCS. PVS: Provisioned by PVS (Physical, blade, and virtual machines). MCS: Provisioned by MCS (VMs only).
Secure ICA Active	Whether SecureICA is active on the session.
Session State	The state of the session. Possible values: Connected, Active, or Disconnected. Other states might occur for sessions on machines with functional levels earlier than L7, such as PreparingSession, Reconnecting, NonBrokeredSession, Other, and Unknown.
Session Change Time	The time of the most recent state change for the session.
Application State	The state of applications in the session. Possible values: PreLogon, PreLaunched, Active, Desktop, Lingering, and NoApps.
Session Support	Whether the machine hosting the session supports multiple or single sessions.
Zone	Name of the zone where the machine hosting the session is located.
SmartAccess Filters	Smart Access tags for the session.
Start Time (UTC)	When the session was started.
State	The summary state of the machine. Possible values: Unregistered, Disconnected, or InUse.
Time in State (UTC)	How long the session has been in its current state.

Column	Description
Delivery Controller	The DNS host name of the controller that the session's hosting machine is registered with.
User Display Name	The full name of the user.
Desktop Display Name	The published name of the machine originally used to launch the session. It's the name displayed on the Citrix Workspace app or StoreFront. For application sessions, it's the name of the first application launched into the session even if that application has since ended. The name keeps unchanged even if the resource is later renamed or removed.

Manage security keys

June 19, 2024

> **Note:**
>
> - You must use this feature in combination with StoreFront 1912 LTSR CU2 or later.
> - The Secure XML feature is supported only on Citrix ADC and Citrix Gateway release 12.1 and later.

This feature lets you allow only approved StoreFront and Citrix Gateway machines to communicate with Citrix Delivery Controllers. After you enable this feature, any requests that do not contain the key are blocked. Use this feature to add an extra layer of security to protect against attacks originating from the internal network.

A general workflow to use this feature is as follows:

1. Display security key settings in the Full Configuration interface. (Use the Remote PowerShell SDK)
2. Configure settings for your deployment. (Use the Full Configuration interface or Remote PowerShell SDK).
3. Configure settings in StoreFront. (Use PowerShell).
4. Configure settings in Citrix ADC.

Display security key settings in the Full Configuration interface

By default, settings for security keys are hidden from the Full Configuration interface. To display them in that interface, use the Remote PowerShell SDK. For more information about the Remote PowerShell SDK, see SDKs and APIs.

Detailed steps are as follows:

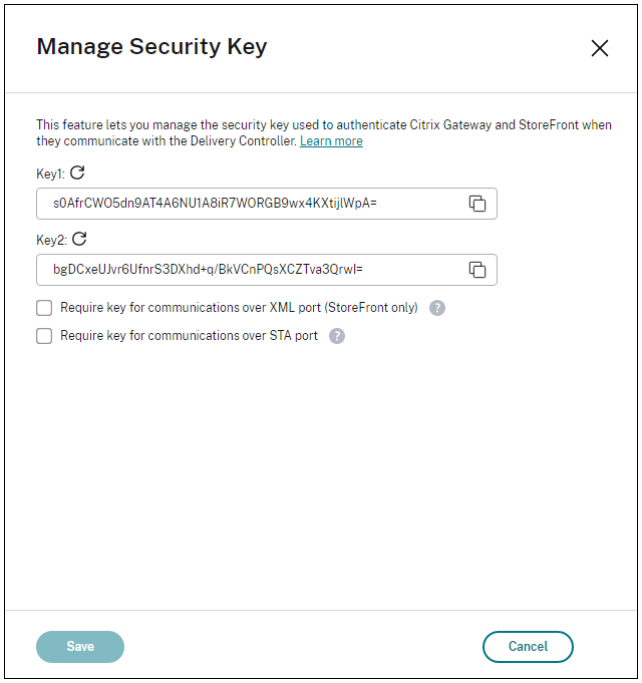
1. Run the Remote PowerShell SDK.
2. In a command window, run the following commands:
   - `Add-PSSnapIn Citrix*`. This command adds the Citrix snap-ins.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

Configure settings for your deployment

You can configure settings for your deployment by using Full Configuration or PowerShell.

Use the Full Configuration interface

After enabling the feature, navigate to **Full Configuration > Settings > Manage security key** and click **Edit**. The **Manage Security Key** blade appears. Click **Save** to apply your changes and to exit the blade.



> **Important:**
>
> - There are two keys available for use. You can use the same key or different keys for communications over the XML and STA ports. We recommend that you use only one key at a time. The unused key is used only for key rotation.
> - Do not click the refresh icon to update the key already in use. If you do, service interruption will occur.

Click the refresh icon to generate new keys.

Require key for communications over XML port (StoreFront only). If selected, require a key to authenticate communications over the XML port. StoreFront communicates with Citrix Cloud over this port. For information about changing the XML port, see Knowledge Center article CTX127945.

Require key for communications over STA port. If selected, require a key to authenticate communications over the STA port. Citrix Gateway and StoreFront communicate with Citrix Cloud over this port. For information about changing the STA port, see Knowledge Center article CTX101988.

After applying your changes, click **Close** to exit the **Manage Security Key** blade.

Use the Remote PowerShell SDK

The following are PowerShell steps equivalent to the operations performed in the Full Configuration interface.

1. Run the Remote PowerShell SDK.
2. In a command window, run the following command:
   - `Add-PSSnapIn Citrix*`
3. Run the following commands to generate a key and set up Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Run the following commands to generate a key and set up Key2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Run one or both of the following commands to enable the use of a key in authenticating communications:
   - To authenticate communications over the XML port:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`

- To authenticate communications over the STA port:
  - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

See the PowerShell command help for guidance and syntax.

Configure settings in StoreFront

After completing the settings for your deployment, you need to configure relevant settings in StoreFront by using PowerShell.

On the StoreFront server, run the following PowerShell commands:

To configure the key for communications over the XML port, use command Set-STFStoreFarm. For example:

```
1 $store = Get-STFStoreService -VirtualPath [Path to store]
2 $farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
     name]
3 Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
     XMLValidationSecret [secret]
4 <!--NeedCopy-->
```

Enter the appropriate values for the following parameters:

- `Path to store`
- `Resource feed name`
- `secret`

To configure the key for communications over the STA port, use the `New-STFSecureTicketAuthority` and `Set-STFRoamingGateway` commands. For example:

```
1 $gateway = Get-STFRoamingGateway -Name [Gateway name]
2 $sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
     StaValidationEnabled $true -StaValidationSecret [secret]
3 $sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
     StaValidationEnabled $true -StaValidationSecret [secret]
4 Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
     $sta1,$sta2
5 <!--NeedCopy-->
```

Enter the appropriate values for the following parameters:

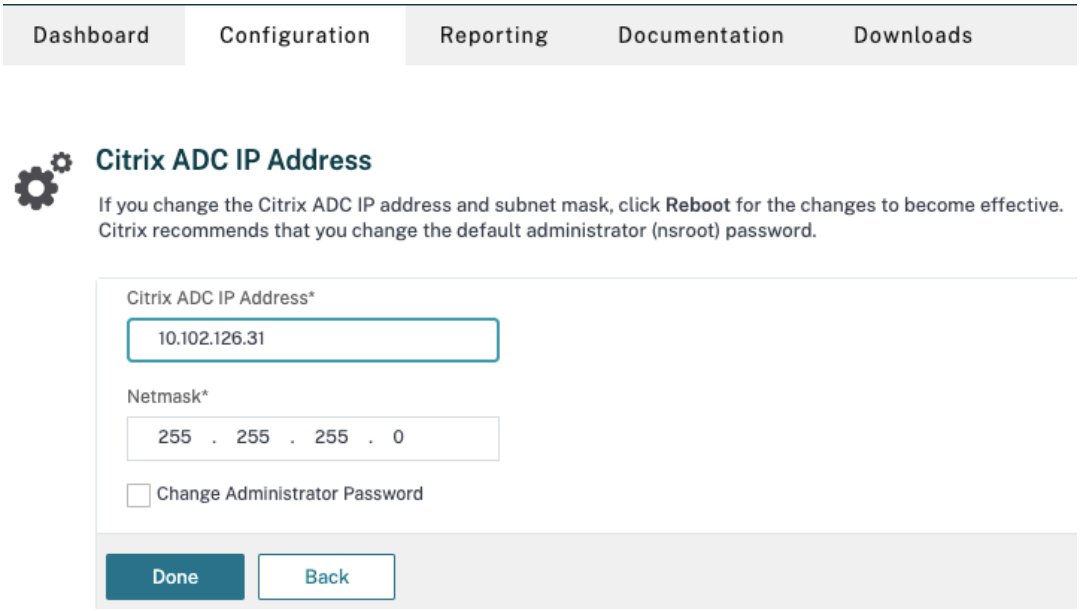
- `Gateway name`
- `STA URL`
- `Secret`

See the PowerShell command help for guidance and syntax.

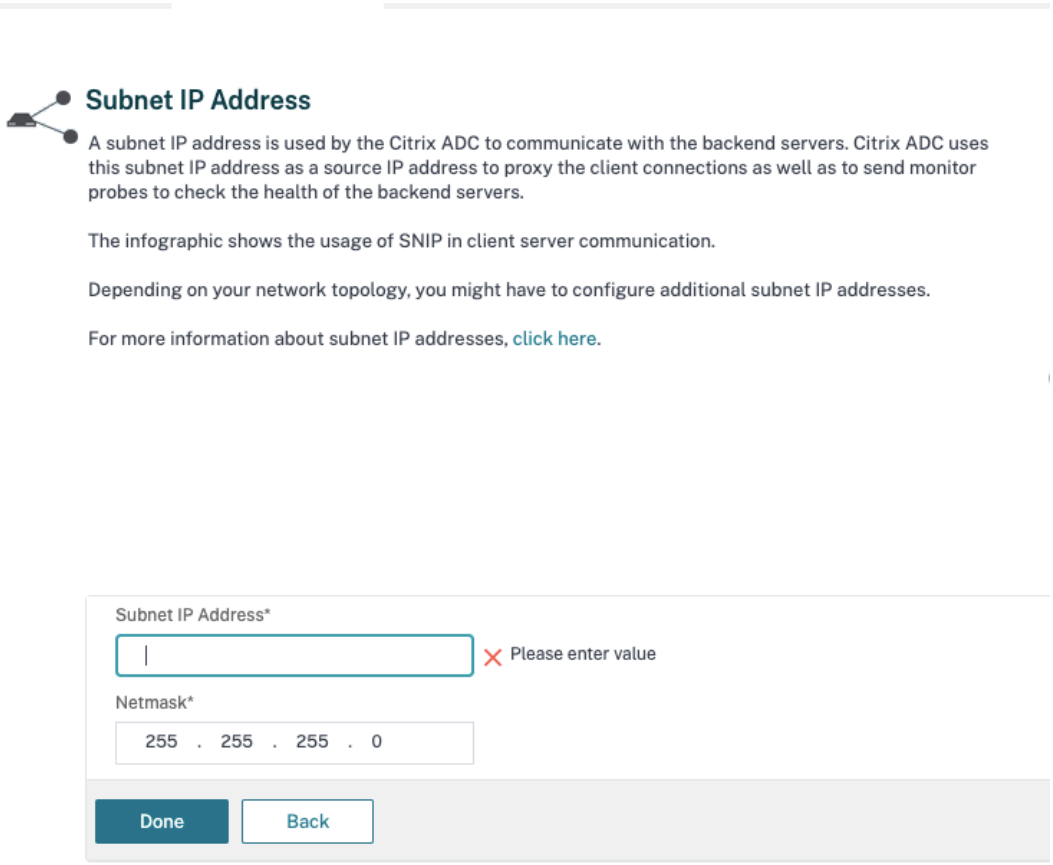
Configure settings in Citrix ADC

> **Note:**
>
> Configuring this feature in Citrix ADC is not required unless you use Citrix ADC as your gateway. If you use Citrix ADC, follow the steps below.

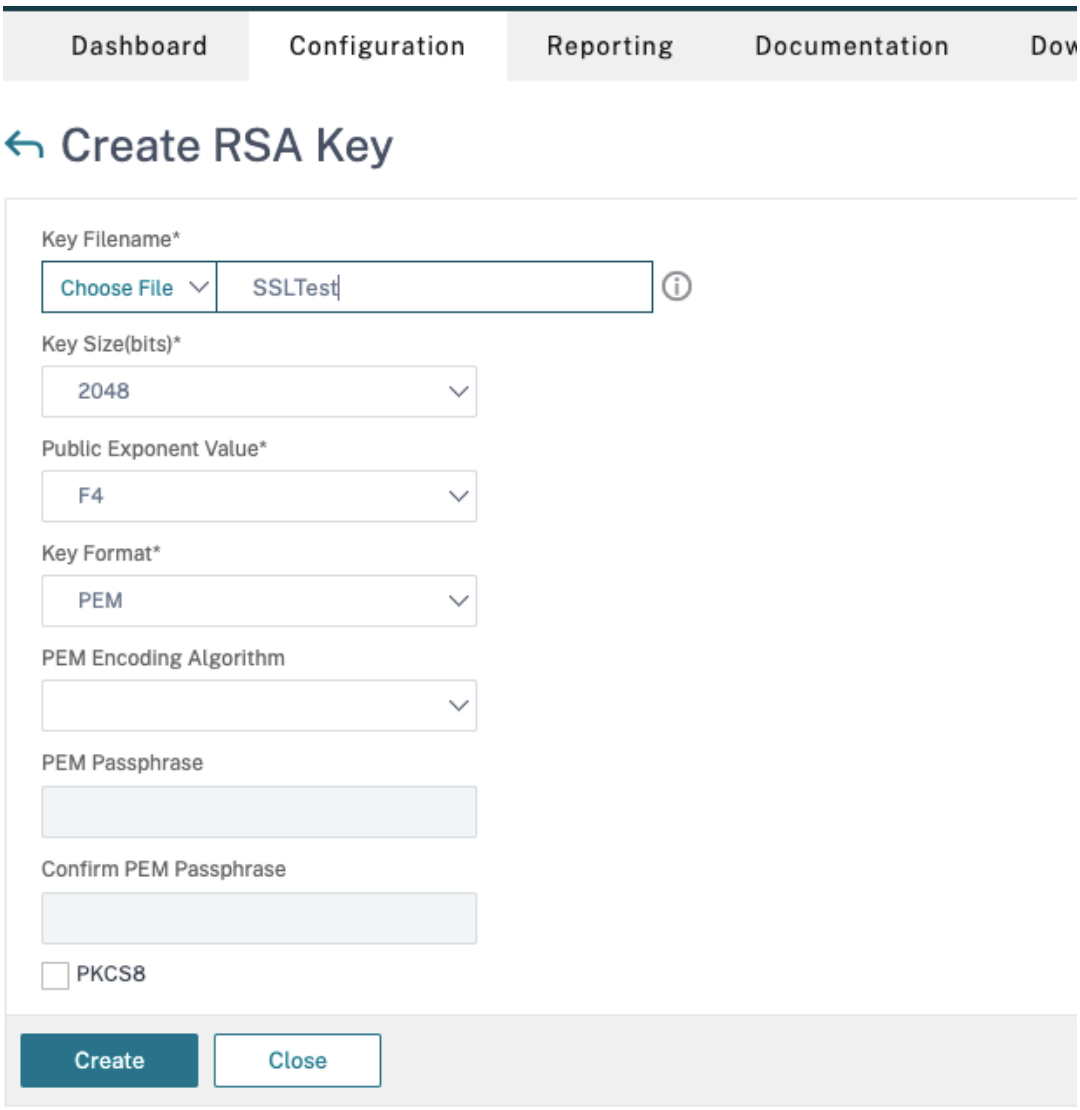
1. Ensure that the following prerequisite configuration is already in place:
   - The following Citrix ADC related IP addresses are configured.
     - Citrix ADC Management IP (NSIP) address for accessing the Citrix ADC console. For details, see Configuring the NSIP address.



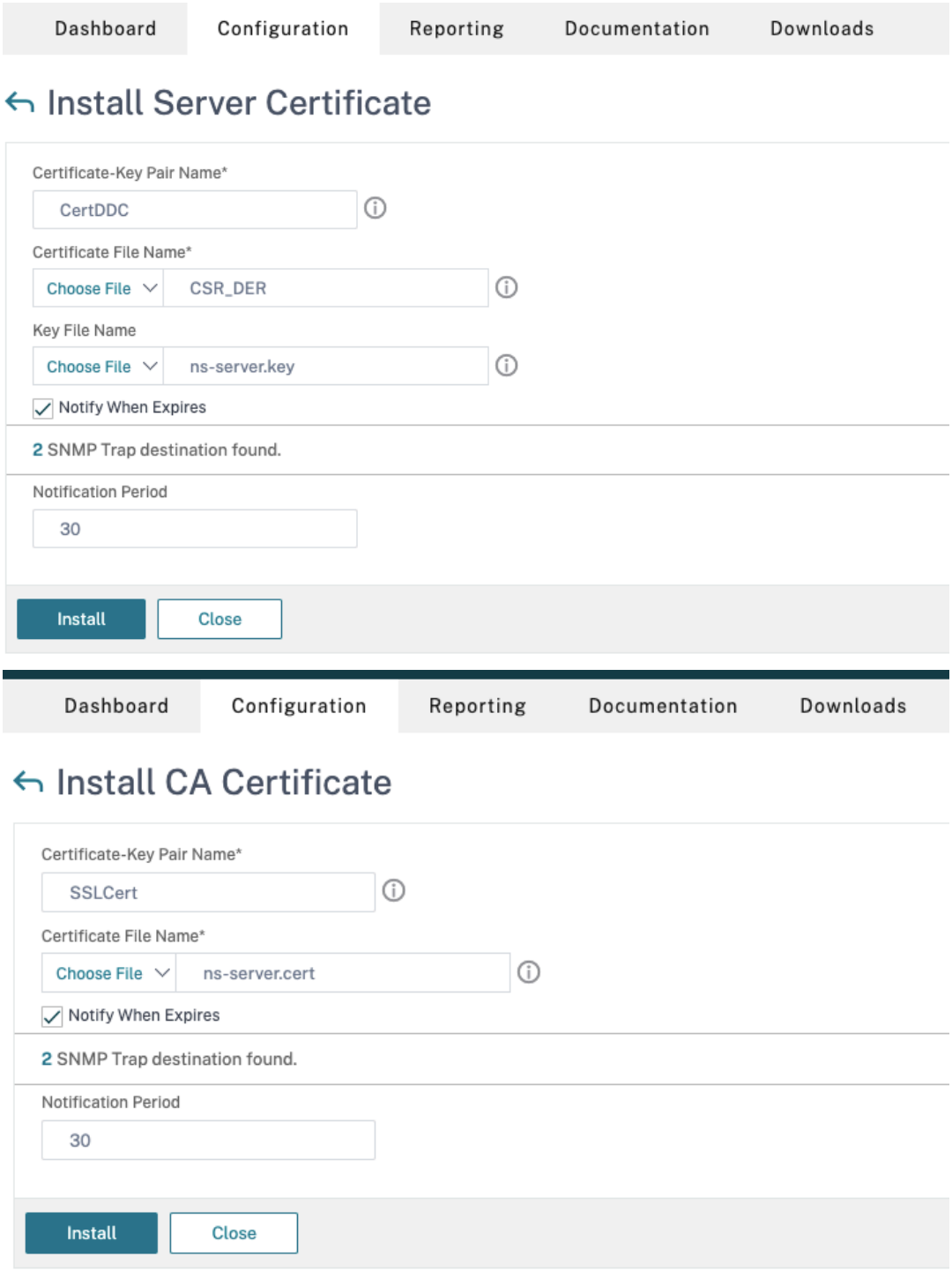
     - Subnet IP (SNIP) address for enabling communication between the Citrix ADC appliance and the back-end servers. For details, see Configuring Subnet IP Addresses.
     - Citrix Gateway virtual IP address and load balancer virtual IP address to log in to the ADC appliance for session launch. For details, see Create a virtual server.



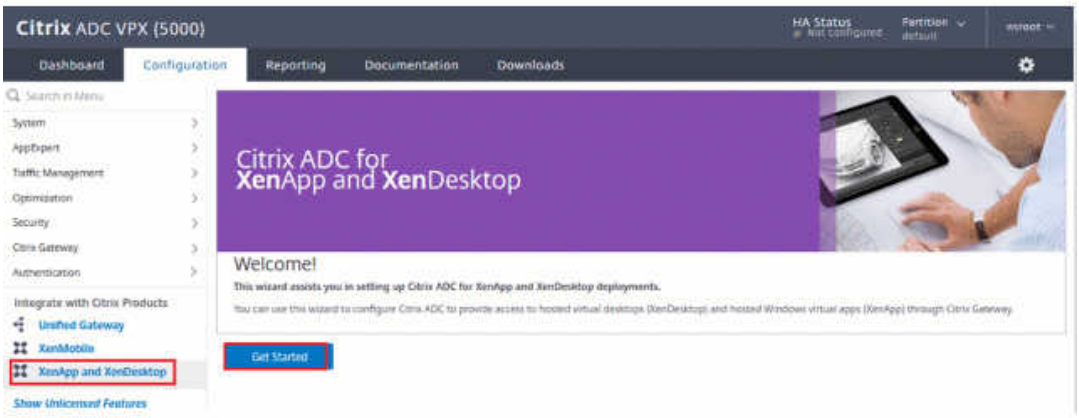
- The required modes and features in the Citrix ADC appliance are enabled.
  - To enable the modes, in the Citrix ADC GUI go to **System > Settings > Configure Mode**.
  - To enable the features, in the Citrix ADC GUI go to **System > Settings > Configure Basic Features**.
- Certificates related configurations are complete.
  - The Certificate Signing Request (CSR) is created. For details, see Create a certificate.



- The server and CA certificates and root certificates are installed. For details, see Install, link, and updates.

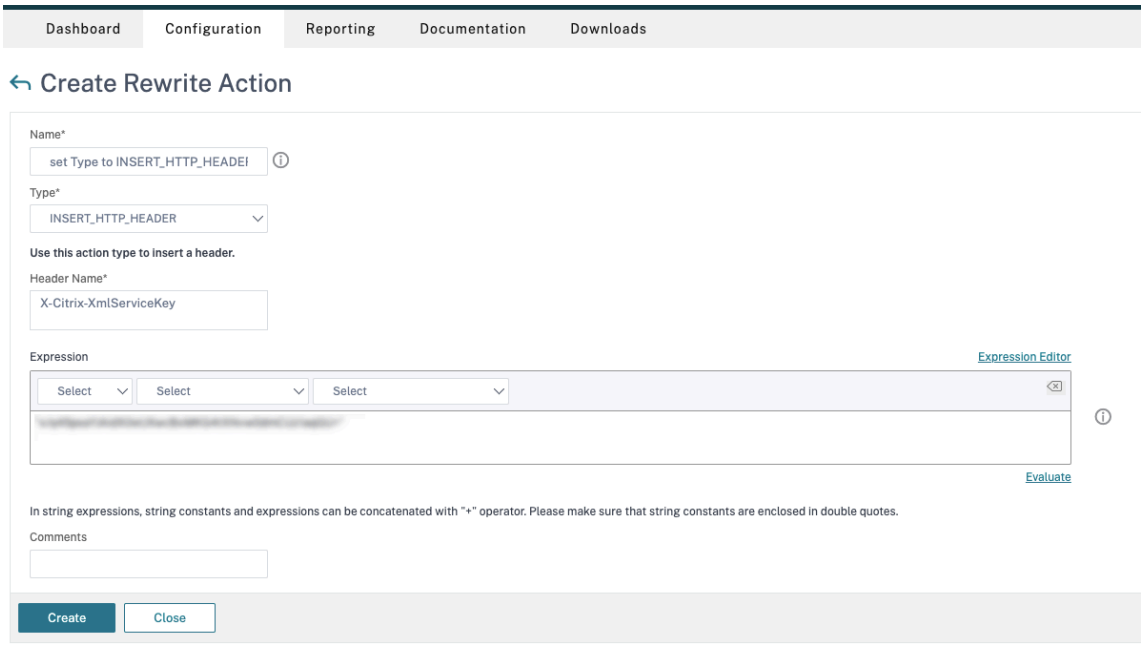


- A Citrix Gateway has been created for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Test the connectivity by clicking the **Test STA Connectivity** button to confirm that the virtual servers are online. For details, see Setting up Citrix ADC for Citrix Virtual Apps and Desktops.

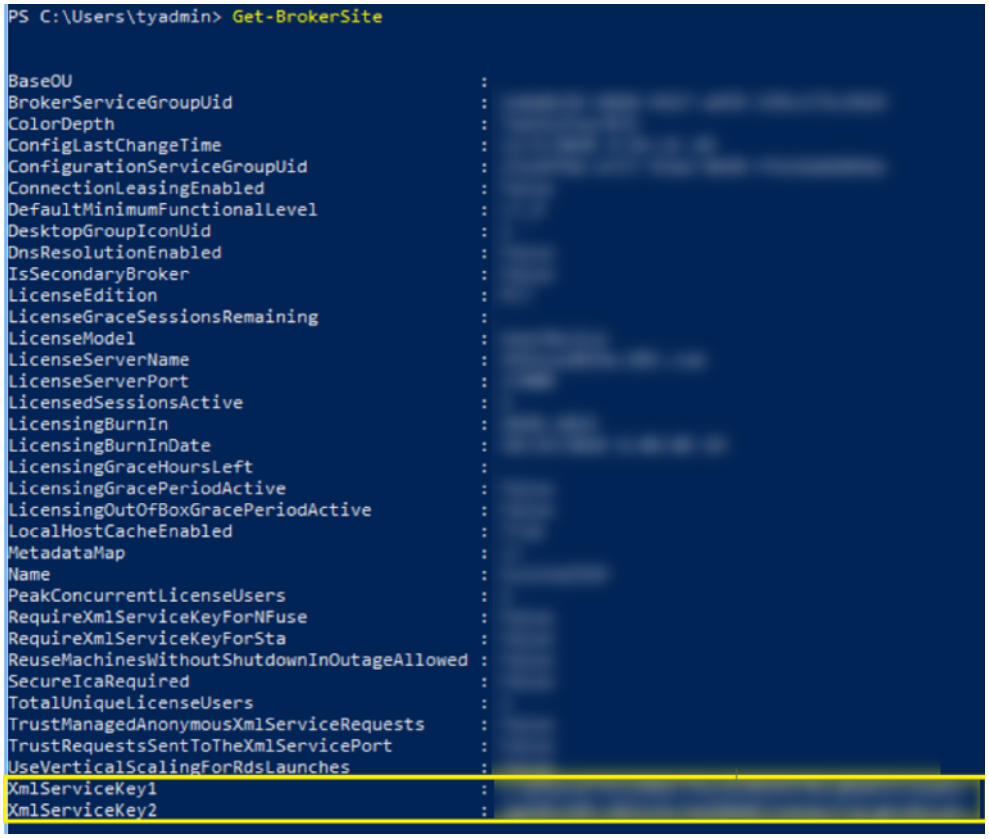


2. Add a rewrite action. For details, see Configuring a Rewrite Action.

   a) Go to **AppExpert > Rewrite > Actions**.
   b) Click **Add** to add a new rewrite action. You can name the action as "set Type to INSERT_HTTP_HEADER".



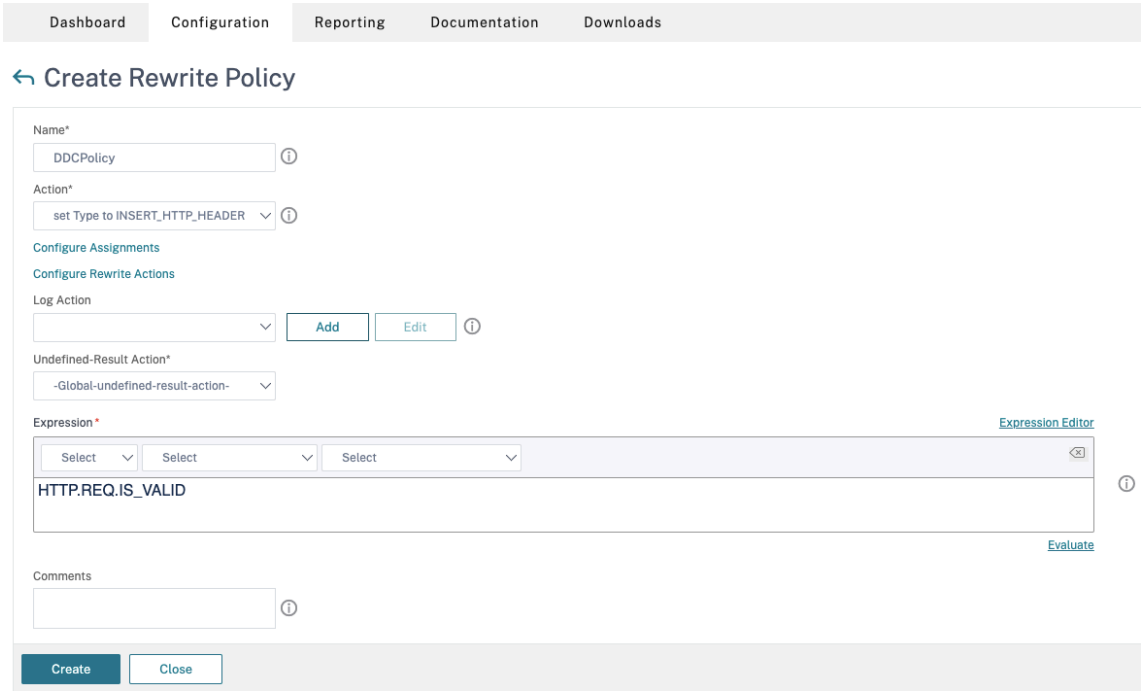
   a) In **Type**, select **INSERT_HTTP_HEADER**.
   b) In **Header Name**, enter X-Citrix-XmlServiceKey.
   c) In **Expression**, add <XmlServiceKey1 value> with the quotes. You can copy the XmlServiceKey1 value from your Desktop Delivery Controller configuration.



3. Add a rewrite policy. For details, see Configuring a Rewrite Policy.

    a) Go to **AppExpert > Rewrite > Policies**.

    b) Click **Add** to add a new policy.



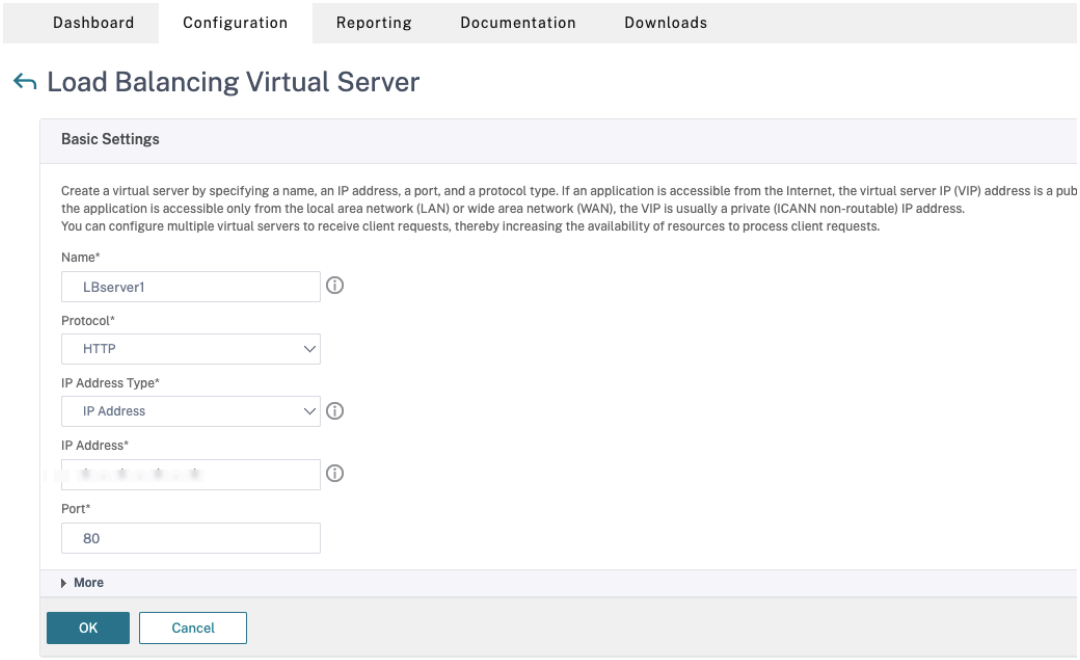
a) In **Action**, select the action created in the earlier step.
b) In **Expression**, add HTTP.REQ.IS_VALID.
c) Click **OK**.

4. Set up load balancing. You must configure one load balancing virtual server per STA server. If not the sessions fail to launch.

   For details, see Set up basic load balancing.

   a) Create a load balancing virtual server.

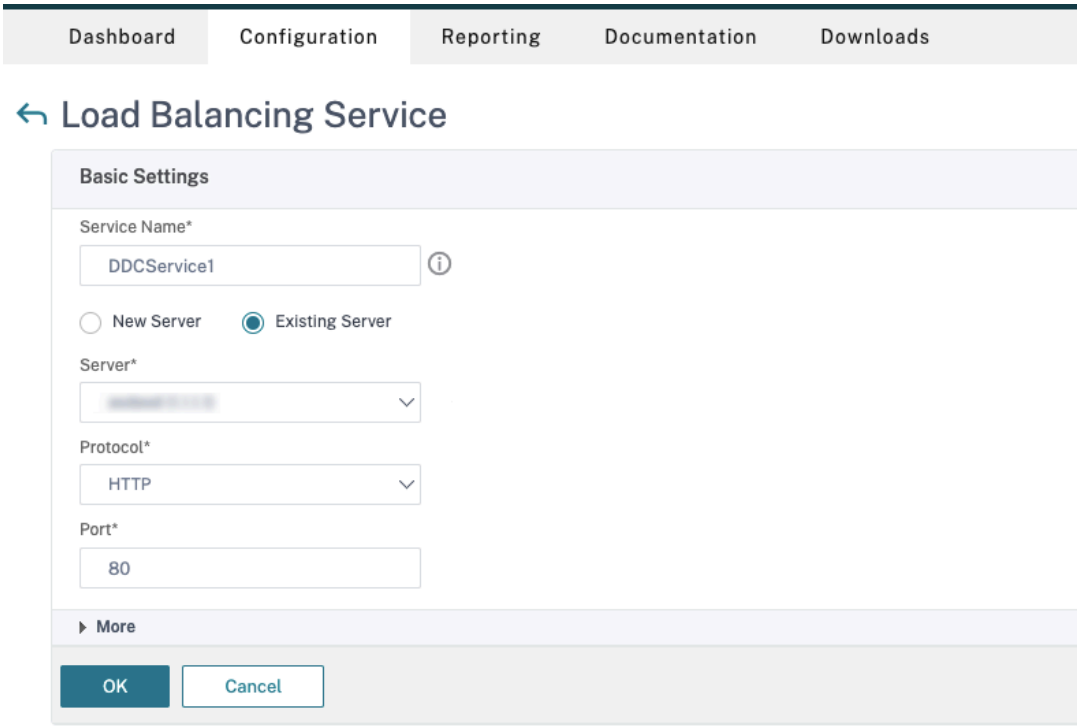
      - Go to **Traffic Management > Load Balancing > Servers**.
      - In **Virtual Servers** page, click **Add**.



- In **Protocol**, select **HTTP**.
- Add the load balancing virtual IP address and in **Port** select **80**.
- Click **OK**.

b) Create a load balancing service.

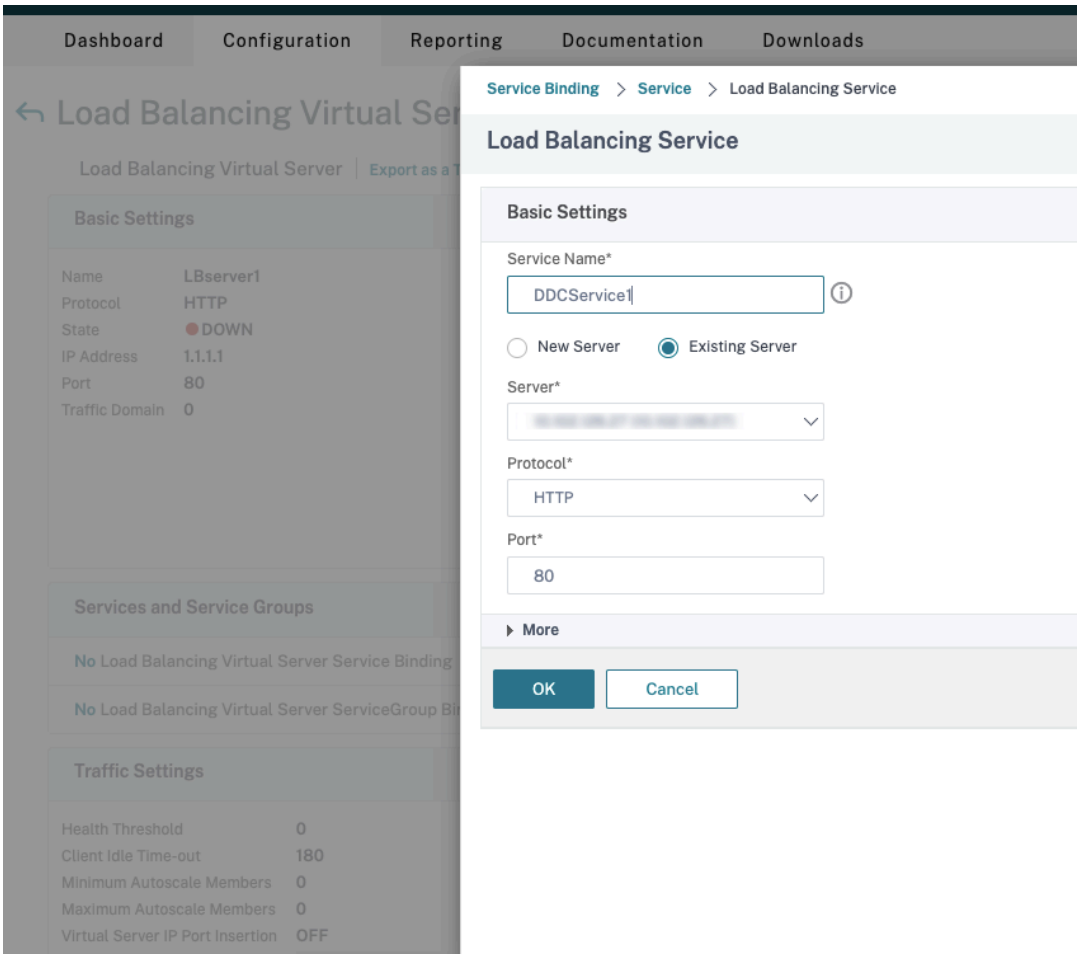
- Go to **Traffic Management > Load Balancing > Services**.



- In **Existing Server**, select the virtual server created in the previous step.
- In **Protocol**, select **HTTP** and in **Port** select **80**.
- Click **OK,** and then click **Done**.

c) Bind the service to the virtual server.

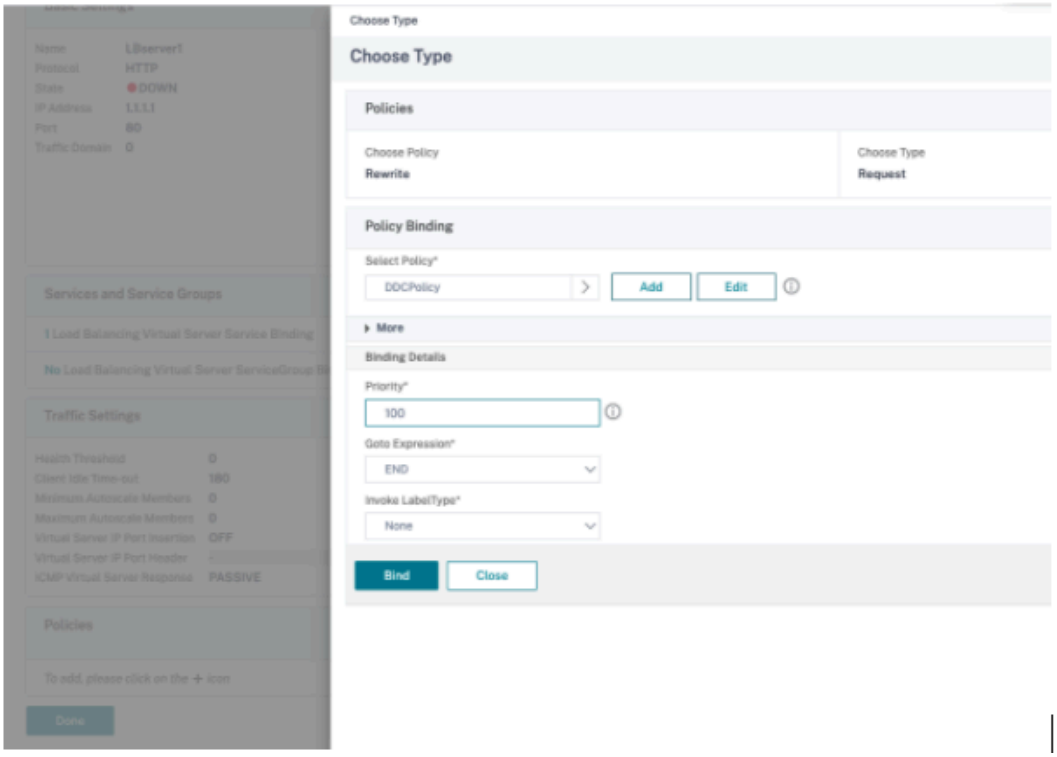
- Select the virtual server created earlier and click **Edit**.
- In **Services and Service Groups**, click **No Load Balancing Virtual Server Service Binding**.



- In **Service Binding**, select Citrix DaaS created earlier.
- Click **Bind**.

d) Bind the rewrite policy created earlier to the virtual server.

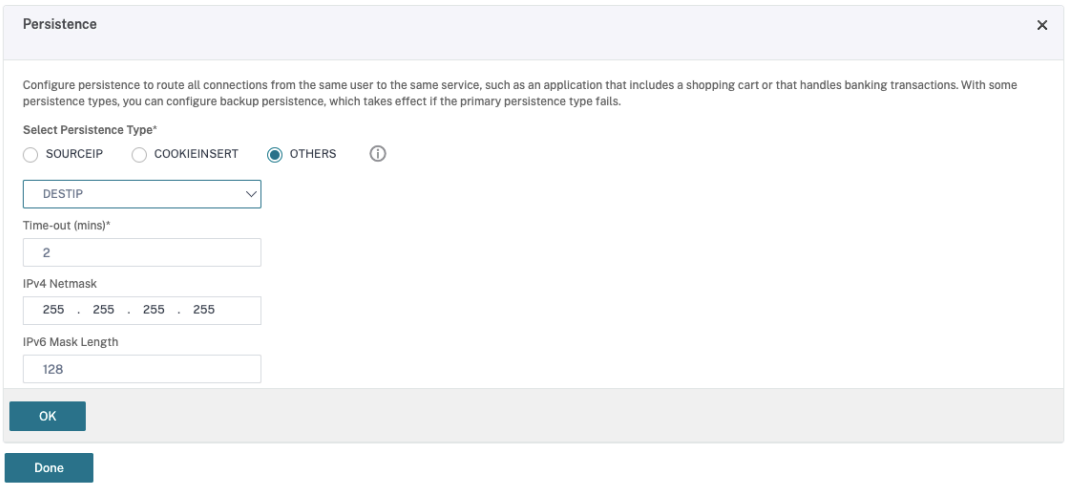
- Select the virtual server created earlier and click **Edit**.
- In **Advanced Settings**, click **Policies,** and then in **Policies** section click **+**.



- In **Choose Policy**, select **Rewrite** and in **Choose Type**, select **Request**.
- Click **Continue**.
- In **Select Policy**, select the rewrite policy created earlier.
- Click **Bind**.
- Click **Done**.

e) Set up persistence for the virtual server, if necessary.

- Select the virtual server created earlier and click **Edit**.
- In **Advanced Settings**, click **Persistence**.



- Select persistence type as **Others**.

- Select **DESTIP** to create persistence sessions based on the IP address of the service selected by the virtual server (the destination IP address)
- In **IPv4 Netmask**, add network mask same as that of the DDC.
- Click **OK**.

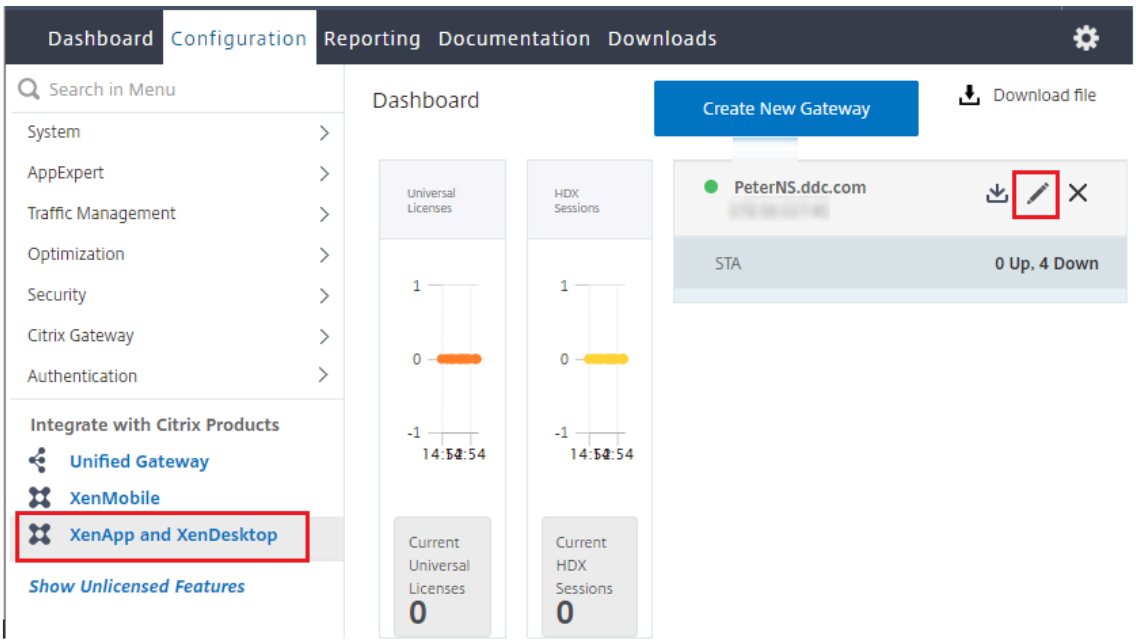
f) Repeat these steps for the other virtual server as well.

Configuration changes if the Citrix ADC appliance is already configured with Citrix DaaS

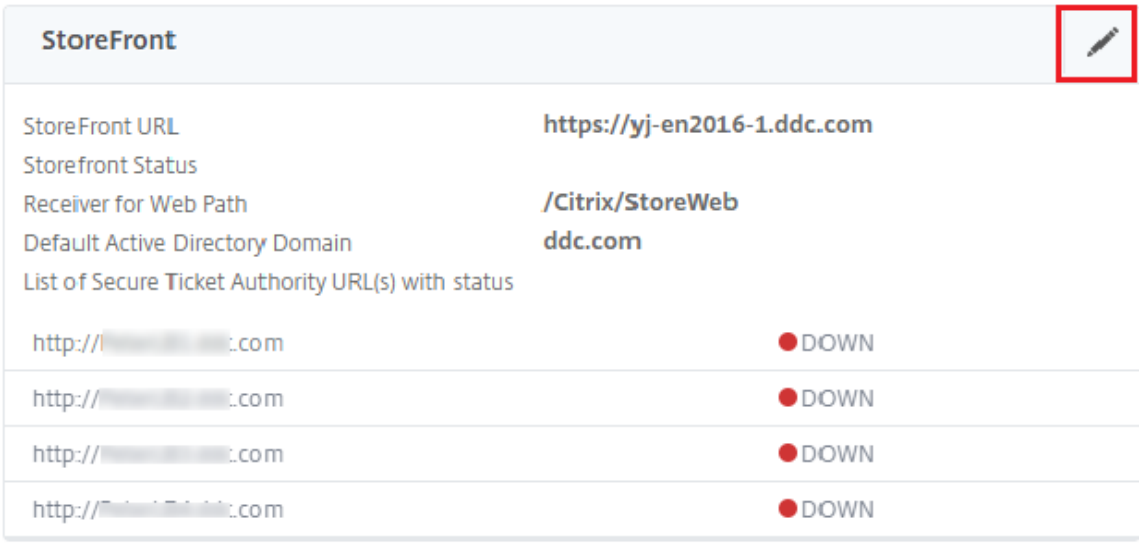
If you have already configured the Citrix ADC appliance with Citrix DaaS, then to use the Secure XML feature, you must make the following configuration changes.

- Before the session launch, change the **Security Ticket Authority URL** of the gateway to use the FQDNs of the load balancing virtual servers.
- Ensure that the `TrustRequestsSentToTheXmlServicePort` parameter is set to False. By default, `TrustRequestsSentToTheXmlServicePort` parameter is set to False. However, if the customer has already configured the Citrix ADC for Citrix DaaS, then the `TrustRequestsSentToTheXmlServicePort` is set to True.

1. In the Citrix ADC GUI, go to **Configuration > Integrate with Citrix Products** and click **XenApp and XenDesktop**.
2. Select the gateway instance and click the edit icon.

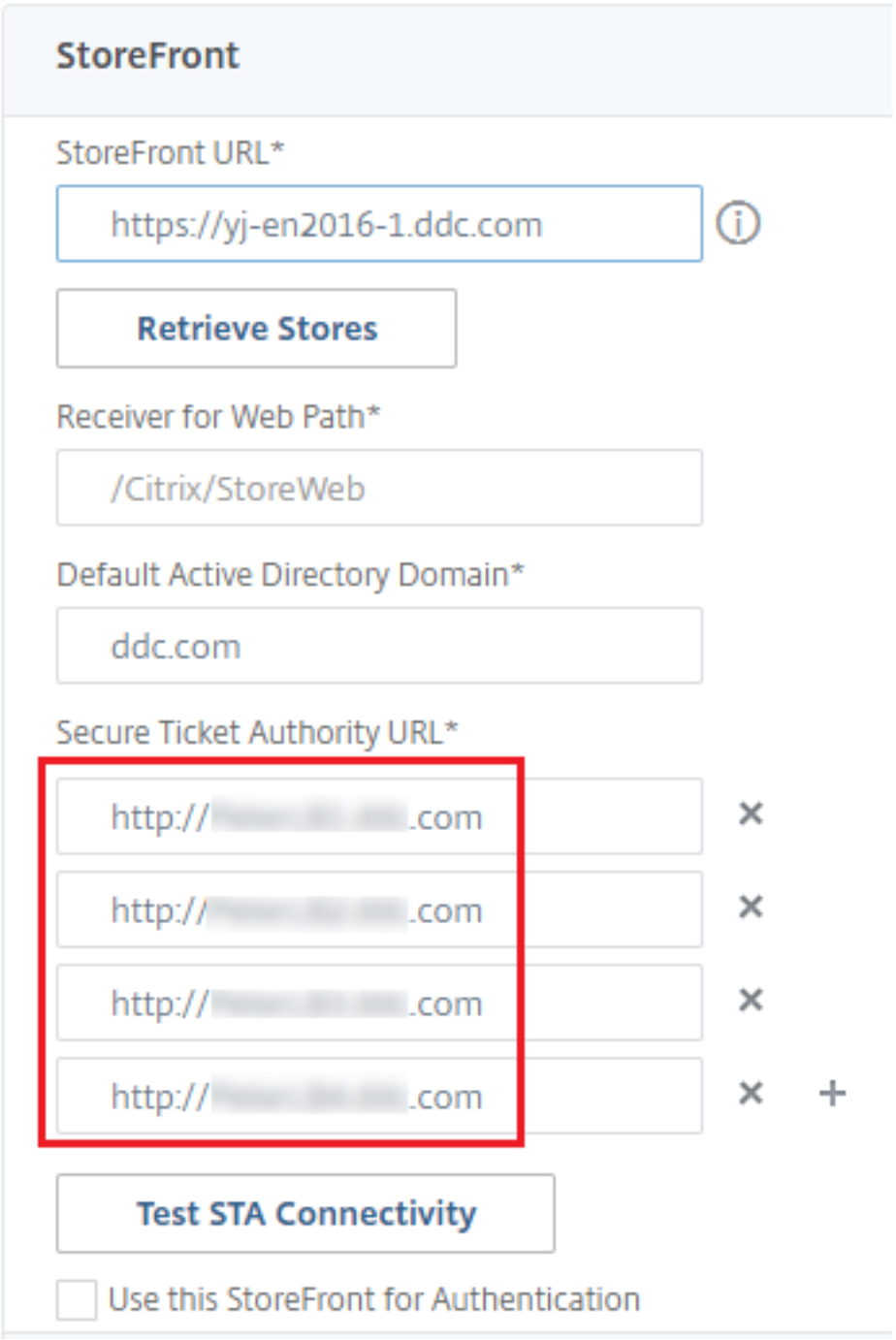


3. In the StoreFront pane, click the edit icon.



4. Add the **Secure Ticket Authority URL**.

   - If the Secure XML feature is enabled, then the STA URL must be the URL of the load balancing service.
   - If the Secure XML feature is disabled, then the STA URL must be the URL of STA (DDC's address) and the TrustRequestsSentToTheXmlServicePort parameter on the DDC must be set to True.



Session resilience settings

March 6, 2024

Maintaining session activity is critical to providing the best user experience. Losing connectivity due

to unreliable networks, highly variable network latency, and range limitations of wireless devices can lead to user frustration. Being able to move quickly between workstations and access the same set of applications each time they log on is a priority for many mobile workers such as healthcare workers in a hospital.

The features described in this article optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

Session reliability

Session Reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application that they are using until network connectivity resumes.

This feature is especially useful for mobile users with wireless connections. For example, a user with a wireless connection enters a railroad tunnel and momentarily loses connectivity. Ordinarily, the session is disconnected and disappears from the user's screen, and the user has to reconnect to the disconnected session. With Session Reliability, the session remains active on the machine. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

Citrix Workspace app users cannot override the Controller setting.

You can use Session Reliability with Transport Layer Security (TLS). TLS encrypts only the data sent between the user device and Citrix Gateway.

Enable and configure Session Reliability with the following policy settings:

- The Session reliability connections policy setting allows or prevents session reliability.
- The Session reliability timeout policy setting has a default of 180 seconds, or three minutes. Although you can extend the amount of time Session Reliability keeps a session open, this feature is designed for user convenience and therefore does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, the chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.
- Incoming session reliability connections use port 2598, unless you change the port number in the Session reliability port number policy setting.
- If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect

authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes, or disconnects, the user session after the amount of time you specify in the Session reliability timeout policy setting. After that, the Auto Client Reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.

Auto Client Reconnect

With the Auto Client Reconnect feature, Citrix Workspace app can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically. When this feature is enabled on the server, users do not have to reconnect manually to continue working.

For application sessions, Citrix Workspace app attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, Citrix Workspace app attempts to reconnect to the session for a specified time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this time is five minutes. To change this period, edit this registry on the user device:

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

Where `seconds` is the number of seconds after which no more attempts are made to reconnect the session.

Enable and configure Auto Client Reconnect with the following policy settings:

- **Auto client reconnect:** Enables or disables automatic reconnection by Citrix Workspace app after a connection has been interrupted.
- **Auto client reconnect authentication:** Enables or disables the requirement for user authentication after automatic reconnection.
- **Auto client reconnect logging:** Enables or disables logging of reconnection events in the event log. Logging is disabled by default. When enabled, the server's System Log captures information about successful and failed automatic reconnection events. Each server stores information about reconnection events in its own system log. The site does not provide a combined log of reconnection events for all servers.

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on, the server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to Citrix Workspace app. Citrix Workspace app submits the key to the server for reconnection. The server decrypts the credentials and

submits them to Windows Logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions.

Cookies are not used if you enable the auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Citrix Workspace app attempts to reconnect automatically.

For maximum protection of user credentials and sessions, use encryption for all communication between clients and the Site.

Disable Auto Client Reconnect on Citrix Workspace app for Windows by using the icaclient.adm file. For more information, see the documentation for your Citrix Workspace app for Windows version.

Settings for connections also affect Auto Client Reconnect:

- By default, Auto Client Reconnect is enabled through policy settings at the Site level, as described above. User reauthentication is not required. However, if a server's ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. Auto Client Reconnect works only if the server disconnects sessions when there is a broken or timed out connection. In this context, the ICA TCP connection refers to a server's virtual port (rather than an actual network connection) that is used for sessions on TCP/IP networks.
- By default, the ICA TCP connection on a server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by Citrix Workspace app.
- The connection can be configured to reset or log off sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new session. Rather than restoring a user to the same place in the application in use, the application is restarted.
- If the server is configured to reset sessions, Auto Client Reconnect creates a session. This process requires users to enter their credentials to log on to the server.
- Automatic reconnection can fail if Citrix Workspace app or the plug-in submits incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection.

ICA Keep-Alive

Enabling the ICA Keep-Alive feature prevents broken connections from being disconnected. When enabled, if the server detects no activity (for example, no clock change, no mouse movement, no screen updates), this feature prevents Remote Desktop Services from disconnecting that session. The server sends keep-alive packets every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

> **Important:**
>
> ICA Keep-Alive works only if you are not using Session Reliability. Session Reliability has its own mechanisms to prevent broken connections from being disconnected. Configure ICA Keep-Alive only for connections that do not use Session Reliability.

ICA Keep-Alive settings override keep-alive settings that are configured in the Microsoft Windows Group Policy.

Enable and configure ICA Keep-Alive with the following policy settings:

- **ICA keep alive timeout:** Specifies the interval (1–3600 seconds) used to send ICA keep-alive messages. Do not configure this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern.

  The default interval is 60 seconds: ICA Keep-Alive packets are sent to user devices every 60 seconds. If a user device does not respond in 60 seconds, the status of the ICA sessions changes to disconnected.

- **ICA keep alives:** Sends or prevents sending ICA keep-alive messages.

Workspace control

Workspace control lets desktops and applications follow a user from one device to another. This ability to roam enables a user to access all desktops or open applications from anywhere simply by logging on, without having to restart the desktops or applications on each device. For example, workspace control can assist healthcare workers in a hospital who need to move quickly among different workstations and access the same set of applications each time they log on. If you configure workspace control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

Workspace control affects the following activities:

- **Logging on:** By default, workspace control enables users to reconnect automatically to all running desktops and applications when logging on, bypassing the need to reopen them manually. Through workspace control, users can open disconnected desktops or applications, and any that are active on another client device. Disconnecting from a desktop or application leaves it running on the server. If you have roaming users who must keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.

- **Reconnecting:** After logging on to the server, users can reconnect to all of their desktops or applications at any time by clicking Reconnect. By default, Reconnect opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect to open only those desktops or applications that the user disconnected from previously.
- **Logging off:** For users opening desktops or applications through StoreFront, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.
- **Disconnecting:** Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.

Workspace control is available for users who access desktops and applications through a Citrix StoreFront connection, or through the Citrix Workspace app. By default, workspace control is disabled for virtual desktop sessions, but is enabled for hosted applications. Session sharing does not occur by default between published desktops and any published applications running inside those desktops.

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is logged on to the session. For example, if a healthcare worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's x-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the x-ray laboratory go into effect at the session startup.

You can customize which printers appear to users when they change locations. You can also control whether users can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

For information about enabling and configuring workspace control for users, see the StoreFront documentation.

Session roaming

> **Note:**
>
> The following information guides you to configure session roaming using PowerShell. You can use the Full Configuration management interface instead. For more information, see Manage delivery groups.

By default, sessions roam between client devices with the user. When the user launches a session and then moves to another device, the same session is used and applications are simultaneously available on both devices. You can view the applications on multiple devices. The applications follow, regardless of the device or whether current sessions exist. Often, printers and other resources assigned to the application also follow.

While this default behavior offers many advantages, it might not be ideal in all cases. You can prevent session roaming using the PowerShell SDK.

Example 1: A medical professional is using two devices, completing an insurance form on a desktop PC, and looking at patient information on a tablet.

- If session roaming is enabled, both applications appear on both devices (an application launched on one device is visible on all devices in use). This might not meet the security requirements.
- If session roaming is disabled, the patient record does not appear on the desktop PC, and the insurance form does not appear on the tablet.

Example 2: A production manager launches an application on the PC in his office. The device name and location determine which printers and other resources are available for that session. Later in the day, he goes to an office in the next building for a meeting that will require him to use a printer.

- If session roaming is enabled, the production manager would probably be unable to access the printers near the meeting room, because the applications he launched earlier in his office resulted in the assignment of printers and other resources near that location.
- If session roaming is disabled, when he logs on to a different machine (using the same credentials), a new session is started, and nearby printers and resources are available.

Configure session roaming

To configure session roaming, use the following entitlement policy rule cmdlets with the "SessionReconnection"property. Optionally, you can also specify the "LeasingBehavior"property.

For desktop sessions:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

For application sessions:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Where `value` can be one of the following:

- **Always:** Sessions always roam, regardless of the client device and whether the session is connected or disconnected. This is the default value.
- **DisconnectedOnly:** Reconnect only to sessions that are already disconnected; otherwise, launch a new session. (Sessions can roam between client devices by first disconnecting them, or using workspace control to explicitly roam them.) An active connected session from another client device is never used. Instead, a new session is launched.

- **SameEndpointOnly:** A user gets a unique session for each client device that they use. This completely disables roaming. Users can reconnect only to the same device that was previously used in the session.

The "LeasingBehavior"property is described below.

Effects from other setting:

Disabling session roaming is affected by the application limit "Allow only one instance of the application per user"in the application's properties in the Delivery Group.

- If you disable session roaming, then disable the "Allow only one instance …"application limit.
- If you enable the "Allow only one instance …"application limit, do not configure either of the two values that allow new sessions on new devices.

Logon interval

If a virtual machine containing a desktop VDA closes before the logon process completes, you can allocate more time to the process. The default for 7.6 and later versions is 180 seconds (the default for 7.0-7.5 is 90 seconds).

On the machine (or the master image used in a machine catalog), set the following registry key:

Key: `HKLM\SOFTWARE\Citrix\PortICA`

- Value: `AutoLogonTimeout`
- Type: `DWORD`
- Specify a decimal time in seconds, in the range 0 to 3600.

If you change the master image, roll out the new image to the catalog. For more information, see Change the master image.

This setting applies only to VMs with single-session desktop (workstation) VDAs. Microsoft controls the logon timeout on machines with multi-session server VDAs.

Tags

October 27, 2023

Introduction

Tags are strings that identify items such as machines, applications, desktops, delivery groups, application groups, and policies. After creating a tag and adding it to an item, you can tailor certain operations

to apply only to items that have a specified tag.

- Tailor search displays in the Full Configuration management interface.

  For example, to display only applications that have been optimized for testers, create a tag named "test"and then add (apply) it to those applications. You can now filter the search with the tag "test".

- Publish applications from an application group or specific desktops from a delivery group, considering only a subset of the machines in selected delivery groups. This is called a *tag restriction*.

  With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with deploying and managing more machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a delivery group. Its functionality is similar, but not identical, to worker groups in XenApp releases earlier than 7.x.

  Using an application group or desktops with a tag restriction can be helpful when isolating and troubleshooting a subset of machines in a delivery group.

  Details and examples of using a tag restriction are described later in this article.

- Schedule periodic restarts for a subset of machines in a delivery group.

  Using a tag restriction for machines enables you to use new PowerShell cmdlets to configure multiple restart schedules for subsets of machines in a delivery group. For examples and details, see Manage delivery groups.

- Tailor the application (assignment) of Citrix policies to machines in delivery groups, delivery group types, or OUs that have (or don't have) a specified tag.

  For example, if you want to apply a Citrix policy only to the more powerful workstations, add a tag named "high power"to those machines. Then, on the **Assign Policy** page of the Create Policy wizard, select that tag and the **Enable** check box. You can also add a tag to a delivery group and then apply a Citrix policy to that group. For details, see Create policies.

You can apply tags to:

- Machines
- Applications
- Machine catalogs
- Delivery groups
- Application groups

You can configure a tag restriction when creating or editing the following in the Full Configuration management interface:

- A desktop in a shared delivery group
- An application group

Tag restrictions for a desktop or an application group

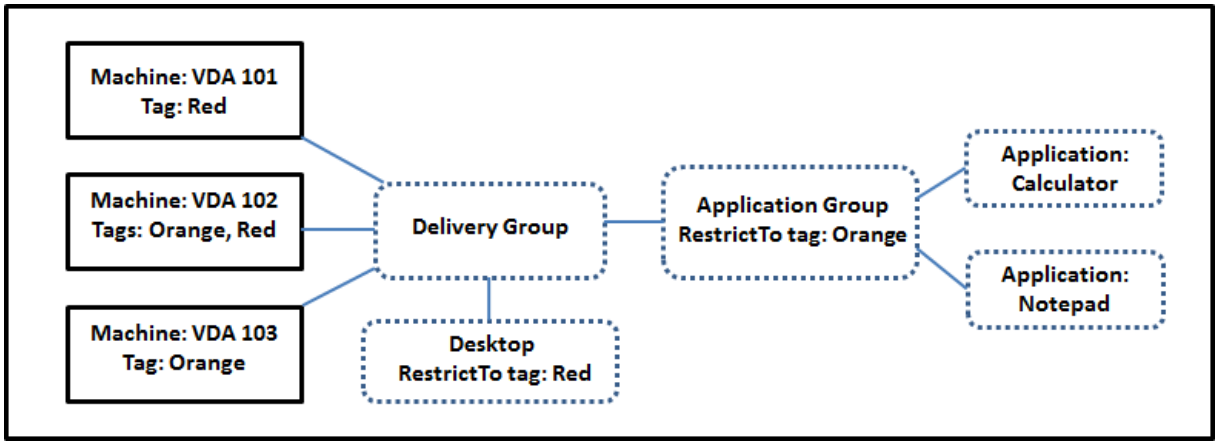
A tag restriction involves several steps:

- Create the tag and then add (apply) it to machines.
- Create or edit a group with the tag restriction (in other words, restrict launches to machines with tag *x*).

A tag restriction extends the Controller's machine selection process. The Controller selects a machine from an associated delivery group, subject to access policy, configured user lists, zone preference, and launch readiness, plus the tag restriction (if present). For applications, the Controller falls back to other delivery groups in priority order, applying the same machine selection rules for each considered delivery group.

Example 1: Simple layout

This example introduces a simple layout that uses tag restrictions to limit which machines are considered for certain desktop and application launches. There is one shared delivery group, one published desktop, and one application group configured with two applications.



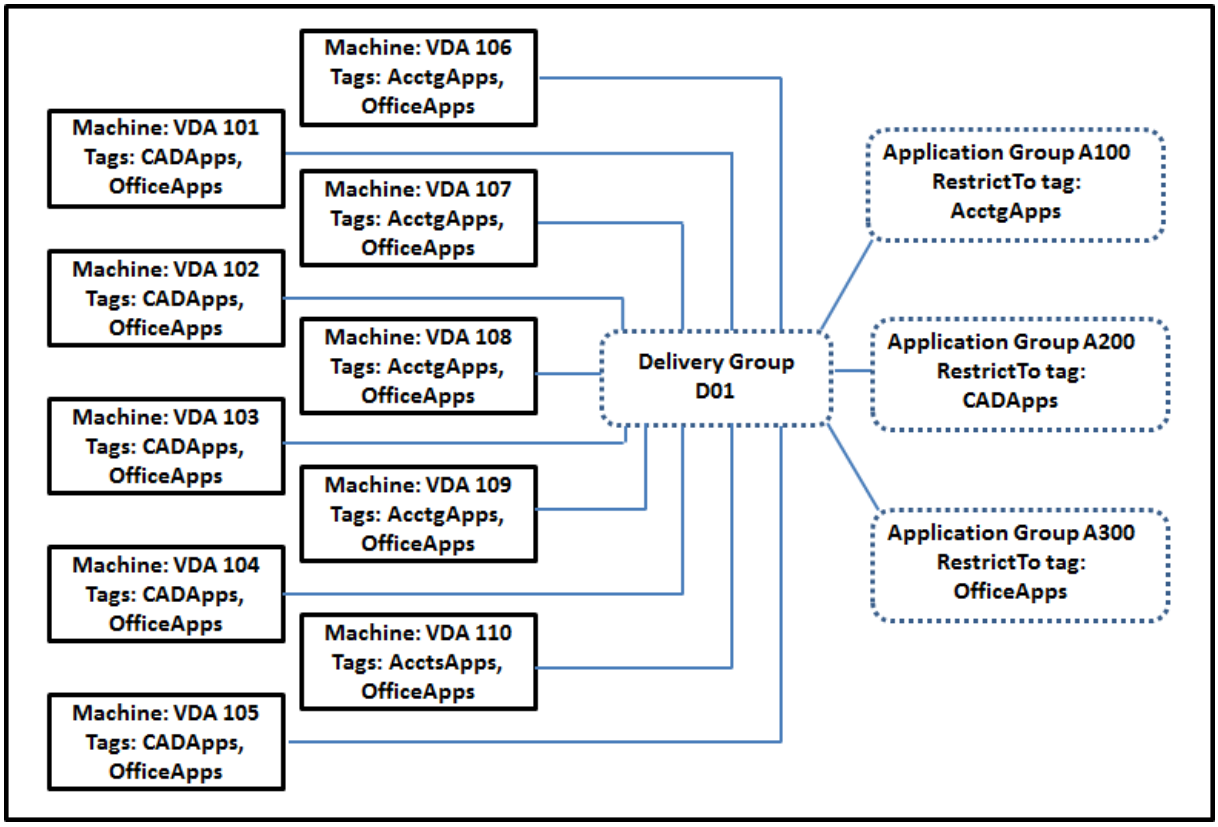
- Tags have been added to each of the three machines (VDA 101-103).
- The desktop in the delivery group was created with a tag restriction named `Red`. So, that desktop can be launched only on machines in that delivery group that have the tag `Red`: VDA 101 and 102.
- The application group was created with the `Orange` tag restriction. So, each of its applications (`Calculator` and `Notepad`) can be launched only on machines in that delivery group that have the tag `Orange`: VDA 102 and 103.

Machine VDA 102 has both tags (`Red` and `Orange`), so it can be considered for launching the applications and the desktop.

Example 2: More complex layout

This example contains several application groups that were created with tag restrictions. This results in the ability to deliver more applications with fewer machines than would otherwise be needed if you used only delivery groups.

How to configure example 2 shows the steps used to create and apply the tags, and then configure the tag restrictions in this example.



This example uses 10 machines (VDA 101-110), one delivery group (`D01`), and three application groups (`A100`, `A200`, `A300`). By applying tags to each machine and then specifying tag restrictions when creating each application group:

- Accounting users in the group can access the apps they need on five machines (VDA 101–105)
- CAD designers in the group can access the apps they need on five machines (VDA 106-110)
- Users in the group who need Office applications can access the Office apps on 10 machines (VDA 101-110)

Only 10 machines are used, with only one delivery group. Using delivery groups alone (without application groups) would require twice as many machines, because a machine can belong to only one delivery group.

Manage tags and tag restrictions

Tags are created, added (applied), edited, and deleted from selected items through the **Manage Tags** action in the Full Configuration management interface.

(Exception: Tags used for policy assignments are created, edited, and deleted through the **Manage Tags** action. However, you apply (assign) tags when you create the policy. See Create policies for details.)

Tag restrictions are configured when you create or edit desktops in delivery groups, and when you create and edit application groups.

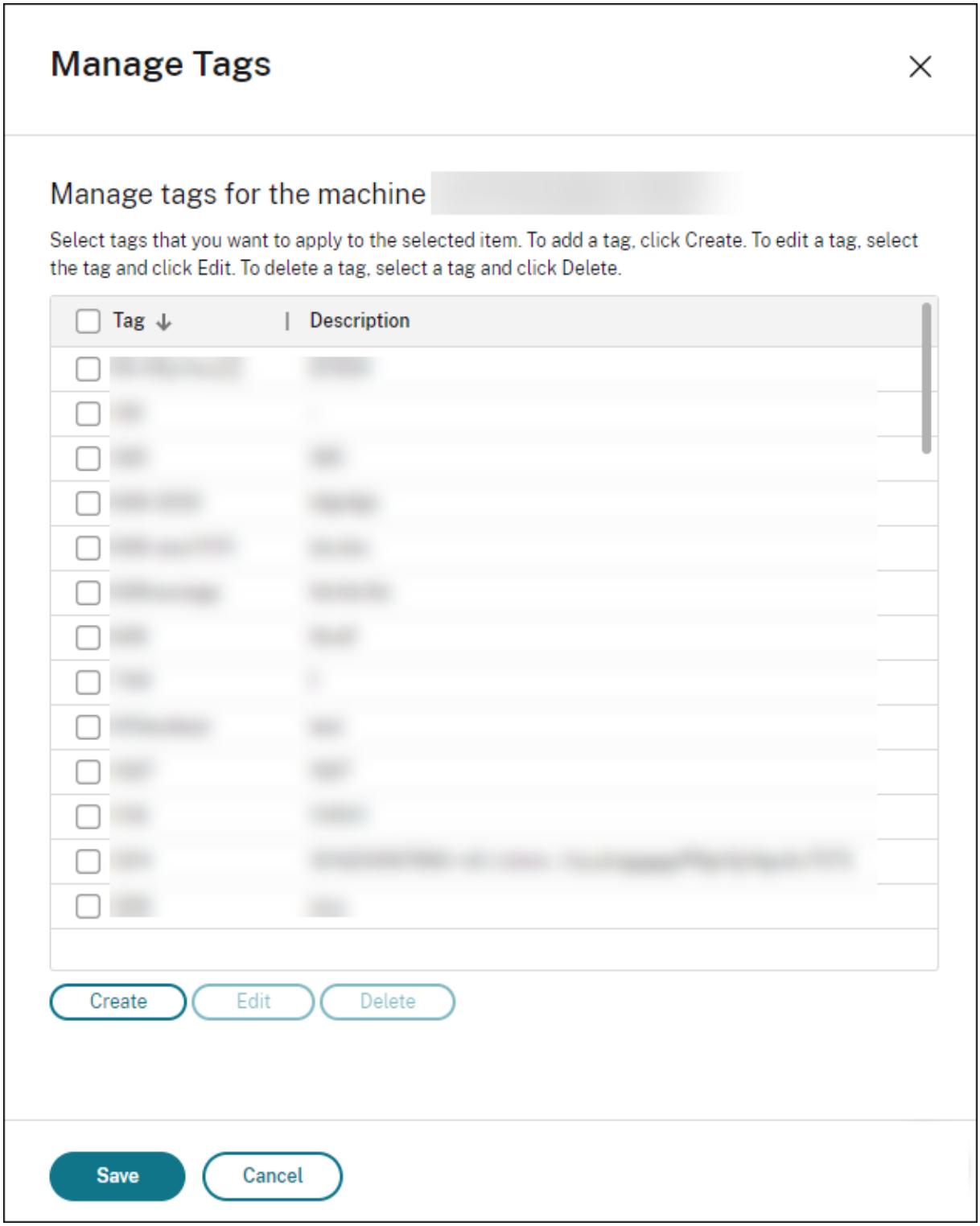
Use the Manage Tags feature

From **Manage > Full Configuration**, select the items to which you want to apply a tag. The items include:

- One or more machines
- One or more applications
- A desktop, a delivery group, or an application group
- A machine catalog

Then select **Manage Tags** in the action bar. The **Manage Tags** dialog box lists all existing tags, not just those for the items you selected.

- An enabled check box indicates that the tag has already been added to the selected items. (In the screen capture below, the selected machine has a tag named "Tag1"applied.)
- If you select more than one item, a check box containing a hyphen indicates that some but not all selected items have that tag added.



The following actions are available from the **Manage Tags** dialog box. Review Cautions when working with tags.

- **To create a tag:**

Select **Create.** Enter a name and description. Tag names must be unique and are not case-sensitive. Then select **Save**.

Creating a tag does not automatically apply it to any items you have selected. Use the check boxes to apply the tag.

- **To add (apply) one or more tags:**

  Enable the check box next to the tag name. A check box containing a hyphen indicates that some, but not all selected items already have the tag applied. When you select multiple items and a tag's check box has a hyphen, changing it to a check mark affects all selected machines.

  If you attempt to add a tag to machines, and that tag is used as a restriction in an application group, you are warned that the action can make those machines available for launch. If that's what you intend, proceed.

- **To remove one or more tags:**

  Clear the check box next to the tag name. A check box containing a hyphen indicates that some, but not all selected items already have the tag applied. When you select multiple items and a tag's check box has a hyphen, clearing the check box removes the tag from all selected machines.

  If you try to remove a tag restriction from a machine, you're warned that the action can affect the machines considered for launch. If that's what you intend, proceed.

- **To edit a tag:**

  Select a tag and then select **Edit**. Enter a new name, description, or both. You can edit only one tag at a time.

- **To delete one or more tags:**

  Select the tags and then select **Delete**. The **Delete Tag** dialog box indicates how many items currently use the selected tags (for example "2 machines"). Select an item to display more information (for example, the names of the two machines that have the tag applied). Confirm whether you want to delete the tags.

  You cannot delete a tag that is used as a restriction. First, edit the application group and remove the tag restriction or select a different tag.

When you're done in the **Manage Tags** dialog box, select **Save**.

To see if a machine has any tags applied: Select **Delivery Groups** in the left pane. Select a delivery group then select **View Machines** in the action bar. Select a machine and then select the **Tags** tab on the **Details** pane.

Manage tag restrictions

Configuring a tag restriction is a multi-step process: You first create the tag and add/apply it to machines. Then, you add the restriction to the application group or the desktop.

- **Create and apply the tag:**

  Create the tag and then add (apply) it to the machines that the tag restriction will affect, using **Manage Tags** actions.

- **To add a tag restriction to an application group:**

  Create or edit the application group. On the **Delivery Groups** page, select **Restrict launches to machines with the tag** and then select the tag from the list.

- **To change or remove the tag restriction on an application group:**

  Edit the group. On the **Delivery Groups** page, either select a different tag from the list or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

- **To add a tag restriction to a desktop:**

  Create or edit a delivery group. Select **Add** or **Edit** on the **Desktops** page. In the **Add Desktop** dialog box, select **Restrict launches to machines with the tag** and then select the tag from the menu.

- **To change or remove the tag restriction on a delivery group:**

  Edit the group. On the **Desktops** page, select **Edit**. In the dialog box, either select a different tag from the list or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

Cautions when working with tags

A tag applied to an item can be used for different purposes. Keep in mind that adding, removing, and deleting a tag can have unintended effects. You can use a tag to sort machine displays when using search in the Full Configuration management interface. You can use the same tag as a restriction when configuring an application group or a desktop. That action limits launch consideration to only machines in specified delivery groups that have that tag.

If you add a tag to machines after that tag is configured as a desktop or application group tag restriction, you are warned that might make the machines available for launching more applications or desktops. If that's what you intend, proceed. If not, cancel the operation.

For example, let's say you create an application group with the Red tag restriction. Later, you add several other machines in the same delivery groups used by that application group. If you then try to add the Red tag to those machines, you see a message similar to: "The tag Red is used as a restriction

on the following application groups. Adding this tag might make the selected machines available to launch applications in this application group."You can then confirm or cancel adding that tag to those additional machines.

Similarly, when a tag is used in an application group to restrict launches, you cannot delete the tag until you edit the group and remove it as a restriction. (If you were allowed to delete that tag, it might result in allowing applications to launch on all machines in the delivery groups associated with the application group.) The same prohibition against deleting a tag applies if the tag is being used as a restriction for desktop launches. After you edit the application group or desktops in the delivery group to remove that tag restriction, you can delete the tag.

All machines might not have the same sets of applications. A user can belong to more than one application group, each with a different tag restriction and different or overlapping sets of machines from delivery groups. The following table lists how machine considerations are decided.

When an application has been added to	These machines in the selected delivery groups are considered for launch
One application group with no tag restriction	Any machine.
One application group with tag restriction A	Machines that have tag A applied.
Two application groups, one with tag restriction A and the other with tag restriction B	Machines that have tag A and tag B. If none is available, then machines that have tag A or tag B.
Two application groups, one with tag restriction A and the other with no tag restriction	Machines that have tag A. If none is available, then any machine.

If you used a tag restriction in a machine restart schedule, any changes you make that affect tag applications or restrictions affect the next machine restart cycle. It does not affect any restart cycles that is in progress while the changes are being made.

How to configure example 2

The following sequence shows the steps to create and apply tags, and then configure tag restrictions for the application groups illustrated in the earlier second example.

VDAs and applications have already been installed on the machines and the delivery group has been created.

Create and apply tags to the machines:

1. From **Manage > Full Configuration**, select **Delivery Groups** in the left pane. Select delivery group `D01` and then select **View Machines** in the action bar.
2. Select machines VDA 101-105 and then select **Manage Tags** in the action bar.

3. In the **Manage Tags** dialog box, select **Create**. Create a tag named `CADApps`. Select **OK**.
4. Select **Create** again and create a tag named `OfficeApps`. Select **OK**.
5. Add (apply) the newly created tags to the selected machines by enabling the check boxes next to each tag's name (`CADApps` and `OfficeApps`). Then close the dialog box.
6. Select delivery group `D01`. Select **View Machines** in the action bar.
7. Select machines VDA 106-110 and then select **Manage Tags** in the action bar.
8. In the **Manage Tags** dialog box, select **Create**. Create a tag named `AcctgApps`. Select **OK**.
9. Apply the newly created `AcctgApps` tag and the `OfficeApps` tag to the selected machines by selecting the check boxes next to each tag's name. Then close the dialog box.

Create the application groups with tag restrictions.

1. From **Manage > Full Configuration**, select **Applications** in the left pane.
2. Select **Create Application Group** in the action bar. The wizard launches.
3. On the **Delivery Groups** page, select delivery group `D01`. Select **Restrict launches to machines with tag** and then select the `AcctgApps` tag from the list.
4. Complete the wizard, specifying the accounting users and the accounting applications. (When adding the application, choose the **From Start menu** source, which searches for the application on the machines that have the `AcctgApps` tag.) On the **Summary** page, name the group `A100` .
5. Repeat the preceding steps to create application group `A200`, specifying machines that have the `CADApps` tag, plus the appropriate users and applications.
6. Repeat steps to create application group `A300`, specifying machines that have the `OfficeApps` tag, plus the appropriate users and applications.

Apply tags to machine catalogs

You can use **Manage > Full Configuration** or PowerShell to apply tags to machine catalogs.

- Using the management interface is described in Manage tags. Catalog displays do not indicate whether tags are applied.
- To use PowerShell, see Use PowerShell to apply tags to catalogs.

Here is an example of using tags with catalogs:

- A delivery group contains machines from several catalogs, but you want an operation (such as a restart schedule) to affect only the machines in a specific catalog. Applying a tag to that catalog accomplishes that goal.

Use PowerShell to apply tags to catalogs

The following PowerShell cmdlets are available:

- You can pass catalog objects to cmdlets such as `Add-BrokerTag` and `Remove-BrokerTag`.
- `Get-BrokerTagUsage` shows how many catalogs contain tags.
- `Get-BrokerCatalog` has a property named `Tags`.

For example, the following cmdlets add a previously created tag named `fy2018` to the catalog named `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`.

See the PowerShell cmdlet help for guidance and syntax.

Auto tags (Preview)

Auto-tagging allows administrators to set and remove tags on various DaaS objects automatically, based on custom rules. This enhancement eliminates the need to maintain different scripts that run periodically for environment optimization.

Use cases

With auto-tagging, you can implement rules relevant to your business drivers, such as reducing costs, optimizing the infrastructure, and driving consumption. The following are some of the use cases:

- **Reclaim unused VDIs** - To release the dedicated workloads that have not been used for more than a pre-configured number of days to the available pool.
- **Remove App clutter** - To reduce application clutter by identifying the applications that have not been used for more than a pre-configured number of days.
- **DGs with less than X functional level** - To find delivery groups with less than a specific functional level.
- **Inactive users** - To reclaim resources of users who have not logged on for more than a pre-configured number of days.

PowerShell commands

You can create autotags using PowerShell commands. After an autotag rule is created, it is evaluated at a frequency of 600 seconds. For more information, see New-BrokerAutoTagRule.

Examples `New-BrokerAutoTagRule` uses the same object type and filter parameters as the `Get-BrokerMachine` commandlet. For more information, see GetBrokerMachine.

1. Tag dedicated VDIs that have not been used for more than 30 days with and ID 123:

    a) Define a tag to tag the unused VDIs with, say **unused-VDI**.

    - Tag name : unused-VDI

- Tag ID : 123

b) Create the auto-tagging rule to tag unused machines. Define the rule parameters:

- Name : Generic name for the rule.
- Object type : Machine.
- Rule text : Static, assigned machines whose last connection time is > 30 days or no value.
- Tag Uid : The tag id that you want to associate with, 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -
RuleText "-AllocationType Static -IsAssigned $true -Filter {
SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt '-30'
 -or LastConnectionTime -eq `$null )} " -TagUid 123
```

c) Check machines marked with the tag **unused-VDI** and release them.

2. To tag delivery groups with less than X functional level (using **L7_20** as the threshold functional level):

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-
RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid
 123
```

3. To tag user visible apps published without a folder:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-
TagUid 123
```

More information

Blog post: How to assign desktops to specific servers.

Time zone setup

February 29, 2024

Customize the date and time format in the management console according to your preferences.

> **Note:**
>
> This setting is specific to each user account.

1. Go to **Full Configuration > Settings > Date and Time**.

2. Click **Edit** to configure the following settings:

   - **Time format:**
     - Select to display the time using a 12-hour clock (09:00 PM, for example) or a 24-hour clock (21:00, for example).

     > **Note:**
     >
     > Select the **Same as local** option if you want the format to align with your browser's time zone.

   - **Date format:**
     - Configure the date format to match your preferences, such as yyyy/MM/dd.

     > **Note:**
     >
     > Select the **Same as local** option if you want the format to align with your browser's time zone.

   - **Time zone:**
     - **UTC:** Display the date and time in UTC throughout the user interface. Mouseovers display the date and time local to your time zone.
     - **Local time zone:** Display the date and time in your local time zone throughout the user interface. Mouseovers display the date and time in UTC.

Troubleshoot VDA registration and session launch issues

March 23, 2022

We offer a health check feature that lets you gauge the health of VDAs. The feature lets you identify possible causes for common VDA registration and session launch issues through the Full Configuration management interface.

Unlike Cloud Health Check, a standalone tool for gauging the health and availability of the site and its other components, the feature is available as the **Run Health Check** action in the Full Configuration management interface.

The **Run Health Check** action can run the same checks as Cloud Health Check except the following ones:

- For VDA registration:

  - VDA communication port availability

- For session launches on VDAs:
  - Session launch communication port availability
  - VDA application launch path

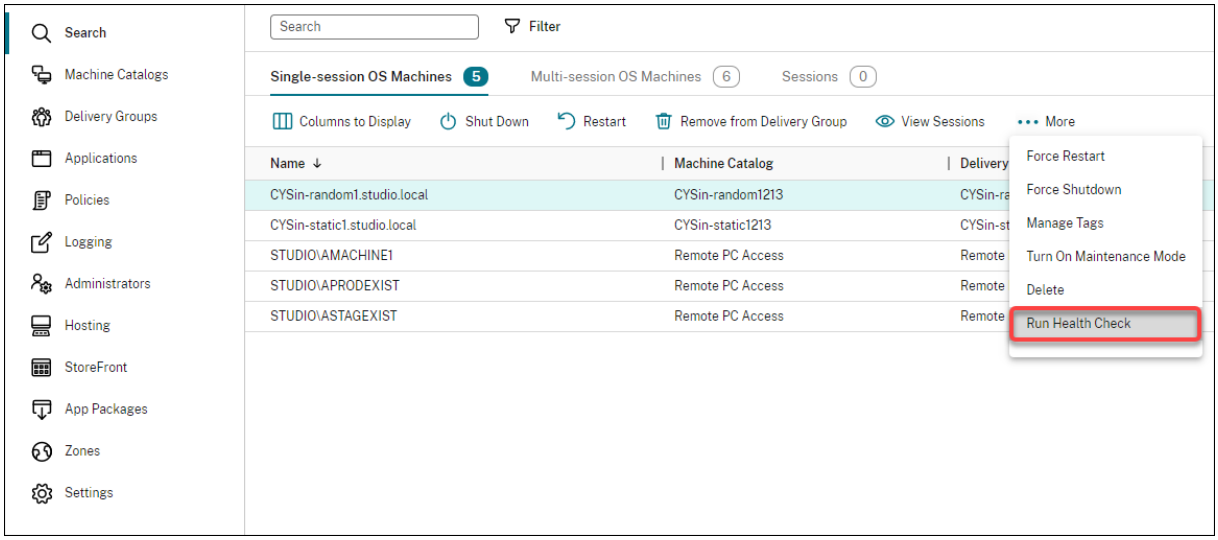
Prerequisites

Before you use the feature, verify that you meet the following prerequisites:

- Windows VDAs
- VDA version 2109 or later
- VDAs are registered

Run health checks for VDAs

1. In the Full Configuration management interface, go to the **Search** node.
2. Select one or more machines and then select **Run Health Check** from the action bar.

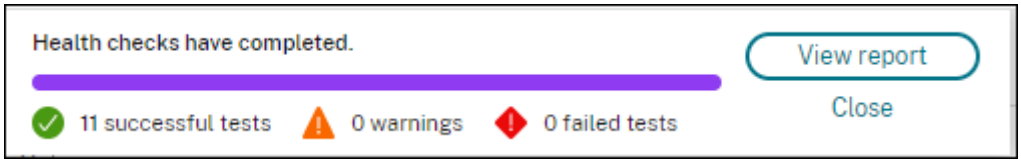


> **Note:**
>
> Currently, you can run health checks only for registered VDAs. The **Run Health Check** action is unavailable for unregistered VDAs.

After you select **Run Health Check**, a window appears, displaying the progress of the health checks. Wait until the heath checks complete or click **Cancel** to cancel the checks. If necessary, you can move the window.

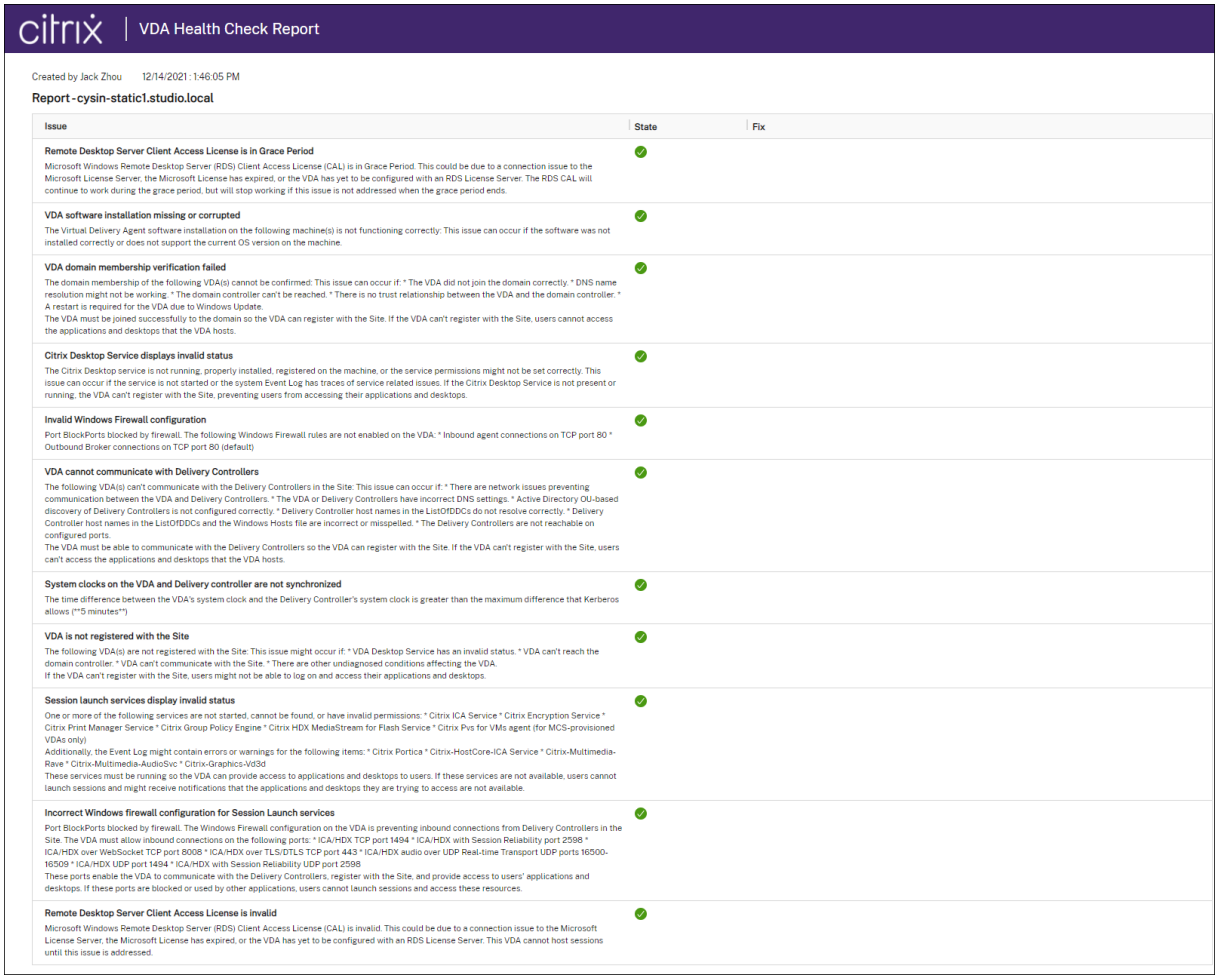
> **Note:**
>
> In scenarios where a "health checks in progress"window already exists, you cannot run additional health checks until the existing health checks complete.

After the health checks complete, the following two buttons appear: **View report** and **Close**. To view the results of the health checks, click **View report**.



The health check report opens in a new browser tab. The report contains the following elements:

- Time and date when the results report was generated
- The person who ran the health checks
- Checks run on the target machines
- Issues found, along with fix recommendations



You can run health checks individually and in batches.

> **Note:**
>
> When running health checks in batches, select no more than 10 machines. Otherwise, the **Run Health Check** action is unavailable.

User access

June 11, 2024

There are two primary components that provide access to applications and desktops in Citrix DaaS deployments:

- **Citrix Workspace**: Citrix Workspace is a service managed by Citrix. This is the simplest way to provide access to DaaS resources, requiring no deployment effort and always kept up to date with the latest features.

- **On-premises StoreFront**: StoreFront is an on-premise product that you install in your own environment. This is recommended when you need to aggregate resources from DaaS and on-prem CVAD deployments or where you need more control of the deployment. You can deploy a Citrix Gateway to allow users to authenticate and connect to StoreFront from outside your internal network.

In either case, end-users access their workspaces or stores using Citrix Workspace app, either in a web browser or a locally installed app.

Using Citrix Workspace

Access to workspaces occurs through one or more URL `https://<subdomain>.cloud.com`, where you can choose `<subdomain>`. Alternatively you can register your own custom domain.

For more information about using Citrix Workspace, see:

- Configure workspaces: For configuring access and customizations.
- Secure workspaces: For configuring authentication.
- Manage your workspace experience: For understanding how end-users access their workspace and how it appears.

To provide remote access for to the resources managed by DaaS, you can use either Citrix Gateway service or your own Citrix Gateway.

- To use the Citrix Gateway service:
  1. In **Citrix Cloud > Resource Locations**, select **Gateway** for the resource location you want to use.
  2. Select **Gateway Service** and then click **Save**.
  3. In **Citrix Cloud > Workspace Configuration > Service Integrations**, locate the Gateway service and select **Enable** from the ellipsis menu.
- To use your own Citrix Gateway:
  1. Set up Citrix Gateway as an ICA Proxy (No authentication or session policies are needed).
  2. Configure a resource location to use Citrix Gateway:
     a) In **Citrix Cloud > Resource Locations**, select **Gateway** for the resource location you want to use.
     b) Select **Traditional Gateway** and enter the external FQDN. Do not add a protocol. Ports are optional. Combination remote and internal access is not supported in Citrix Workspace.
  3. Bind Citrix Cloud Connectors as Secure Ticket Authority (STA) servers to Citrix Gateway. For details, see CTX232640.

> **Note:**
>
> Only Citrix Cloud Connector machines are supported for use as STA servers with Citrix Gateway. Using other connectors as STA servers, such as Connector Appliance, isn't supported.

For more information about the Citrix Gateway service and Citrix Gateway, see Citrix Gateway.

Service continuity

Service continuity allows users to connect resources when Citrix Cloud is not available. For more information, see Service continuity.

Using on-premises StoreFront

StoreFront is a Windows application that you can install on your own servers to provide access to CVAD, DaaS and SPA resources. It connects to DaaS using Citrix Cloud Connectors that proxies the requests to Citrix Cloud. The connector encrypts passwords before they are sent to Citrix Cloud, using a key that is returned directly to Citrix Workspace app and never sent to the cloud.

1. Install the connectors. You should have at least two connectors in each location for redundancy.
2. Ensure the Cloud Connector can reach the Cloud NFuse/STA URL at (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` and `ctxsta.dll`).
3. Enable HTTPS on the connector to ensure data between StoreFront and the Cloud connector is encrypted, see How to Enable SSL on Cloud Connectors to Secure XML Traffic.
4. If you do not already have a StoreFront deployment, Install StoreFront and Create a deployment.
5. Add a resource feed to your StoreFront store. In the server list including all cloud connectors. Choose the HTTPS protocol.

End user access

To provide access to end-users using Citrix Workspace app, see User access options

Remote access using Citrix Gateway

You should not expose your StoreFront server directly to the internet. Instead provide authentication and remote access using Citrix Gateway. You can also use a Citrix Gateway for internal access to take advantage of its security features.

- Deploy a NetScaler Gateway appliance. See the NetScaler Gateway documentation for details.

- Configure the Gateway for remote access to your StoreFront store. For the STA servers, you can use the Cloud Connectors.
- Add the Citrix Gateway to StoreFront. Use the same list of STA servers you configured on your gateway.

Local Host Cache

Local Host Cache enables connection brokering operations in Citrix DaaS deployment to continue when Cloud Connectors cannot communicate with Citrix Cloud.

The Local Host Cache feature works only in resource locations containing a customer-deployed on-premises StoreFront. Local Host Cache is not supported for use with Citrix Workspace.

Each resource location must have a customer-deployed on-premises StoreFront. Verify that the resource location contains a local StoreFront that points to all the Cloud Connectors in that resource location.

For more information, see Local Host Cache.

Virtual IP and virtual loopback

March 23, 2022

> **Important:**
>
> Windows 10 Enterprise multi-session doesn't support Remote Desktop IP Virtualization (Virtual IP) and we don't support Virtual IP nor virtual loopback on Windows 10 Enterprise multi-session.

Virtual IP and virtual loopback features are supported on Windows Server 2016 machines. These features do not apply to Windows desktop OS machines.

The Microsoft virtual IP address feature provides a published application with a unique dynamically assigned IP address for each session. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a Citrix Virtual Apps environment, a unique IP address is required for each device.

Virtual IP and virtual loopback are independent features. You can use either or both.

Administrator action synopsis:

- To use Microsoft virtual IP, enable and configure it on the Windows server. (Citrix policy settings are not needed.)
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

Virtual IP

When virtual IP is enabled and configured on the Windows server, each configured application running in a session appears to have a unique address. Users access these applications on a Citrix Virtual Apps server in the same way they access any other published application. A process requires virtual IP in either of the following cases:

- The process uses a hard-coded TCP port number
- The process uses Windows sockets and requires a unique IP address or a specified TCP port number

To determine if an application needs to use virtual IP addresses:

1. Obtain the TCPView tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports.
2. Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
3. Launch the application and use TCPView to see which IP addresses and ports are opened by the application and which process names are opening these ports.
4. Configure any processes that open the IP address of the server, 0.0.0.0, or 127.0.0.1.
5. To ensure that an application does not open the same IP address on a different port, launch an additional instance of the application.

How Microsoft Remote Desktop (RD) IP virtualization works

- Virtual IP addressing must be enabled on the Microsoft server.

  For example, in a Windows Server 2016 environment, from Server Manager, expand **Remote Desktop Services > RD Session Host Connections** to enable the RD IP Virtualization feature and configure the settings to dynamically assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) server on a per-session or per-program basis. See the Microsoft documentation for instructions.

- After the feature is enabled, at session start-up, the server requests dynamically assigned IP addresses from the DHCP server.

- The RD IP Virtualization feature assigns IP addresses to remote desktop connections per-session or per-program. If you assign IP addresses for multiple programs, they share a per-session IP address.
- After an address is assigned to a session, the session uses the virtual address rather than the primary IP address for the system whenever the following calls are made: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

When using the Microsoft IP virtualization feature within the Remote Desktop session hosting configuration, applications are bound to specific IP addresses by inserting a "filter"component between the application and Winsock function calls. The application then sees only the IP address it should use. Any attempt by the application to listen for TCP or UDP communications is bound to its allocated virtual IP address (or loopback address) automatically, and any originating connections opened by the application originate from the IP address bound to the application.

In functions that return an address (such as `GetAddrInfo()`, which is controlled by a Windows policy), if the local host IP address is requested, virtual IP looks at the returned IP address and changes it to the virtual IP address of the session. Applications that attempt to get the IP address of the local server through such name functions see only the unique virtual IP address assigned to that session. This IP address is often used in subsequent socket calls, such as bind or connect. For more information about Windows policies, see RDS IP Virtualization in Windows Server.

Often, an application requests to bind to a port for listening on the address 0.0.0.0. When an application does this and uses a static port, you cannot launch more than one instance of the application. The virtual IP address feature also looks for 0.0.0.0 in these call types and changes the call to listen on the specific virtual IP address, which enables more than one application to listen on the same port on the same computer because they are all listening on different addresses. The call is changed only if it is in an ICA session and the virtual IP address feature is enabled. For example, if two instances of an application running in different sessions both try to bind to all interfaces (0.0.0.0) and a specific port (such as 9000), they are bound to VIPAddress1:9000 and VIPAddress2:9000 and there is no conflict.

Virtual loopback

Enabling the Citrix virtual IP loopback policy settings allows each session to have its own loopback address for communication. When an application uses the localhost address (default = 127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X, where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0), to the maximum of 127.255.255.255.

A process requires virtual loopback in either of the following cases:

- The process uses the Windows socket loopback (localhost) address (127.0.0.1)
- The process uses a hard-coded TCP port number

Use the virtual loopback policy settings for applications that use a loopback address for interprocess communication. No additional configuration is required. Virtual loopback has no dependency on Virtual IP, so you do not have to configure the Microsoft server.

- Virtual IP loopback support. When enabled, this policy setting allows each session to have its own virtual loopback address. This setting is disabled by default. The feature applies only to applications specified with the Virtual IP virtual loopback programs list policy setting.
- Virtual IP virtual loopback programs list. This policy setting specifies the applications that use the virtual IP loopback feature. This setting applies only when the Virtual IP loopback support policy setting is enabled.

Related feature

You can use the following registry settings to ensure that virtual loopback is given preference over virtual IP; this is called preferred loopback. However, proceed with caution:

- Use preferred loopback only if both Virtual IP and virtual loopback are enabled; otherwise, you may have unintended results.
- Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Run regedit on the servers where the applications reside.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Name: PreferLoopback, Type: REG_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <list of processes>

Zones

April 26, 2024

Introduction

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments that span widely dispersed locations connected by a WAN can face challenges from network latency and reliability.

Using zones can help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of the WAN. In Citrix DaaS environment, each resource location is considered a zone.

Zones can be helpful in deployments of all sizes. You can use zones to keep applications and desktops closer to users, which improves performance. Zones can be used for disaster recovery, geographically distant data centers, branch offices, a cloud, or an availability zone in a cloud.

Throughout this article, the term local refers to the zone being discussed. For example, "A VDA registers with a local Cloud Connector"means that a VDA registers with a Cloud Connector in the zone where the VDA is located.

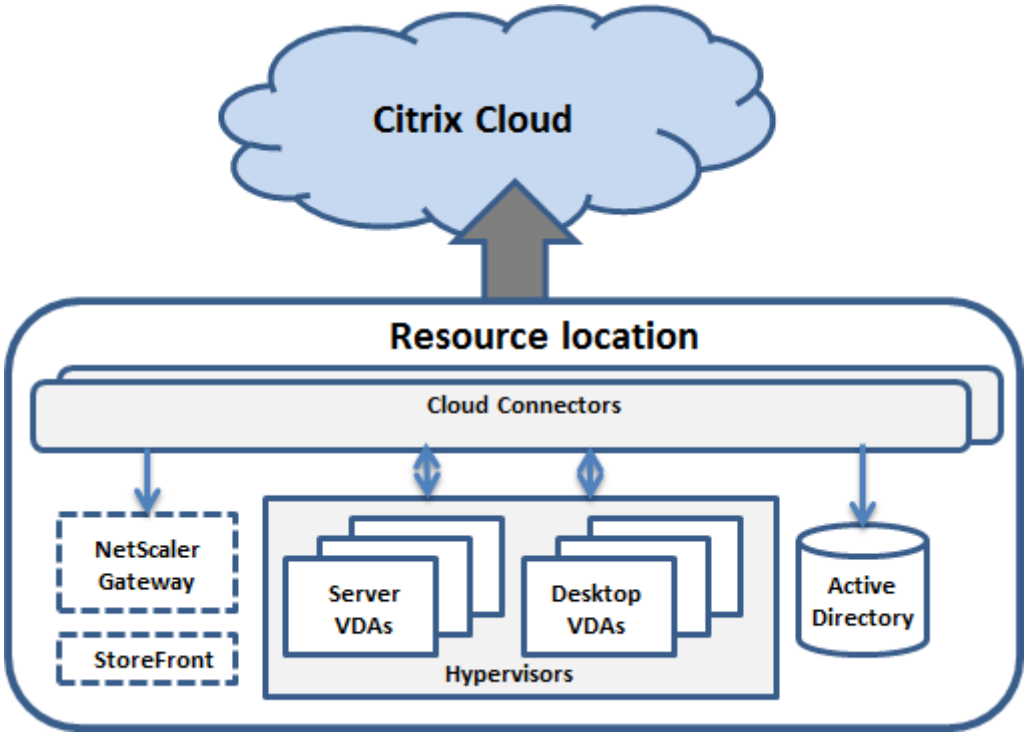
Differences from zones in on-premises Citrix Virtual Apps and Desktops environments

Zones in Citrix DaaS environment are similar, but not identical to zones in an on-premises Citrix Virtual Apps and Desktops deployment.

- In Citrix DaaS, zones are created automatically when you create a resource location and add a Cloud Connector to it. Unlike an on-premises deployment, Citrix DaaS environment does not classify zones as primary or satellite.
- In XenApp version 6.5 and earlier, zones included data collectors. Citrix DaaS does not use data collectors for zones. Also, failover and preferred zones work differently.

What's in a zone

A zone is equivalent to a resource location. When you create a resource location and install a Cloud Connector, a zone is automatically created for you. Each zone can have a different set of resources, based on your unique needs and environment.



Each zone must always have at least one Cloud Connector, and preferably two or more, for redundancy.

You can place machine catalogs, hypervisors, host connections, users, and applications in a zone. A zone can also contain Citrix Gateway and StoreFront servers. To use the Local Host Cache feature, a zone must have a StoreFront server.

Zones are supported with Citrix Workspace and the Citrix Gateway service.

Placing items in a zone affects how Citrix DaaS interacts with them and with other objects related to them.

- When a hypervisor connection is placed in a zone, it is assumed that all the hypervisors managed through that connection also reside in that zone.
- When a machine catalog is placed in a zone, it is assumed that all VDAs in the catalog are in the zone.
- Citrix Gateway instances can be added to zones. When you create a resource location, you are offered the option to add a Citrix Gateway. When a Citrix Gateway is associated with a zone, it is preferred for use when connections to VDAs in that zone are used.
- Ideally, Citrix Gateway in a zone is used for user connections coming into that zone from other zones or external locations. You can also use it for connections within the zone.
- After you create more resource locations and install Cloud Connectors in them (which automatically creates more zones), you can move resources between zones. This flexibility comes with the risk of separating items that work best in close proximity. For example, moving a catalog to a different zone than the connection (host) that creates the machines in the catalog, can affect

performance. So, consider potential unintended effects before moving items between zones. Keep a catalog and the host connection it uses in the same zone.

If the connection between a zone and Citrix Cloud fails, the Local Host Cache feature enables a Cloud Connector in the zone to continue brokering connections to VDAs in that zone. (The zone must have StoreFront installed.) For example, this is effective in an office where workers use the local StoreFront site to access their local resources, even if the WAN link connecting their office to the corporate network fails. For more information, see Local Host Cache.

Where VDAs register

VDAs must be minimum version 7.7 to use these zone registration features:

- A VDA in a zone registers with a local Cloud Connector.
  - As long as that Cloud Connector can communicate with Citrix Cloud, normal operations continue.
  - If that Cloud Connector is operational but cannot communicate with Citrix Cloud (and that zone has a local StoreFront), it enters Local Host Cache outage mode.
  - If a Cloud Connector fails, VDAs in that zone attempt to register with other local Cloud Connectors. A VDA in one zone never attempts to register with a Cloud Connector in another zone.
- If you add or remove a Cloud Connector in a zone (using the Citrix Cloud management console), and auto-update is enabled, VDAs in that zone receive updated lists of available local Cloud Connectors, so they know with whom they can register and accept connections from.
- If you move a machine catalog to another zone (using the Full Configuration management interface), the VDAs in that catalog re-register with Cloud Connectors in the zone where you moved the catalog. When you move a catalog, ensure you also move any associated host connection to the same zone.
- During an outage (when Cloud Connectors in a zone cannot communicate with Citrix Cloud), only the resources associated with machines that are registered in that zone are available.

Zone preference

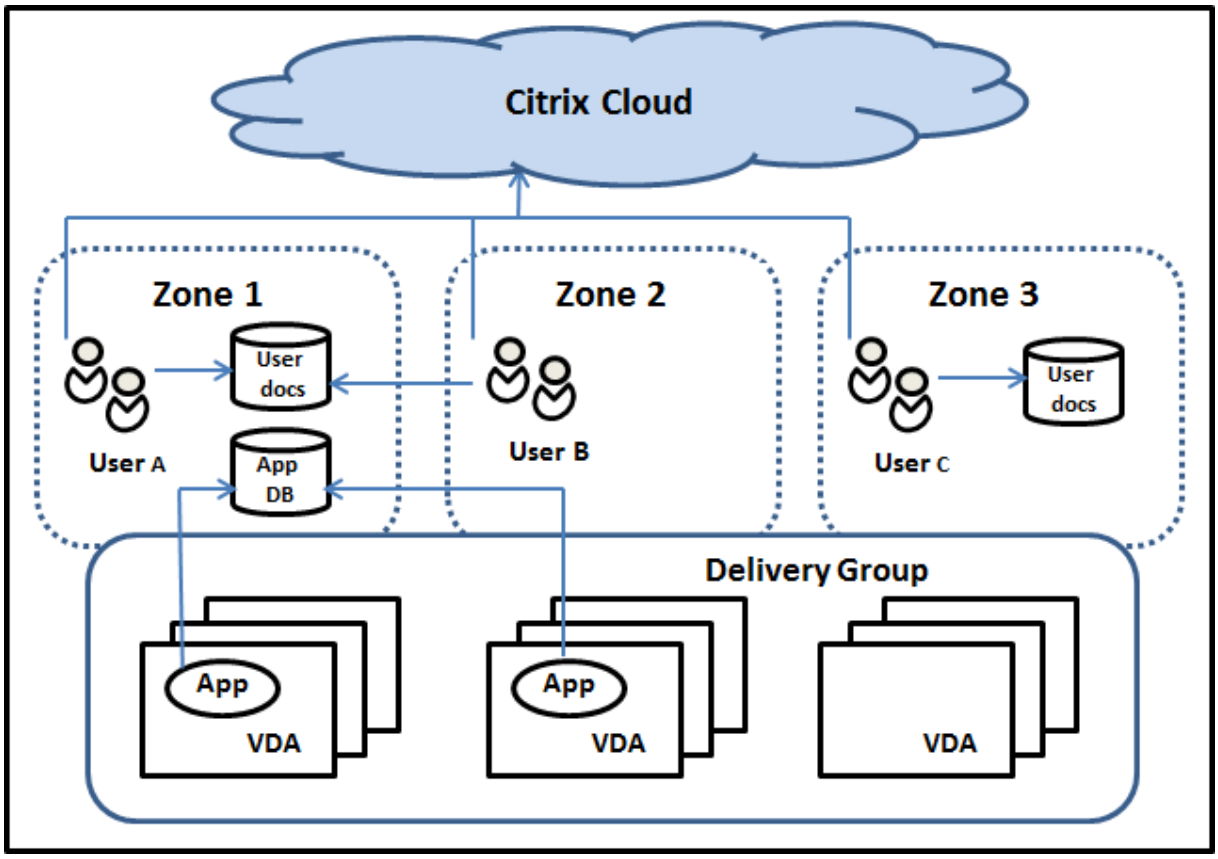
In a multi-zone Site, the zone preference feature offers the administrator more flexibility to control which VDA is used to launch an application or desktop.

How zone preference works

There are three forms of zone preference. You might prefer to use a VDA in a particular zone, based on:

- Where the application's data is stored. This is referred to as the application home.
- The location of the user's home data, such as a profile or home share. This is referred to as the user home.
- The user's current location (where the Citrix Workspace app is running). This is referred to as the user location. User location requires minimum StoreFront 3.7 and Citrix Gateway (formerly NetScaler Gateway) 11.0-65.x.

The following graphic shows an example multi-zone configuration.



In this example, VDAs are spread among three zones, but they are all in the same delivery group. Therefore, Citrix DaaS broker might have a choice which VDA to use for a user launch request. This example illustrates that users can be running their Citrix Workspace app endpoints at different locations. User A is using a device with Citrix Workspace app in zone 1. User B is using a device in zone 2. Similarly, a user's documents can be stored in different locations. Users A and B use a share located in zone 1. User C uses a share in zone 3. Also, one of the published applications uses a database located in zone 1.

You associate a user or application with a zone by configuring a home zone for the user or application. The broker then uses those associations to help select the zone where a session will be launched, if resources are available. You:

- Configure the home zone for a user by adding a user to a zone.

- Configure the home zone for an application by editing the application's properties.

A user or an application can have only one home zone at a time. (An exception for users can occur when multiple zone memberships occur because of user group membership. However, even in this case, the broker uses only one home zone.)

Although zone preferences for users and applications can be configured, the broker selects only one preferred zone for a launch. The default priority order for selecting the preferred zone is: application home > user home > user location. When a user launches an application:

- If that application has a configured zone association (an application home), then the preferred zone is the home zone for that application.
- If the application does not have a configured zone association, but the user does (a user home), then the preferred zone is the home zone for that user.
- If neither the application nor the user has a configured zone association, then the preferred zone is the zone where the user is running a Citrix Workspace app instance (the user location). If that zone is not defined, a random VDA and zone selection is used. Load balancing is applied to all VDAs in the preferred zone. If there is no preferred zone, load balancing is applied to all VDAs in the delivery group.

Tailoring zone preference

When you configure (or remove) a home zone for a user or an application, you can also further restrict how zone preference is (or is not) used.

- **Mandatory user home zone use:** In a delivery group, you can specify "Launch the session in the user's home zone (if the user has a home zone), with no failover to a different zone if resources are not available in the home zone."This restriction is helpful if you want to avoid the risk of copying large profiles or data files between zones. In other words, you would rather deny a session launch than launch the session in a different zone.
- **Mandatory application home zone use:** Similarly, when you configure a home zone for an application, you can specify "launch the application only in that zone, with no failover to a different zone if resources are not available in the application's home zone."
- **No application home zone, and ignore configured user home zone:** If you do not specify a home zone for an application, you can also specify "do not consider any configured user zones when launching that application."For example, use the user location zone preference if you want users to run a specific application on a VDA close to their machine, even though some users might have a different home zone.

How preferred zones affect session use

When a user launches an application or desktop, the broker prefers using the preferred zone rather than using an existing session.

If the user launching an application or desktop already has a session that is suitable for the resource being launched (for example, can use session sharing for an application, or a session already running the resource being launched), but that session is on a VDA in a zone other than the preferred zone for the user/application, then the system might create a new session. This action satisfies launching in the correct zone (if it has available capacity), ahead of reconnecting to a session in a less-preferred zone for that user's session requirements.

To prevent an orphan session that can no longer be reached, reconnection is allowed to existing disconnected sessions, even if they are in a non-preferred zone.

The order of desirability for sessions to satisfy a launch is:

1. Reconnect to an existing session in the preferred zone.
2. Reconnect to an existing disconnected session in a non-preferred zone.
3. Start a new session in the preferred zone.
4. Reconnect to a connected existing session in a non-preferred zone.
5. Start a new session in a non-preferred zone.

Other zone preference considerations

- If you configure a home zone for a user group (such as a security group), that group's users (through direct or indirect membership) are associated with the specified zone. However, a user can be a member of multiple security groups, and therefore might have a different home zone configured through other group membership. In such cases, determination of that user's home zone can be ambiguous.

  If a user has a configured home zone that was not acquired through group membership, that zone is used for zone preference. Any zone associations acquired through group membership are ignored.

  If the user has multiple different zone associations acquired solely through group membership, the broker chooses among the zones randomly. After the broker makes this choice, that zone is used for subsequent session launches, until the user's group membership changes.

- The user location zone preference requires detection of Citrix Workspace app on the endpoint device by the Citrix Gateway through which that device is connecting. The Citrix must be configured to associate ranges of IP addresses with particular zones. Discovered zone identity must be passed through StoreFront to Citrix DaaS.

Although written for on-premises use of zones, the Zone Preference Internals blog post contains relevant technical details.

Permissions to manage zones

A Full Administrator can perform all supported zone management tasks. Moving items between zones does not require zone-related permissions (except zone read permission). However, you must have edit permission for the items you are moving. For example, to move a machine catalog from one zone to another, you must have edit permission for that catalog.

If you use Citrix Provisioning: The current Citrix Provisioning console is not aware of zones, so Citrix recommends using the **Manage > Full Configuration** interface to create machine catalogs that you want to place in specific zones. After you create the catalog, you can use the Citrix Provisioning console to provision machines in that catalog.

Zone creation

When you create a resource location in Citrix Cloud and then add a Cloud Connector to that resource location, Citrix DaaS automatically creates and names a zone. You can optionally add a description later.

After you create more than one resource location (and the zones are created automatically), you can move resources from one zone to another.

Resource locations and zones are synchronized periodically, typically and approximately every five minutes. So, if you change a resource location's name in Citrix Cloud, that change is propagated to the associated zone within five minutes.

Add or change a zone description

Although you cannot change a zone's name, you can add or change its description.

1. From **Manage > Full Configuration**, select **Zones** in the left pane.
2. Select a zone in the middle pane and then select **Edit Zone** in the action bar.
3. Add or change the zone description.
4. Select **OK** or **Apply.**

Move resources from one zone to another zone

1. From **Manage > Full Configuration**, select **Zones** in the left pane.
2. Select a zone in the middle pane, and then select one or more items.

3. Either drag the items to the destination zone or select **Move Items** in the action bar, and then specify which zone to move them to. (Although you can select Cloud Connectors, you cannot actually move them to a different zone.)

A confirmation message lists the items you selected and asks if you are sure that you want to move all of them.

Remember: When a machine catalog uses a host connection to a hypervisor or cloud service, ensure that the catalog and the connection are in the same zone. Otherwise, performance can be affected. If you move one, move the other, too.

Zone deletion

You cannot delete a zone. However, you can delete a resource location (after removing its Cloud Connectors). Deleting the resource location automatically deletes the zone.

- If the zone does not contain any items (such as catalogs, connections, applications, or users), the zone is deleted during the next synchronization between zones and resource locations. Synchronization occurs every five minutes.
- If the zone contains items, the zone is automatically deleted after all items are removed.

Add a home zone for a user

Configuring a home zone for a user is also known as *adding a user to a zone*.

1. From **Manage > Full Configuration**, select **Zones** in the left pane.
2. Select a zone in the middle pane and then select **Add Users to Zone** in the action bar.
3. In the **Add Users to Zone** dialog box, select **Add**, and then select the users and user groups to add to the zone. If you specify users who already have a home zone, a message offers two choices: **Yes** = add only those users you specified who do not have a home zone; **No** = return to the user selection dialog.
4. Select **OK**.

For users with a configured home zone, you can require that sessions launch only from their home zone:

1. Create or edit a delivery group.
2. On the **Users** page, select the **Sessions must launch in a user's home zone, if configured** check box.

All sessions launched by a user in that delivery group must launch from machines in that user's home zone. If a user in the delivery group does not have a configured home zone, this setting has no effect.

Remove a home zone for a user

This procedure is also known as removing a user from a zone.

1. From **Manage > Full Configuration**, select **Zones** in the left pane.
2. Select a zone in the middle pane and then select **Remove Users from Zone** in the action bar.
3. In the **Add Users to Zone** dialog box, select **Remove**, and then select the users and groups to remove from the zone. This action removes the users only from the zone. Those users remain in the delivery groups to which they belong.
4. Confirm the removal when prompted.

Manage home zones for applications

Configuring a home zone for an application is also known as adding an application to a zone. By default, in a multi-zone environment, an application does not have a home zone.

An application's home zone is specified in the application's properties. You can configure application properties when you add the application to a group or later.

- When creating a delivery group or adding applications to existing groups, select **Properties** on the **Applications** page of the wizard.
- To change an application's properties after the application is added, select **Zones** in the left pane. Select an application and then select **Properties** in the action bar.

On the **Zones** page of the application's properties/settings:

- If you want the application to have a home zone:
  - Select the **Use the selected zone to decide** radio button and then select the zone.
  - If you want the application to launch only from the selected zone (and not from any other zone), select the check box under the zone selection.
- If you do not want the application to have a home zone:
  - Select the **Do not configure a home zone** radio button.
  - If you do not want the broker to consider any configured user zones when launching this application, select the check box under the radio button. In this case, neither application nor user home zones are used to determine where to launch this application.

Other actions that include specifying zones

If you have more than one zone, you can specify a zone when you add a host connection or create a catalog. Zones are listed alphabetically in selection lists. By default, the first alphabetical name is selected.

Troubleshooting

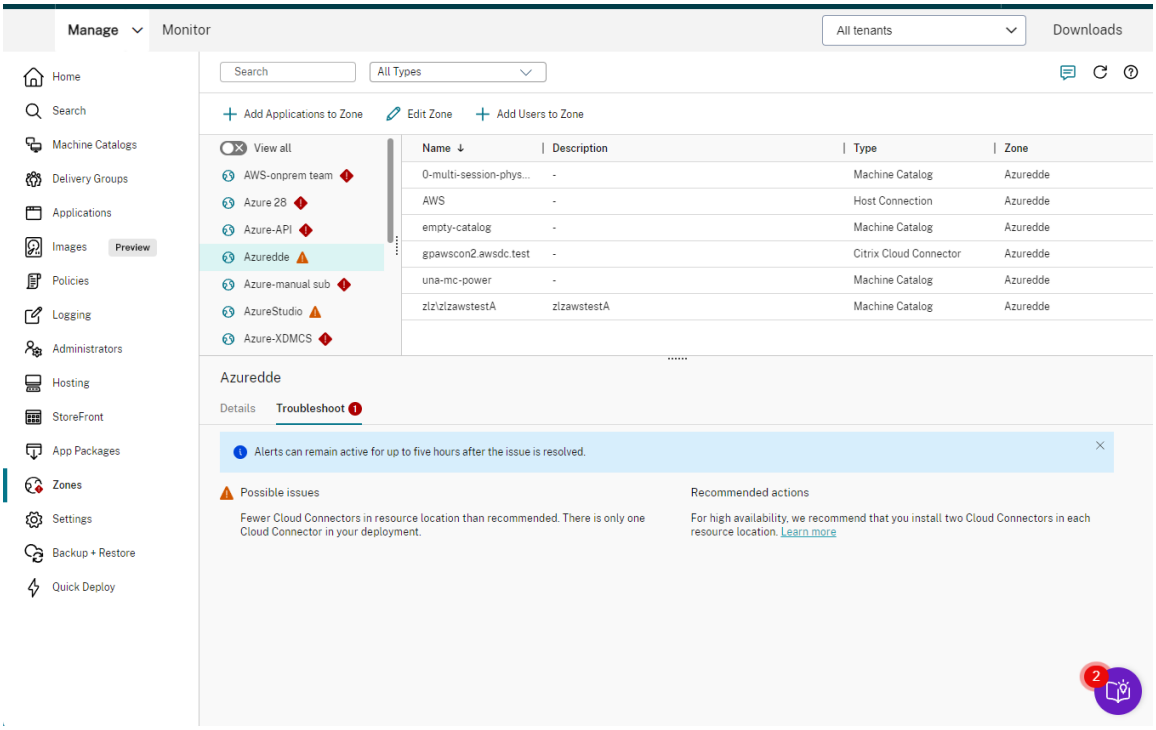
Full Configuration gives you proactive alerts to make sure that your Local Host Cache and zones are configured correctly so that you can resolve the issues in time before an outage impacts your users. This feature helps in maintaining continued user access to mission-critical workloads.

A **Troubleshoot** tab appears for each zone with issues.

To check zone-related issues, follow these steps:

1. Go to **Full Configuration > Zones** and click the zone with the warning icon.
2. Go to the **Troubleshoot** tab in the lower pane and read the information there.

> **Note:**
>
> Diagnostics are updated on an hourly basis.
>
> Troubleshooting information example:



The following table provides a complete list of zone-related warnings and errors:

Severity	Possible issues	Recommended actions
Warning	Resource location contains multiple domains. With multiple domains in a resource location, if the trust relationships are not configured properly, it might take longer for VDAs to register. Also, VDAs might fail to register in high-availability mode.	Ensure that trust relationships between domains in this resource location are configured properly. See Citrix Cloud Connector Technical Details.
Warning	More host connections in resource location than recommended. Exceeding the limit might result in performance degradation, thus affecting user experience.	Reduce the number of host connections in this resource location to no more than the recommended limit. See Limits.
Warning	Fewer logical CPU processors than recommended. In high-availability mode, there might be performance degradation.	Ensure that each Cloud Connector meets the minimum logical CPU processor requirements. See Local Host Cache.
Warning	Fewer Cloud Connectors in resource location than recommended. There is only one Cloud Connector in your deployment.	For high availability, we recommend that you install two Cloud Connectors in each resource location. See Citrix Cloud Connector Technical Details.
Warning	Less RAM than recommended on at least one Cloud Connector. In high-availability mode, there might be performance degradation.	Ensure that each Cloud Connector meets the minimum RAM requirements. See Size and scale considerations for Cloud Connectors.

Severity	Possible issues	Recommended actions
Error	More VDAs in resource location than recommended. In high-availability mode, Local Host Cache allows only 10,000 VDAs to register. Registration attempts by additional VDAs will fail.	Reduce the number of VDAs in this resource location to no more than the recommended limit. See Limits.
Error	Cloud Connectors in the zone are unreachable. None of the Cloud Connectors in the zone can be reached. VDAs in this resource location might be unavailable unless Local Host Cache or Service Continuity is configured for your deployment.	Review the connectivity of the Cloud Connectors in the zone and check the registry to verify whether LHC mode is forced via the registry. If the registry doesn't force LHC, consider running the Cloud Connector Connectivity Check Utility. If the issue persists, open a support ticket.

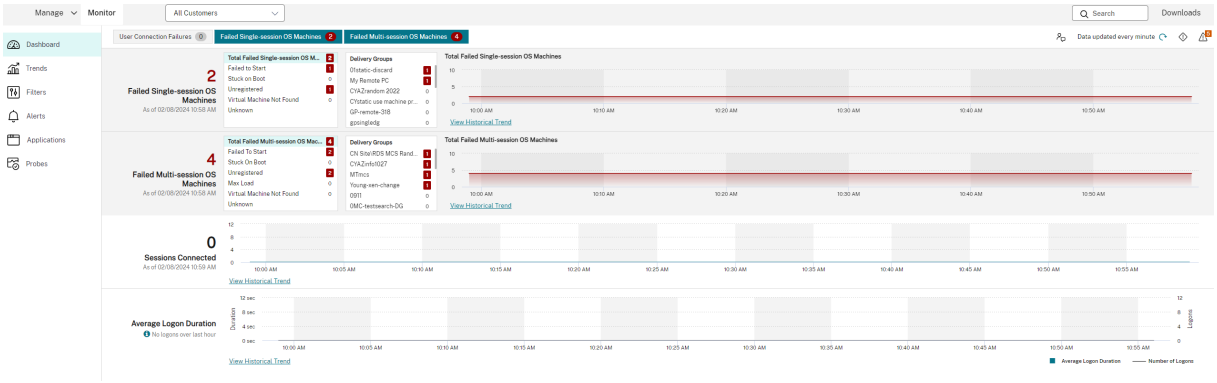
Monitor

February 8, 2024

Administrators and help-desk personnel can monitor Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) from **Monitor**, the monitoring and troubleshooting console. The **Monitor** tab displays a dashboard to monitor, troubleshoot, and perform support tasks for subscribers.

> **Note:**
>
> Monitor is available as the Director console to monitor and troubleshoot Citrix Virtual Apps and Desktops Current Release and LTSR deployments.

To access **Monitor**, sign in to Citrix Cloud. In the upper left menu, select **My Services > DaaS**. Click **Monitor**.



> **Note:**
>
> The recommended optimal screen resolution for viewing Citrix Monitor is 1440 x 1024.

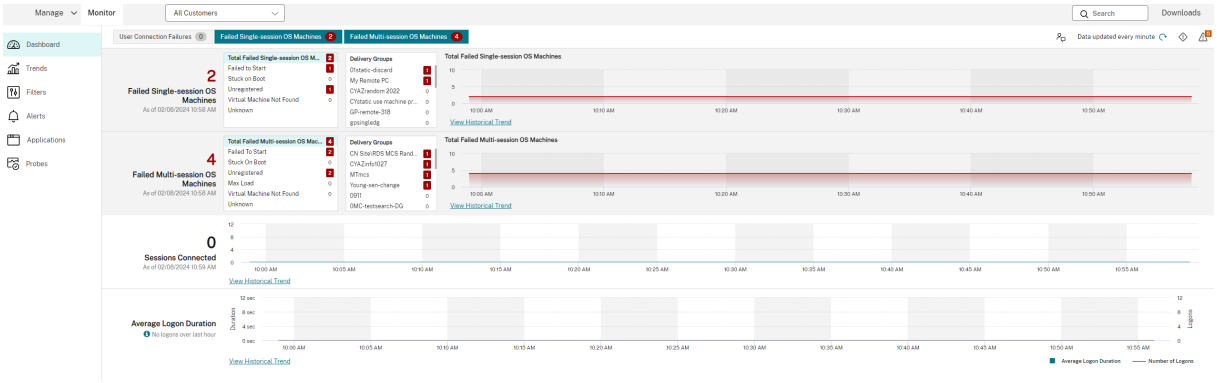
Monitor provides:

- Real-time data from the Broker Agent using a unified console integrated with Analytics and Performance Manager.
- Analytics includes performance management for health and capacity assurance, and historical trending to identify bottlenecks in your Citrix DaaS environment.
- Historical data stored in the Monitor database to access the Configuration Logging database.
- Gain visibility into the end-user experience for virtual applications, desktops, and users for Citrix DaaS.
- Monitor uses a troubleshooting dashboard that provides real-time and historical health monitoring of Citrix DaaS. This feature allows you to see failures in real time, providing a better idea of what the end users are experiencing.

Site Analytics

March 11, 2024

The Monitor dashboard provides a centralized location to monitor the health and usage of a site.



If there're currently no failures and no failures have occurred in the past 60 minutes, the panels stay collapsed. When there are failures, the specific failure panel automatically appears.

Panel	Description
User Connection Failures	Connection failures over the last 60 minutes. Click the categories next to the total number to view metrics for that type of failure. In the adjacent table, that number is further categorized based on each delivery group. Connection failures include failures caused by application limits being reached. For more information on application limits, see Applications.
Failed Single-session OS Machines or Failed Multi-session OS Machines	Total failures in the last 60 minutes categorized based on each delivery groups. Failures broken out by types, including failed to start, stuck on boot, and unregistered. For Multi-session OS machines, failures also include machines reaching maximum load.
Sessions Connected	Connected sessions across all delivery groups for the last 60 minutes.
Average Logon Duration	Log on data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Log on data for VDAs earlier than XenDesktop 7.0 isn't included in this average. For more information, see Diagnose user logon issues.

> **Note:**
>
> When the type of host you're using doesn't support any particular metric, there's no icon appears for that particular metric. For example, no health information is available for System Center Virtual Machine Manager (SCVMM) hosts, AWS and CloudStack.

Continue to troubleshoot issues using these options (which are documented in the preceding sections):

- Control user machine power
- Prevent connections to machines

Monitor sessions

If a session becomes disconnected, it's still active and its applications continue to run. However, the user device is no longer communicating with the server.

Action	Description
View a user's currently connected machine or session	From the Activity Manager and User Details views, view the user's currently connected machine or session. Also, view a list of all machines and sessions to which this user has access. To access this list, click the session switcher icon in the user title bar. For more information, see Restore sessions.
View the total number of connected sessions across all delivery groups	From the Dashboard, in the **Sessions Connected** pane, view the total number of connected sessions across all delivery groups for the last 60 minutes. Then click the large total number, which opens the Filters view. Here, you can display graphical session data based on selected delivery groups and ranges and usage across delivery groups.

Action	Description
End idle sessions	The Sessions Filters view displays data related to all active sessions. You can filter the sessions that are based on Associated User, delivery group, Session State, and Idle Time greater than a threshold time period. From the filtered list, select sessions to log off or disconnect. For more information, see Troubleshoot applications.
View data over a longer period	On the **Trends** view, select the **Sessions** tab to drill down to more specific usage data. You can drill down data for connected and disconnected sessions over a longer period. You can view session totals from earlier than the last 60 minutes. To view this information, click **View historical trends**.

> **Note:**
>
> Consider that a user device is running on a legacy Virtual Delivery Agent (VDA), such as a VDA earlier than version 7, or a Linux VDA. In this case, Monitor can't display complete information about the session. Instead, it displays a message that the information isn't available.

Desktop Assignment Rules limitation:

The Manage console allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the delivery group. StoreFront displays the assigned desktop with the corresponding **Display Name** as per the DAR for the logged in user. However, Monitor does not support DARs and displays the assigned desktop using the delivery group name regardless of the logged in user. As a result, you can't map a specific desktop to a machine in Monitor.

You can map the assigned desktop that is displayed in StoreFront to the delivery group name that is displayed in Monitor. For mapping, use the following PowerShell command:

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "\<Name on StoreFront\>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

Run the preceding PowerShell command using the Remote PowerShell SDK as described in the blog.

Disable the visibility of running applications in the Activity Manager

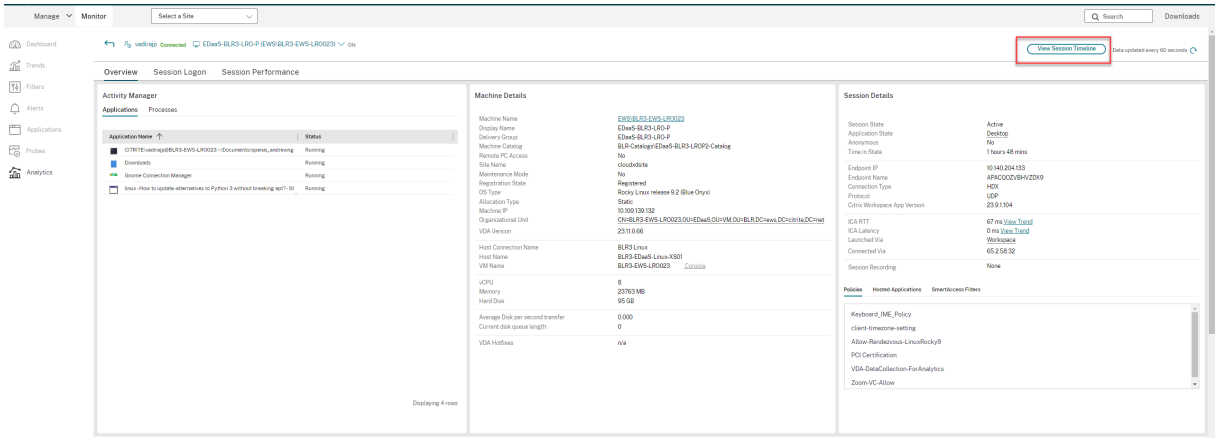
By default, the Activity Manager displays a list of all running applications for a user's session. All administrators who have access to the Activity Manager feature can view this information. For Delegated Administrator roles, this view includes Full Administrator, delivery group Administrator, and Help Desk Administrator.

To protect the privacy of users and the applications that they're running, you can disable the **Applications** tab to list running applications. To do this activity, on the VDA modify the registry key at HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information isn't collected from the VDA and as such not displayed in the Activity Manager.

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix can't guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

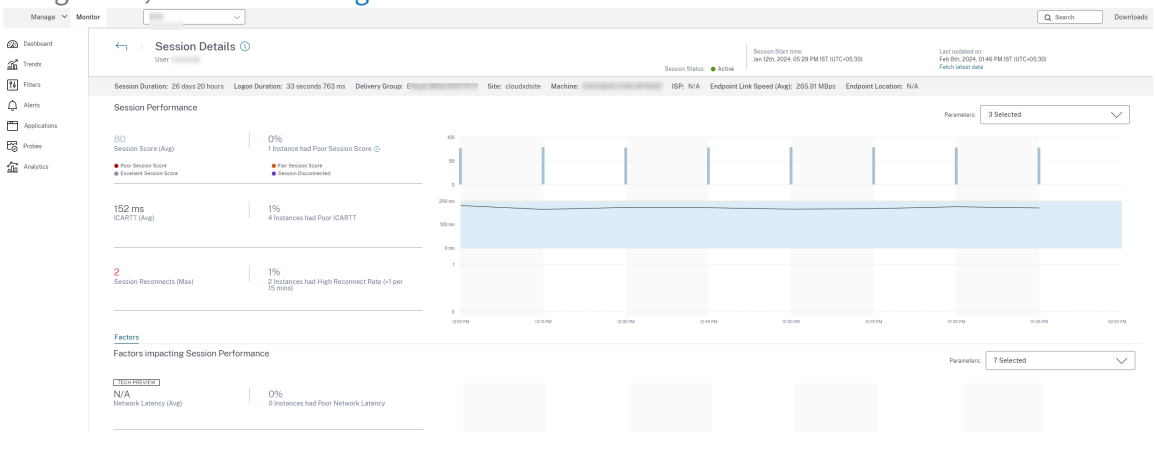
Access Citrix Analytics for Performance - Session Details

The Session Details page from Citrix Analytics for Performance can be accessed Monitor. Click **View Session Timeline** in the **Sessions Details** section of Activity Manager opens the Sessions Details page of Citrix Analytics for Performance within Monitor.



> **Note:**
>
> This feature requires you to have a valid Citrix Analytics for Performance entitlement.
>
> Session Details are available for sessions that are categorized as Excellent, Fair, or Poor Citrix Analytics for Performance. For more information about reasons why a session might not be

categorized, see the Not Categorized article.

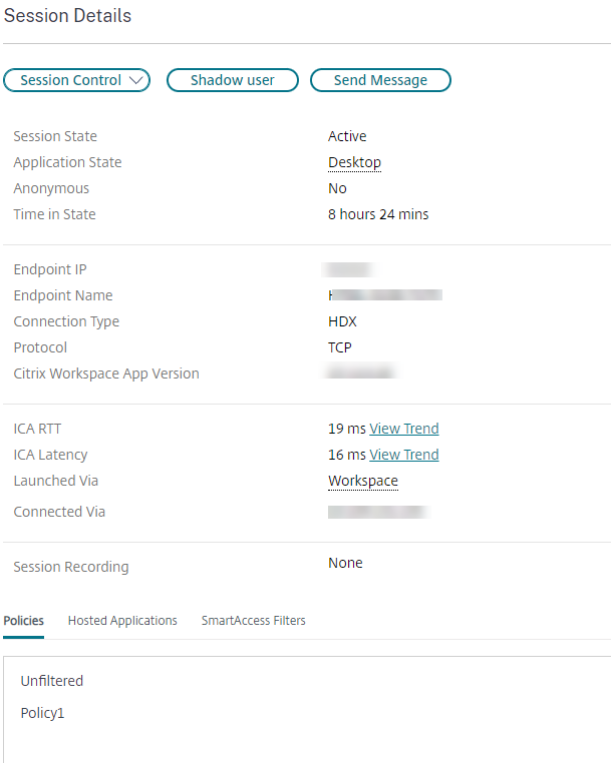


You can view a trend of the session experience for the session for up to the last three days. This trend view also includes the factors that contribute to the session experience. This information complements the live data available in Monitor, used by the help desk admin while troubleshooting issues related to session experience.

For more information about the Session Details page, see Session Details.

Session transport protocol

View the transport protocol in use for the HDX connection type for the current session in the **Session Details** panel. This information is available for sessions launched on VDAs Version 7.13 or later.



Use the **Session Control** drop-down menu in the **Session Details** pane to log off or disconnect a session.

- For **HDX** Connection type,
  - The Protocol is displayed as **UDP**, if EDT is used for the HDX connection.
  - The Protocol is displayed as **TCP**, if TCP is used for the HDX connection.
- For **RDP** Connection type, the Protocol is displayed as **n/a**.

When adaptive transport is configured, the session transport protocol dynamically switches between EDT (over UDP) and TCP, based on the network conditions. If the HDX session can't be established using EDT, it falls back to the TCP protocol.

For more information about adaptive transport configuration, see Adaptive Transport.

Export reports

You can export trends data to generate regular usage and capacity management reports. Export supports PDF, Excel, and CSV report formats. Reports in PDF and Excel formats inculde trends represented as graphs and tables. Reports in CSV-format contain tabular data that you can use to generate views or to archive.

To export a report:

1. Go to the **Trends** tab.
2. Set filter criteria and time period and click **Apply**. The trend graph and table are populated with data.
3. Click **Export** and enter the name and format of the report.

Monitor generates the report based on the filter criteria that you select. If you change the filter criteria, click **Apply** before you click **Export**.

> **Note:**
>
> Export of a large amount of data causes a significant increase in memory and CPU consumption on the Monitor server, the Delivery Controller, and the SQL servers. The supported number of concurrent export operations and the amount of data that can be exported is set to default limits to achieve optimal export performance.

Supported export limits

Exported PDF and Excel reports contain complete graphical charts for the selected filter criteria. However, tabular data in all report formats is truncated beyond the default limits on the number of rows or records in the table. The default number of records supported is defined based on the report format.

Report format	Default number of records supported
PDF	500
Excel	100,000
CSV	100,000 (10,000,000 in **Sessions** tab)

Error Handling

Errors that you might encounter during an Export operation:

- **Director has timed out:** This error can occur because of network issues or high resource usage on the Director server or with the Monitor Service.
- **Monitor has timed out:** This error can occur because of network issues or high resource usage with the Monitor Service or on the SQL server.
- **Max concurrent Export or Preview operations ongoing:** Only one instance of Export or Preview can run at a specific time. If you get the **Max concurrent Export or Preview operations ongoing** error, try the next operation again later.

Monitor hotfixes

To view the hotfixes installed on a specific machine VDA (physical or VM), choose the **Machine Details** view.

Control user machine power states

To control the state of the machines that you select in Monitor, use the Power Control options. These options are available for Single session OS machines, but might not be available for Multi-session OS machines.

> **Note:**
>
> This functionality isn't available for physical machines or machines using Remote PC Access.

Command	Function
Restart	Performs an orderly (soft) shutdown of the VM and all running processes are halted individually before restarting the VM. For example, select machines that appear in Monitor as "failed to start,"and use this command to restart them.
Force Restart	Restarts the VM without first doing any shut-down procedure. This command works in the same way as unplugging a physical server and then plugging it back in and turning it back on.
Shut Down	Performs an orderly (soft) shutdown of the VM. All running processes are halted individually.
Force Shutdown	Shuts down the VM without first doing any shut-down procedure. This command works in the same way as unplugging a physical server. It might not always shut down all running processes, and you risk losing data if you shut down a VM in this way.

Command	Function
Suspend	Suspends a running VM in its current state and stores that state in a file on the default storage repository. This option allows you to shut down the VM's host server and later, after rebooting it, resume the VM, returning it to its original running state.
Resume	Resumes a suspended VM and restores its original running state.
Start	Starts a VM when it is off (also called a cold start).

If power control actions fail, hover the mouse over the alert, and a pop-up message appears with details about the failure.

Prevent connections to machines

Use maintenance mode to prevent new connections temporarily while the appropriate administrator performs maintenance tasks on the image.

When you enable maintenance mode on machines, no new connections are allowed until you disable it. If users are currently logged on, maintenance mode takes effect when all users are logged off. For users who do not log off, send a message informing them that machines are shut down at a certain time. You can use the power controls to force the machines to shut down.

1. Select the machine, such as from the User Details view, or a group of machines in the Filters view.
2. Select **Maintenance Mode**, and turn on the option.

If a user tries to connect to an assigned desktop while it is in maintenance mode, a message appears to indicate that the desktop is unavailable. No new connections can be made until you disable maintenance mode.

Application Analytics

The **Applications** tab displays application-based analytics in a single, consolidated view to help analyze and manage application performance efficiently. You can gain valuable insight into the health and usage information of all applications published on the site. It shows metrics such as the following:

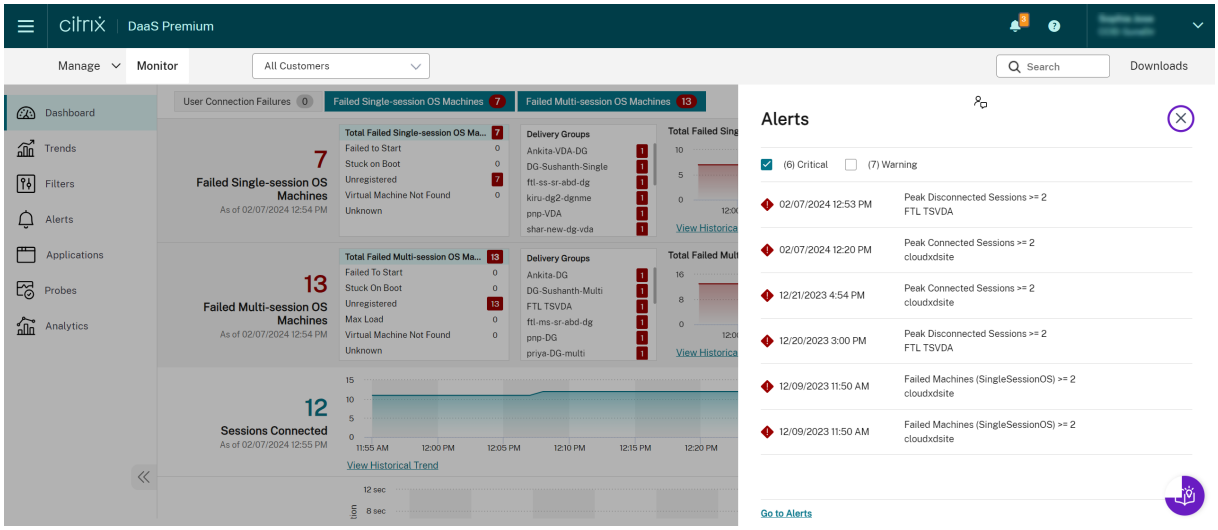
- Probe results
- Number of instances per application
- Faults and errors associated with the published applications

For more information, see the Application Analytics section in **Troubleshooting Applications**.

Alerts and notifications

July 2, 2024

Alerts are displayed in Monitor on the dashboard and other high level views with warning and critical alert symbols. Alerts update automatically every minute; you can also update alerts on demand.

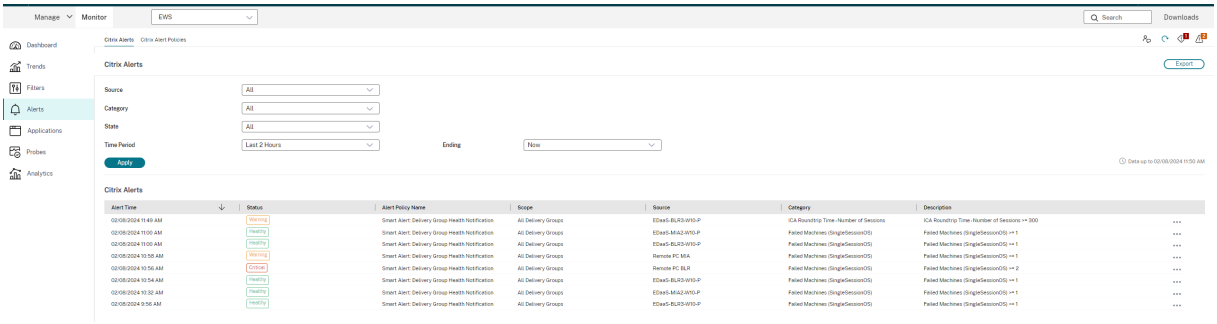


A warning alert (amber triangle) indicates that the warning threshold of a condition has been reached or exceeded.

A critical alert (red circle) shows that the critical threshold of a condition has been reached or exceeded.

You can view more detailed information on alerts by selecting an alert from the sidebar, clicking the **Go to Alerts** link at the bottom of the sidebar or by selecting **Alerts** from the top of the Monitor page.

In the Alerts view, you can filter and export alerts. For example, Failed Multi-session OS machines for a specific delivery group over the last month, or all alerts for a specific user. For more information, see Export reports.



Citrix alerts

Citrix alerts are the ones that originate from Citrix components. You can configure Citrix alerts within Monitor in **Alerts** > **Citrix Alerts Policy**. As part of the configuration, you can set notifications to be sent by email to individuals and groups when alerts exceed the thresholds you have set up. For more information on setting up Citrix Alerts, see Create alerts policies.

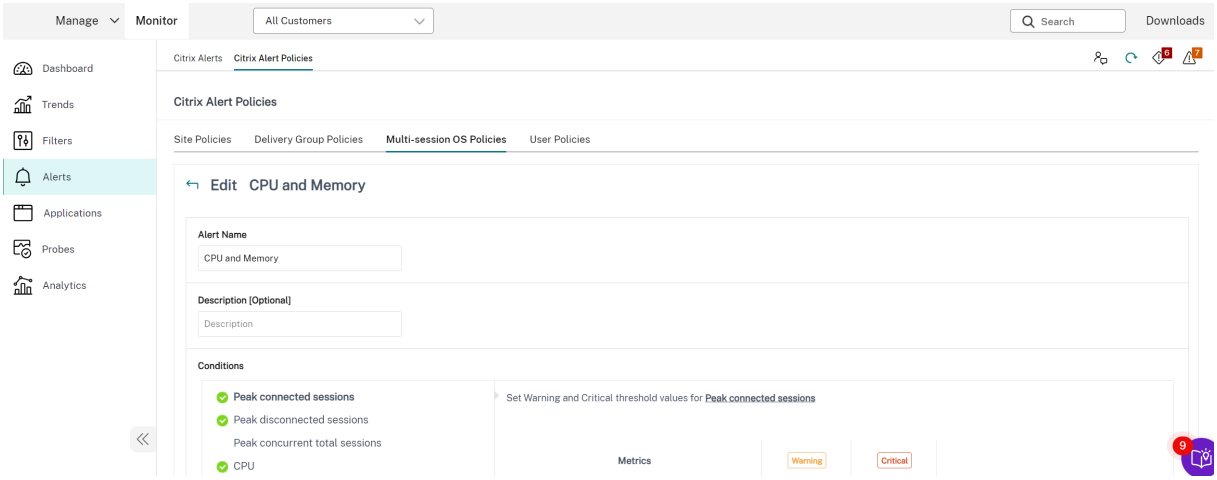
Smart alert policies

A set of built-in alert policies with predefined threshold values are available for delivery groups and Multi-session OS VDAs scope. You can modify the threshold parameters of the built-in alert policies in **Alerts** > **Citrix Alerts Policy**.

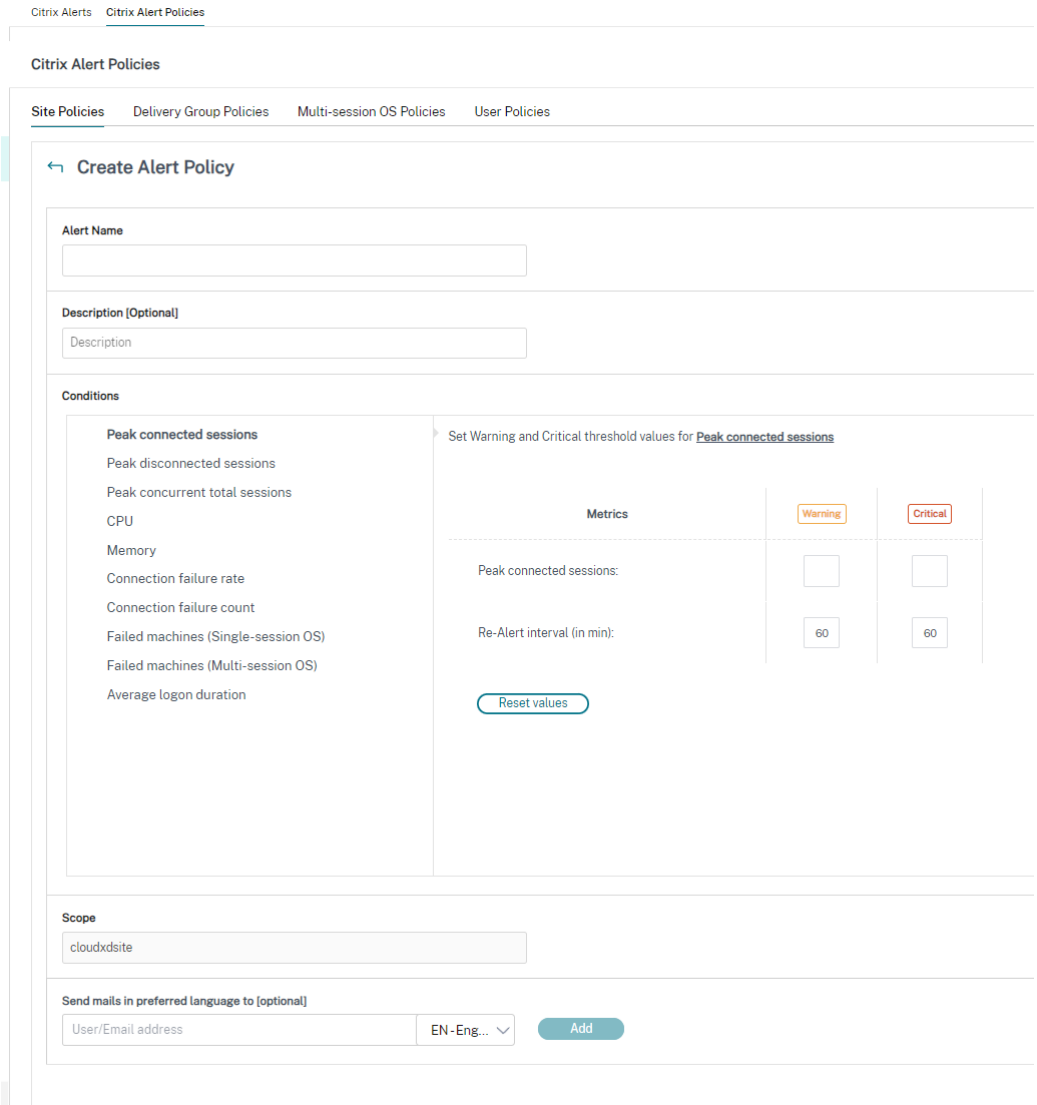
These policies are created when there is at least one alert target -a delivery group or a Multi-session OS VDA defined in your site. Additionally, these built-in alerts are automatically added to a new delivery group or a Multi-session OS VDA.

Built-in alert policies are created only if no corresponding alert rules exist in the Monitor database.

For the threshold values of the built-in alert policies, see the Alerts policies conditions section.



Create alerts policies



To create a new alerts policy, for example, to generate an alert when a specific set of session count criteria are met:

1. Go to **Alerts** > **Citrix Alerts Policy** and select, for example, Multi-session OS Policy.
2. Click **Create**.
3. Name and describe the policy, then set the conditions that have to be met for the alert to be triggered. For example, specify Warning and Critical counts for Peak Connected Sessions, Peak Disconnected Sessions, and Peak Concurrent Total Sessions. Warning values must not be greater than Critical values. For more information, see Alerts policies conditions.
4. Set the Re-alert interval. If the conditions for the alert are still met, the alert is triggered again at this time interval and, if set up in the alert policy, an email notification is generated. A dismissed alert does not generate an email notification at the re-alert interval.

5. Set the Scope. For example, set for a specific delivery group.
6. In Notification preferences, specify who should be notified by email when the alert is triggered. Email notifications are sent via SendGrid. Ensure that the email address `donotreplynotifications@citrix.com` is white-listed in your email setup.
7. Click **Save**.

Creating a policy with 20 or more delivery groups defined in the Scope might take approximately 30 seconds to complete the configuration. A spinner is displayed during this time.

Creating more than 50 policies for up to 20 unique delivery groups (1000 delivery group targets in total) might result in an increase in response time (over 5 seconds).

Moving a machine containing active sessions from one delivery group to another might trigger erroneous delivery group alerts that are defined using machine parameters.

> **Note:**
> After you delete an alert policy, it might take up to 30 minutes for the alert notifications generated by the policy to stop.

Alerts policies conditions

Find below the alert categories, recommended actions to mitigate the alert, and built-in policy conditions if defined. The built-in alert policies are defined for alert and realert intervals of 60 minutes.

Peak Connected Sessions

- Check Monitor Session Trends view for peak connected sessions.
- Check to ensure that there is enough capacity to accommodate the session load.
- Add new machines if needed

Peak Disconnected Sessions

- Check Monitor Session Trends view for peak disconnected sessions.
- Check to ensure that there is enough capacity to accommodate session load.
- Add new machines if needed.
- Log off disconnected sessions if needed

Peak Concurrent Total Sessions

- Check Monitor Session Trends view in Monitor for peak concurrent sessions.
- Check to ensure that there is enough capacity to accommodate session load.

- Add new machines if needed.
- Log off disconnected sessions if needed

CPU

Percentage of CPU usage indicates the overall CPU consumption on the VDA, including that of the processes. You can get more insight into the CPU utilization by individual processes from the **Machine details** page of the corresponding VDA.

- Go to **Machine Details > View Historical Utilization > Top 10 Processes**, identify the processes consuming CPU. Ensure that process monitoring policy is enabled to initiate collection of process level resource usage statistics.
- End the process if necessary.
- Ending the process causes unsaved data to be lost.
- If all is working as expected, add additional CPU resources in the future.

> **Note:**
>
> The policy setting, **Enable resource monitoring** is allowed by default for the monitoring of CPU and memory performance counters on machines with VDAs. If this policy setting is disabled, alerts with CPU and memory conditions are not triggered. For more information, see Monitoring policy settings.

Smart policy conditions:

- **Scope:** Delivery group, Multi-session OS scope
- **Threshold values:** Warning - 80%, Critical - 90%

Memory

Percentage of Memory usage indicates the overall memory consumption on the VDA, including that of the processes. You can get more insight into the memory usage by individual processes from the **Machine details** page of the corresponding VDA.

- Go to **Machine Details > View Historical Utilization > Top 10 Processes**, identify the processes consuming memory. Ensure that process monitoring policy is enabled to initiate collection of process level resource usage statistics.
- End the process if necessary.
- Ending the process causes unsaved data to be lost.
- If all is working as expected, add additional memory in the future.

> **Note:**
>
> The policy setting, **Enable resource monitoring**, is allowed by default for the monitoring of CPU and memory performance counters on machines with VDAs. If this policy setting is disabled, alerts with CPU and memory conditions are not triggered. For more information, see Monitoring policy settings.

Smart policy conditions:

- **Scope:** Delivery group, Multi-session OS scope
- **Threshold values:** Warning - 80%, Critical - 90%

Connection Failure Rate

Percentage of connection failures over the last hour.

- Calculated based on the total failures to total connections attempted.
- Check Monitor Connection Failures Trends view for events logged from the Configuration log.
- Determine if applications or desktops are reachable.

Connection Failure Count

Number of connection failures over the last hour.

- Check Monitor Connection Failures Trends view for events logged from the Configuration log.
- Determine if applications or desktops are reachable.

ICA RTT (Average)

Average ICA round-trip time.

- Check Citrix ADM for a breakdown of the ICA RTT to determine the root cause. For more information, see Citrix ADM documentation.
- If Citrix ADM is not available, check the Monitor User Details view for the ICA RTT and Latency, and determine if it is a network problem or an issue with applications or desktops.

ICA RTT (No. of Sessions)

Number of sessions that exceed the threshold ICA round-trip time.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see Citrix ADM documentation.

- If Citrix ADM is not available, contact the network team to determine the root cause.

  Smart policy conditions:

  - **Scope:** Delivery group, Multi-session OS scope
  - **Threshold values:** Warning - 300 ms for 5 or more sessions, Critical - 400 ms for 10 or more sessions

ICA RTT (% of Sessions)

Percentage of sessions that exceed the average ICA round-trip time.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see Citrix ADM documentation.
- If Citrix ADM is not available, contact the network team to determine the root cause.

ICA RTT (User)

ICA round-trip time that is applied to sessions launched by the specified user. The alert is triggered if ICA RTT is greater than the threshold in at least one session.

Failed Machines (Single session OS)

Number of failed Single session OS machines. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause. For more information, see Troubleshoot user issues.

  Smart policy conditions:

  - **Scope:** Delivery group scope
  - **Threshold values:** Warning - 1, Critical - 2

Failed Machines (Multi-session OS)

Number of failed Multi-session OS machines. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause.

  Smart policy conditions:

  - **Scope:** Delivery group, Multi-session OS scope
  - **Threshold values:** Warning - 1, Critical - 2

Failed Machines (in %)

Percentage of failed single-session and multi-session OS machines in a delivery group calculated based on the number of failed machines. This alert condition allows you to configure alert thresholds as a percentage of failed machines in a delivery group and is calculated every 30 seconds.
Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views. Run Citrix Scout diagnostics to determine the root cause. For more information, see Troubleshoot user issues.

Unregistered machines (in %)

A machine is considered unregistered, when a machine becomes unstable due to a restart or when there is a communication problem between the delivery controller and the virtual machines. The **Unregistered machines (in %)** is the percentage of unregistered single-session and multi-session OS machines in a delivery group calculated based on the number of unregistered machines. This alert condition allows you to configure warning and critical threshold values as a percentage of unregistered machines in a delivery group. You can set an interval for re-alert. You can also add an email to get a notification when the conditions are met for **Unregistered Machines (in %)**. When the critical or warning threshold value is exceeded, alerts and emails are generated. You can view alerts under **Citrix Alerts**. You can filter it by **Unregistered Machines (in %)** category and for the required state and time.

> **Note:**
>
> The critical value must be greater than the warning value.

Policy conditions:

- **Scope**: Single session OS, and Multi-session OS Delivery group
- **Threshold values**: Warning and Critical

Machine uptime alert

Machine uptime in a delivery group is calculated based on the number of hours per day, hours per week, or hours per month for a machine that is turned on in a delivery group. This alert condition allows you to configure alert thresholds as the hours a machine is turned on in a delivery group. The machine uptime alerts works as follows in case of:

- Hours per day - You can specify the number of hours a machine is turned on for a day and is calculated every 30 minutes. The maximum number of hours per day that you can set is 24 hours.

- Hours per week - You can specify the number of hours a machine is turned on for a week and is calculated every six hours. The maximum number of hours per week that you can set is 168 hours.
- Hours per month - You can specify the number of hours a machine is turned on for a month and is calculated once every day. The maximum number of hours per month is 720 hours.
  The minimum re-alert interval value that you can set is 60 minutes. You can enter the number of machines that cross the machine uptime threshold value under the Warning and Critical alerts section. You can also add exceptions for any machines.

For example, if there are five delivery groups added for this alert and if in the first delivery group and fourth delivery group, the number of machines crosses the warning or critical threshold values, the alert is triggered separately for the first delivery group and for the fourth delivery group.

This alert helps the admins to analyze the uptime of the machines and based on this analysis the admins can help in optimizing the cost. You can also receive alert details in a CSV attachment in case of email or through a JSON payload in case of a webhook.

Average Logon Duration

Average logon duration for logons that occurred over the last hour.

- Check the Monitor Dashboard to get up-to-date metrics regarding the logon duration. A large number of users logging in during a short timeframe can increase the logon duration.
- Check the baseline and break down of the logons to narrow down the cause. For more information, see Diagnose user logon issues.

  Smart policy conditions:

  - **Scope:** Delivery group, Multi-session OS scope
  - **Threshold values:** Warning - 45 seconds, Critical - 60 seconds

Logon Duration (User)

Logon duration for logons for the specified user that occurred over the last hour.

Load Evaluator Index

Value of the Load Evaluator Index over the last 5 minutes.

- Check Monitor for Multi-session OS Machines that might have a peak load (Max load). View both Dashboard (failures) and Trends Load Evaluator Index report.

  Smart policy conditions:

- **Scope:** Delivery group, Multi-session OS scope
- **Threshold values:** Warning - 80%, Critical - 90%

Configure alerts policies with webhooks

Apart from email notifications, you can configure alerts policies with webhooks.

Note: This feature requires Delivery Controller(s) version 7.11 or later.

You can configure an alert policy with an HTTP callback or an HTTP POST using PowerShell cmdlets. They are extended to support webhooks.

For information on the creation of a new Octoblu workflow and obtaining the corresponding webhook URL, see the Octoblu Developer Hub.

To configure a webhook URL for a new alert policy or for an existing policy, use the following PowerShell cmdlets.

Create a new alerts policy with a webhook URL:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    Description <Policy description> -Enabled $true -Webhook <Webhook
    URL>
<!--NeedCopy-->
```

Add a webhook URL to an existing alerts policy:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
<!--NeedCopy-->
```

For help on the PowerShell commands, use the PowerShell help, for example:

```
Get-Help  <Set-MonitorNotificationPolicy>
<!--NeedCopy-->
```

Notifications generated from the alert policy trigger the webhook with a POST call to the webhook URL. The POST message contains the notification information in JSON format:

```
{
 "NotificationId" : \<Notification Id\>,

"Target" : \<Notification Target Id\>,

"Condition" : \<Condition that was violated\>,

"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,
```



```
13
14 "Description": \<Description of the Alert policy\>,
15
16 "Scope" : \<Scope of the Alert policy\>,
17
18 "NotificationState": \<Notification state critical, warning, healthy or
       dismissed\>,
19
20 "Site" : \<Site name\> }
21
22 <!--NeedCopy-->
```

Hypervisor Alerts Monitoring

Monitor displays alerts to monitor hypervisor health. Alerts from Citrix Hypervisor and VMware vSphere help monitor hypervisor parameters and states. The connection status to the hypervisor is also monitored to provide an alert if the cluster or pool of hosts is rebooted or unavailable.

To receive hypervisor alerts, ensure that a hosting connection is created in the Manage tab. For more information, see Connections and resources. Only these connections are monitored for hypervisor alerts. The following table describes the various parameters and states of Hypervisor alerts.

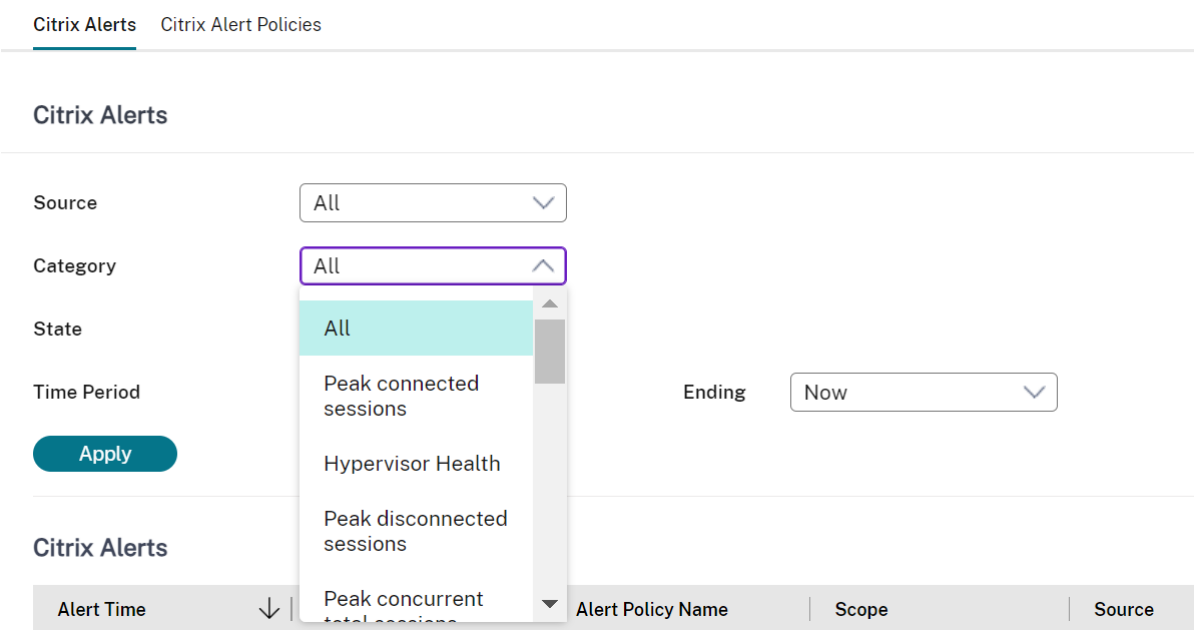
Alert	Supported Hypervisors	Triggered by	Condition	Configuration
CPU usage	Citrix Hypervisor, VMware vSphere	Hypervisor	CPU usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Memory usage	Citrix Hypervisor, VMware vSphere	Hypervisor	Memory usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Network usage	Citrix Hypervisor, VMware vSphere	Hypervisor	Network usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Disk usage	VMware vSphere	Hypervisor	Disk usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.

Alert	Supported Hypervisors	Triggered by	Condition	Configuration
Host connection or power state	VMware vSphere	Hypervisor	Hypervisor Host has been rebooted or is unavailable	Alerts are prebuilt in VMware vSphere. No additional configurations are needed.
Hypervisor connection unavailable	Citrix Hypervisor, VMware vSphere	Delivery Controller	Connection to the hypervisor (pool or cluster) is lost or powered down or rebooted. This alert is generated every hour as long as the connection is unavailable.	Alerts are prebuilt with the Delivery Controller. No additional configurations are needed.

> **Note:**
>
> For more information about configuring alerts, see Citrix XenCenter Alerts or check the VMware vCenter Alerts documentation.

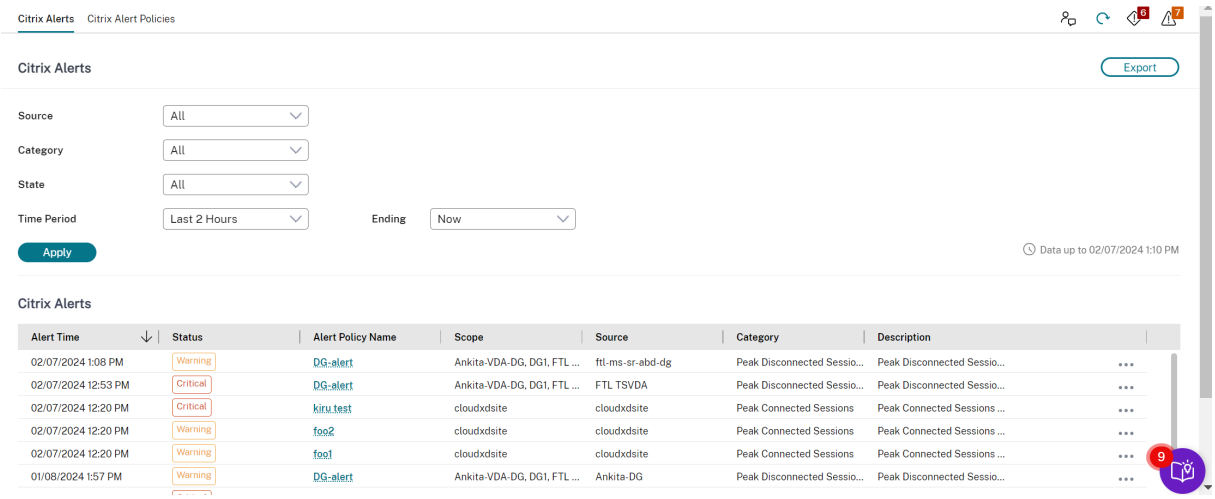
Email notification preference can be configured under **Citrix Alerts Policy > Site Policy > Hypervisor Health**. The threshold conditions for Hypervisor alert policies can be configured, edited, disabled, or deleted from the hypervisor only and not from Monitor. However, modifying email preferences and dismissing an alert can be done in Monitor.

> **Important:**
>
> - All hypervisor alerts older than a day are automatically dismissed.
> - Alerts triggered by the Hypervisor are fetched and displayed in Monitor. However, changes in the life cycle/state of the Hypervisor alerts are not reflected in Monitor.
> - Alerts that are healthy or dismissed or disabled in the Hypervisor console will continue to appear in Monitor and have to be dismissed explicitly.
> - Alerts that are dismissed in Monitor are not dismissed automatically in the Hypervisor console.



A new Alert category called **Hypervisor Health** has been added to enable filtering only the hypervisor alerts. These alerts are displayed once the thresholds are reached or exceeded. Hypervisor alerts can be:

- Critical—critical threshold of the hypervisor alarm policy reached or exceeded
- Warning—warning threshold of the hypervisor alarm policy reached or exceeded
- Dismissed—alert no longer displayed as an active alert

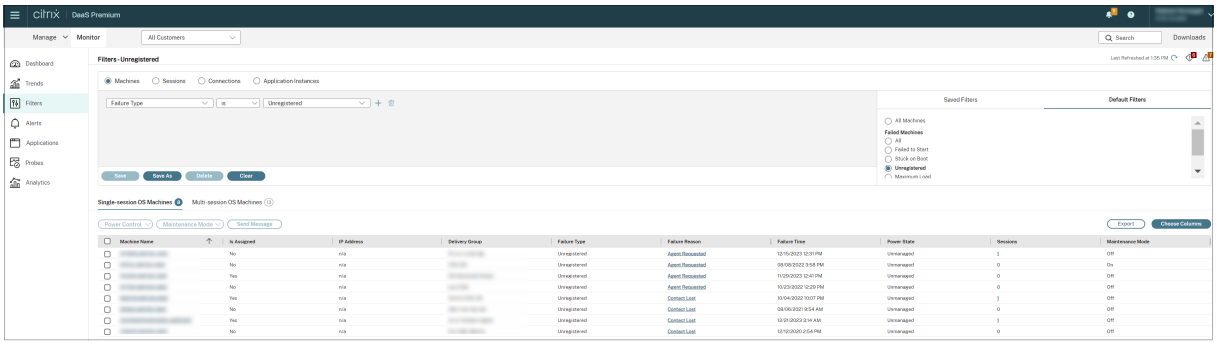


Filter data to troubleshoot failures

July 26, 2023

When you click numbers on the Dashboard or select a predefined Default filter from the **Filters** tab, the Filters view opens to display data based on the selected machine or failure type.

You can create custom-filtered views of machines, connections, sessions, and application instances across all delivery groups and save the search for later access. You can edit a predefined filter and save it as a Saved filter.



1. Select a view:
    - **Machines**. Select Single session OS Machines or Multi-session OS Machines. These views show the number of configured machines. The Multi-session OS Machines tab also includes the load evaluator index, which indicates the distribution of performance counters and tool tips of the session count if you hover over the link.
    - **Sessions**. You can also see the session count from the Sessions view. Use the idle time measurements to identify sessions that are idle beyond a threshold time period. Click the **Associated User** to open the Activity Manager for the user. Clicking the **Endpoint** name opens the Activity Manager for the Endpoint. Clicking **View Details** opens the **User Details** or **Endpoint Details** page respectively. For more information, see User Details.
    - **Connections**. Filter connections by different time periods, including last 60 minutes, last 24 hours, or last 7 days.
    - **Application Instances**. This view displays the properties of all application instances on VDAs of Multi-session and Single session OS. The session idle time measurements are available for Application instances on VDAs of Multi-session OS.
2. Select a filter from the list of Saved or Default filters.
3. Use the drop-down lists to select further filter criteria.
4. Select extra columns, as needed, to troubleshoot further.
5. Save and name your filter.
6. To open the filter later, from the Filters view, select View (Machines, Sessions, Connections, or Application Instances), and select the saved filter.
7. Click **Export** to export the data to CSV format files. Data of up to 100,000 records can be exported.

8. If needed, for **Machines** or **Connections** views, use power controls for all the machines you select in the filtered list. For the Sessions view, use the session controls or option to send messages.
9. In the **Machines** and **Connections** views, click the **Failure Reason** of a failed machine or connection to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended actions for Machine and Connection failures are available in the Citrix Director Failure Reasons Troubleshooting Guide.
10. In the **Machines** view, click a machine name link to go to the corresponding **Machine Details** page. This page displays the details of the machine, provides power controls, displays the CPU, memory, disk monitoring, and GPU monitoring graphs. Also, click **View Historical Utilization** to see the resource utilization trends for the machine. For more information, see Troubleshoot machines.
11. In the **Application Instances** view, sort or filter based on **Idle Time** greater than a threshold time period. Select the idle application instances to end. Log off or Disconnect of an application instance ends all active application instances in the same session. For more information, see Troubleshoot applications. The Application Instances filter page and idle time measurements in the Sessions filter pages are available if VDAs are version 7.13 or later.

> **Note:**
>
> The Manage console allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the delivery group. StoreFront displays the assigned desktop with the corresponding Display Name as per the DAR for the logged in user. However, Monitor does not support DARs and displays the assigned desktop using the delivery group name regardless of the logged in user. As a result, you cannot map a specific desktop to a machine in Monitor. To map the assigned desktop displayed in StoreFront to the delivery group name displayed in Monitor, use the following PowerShell command. Run the PowerShell command using Remote PowerShell SDK as described in the blog.

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "\<Name on StoreFront\>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

Monitor historical trends across a site

July 1, 2024

The Trends view accesses historical trend information of each site for the following parameters:

- sessions
- connection failures
- machine failures
- logon performance
- load evaluation
- capacity management
- machine usage
- resource utilization

To locate this information, click the **Trends** menu.

The zoom-in drill down feature lets you navigate through trend charts by zooming in on a time period (clicking a data point in the graph) and drilling down to see the details associated with the trend. This feature enables you to better understand the details of who or what has been affected by the trends being displayed.

To change the default scope of each graph, apply a different filter to the data.

> **Note:**
>
> - Sessions, failures, and logon performance trend information are available as graphs and tables when the time period is set to Last month (**Ending now**) or shorter. When the time period is chosen as Last month with a custom ending date or as Last year, the trend information is available as graphs but not as tables.
> - Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) supports historical data retention only for 90 days. Hence, one-year trends and reports in Monitor show the last 90 days of data.

Available trends

View trends for sessions: From the Sessions tab, select the delivery group and time period to view more detailed information about the concurrent session count.

The **Session Auto Reconnect** column displays the number of auto reconnects in a session. Auto reconnect is enabled when the Session Reliability or the Auto Client Reconnect policies are in effect. When there is a network interruption on the endpoint, the following policies come into effect:

- Session reliability comes into effect (by default for 3 minutes) where the Citrix Receiver or Citrix Workspace app tries to connect to the VDA.
- Auto client reconnect comes into effect between 3 and 5 minutes where the client tries to connect to the VDA.

Both these reconnects are captured and displayed to the user. This information can take a maximum time of 5 minutes to appear on the Monitor UI after the reconnect occurs.

The auto reconnect information helps you view and troubleshoot network connections having interruptions, and to analyze networks having a seamless experience. You can view the number of reconnects for a specific delivery group or time period selected in the Filters.

A drilldown provides additional information like Session Reliability or Auto Client Reconnect, time stamps, Endpoint IP, and Endpoint Name of the machine where the Workspace app is installed.

By default, logs are sorted by the event time stamps in descending order. This feature is available for Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Receiver for Windows, and Citrix Receiver for Mac. This feature requires VDAs 1906 or later.

For more information about session reconnections, see Sessions. For more information about policies, see Auto client reconnect policy settings and Session reliability policy settings.

Sometimes, the auto reconnect data might not appear in Monitor for the following reasons:

- Workspace app is not sending auto reconnect data to VDA.
- VDA is not sending data to the Monitor service.

> **Note:**
>
> Sometimes, the client IP address might not be obtained correctly if certain Citrix Gateway policies are set.

View trends for connection failures: From the Failures tab, select the connection, machine type, failure type, delivery group, and time period to view a graph containing more detailed information about the user connection failures across your site.

View trends for machine failures: From the Single session OS Machine Failures tab or Multi-session OS Machines tab, select the failure type, delivery group, and time period to view a graph containing more detailed information about the machine failures across your site.

View trends for logon performance: From the Logon Performance tab, select the delivery group and time period to view a graph containing more detailed information about the duration of user logon times across your site and whether the number of logons affects the performance. This view also shows the average duration of the logon phases, such as brokering duration and VM start time. This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions. The table below the graph shows Logon Duration by User Session. You can choose the columns to display and sort the report by any of the columns. You can also export these reports to a .CSV file. For more information, see Diagnose user logon issues.

View trends for load evaluation: From the Load Evaluator Index tab, view a graph containing more detailed information about the load that is distributed among Multi-session OS machines. The filter

options for this graph include the delivery group or Multi-session OS machine in a delivery group, Multi-session OS machine (available only if a Multi-session OS machine in a delivery group was selected), and range. The Load Evaluator Index is displayed as percentages of Total CPU, Memory, Disk or Sessions and is shown in comparison with the number of connected users in the last interval.

View trends for local host cache: From the **Local Host Cache tab**, select the time period, zone, and cloud connector to view the detailed information on data missed during the outage such as number of machines registered, number of machines reconnected, and number of sessions brokered within your site. The displayed data is based on the selected time period, zone, and cloud connector.

You can also view data for all zones and cloud connectors. The default-selected data is for the last 24 hours and for all zones and cloud connectors. The local host cache data is available for the last 2 hours, 24 hours, 7 days, month, and 90 days. The maximum data available is for the last 90 days. For more information on local host cache, see the Local Host Cache documentation. The view shows the following local host cache data per selected zone and cloud connector for the selected time period:

- Start time of the outage
- End time of the outage
- Duration of the outage
- New sessions brokered during the outage
- Number of sessions reconnected during the outage
- Number of machines registered during outage
- Number of machines affected during outage
- The name of the zone
- The name of the cloud connector

View hosted applications usage: From the Capacity Management tab, select the Hosted Applications Usage tab, select the delivery group and time period to view a graph displaying peak concurrent usage and a table displaying application based usage. From the Application Based Usage table, you can choose a specific application to see details and a list of users who are using, or have used, the application.

View single and multi-session OS usage: The Trends view shows the usage of Single session OS by site and by delivery group. When you select site, usage is shown per delivery group. When you select delivery group, usage is shown per User.
The Trends view also shows the usage of Multi-session OS by site, by delivery group, and by Machine. When you select site, usage is shown per delivery group. When you select delivery group, usage is shown per Machine and per User. When Machine is selected usage is shown per User.

View virtual machine usage: From the Machine Usage tab, select Single session OS Machines or Multi-session OS Machines to obtain a real-time view of your VM usage. The page displays the number of Autoscale enabled Multi-session and Single session OS machines that are powered on for a selected delivery group and time period. Also available is the estimated savings achieved by enabling

Autoscale in the selected delivery group, this percentage is calculated using the per machine costs.

The usage trends of Autoscale enabled machines indicate the actual usage of the machines, enabling you to quickly assess your site's capacity needs.

- Single session OS availability - displays the current state of Single session OS machines (VDIs) by availability for the entire site or a specific delivery group.
- Multi-session OS availability - displays the current state of Multi-session OS machines by availability for the entire site or a specific delivery group.

> **Note:**
>
> The grid below the chart displays the delivery group based machine usage data in real-time. The data includes machine availability of all machines independent of Autoscale enablement. The number of machines displayed in the Available Counter column in the grid includes machines in maintenance mode.

The monitoring data consolidation depends on the time period you select.

- Monitoring data for the one day and one week time periods is consolidated per hour.
- Monitoring data for the one month time period is consolidated per day.

The machine status is read at the time of consolidation and any changes during the period in between is not considered. For the consolidation period, refer to the Monitor API documentation.

For more information on monitoring Autoscale enabled machines see the Autoscale article.

View resource utilization: From the Resource Utilization tab, select Single session OS Machines or Multi-session OS Machines to obtain insight into historical trends data for CPU and memory usage, and IOPS and disk latency for each VDI machine for better capacity planning.
This feature requires VDAs **version 7.11** or later.
Graphs show data for average CPU, average memory, average IOPS, disk latency, and peak concurrent sessions. You can drill down to the machine, and view data and charts for the top 10 CPU consuming processes. Filter by delivery group and Time period. CPU, memory usage, and peak concurrent sessions graphs are available for the last 2 hours, 24 hours, 7 days, month, and year. The average IOPS and disk latency graphs are available for the last 24 hours, month, and year.

> **Note:**
>
> - The Monitoring policy setting, Enable Process Monitoring, must be set to "Allowed"to collect and display data in the Top 10 Processes table on the Historic Machine Utilization page. The policy is set to "Prohibited"by default. All resource utilization data is collected by default. This can be disabled using the Enable Resource Monitoring policy setting. The table below the graphs shows the resource utilization data per machine.
> - Average IOPS shows the daily averages. Peak IOPS is calculated as the highest of the IOPS

> averages for the selected time range. (An IOPS average is the hourly average of IOPS collected during the hour on the VDA).
> - The machine drilldown lists processes with average CPU or average memory usage more than 1%, this could mean that sometimes fewer than 10 processes are listed.

View application failures: The Application Failures tab displays failures associated with the published applications on the VDAs.

This feature requires VDAs **version 7.15** or later. Single session OS VDAs running Windows Vista and later, and Multi-session OS VDAs running Windows Server 2008 and later are supported.
For more information, see Historical application failure monitoring.

By default, only application faults from Multi-session OS VDAs are displayed. You can set the monitoring of application failures by using Monitoring policies. For more information, see Monitoring policy settings.

Create customized reports: The Custom Reports tab provides a user interface for generating Custom Reports containing real-time and historical data from the Monitoring database in tabular format.

From the list of previously saved Custom Report queries, you can click **Run and download** to export the report in CSV format, click **Copy OData** to copy and share the corresponding OData query, or click **Edit** to edit the query.
You can create a Custom Report query based on machines, connections, sessions, or application instances. Specify filter conditions based on fields such as machine, delivery group, or time period. Specify the extra columns required in your Custom Report. Preview displays a sample of the report data. Saving the Custom Report query adds it to the list of saved queries.

You can create a Custom Report query based on a copied OData query. To do this, select the OData Query option and paste the copied OData query. You can save the resultant query for execution later.

> **Note:**
>
> The column names in the Preview and Export report generated using OData queries are not localized, but appear in English.

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

> **Note:**
>
> - HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.
> - Delivery groups deleted in the Manage console are available for selection in the Trends filters until data related to them are groomed out. Selecting a deleted delivery group displays

graphs for available data until retention. However, the tables don't show data.
- Moving a machine containing active sessions from one delivery group to another causes the **Resource Utilization and Load Evaluator Index** tables of the new delivery group to display metrics consolidated from the old and new delivery groups.

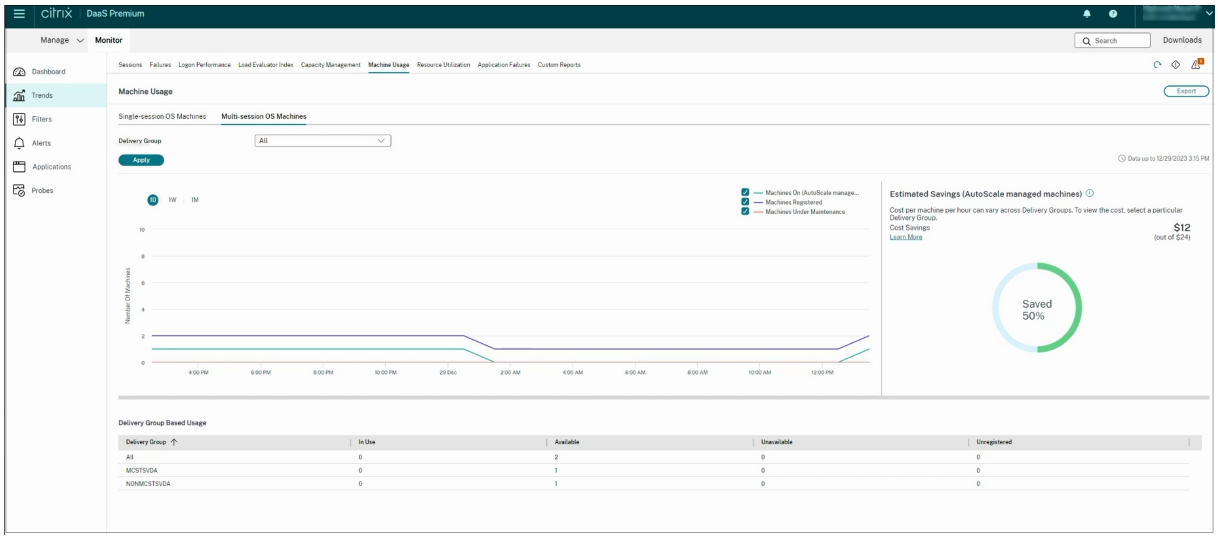
Monitor Autoscale-managed machines

March 23, 2022

Autoscale is a power management feature that enables proactive power management of all registered Multi-session and Single session OS machines in a delivery group. You can configure Autoscale for a selected delivery group from the **Manage** tab. For more information, see Autoscale.
You can monitor the key metrics of Autoscale enabled machines from the **Monitor** tab.

Machine Usage

The **Monitor** > **Trends** > **Machine Usage** page displays the total number of Autoscale enabled Multi-session and Single session OS machines that are powered on for a selected delivery group and time period. This metric indicates the actual usage of machines in the delivery group.
From the **Single session OS Machines** or the **Multi-session OS Machines** tab, select the Delivery group and the time period.



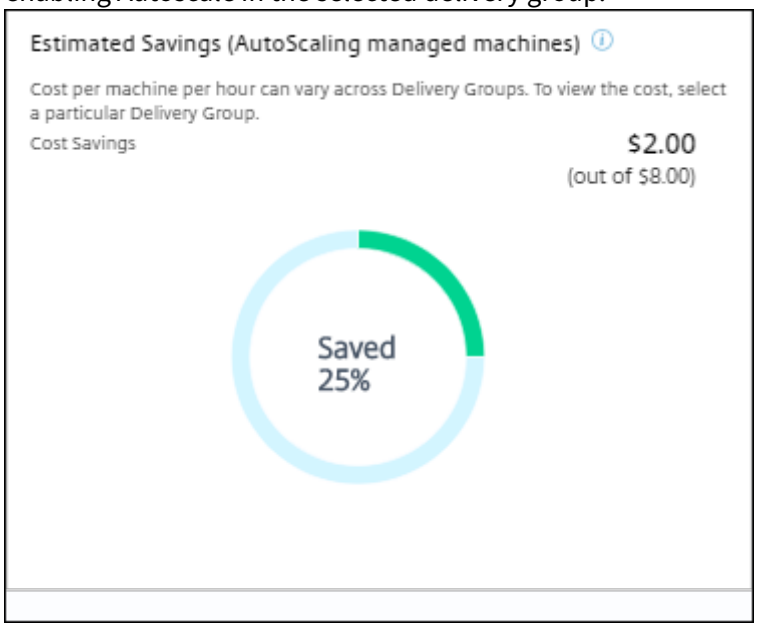
The chart plots the following metrics:

- **Machines On** - the number of Autoscale enabled machines that are powered on
- **Machines Registered** - the number of registered Multi-session or Single session OS machines

- **Machines under Maintenance** - the number of Multi-session or Single session OS machines with maintenance mode switched on

Estimated Savings

The **Monitor** > **Trends** > **Machine Usage** page also displays the estimated cost savings achieved by enabling Autoscale in the selected delivery group.



Estimated Savings is calculated as the percentage of savings per machine per hour (in US $) as configured in **Manage** > **Edit Delivery Group** > **Autoscale**. For more information about configuring the savings per machine, see Autoscale.

When you select all Delivery groups, the average value of Estimated Savings across all the delivery groups is displayed.
The estimated savings help administrators consolidate the existing infrastructure and plan the capacity to achieve maximum savings and utilization.

Alert notifications for machines and sessions

The Monitor Dashboard displays alert notifications that can be further drilled down. Alert details are displayed on the **Monitor** > **Alerts** page.

- To create an alert policy in a delivery group, go to **Monitor** > **Alerts** > **Citrix Alerts Policy** > **Delivery Group Policy**.
- Here, you can set the following Warning and Critical thresholds:
  - Failed Machines (Single session OS) and Failed Machines (Multi-session OS),

  - Peak Connected Sessions, Peak Disconnected Sessions and Peak Concurrent Total Sessions in the delivery group.

- Alerts are generated when the corresponding metric in the delivery group reaches the threshold.

For more details regarding the alert policy conditions and creation of new alert policies, see Alerts and notifications.

Machine status

- **Monitor** > **Filters** > **Machines** displays the power state of all machines in a tabular format. You can filter by a specific delivery group.
- **Monitor** > **Filters** > **Sessions** displays filter by the Machine name to see the associated sessions and their real-time status.
- In **Monitor** > **Trends** > **Sessions**, select your delivery group and time period to see the trend of the sessions and their associated metrics.

For more information, see Filter data to troubleshoot failures.

Load Evaluation trends

The **Monitor** > **Trends** > **Load Evaluator Index** page displays a graph with detailed information about the load that is distributed among the Multi-session OS machines. The filter options for this graph include the delivery group or Multi-session OS machine in a delivery group, Multi-session OS machine (available only if Multi-session OS machine in a delivery group was selected), and range. The Load Evaluator Index is displayed as percentages of Total CPU, Memory, Disk, or Sessions and is shown in comparison with the number of connected users in the last interval.

Troubleshoot deployments

March 11, 2024

As a help desk administrator, you can search for the user reporting an issue. And, then display details of sessions or applications associated with that user.

Similarly, you can search for machines or endpoints where issues are reported. Issues can be quickly resolved by monitoring the relevant metrics and performing suitable actions.

The following actions are available:

- ending an unresponsive application or process

- shadowing operations on the user's machine
- logging off an unresponsive session
- restarting the machine
- putting a machine into maintenance mode
- resetting the user profile

Troubleshoot applications

June 6, 2024

Application Analytics

The **Applications** view displays application-based analytics in a single, consolidated view to help analyze and manage application performance efficiently. You can gain valuable insight into the health and usage information of all applications published on the site. The default view helps identify the top running applications.
This feature requires VDAs Version 7.15 or later.

The **Probe Result** column displays the result of application probing run in the last 24 hours. Click the probe result link to see more details in the **Trends** > **Probe Results** page. For more details on how to configure application probes, see Application and Desktop Probing.

The **Instances** column displays usage of the applications. It indicates the number of application instances currently running (both connected and disconnected instances). To troubleshoot further, click the **Instances** field to see the corresponding **Application Instances** filters page. Here, you can select application instances to log off or disconnect.

> **Note:**
>
> For custom scope administrators, Monitor does not display application instances created under application groups. To view all application instances, you must be a full administrator. For more information, see Knowledge Center article CTX256001.

Monitor the health of published applications in your site with the **Application Faults** and the **Application Errors** columns. These columns display the aggregated number of faults and errors that have

occurred while launching the corresponding application in the last one hour. Click the **Application Faults** or **Application Errors** field to see failure details on the **Trends** > **Application Failures** page corresponding to the selected application.

The application failure policy settings govern the availability and display of faults and errors. For more information about the policies and how to modify them, see Policies for application failure monitoring in Monitoring policy settings.

Real-time application monitoring

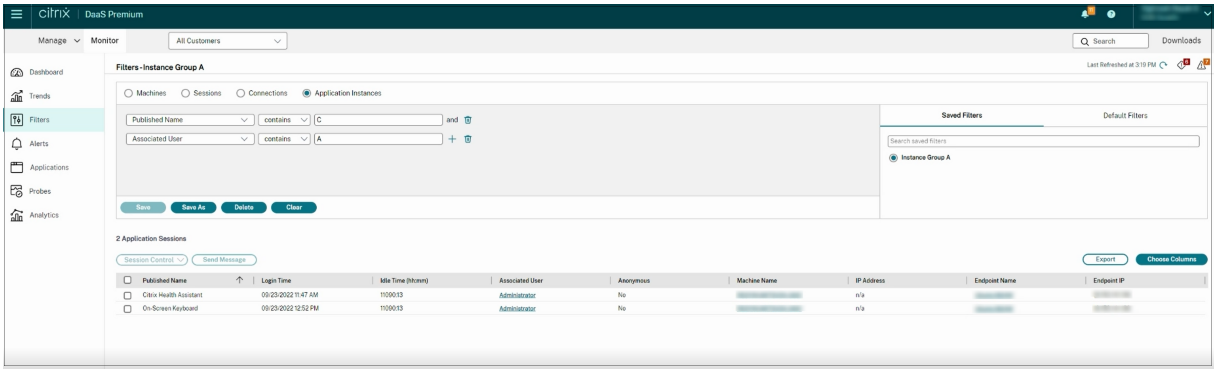
You can troubleshoot applications and sessions by using the idle time metric to identify instances that are idle beyond a specific time limit.

Typical use cases for application-based troubleshooting are in the healthcare sector, where employees share application licenses. There, you must end idle sessions and application instances to purge the Citrix Virtual Apps and Desktops environment, to reconfigure poorly performing servers, or to maintain and upgrade applications.

The **Application Instances** filter page lists all application instances on VDAs of Multi-session and Single session OS. The associated idle time measurements are displayed for application instances on VDAs of Multi-session OS that have been idle for at least 10 minutes.

> **Note:**
>
> The Application Instances metrics are available on sites of all license editions.

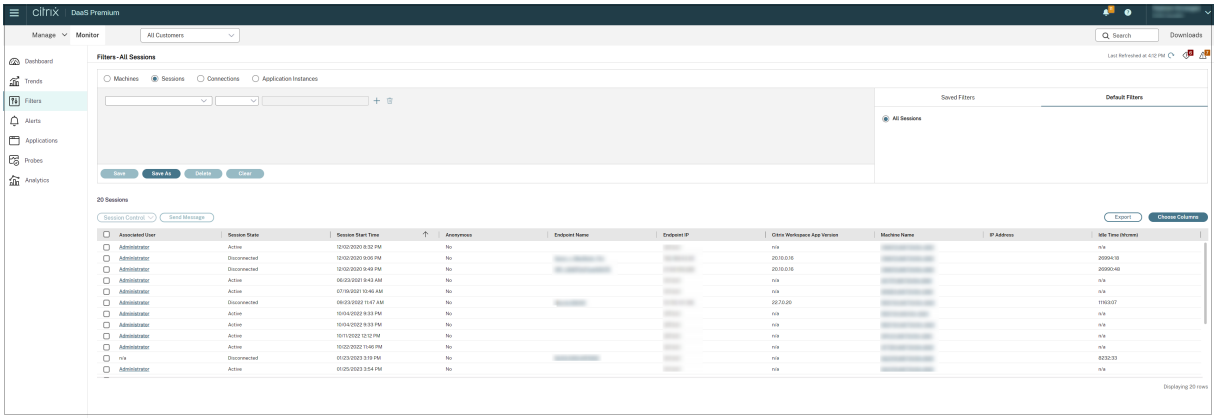
Use this information to identify the application instances that are idle beyond a specific time period and log off or disconnect them as appropriate. To do this, select **Filters > Application Instances** and select a pre-saved filter or choose **All Application Instances** and create your own filter.



An example of a filter would be as follows. As **Filter by** criteria, choose **Published Name** (of the application) and **Idle Time**. Then, set **Idle Time** to **greater than or equal to** a specific time limit and save the filter for reuse. From the filtered list, select the application instances. Select option to send messages or from the **Session Control** drop-down, choose **Logoff** or **Disconnect** to end the instances.

> **Note:**
>
> Logging off or disconnecting an application instance logs off or disconnects the current session, thereby ending all application instances that belong to the same session.

You can identify idle sessions from the **Sessions** filter page using the session state and the session idle time metric. Sort by the **Idle Time** column or define a filter to identify sessions that are idle beyond a specific time limit. Idle time is listed for sessions on VDAs of Multi-session OS that have been idle for at least 10 minutes.



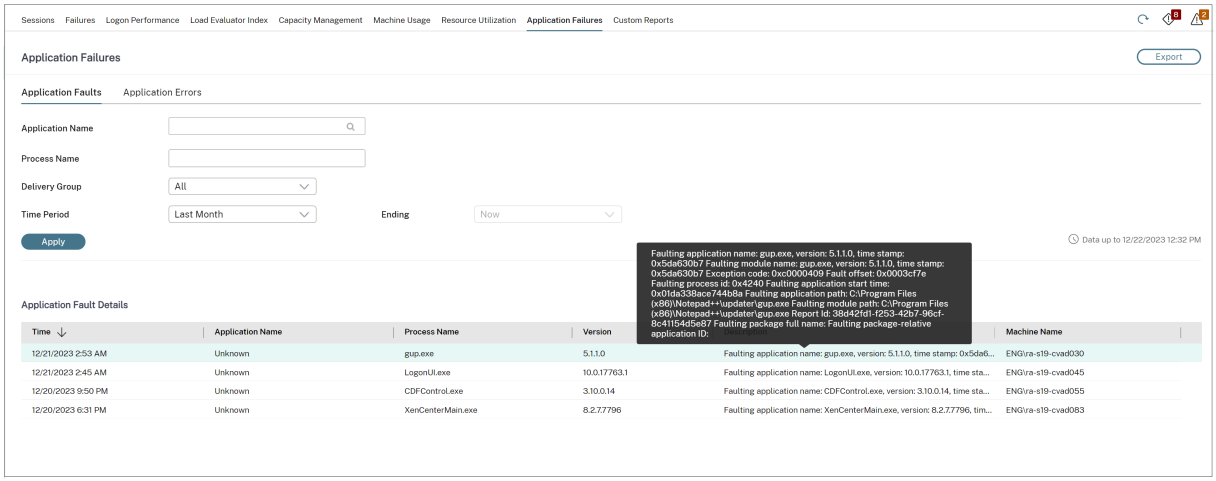
The **Idle time** is displayed as **N/A** when the session or application instance

- has not been idle for more than 10 minutes,
- is launched on a VDA of Single session OS, or
- is launched on a VDA running Version 7.12 or earlier.

Historical application failure monitoring

The **Trends** -> **Application Failures** tab displays failures associated with the published applications on the VDAs.

For more information about the availability of the application failure trends, see Data granularity and retention article. The application failures that are logged to the Event Viewer with source "Application Errors"are monitored. Click **Export** to generate reports in CSV, Excel, or PDF formats



The failures are displayed as **Application Faults** or **Application Errors** based on their severity. The Application Faults tab displays failures associated with loss of functionality or data. Application Errors indicate problems that are not immediately relevant; they signify conditions that might cause future problems.

You can filter the failures based on **Published Application Name**, **Process Name** or **Delivery Group,** and **Time Period.** The table displays the fault or error code and a brief description of the failure. The detailed failure description is displayed as a tooltip.

> **Note:**
>
> The Published Application name is displayed as "Unknown"when the corresponding application name cannot be derived. This typically occurs when a launched application fails in a desktop session or when it fails due to an unhandled exception caused by a dependent executable.

By default, only faults of applications hosted on Multi-session OS VDAs are monitored. You can modify the monitoring settings through the Monitoring Group Policies: Enable monitoring of application failures, Enable monitoring of application failures on Single session OS VDAs, and List of applications excluded from failure monitoring. For more information, see Policies for application failure monitoring in Monitoring policy settings.

The **Trends > Application Probe Results** page displays the results of application probing executed in the site for the last 24 hours and 7 days. For more details on how to configure application probes, see Application Probing.

Application probing

January 5, 2023

Application probing automates the process of checking the health of Citrix Virtual Apps that are published in a site. The results of application probing are available in the **Monitor** tab of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Citrix Probe Agent supports sites hosted on Citrix Cloud Japan and Citrix Cloud Government Control Planes.

Ensure that the endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1808 or later. Workspace app for Unified Windows Platform (UWP) is not supported.

Requirements:

- Endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1906 or later. Workspace app for Unified Windows Platform (UWP) is not supported.
- Citrix Probe Agent supports the default form-based authentication as supported by Citrix WorkSpace. Citrix Probe Agent doesn't support other authentication methods like Single Sign-On (SSO) or Multi Factor Authentication (MFA). Similarly, Citrix Probe Agent works only when there is no proxy server or load balancer like Citrix Gateway or Citrix ADC deployed.
- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine where you want to install the Probe Agent.
- To use the probing agent in Citrix Cloud Japan Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region"to 2. To use the probing agent in Citrix Cloud Government Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 3.

User accounts/permissions required to run Application Probing are as follows:

- A unique Workspace user to probe on each endpoint machine. The Workspace user is not required to be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines
- A full administrator user account with the following permissions. Reusing existing user accounts for application probing might log off from the users' active sessions.
  - Delivery group permissions:
    - Read-only
  - Director permissions:
    - Create\Edit\Remove Probe Configurations
    - View Configurations page
    - View Trends page

Configure Application Probing

Configure your application probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the applications, hosting machine or connection before the users experience them.

Citrix Probe Agent version 2103 supports site aggregation. Applications and desktops can be enumerated and launched from aggregated sites. When you configure the probe agent, select the **Workspace (StoreFront) Site Aggregation Enabled** option to enable enumeration of applications and desktops from aggregated sites. The following combinations of sites are supported:

- Multiple on-premises sites having one StoreFront URL.
- On-premises and cloud sites having either a StoreFront or Workspace URL.
- Multiple cloud sites having one Workspace URL.

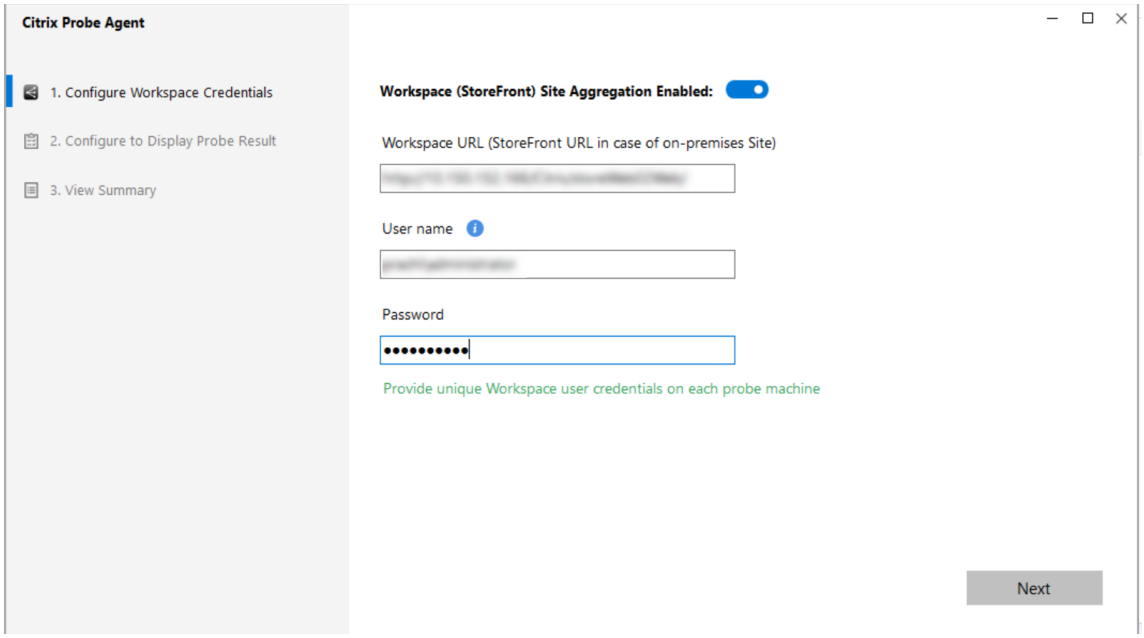
> **Note:**
>
> You must create separate administrators or users to configure probes that have access to only one site.

Step 1: Install and configure the Citrix Probe Agent

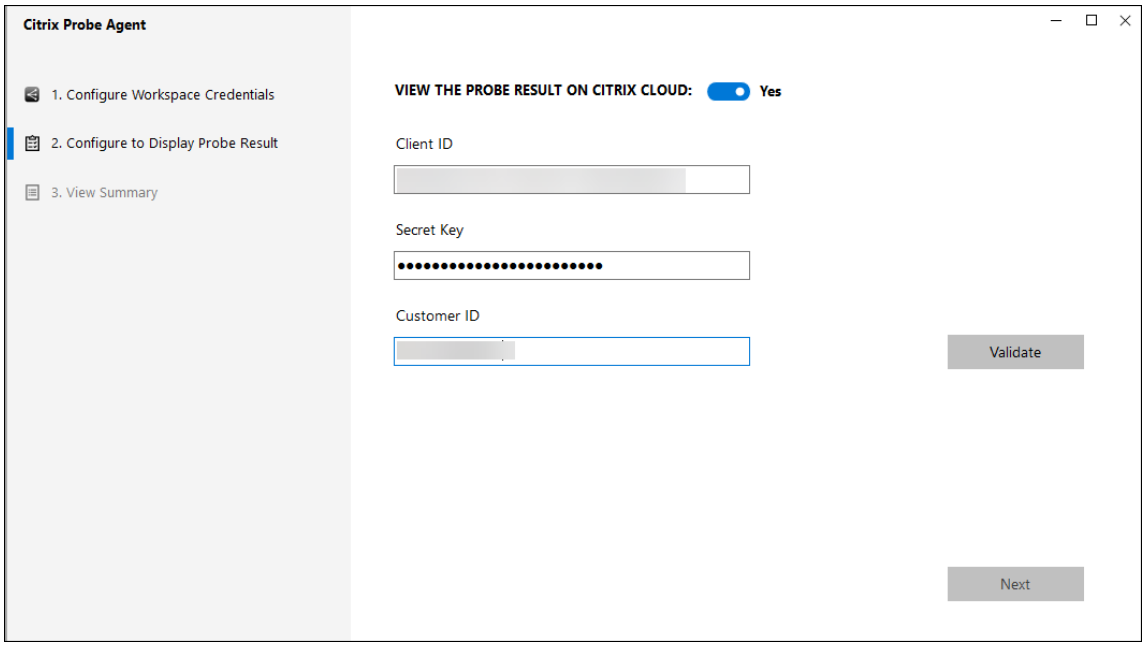
The Citrix Probe Agent is a Windows executable that simulates the actual application launch by the user through Citrix Workspace. It tests application launches as configured in Monitor and reports back the results to Monitor.

1. Identify endpoint machines from where you want to run application probing.
2. Users with administrative privileges can install and configure the Citrix Probe Agent on the endpoint machine. Download the Citrix Probe Agent executable available at https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Start the agent and configure your Citrix Workspace credentials. Configure a unique Workspace user on each endpoint machine. The credentials are encrypted and stored securely.

   > **Notes:**
   >
   > - To access the site to be probed from outside the network, type the login URL for Citrix Gateway in the **Workspace URL** field. Citrix Gateway automatically routes the request to the corresponding site Workspace URL.
   > - Use NetBIOS as the domain name in the user name field. For example, NetBIOS/username.
   > - App probing supports Citrix Content Collaboration service using Workspace authentication (AD only).



4. On the **Configure To Display Probe Result** tab, enter credentials to access Citrix DaaS. You can find the Customer Name or Customer ID, Client ID, and Secret Key from the API Access page in the Citrix Cloud console.



Step 2: Configure Application probing in the Monitor tab

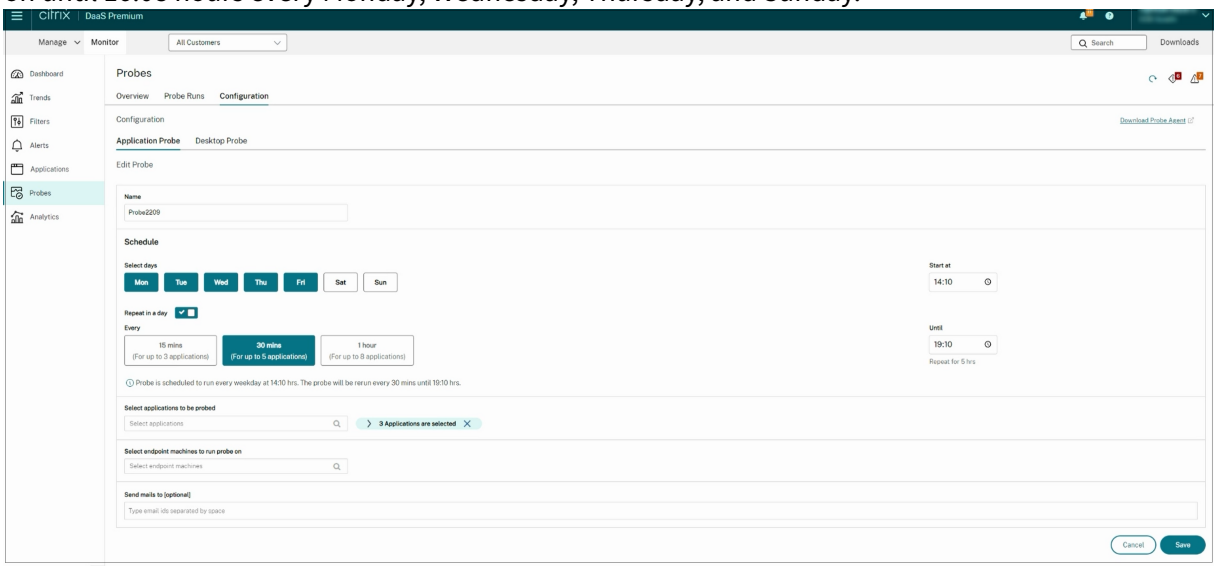
1. In Citrix DaaS, go to **Configuration** > **Probe Configuration** > **Application Probe** and click **Create Probe**:
2. In the **Create Probe** page, enter the name of the probe.

3. Select the schedule:

    a) Choose the days of the week on which you want the probe to run.
    b) Enter the start time at which you want the probe to run.
    c) In addition, you can choose the **Repeat in a day** option. Enter the end time and the interval in which you want the probe to repeat within a day. For example, the configuration below helps run application probes from 12:08 hours until 16:34 hours repeating every 30 minutes every Monday, Wednesday, Thursday, and Sunday.

4. Select the recommended number of applications to be probed depending on the interval.
5. Select the endpoint machines on which the probe must run.
6. Enter the email addresses to which the failure probe results are sent and click **Save**.

In this configuration, the application sessions launch at 12:08 hours, 12:38 hours, 13:08 hours, and so on until 16:08 hours every Monday, Wednesday, Thursday, and Sunday.



> **Note:**
>
> - Configure your email server in **Alerts** > **Email Server Configuration**.
> - After configuration in the **Monitor** tab, the agent runs configured probes starting the next hour.
> - The probes that were set up before the **Repeat in a day** option was introduced continue to run at their scheduled time. They have the **Repeat in a day** option disabled by default.

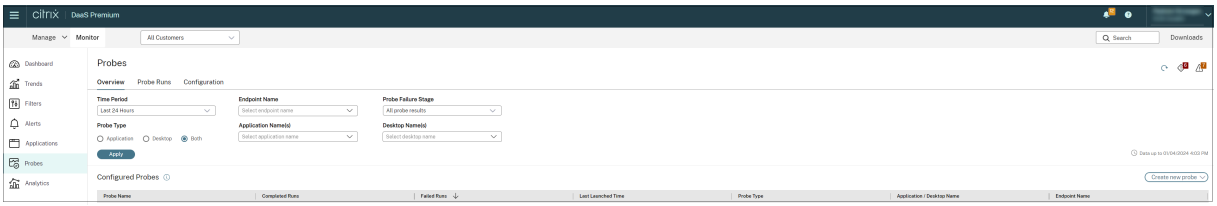
Step 3: Probe execution

The agent runs application probing as per the probe configuration it fetches from Monitor every hour. It launches selected applications serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

- **Workspace Reachability** - configured Workspace URL is not reachable.
- **Workspace Authentication** - configured Workspace credentials are invalid.
- **Workspace Enumeration** - Workspace Enumerate applications list does not contain the application to be probed.
- **ICA download** - the ICA file is not available.
- **Application launch** –the application cannot be launched.

Step 4: View probe results

You can view the latest probe results in Citrix DaaS > **Applications** page.



To troubleshoot further, click the probe result link to see more details on the **Trends** > **Application Probe Results** page.

The consolidated probe results data is available for the last 24 hours or last 7 days time periods on this page. You can see the stage in which the probe failed. You can filter the table for a specific application, probe failure stage, or endpoint machine.

Desktop probing

February 2, 2023

Desktop probing automates the process of checking the health of Citrix Virtual Desktops that are published in a site. The results of desktop probing are available in Monitor. Citrix Probe Agent now supports sites hosted on Citrix Cloud Japan and Citrix Cloud Government Control Planes.

In Monitor's Configuration page, configure the desktops to be probed, the endpoint machines to run the probe on, and the probe time. The agent tests the launch of selected desktops using Workspace and reports the results back to Monitor. The probe results are displayed on the Monitor UI –the last 24-hours'data on the Applications page and historical probe data on the **Trends > Probe Results > Desktop Probe Results** page.

Here, you can see the stage when the probe failure occurred - Workspace Reachability, Workspace Authentication, Workspace Enumeration, ICA download, or Desktop launch. The failure report is sent to the configured email addresses.

You can schedule your desktop probes to run during off-peak hours across multiple geographies. The comprehensive results can help to proactively troubleshoot issues related to provisioned desktops, hosting machines or connections before the users experience them.

This feature requires Probe Agent 1903 or later.

Requirements:

- Endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1906 or later. Workspace app for Unified Windows Platform (UWP) is not supported.
- Citrix Probe Agent supports the default form-based authentication as supported by StoreFront and Citrix WorkSpace. Citrix Probe Agent doesn't support other authentication methods like Single Sign-On (SSO) or Multi Factor Authentication (MFA). Similarly, Citrix Probe Agent works only when there is no proxy server or load balancer like Citrix Gateway or Citrix ADC deployed.
- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine where you want to install the Probe Agent.
- To use the probing agent in Citrix Cloud Japan Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region"to 2. To use the probing agent in Citrix Cloud Government Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 3.

User accounts or permissions required to run Desktop probing:

- A unique Workspace user to probe on each endpoint machine. The Workspace user need not be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines
- A full administrator user account or a custom role with the following permissions. Reusing normal user accounts for desktop probing might log off the users' from the active sessions.
  - Delivery group permissions:
    - Read-only
  - Monitor permissions:
    - Create, Edit, Remove Alert Email Server Configuration - if the email server is not already configured
    - Create, Edit, Remove Probe Configurations
    - View Configurations page
    - View Trends page

Configure desktop probing

You can schedule your desktop probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the desktops, hosting machine or connection before the users experience them.

Citrix Probe Agent version 2103 supports site aggregation. Applications and desktops can be enumerated and launched from aggregated sites. When you configure the probe agent, select the **Workspace (StoreFront) Site Aggregation Enabled** option to enable enumeration of applications and desktops from aggregated sites. The following combinations of sites are supported:

- Multiple on-premises sites having one StoreFront URL.
- On-premises and cloud sites having either a StoreFront or Workspace URL.
- Multiple cloud sites having one Workspace URL.

> **Note:**
>
> You must create separate administrators or users to configure probes that have access to only one site.

Step 1: Install and configure the Citrix Probe Agent

The Citrix Probe Agent is a Windows executable that simulates the actual desktop launch by the user through Workspace. It tests desktop launches as configured in Monitor and reports back the results to Monitor.

1. Identify endpoint machines from where you want to run desktop probing.
2. Users with administrative privileges can install and configure the Citrix Probe Agent on the endpoint machine. Download the Citrix Probe Agent executable available at https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Start the agent and configure your Workspace Receiver for Web credentials. Configure a unique Workspace user on each endpoint machine. The credentials are encrypted and stored securely.

   > **Notes:**
   >
   > - To access the site to be probed from outside the network, type the Citrix Gateway login page URL on the Workspace URL field. Citrix Gateway automatically routes the request to the corresponding site Workspace URL. This feature is available for Citrix Gateway version 12.1 or later.
   > - Use NetBIOS as the domain name in the user name field. For example, NetBIOS/username.
   > - Desktop probing supports Citrix Content Collaboration service using Workspace au-

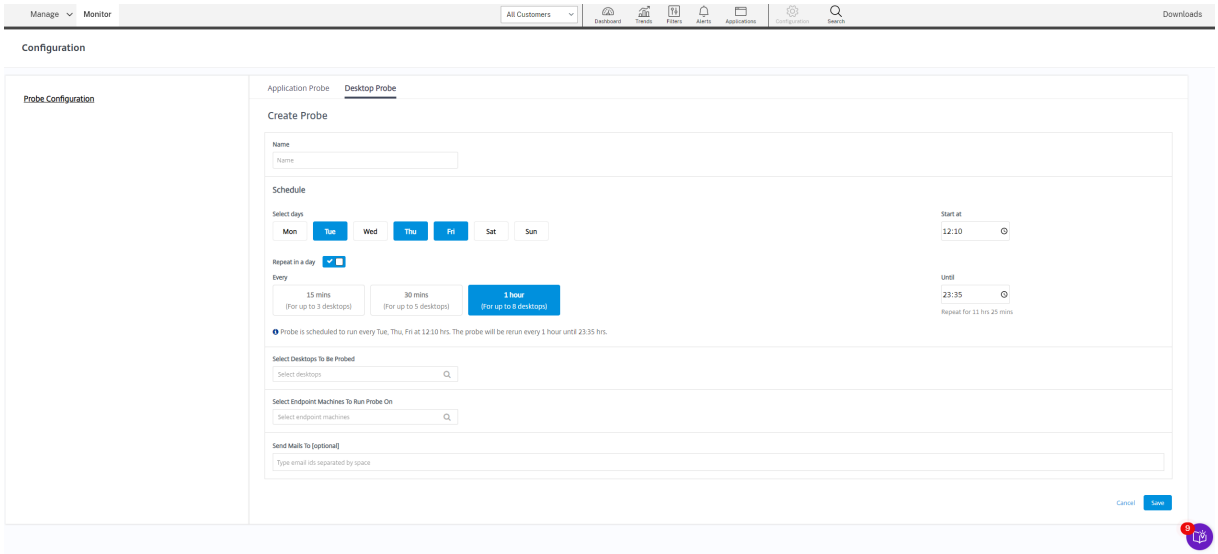
> thentication (AD only).
> - You must enable Interactive Logon for the configured unique StoreFront user.

4. On the **Configure To Display Probe Result** tab, enter your Monitor credentials. You can find the Customer Name or Customer ID, Client ID, and Secret Key from the API Access page in the Citrix Cloud console.

Step 2: Configure desktop probing in Monitor

1. In Citrix DaaS, go to **Configuration** > **Probe Configuration** > **Application Probe** and click **Create Probe**.
2. In the **Create Probe** page, enter the name of the probe.
3. Select the schedule:
   a) Choose the days of the week on which you want the probe to run.
   b) Enter the start time at which you want the probe to run.
   c) In addition, you can choose the **Repeat in a day** option. Enter the end time and the interval in which you want the probe to repeat within a day. For example, the configuration below helps run desktop probes from 12:10 hours until 23:35 hours repeating every hour every Tuesday, Thursday, and Friday.
4. Select the recommended number of desktops to be probed depending on the interval.
5. Select the endpoint machines on which the probe must run.
6. Enter the email addresses to which the failure probe results are sent and click **Save**.

In this configuration, the desktop sessions launch at 12:10 hours, 13:10 hours, 14:10 hours, and so on until 23:10 hours every Tuesday, Thursday, and Friday.



> **Note:**
>
> - Configure your email server in **Alerts** > **Email Server Configuration**.
> - After desktop probing configuration is complete, the agent runs the configured probes starting the next hour.
> - The probes that were set up before the **Repeat in a day** option was introduced continue to run at their scheduled time. They have the **Repeat in a day** option disabled by default.

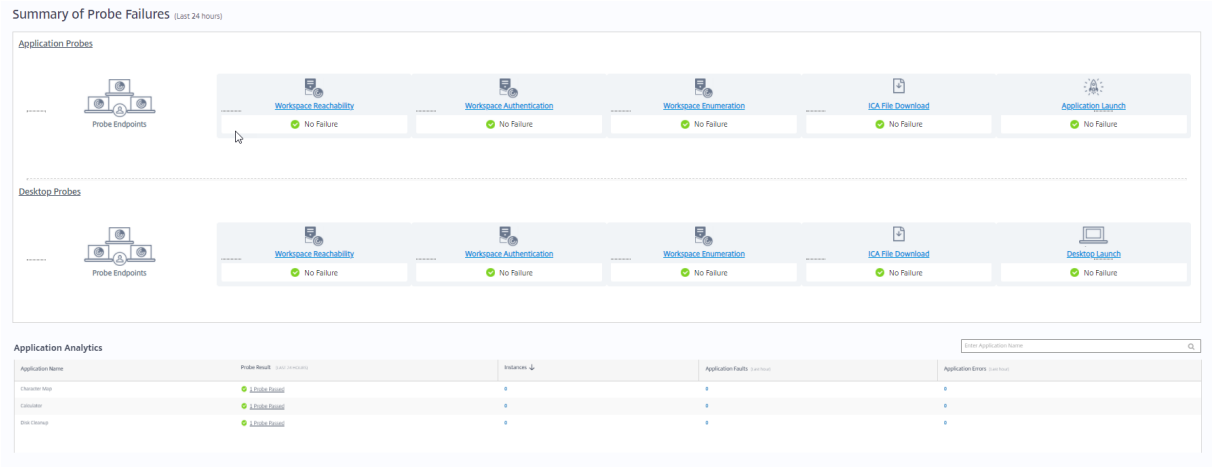
Step 3: Probe execution

The agent runs desktop probing as per the probe configuration it fetches from Monitor periodically. It launches selected desktops serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

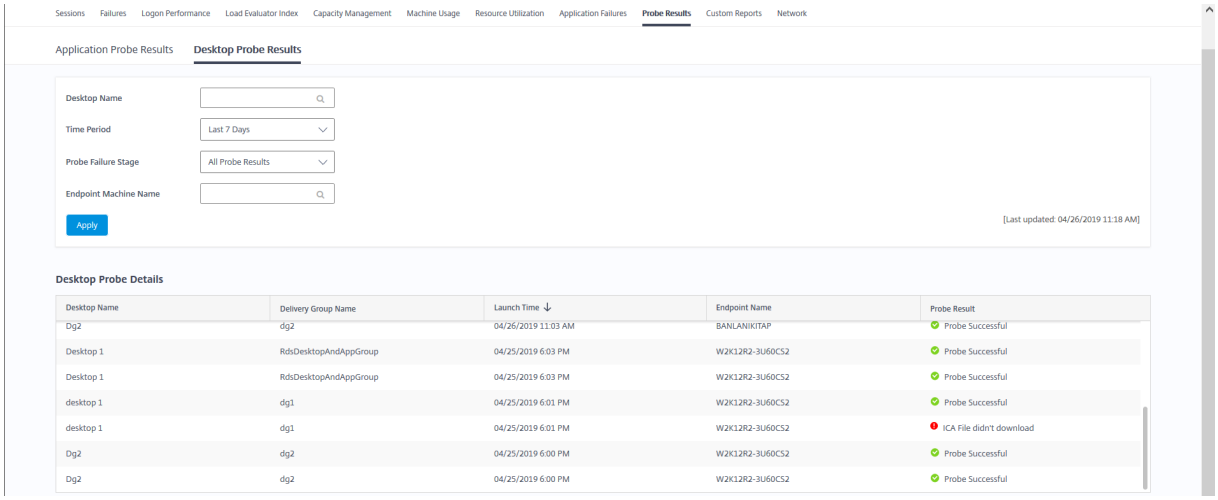
- **Workspace Reachability** - configured Workspace URL is not reachable.
- **Workspace Authentication** - configured Workspace credentials are invalid.
- **Workspace Enumeration** - Workspace Enumerate desktops list does not contain the desktop to be probed.
- **ICA download** - the ICA file is not available.
- **Desktop launch** –the desktop cannot be launched.

Step 4: View probe results

You can view the latest probe results on the **Desktops** page.



To troubleshoot further, click the probe result link to see more details on the **Trends** >**Probe Results** > **Desktop Probe Results** page.



The consolidated probe results data is available for the last 24 hours or last 7 days time periods on this page. You can see the stage in which the probe failed. You can filter the table for a specific desktop, probe failure stage, or endpoint machine.

Troubleshoot machines

June 13, 2024

> **Note:**
>
> **Citrix Health Assistant** is a tool to troubleshoot configuration issues in unregistered VDAs. The tool automates a number of health checks to identify possible root causes for VDA registration failures and issues in session launch and time zone redirection configuration. The Knowledge Center article, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contains the **Citrix Health Assistant** tool download and usage instructions.

The **Filters > Machines** view in the Monitor tab displays the machines configured in the site. The Multi-session OS Machines tab includes the load evaluator index, which indicates the distribution of performance counters and tooltips of the session count if you hover over the link.

Click the **Failure Reason** column of a failed machine to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended actions for machine and connection failures are available in the Citrix Director Failure Reasons Troubleshooting Guide.

Click the machine name link to go to the **Machine Details** page.

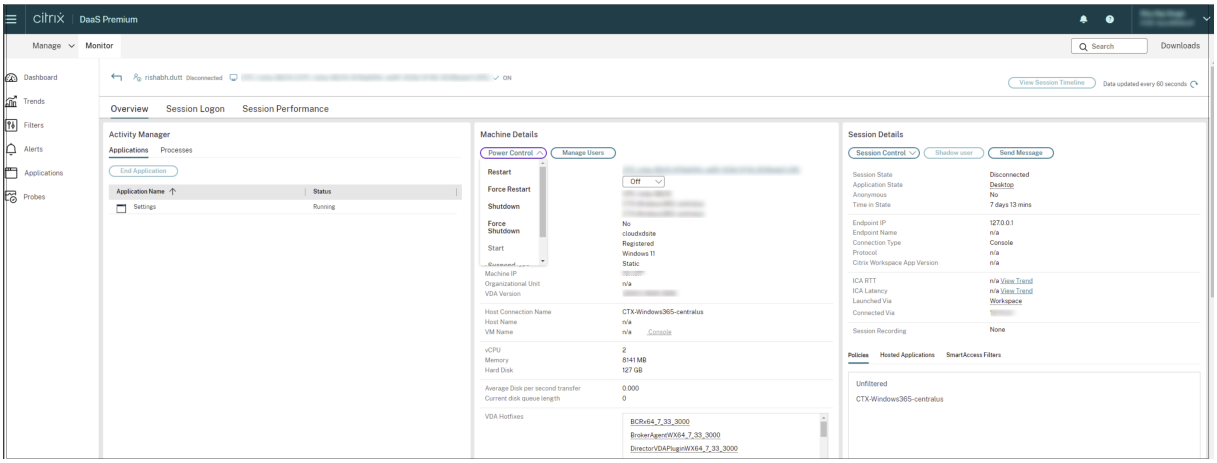
The Machine Details page lists the machine details, infrastructure details, and details of the hotfixes applied on the machine.

Support for HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops:

> **Note:**
>
> For HDX Plus for Windows 365 Cloud PCs, only the Restart and Force Restart Power Control options are available. For Azure Virtual Desktops (AVD) all Power Control options are available.

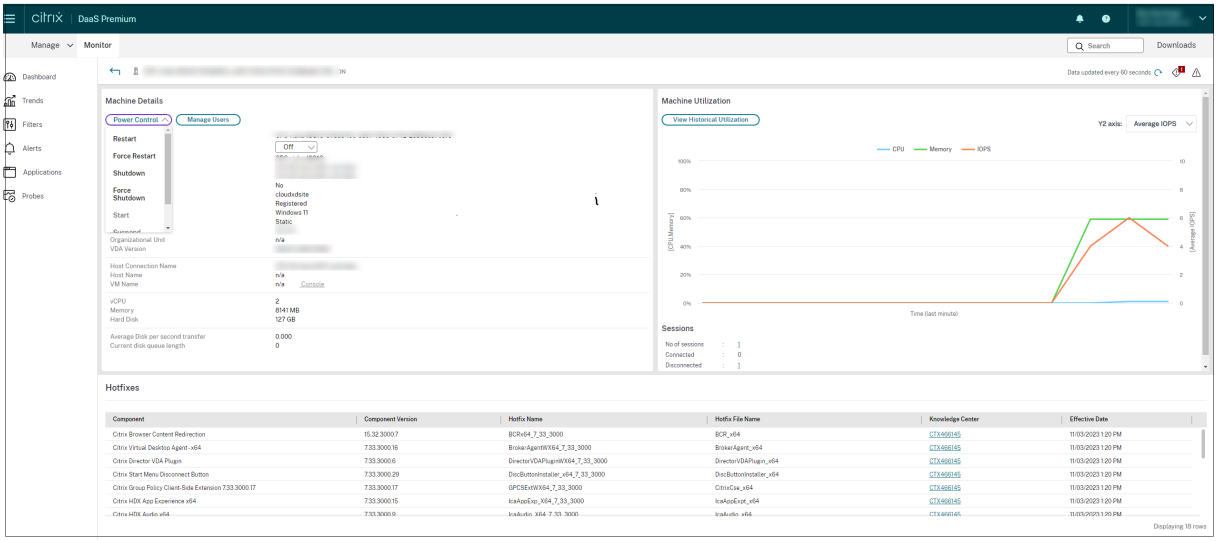
You can view the available Power Control options using one of the following methods:

Click **Filters** >**Sessions** > **View Details** > **Machine Details** > **Power Control** drop-down list and select an option to assign the required power control option for a machine.



Or,

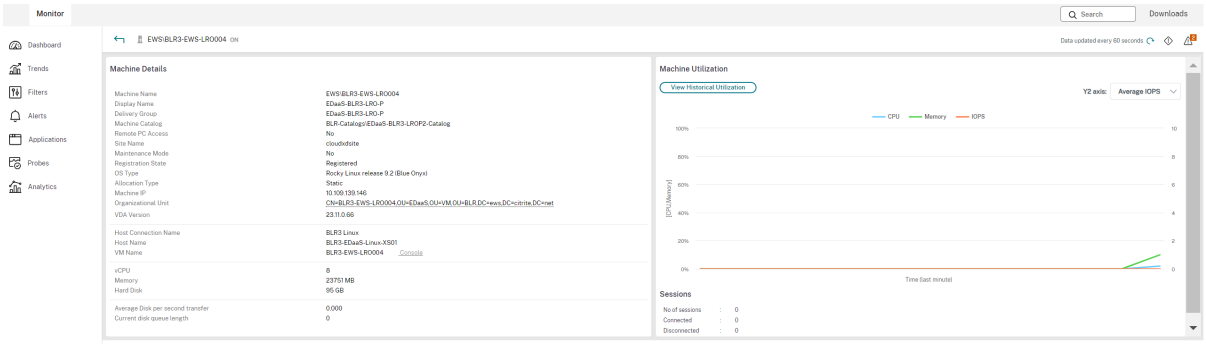
Click **Filters** > **Machine** > **Machine Details** > **Power Control** drop-down list and select an option to assign the required power control option for a machine.



Machine-based real-time resource utilization

The **Machine Utilization** panel displays graphs showing real-time utilization of CPU and memory. In addition, disk and GPU monitoring graphs are available for sites with VDA versions 7.14 and later.

Disk monitoring graphs, average IOPS, and disk latency are important performance measurements that help you monitor and troubleshoot issues related to VDA disks. The Average IOPS graph displays the average number of reads and writes to a disk. Select **Disk Latency** to see a graph of the delay between a request for data and its return from the disk, measured in milliseconds.



GPU Utilization

Select **GPU Utilization** to see the percentage utilization of the GPU, the GPU memory, and of the Encoder and the Decoder to troubleshoot GPU-related issues on multi-session and single-session OS VDAs.

Supported GPU versions:

- NVIDIA Tesla M60 GPUs running Display Driver version 369.17 or later. For more information, see NVIDIA vGPU Software.
- AMD Radeon Instinct MI25 GPUs and AMD EPYC 7V12(Rome) CPUs. For more information, see AMD Drivers and Support.

Drivers:

The appropriate drivers or extensions must be installed on the VDAs.

- For NVIDIA GPUs, install GRID drivers manually or via extensions. For more information, see NVIDIA vGPU Software.
  - Note that for NVIDIA, only GRID drivers are supported. CUDA drivers do not work with the NVadsA10 v5-series and are not supported.
  - For a sample process to install Nvidia Grid GPU drivers via extensions on Azure based machines, see NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.

  - For a sample process to install Nvidia Grid GPU drivers manually, see Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.

- For AMD GPUs, install AMD graphics drivers manually or via extensions. For more information, see AMD Drivers and Support.

  - For a sample process to install AMD GPU drivers via extensions on Azure based machines, see AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - For a sample process to install AMD GPU drivers manually on Azure machines, see Install AMD GPU drivers on N-series VMs running Windows.

Usage Notes:

- The GPU Utilization graphs are available only for VDAs running 64-bit Windows.
- The AMD GPU Utilization graphs are available only for VDAs running Citrix Virtual Apps and Desktops 7 2212 or later.
- The VDAs must have HDX 3D Pro enabled to provide GPU acceleration. For more information, see GPU acceleration for Windows Single-session OS and GPU acceleration for Windows Multi-session OS.
- When a VDA accesses more than one GPU, the utilization graph displays the average of the GPU metrics collected from the individual GPUs. The GPU metrics are collected for the entire VDA and not for individual processes.
- For AMD, encoder and decoder usage are not supported separately. Any encoding/ decoding workload using the GPU will be reported as the general 3D load on GPU usage.
- Ensure that you install the NVIDIA WMI during installation. This window is available only during manual installation.
- If drivers are installed but Director does not detect GPU

  - Check Task Manager. If drivers are installed properly, the GPU should show up in Task Manager.
  - Check if the machine is registered. Sometimes machines may take some time to be detected as online.

- If the GPU usage shows no activity in Director, make sure that the workload you are running is using the GPU. For graphics workloads, this can be enabled from Settings > System > Display > Graphics Settings > Choose the app to set preference. Make sure to turn on High Performance. Sometimes, Windows defaults to using the CPU for graphics workloads when this is set to system default or power saving, based on other settings.
- The data is updated every minute and the data visualization starts within a minute of selecting **GPU Utilization**.

Machine-based historical resource utilization

In the **Machine Utilization** panel, click **View Historical Utilization** to view the historical usage of resources on the selected machine.
The utilization graphs include critical performance counters of CPU, memory, peak concurrent sessions, average IOPS, and disk latency.

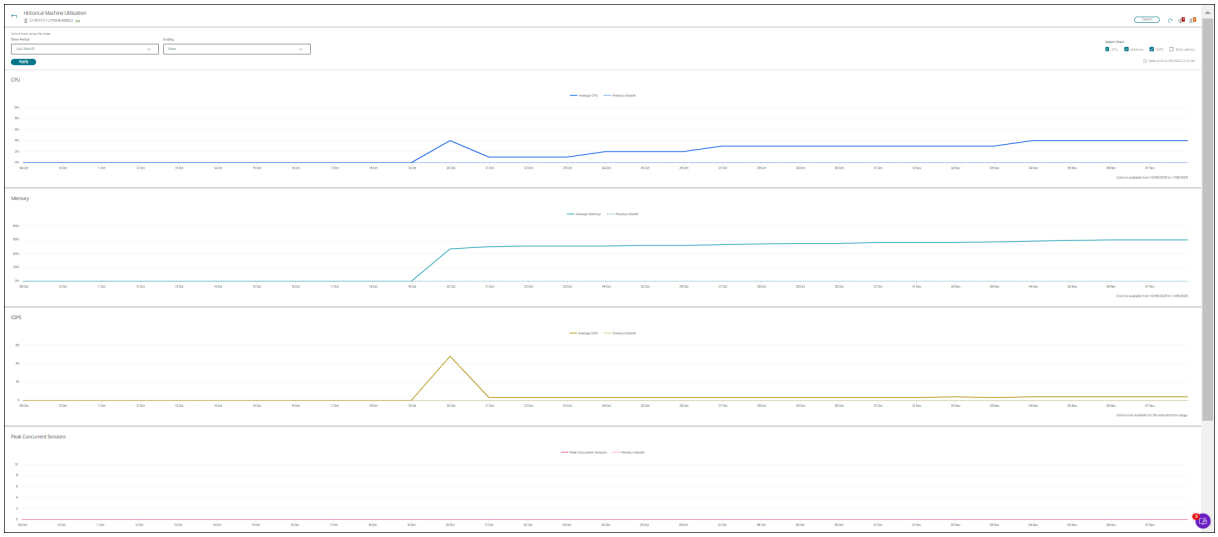
> **Note:**
>
> The Monitoring policy setting, **Enable Process Monitoring**, must be set to Allowed to collect, and display data in the Top 10 Processes table on the Historic Machine Utilization page. The collection is prohibited by default.

The CPU and memory utilization, average IOPS, and disk latency data is collected by default. You can disable the collection by using the **Enable Resource Monitoring** policy setting.

1. From the **Machine Utilization** panel in the **Machine Details** view, select **View Historical Utilization**.
2. In the **Historical Machine Utilization** page, set **Time Period** to view usage for the last 2 hours, 24 hours, 7 days, month, or year.

   > **Note:**
   >
   > Average IOPS and disk latency usage data are available only for the last 24 hours, month, and year ending now. Custom end time is not supported.

3. Click **Apply** and select the required graphs.
4. Hover over different sections of the graph to view more information for the selected time period.



For example, if you select **Last 2 hours**, the baseline period is the 2 hours prior to the selected time range. View the CPU, memory, and session trend over the last 2 hours and the baseline time. If you select **Last month**, the baseline period is the previous month. Select to view the Average IOPS and disk latency over the last month and the baseline time.

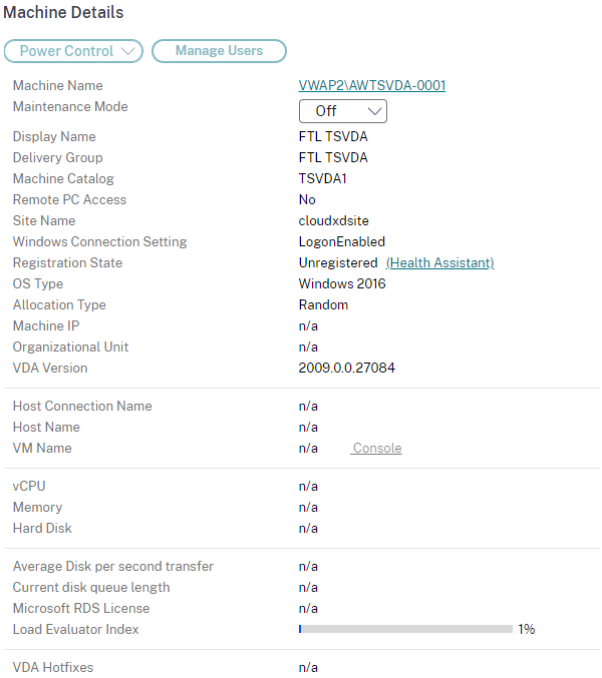
1. Click **Export** to export the resource utilization data for the selected period. For more information, see Export reports section in Monitor Deployments.
2. Below the graphs, the table lists the top 10 processes based on CPU or memory utilization. You can sort by any of the columns, which show Application Name, User Name, Session ID, Average CPU, Peak CPU, Average Memory, and Peak Memory over the selected time range. The IOPS and Disk Latency columns cannot be sorted.

   > **Note:**
   >
   > - The session ID for system processes is displayed as "0000".
   > - If a site that belongs to the Citrix Cloud Japan or the Citrix Cloud Government plane contains more than 5000 machines, process data is available for up to 2000 machines only. The Process Monitoring policy must be enabled on these machines.

3. To view the historical trend on the resource consumption of a particular process, drill into any of the Top 10 processes.

Machine Console access

You can access the consoles of Desktop and Multi-session OS machines hosted on XenServer Version 7.3 and later directly from Monitor. This way, you don't require XenCenter to troubleshoot issues on XenServer hosted VDAs. For this feature to be available, the XenServer hosting the machine must be of Version 7.3 or later and must be accessible from the Monitor.



To troubleshoot a machine, click the **Console** link in the corresponding Machine Details panel. After authentication of the host credentials you provide, the machine console opens in a separate tab using noVNC, a web-based VNC client. You now have keyboard and mouse access the console.

> **Note:**
>
> - This feature is not supported on Internet Explorer 11.
> - If the mouse pointer on the machine console is misaligned, see CTX230727 for steps to fix the issue.
> - Console access is launched on a new tab, ensure that your browser settings allow pop-ups.
> - For security reasons, Citrix recommends that you install SSL certificates on your browser.

Inspect machines with recent power actions

You can now inspect machines with the status of the success and failed power actions. This feature helps you to analyze the following:

- Power on failure which causes user issues
- Power off failure which increases cost

> **Note:**
>
> Data is available only for the power-managed machine. Data isn't available for the power actions taken before the feature was supported.

You can view the power action status of the machines using the following ways:

From **Filters** -> **Machines** tab. In this case, by default the **Power Action Time** and the **Power Action Result** columns are visible. You can also select the columns that you want to visible.

From **Cost Optimization** tab. In this case, the default filter is **Power Action Triggered By** is set to *Autoscale* and the **Power Action Result** is set to *Failed*.

With this feature, you can view the details of the power action controls. For example, you can view who triggered the action, which action changed the power state, the reason for failure, and the time when the action is completed. You can also export these details.

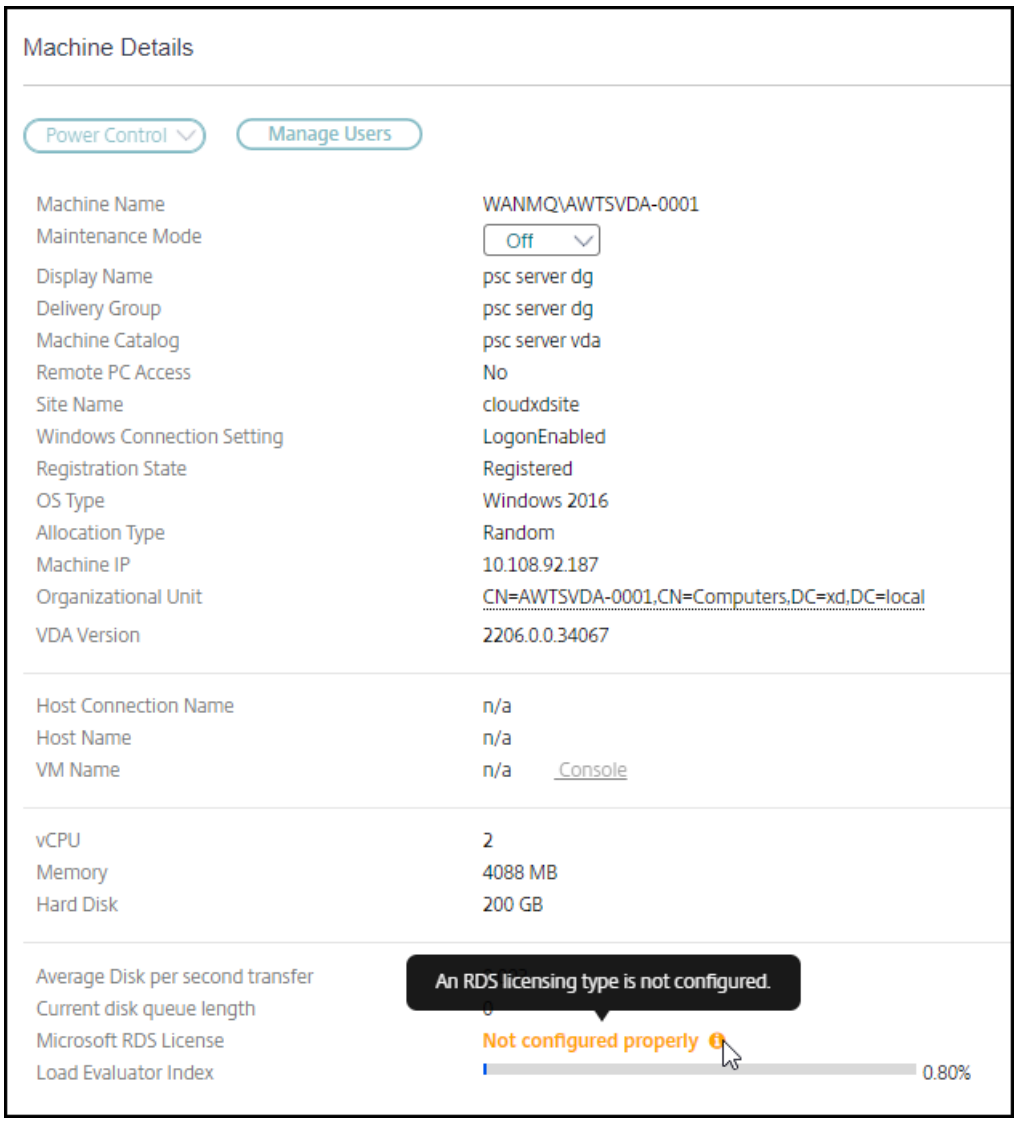
The following filters are added to view the power action status:

Filter	Description
Power Action Result	Displays the result of the power action. The possible filter values are success and failed.
Power Action Triggered By	Displays who or what triggered the power action. The possible filter values are the following • Autoscale - This value appears when a power action is triggered by the following • When admin shut-down a VM to clean the VM's OS disk back to its initial state • When a VM is shut down or suspended based on the set policies • When a VM is made available based on the pool size or buffer size configuration • Admin - This value appears when a power action is triggered by an admin. The possible examples are when admin requests for turn off, turn on, suspend, resume, restart, or reboot a VM. • User - This value appears when a power action is triggered by a user. The examples are when a user resets, turn on, or resume work on the VM. • Others - This value appears when power action is triggered by scheduled and by unknown reasons.
Last Power Action	Displays the exact power action happened on the machine such as power-on, power off, shut down, restart, reset, resume, and so on

Filter	Description
Power Action Time	The time when the power action is completed. The possible filter values are last minute, last 5 minutes, last 30 minutes, last hour, today, last 24 hours, and yesterday.
Power Action Failure Reason	Displays the reason for failure. The possible filter values are hypervisor reported failure, hypervisor rate limit exceeded, unknown error, and none. If there is a successful action, it shows "None".

Microsoft RDS license health

You can view the status of Microsoft RDS license in the Machine Details panel in the **Machine Details** and the **User Details** page for Multi-session OS machines.



One of the following messages is displayed:

- License available
- Not configured properly (warning)
- License error (error)
- Incompatible VDA version (error)

> **Note:**
>
> The Microsoft RDS license health status for machines under grace period with valid license displays a **License available** message in green. Renew your license before they expire.

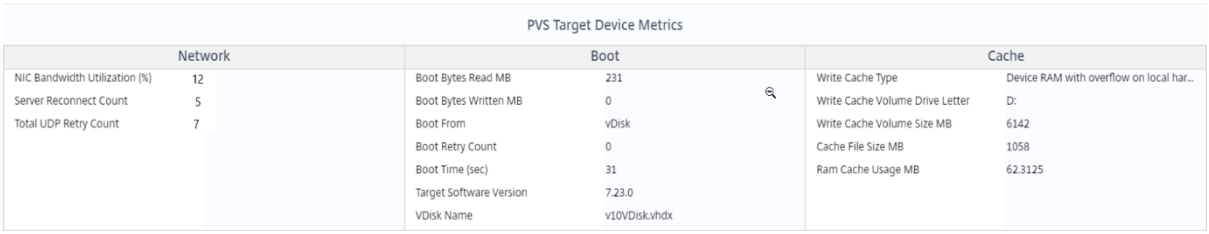
For warning and error messages, hover over the info icon to view additional information as given in the following table.

Message Type	Messages in Monitor
Error	Available for VDAs version 7.16 and later.
Error	New RDS connections are not allowed.
Error	Microsoft RDS license has exceeded its grace period.
Error	A License Server is not configured for the required OS level with the Per Device Client Access licensing type.
Error	The configured License Server is incompatible with the RDS Host OS level with the Per Device Client Access licensing type.
Warning	Personal Terminal Server is not a valid RDS licensing type in a Citrix Virtual Apps and Desktops deployment.
Warning	Remote Desktop for Administration is not a valid licensing type in a Citrix Virtual Apps and Desktops deployment.
Warning	An RDS licensing type is not configured.
Warning	The Domain Controller or License Server is unreachable with the Per User Client Access RDS licensing type.
Warning	With the Per Device Client Access licensing type, the Client Device license could not be determined since the license server for the required OS level is unreachable.

> **Note:**
>
> This feature is applicable only for Microsoft RDS CAL (Client Access License).

PVS target device metrics

You can view the status of PVS target devices for single-session and multi-session OS machines on the **Machine Details** page in Monitor. Several metrics for **Network**, **Boot**, and **Cache** are available on this panel. These metrics help you monitor and troubleshoot PVS target devices to ensure that they are up and running.



Network:

- Network Bandwidth Utilization: Average bandwidth utilization across all NICs.
- Server Reconnect Count: Number of times the server has reconnected due to network issues or server rebalancing or shutdowns and restarts of the Citrix Provisioning Stream Service.
- Total UDP Retry Count: Number of times the provisioning target device has tried to reconnect to the provisioning server using UDP. This metric helps you to know if there are any network issues in the Citrix Provisioning Stream Service (for example, bad switch configurations).

Boot:

- Boot Bytes Read MB: Bytes read while booting.
- Boot Byes Written MB: Bytes written while booting.
- Boot From: Boot medium (vDisk, local disk, and so on).
- Boot Retry Count: Number of retries to boot the machine.
- Boot Time: Time taken to boot the machine, in seconds. By default, there is a 5 second delay between retries. If this delay grows into double digits, there is a significant increase in boot time. Check your provisioning configuration to resolve this issue.
- Target Software Version: Version of the Provisioning target device software.
- vDisk Name: vDisk from which the Provisioning target device is booting.

Cache:

- Write Cache Type: vDisk can be set to different types of cache. For more information, see Knowledge Center article CTX119469.
- Write Cache Volume Drive Letter: Drive letter for write cache types involving drives.
- Write Cache Volume Size MB: Total configured volume size for write cache.
- Cache File Size MB: Current cache file size (cache on device RAM with overflow on hard disk).
- Ram Cache Usage MB: Current RAM cache size (cache on device RAM with overflow on hard disk). Use Overflow to disk only if necessary. This metric is useful when setting or optimizing the proper size of RAM cache.

For more information, see Using the Status Tray on a target device.

Provisioning target device metrics is available only on:

- Provisioning machines.
- Provisioning target device version 7.19 and later.
- VDA version 2003 and later.

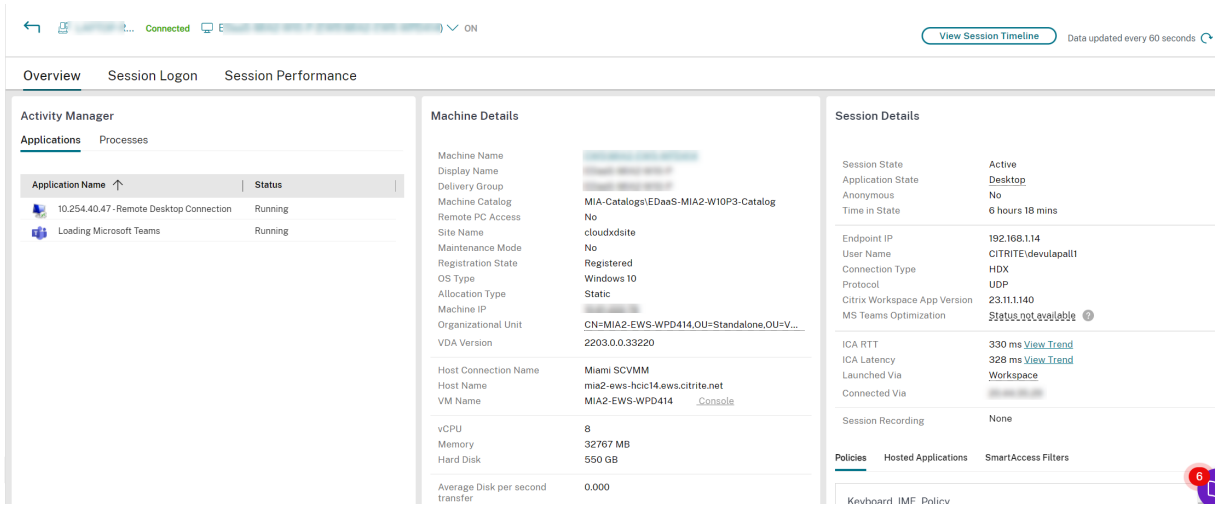
> **Note:**
>
> Metrics for Server Reconnect Count and UDP Retry Count are available only for Provisioning target version 1912 CU2 and later.

Troubleshoot user issues

April 30, 2024

Use the Monitor's **Help Desk** view (**Activity Manager** page) to view information about the user or endpoint.

Clicking **View Details** from the Activity Manager for User opens the **User Details** page.
Clicking **View Details** from the Activity Manager for Endpoint opens the **Endpoint Details** page.



If the user had started more than one session, the session selector is displayed.

Choose a session to view the details.

- Check details about the session, user's sign in experience, session startup, connection, and applications.
- you can Shadow the user's machine.
- Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

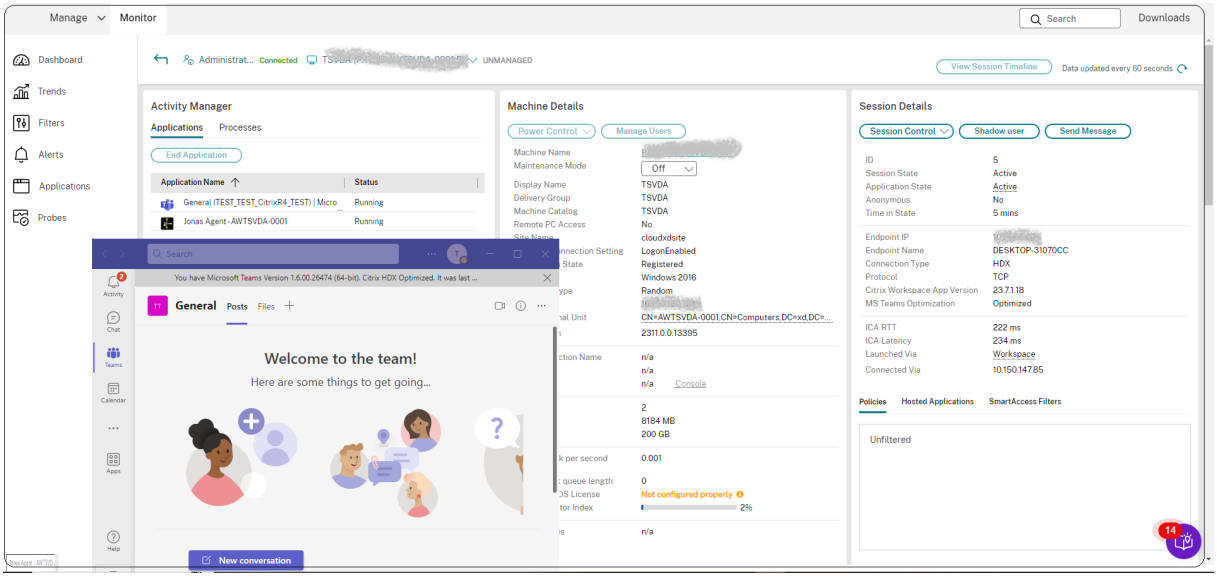
Microsoft Teams optimization status

Citrix Monitor displays the Microsoft Teams optimization status for HDX sessions in the **User Details** page > **Session Details** panel > **MS Teams Optimization** field. Microsoft Teams being optimized is critical for the better user experience such as clear audio and video. Visibility of the Microsoft Teams optimization status is useful in reducing the time required to resolve tickets and helps administrators identify important metrics during troubleshooting.

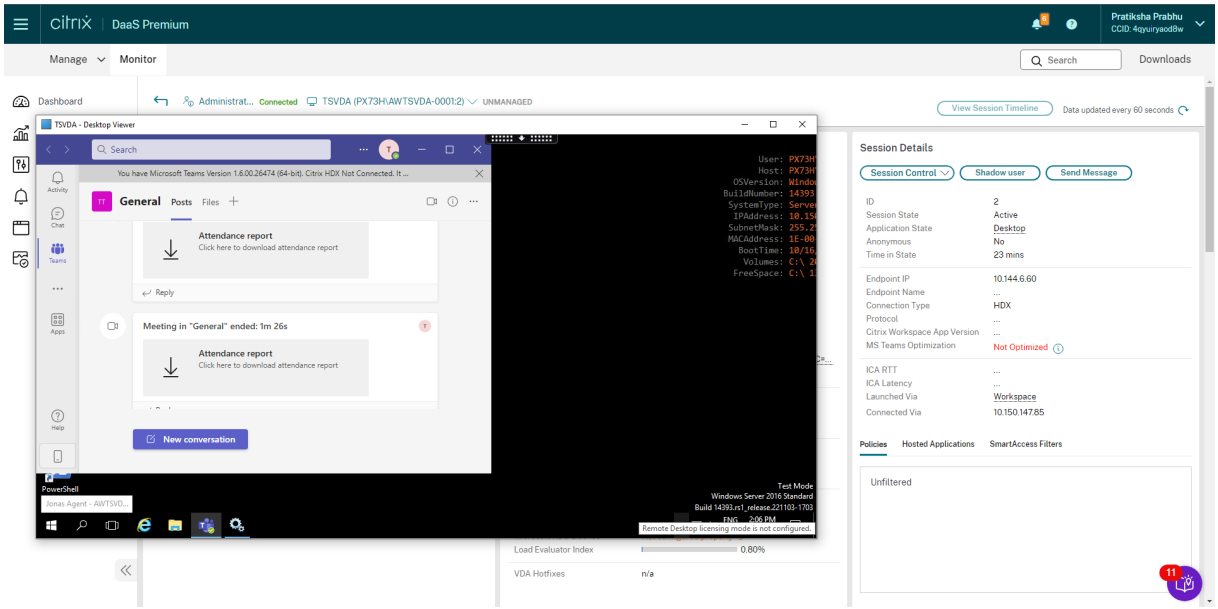
> **Note:**
>
> Citrix Monitor supports Microsoft Teams version 2.1 or earlier.

Prerequisites:

- Citrix Workspace app versions supported are listed in Optimization for Microsoft Teams.
- Microsoft Teams runs as a published app or inside a published desktop.
- Crucial services such as the Citrix HDX HTML5 Video Redirection Service, are running.



If the Microsoft Teams isn't optimized, the tooltip provides a link to an external troubleshooting live article from HDX containing tips to optimize Microsoft Teams. Troubleshooting HDX Optimization.



Troubleshooting tips

User issue	Suggestions
Logon takes a long time or fails intermittently or repeatedly	Diagnose user logon issues
Session startup takes a long time or fails intermittently or repeatedly	Diagnose session startup issues

User issue	Suggestions
Identify the components involved in establishing the session	Analyze the Session Topology view
Session response is slow or not responding	Diagnose session performance issues
Application is slow or not responding	Resolve application failures
Connection failed	Restore desktop connections
Session is slow or not responding	Restore sessions
Video is slow or poor quality	Run HDX channel system reports

> **Note:**
>
> To make sure that the machine is not in maintenance mode, from the User Details view, review the Machine Details panel.

Session Performance

The **Session Performance** tab has enhanced troubleshooting workflows starting with the ability to correlate real-time metrics in identifying issues within user sessions. The **Session Topology** panel provides a visual representation of the in-session path for connected HDX sessions. The **Performance Metrics** panel provides trends for the session metrics like ICARTT, ICA Latency, Frames Per Second, Output Bandwidth Available, and Output Bandwidth Consumed help indicate how these metrics have performed over time. For more information, see Diagnose session performance issues.

Search tips

Search for username is conducted across all configured Active Directories.

When you type a multiuser machine name in a Search field, the Machine Details for the specified machine are displayed.

When you type an endpoint name in a Search field, the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint are listed. This list enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

The search results also include users who aren't currently using or assigned to a machine.

- Searches aren't case-sensitive.
- Partial entries produce a list of possible matches.

- After you type a few letters of a two-part name, separated by a space, the results include matches for both strings. The examples for two-part names are user name, family name and first name, or display name. For example, if you type "jo rob", the results might include strings such as "John Robertson"or "Robert Jones".

To return to the landing page, click the **Monitor** tab.

Diagnose session startup issues

February 7, 2024

In addition to the logon process phases mentioned in the Diagnose user logon issues section, Monitor displays the session startup duration. This duration is divided into the Workspace App Session Startup duration and the VDA Session Startup duration on the **User Details** and **Endpoint Details** pages. These two durations further contain individual phases whose startup durations are also displayed. This data helps you to understand and troubleshoot high session startup duration. Further, the time duration for each phase involved in the session startup helps in troubleshooting issues associated with individual phases. For example, if the Drive Mapping time is high, you can check to see whether all the valid drives are mapped correctly in the GPO or script.

Prerequisites

Ensure that the following prerequisites are met for session startup duration data to be displayed:

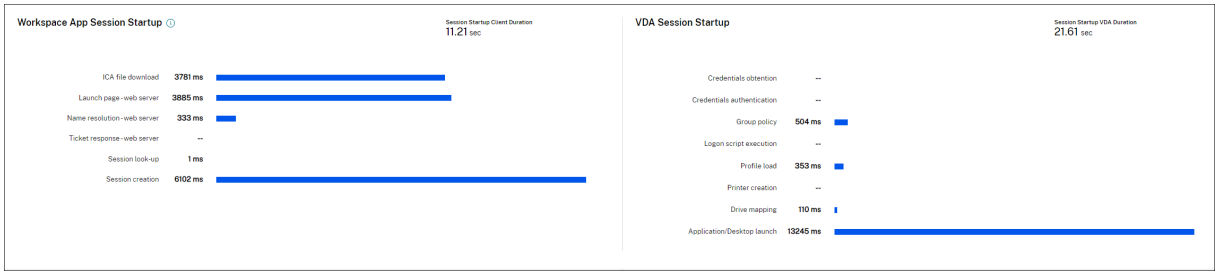
- VDA 1903 or later.
- Citrix End User Experience Monitoring (EUEM) service must be running on the VDA.

Limitations

The following limitations apply when Monitor displays the session startup duration data:

- Session startup duration is available only for HDX sessions.
- For session launches from iOS and Android OS, only VDA Startup Duration is available.
- IFDCD is available only when Workspace App is detected while launching from a browser.
- For session launches from macOS, IFDCD is available for Workspace App 1902 and later only.
- For session launches from Windows OS, IFDCD is available for Workspace app 1902 and later. For earlier versions, IFDCD is displayed for only app launches from a browser with Workspace app detected.

> **Notes:**
>
> - If you face issues in the sessions startup duration display after the prerequisites are met, view the Monitor server and VDA logs as described in CTX130320.
>
> For shared sessions (multiple applications launched in the same session), the Workspace App Startup metrics are displayed for the latest connection or the latest application launch.
> - Some metrics in VDA Session Startup are not applicable on reconnects. In such cases, a message is displayed.



Workspace App session startup phases

Session Startup Client Duration (SSCD)

When this metric is high, it indicates a client-side issue that is causing long start times. Review subsequent metrics to determine the probable root cause of the issue. SSCD starts as close as possible to the time of the request (mouse click) and ends when the ICA connection between the client device and VDA has been established. For a shared session, this duration is much smaller, as much of the setup costs associated with the creation of a new connection to the server are not incurred. At the next level down, there are several detailed metrics available.

ICA File Download Duration (IFDCD)

IFDCD is the time taken for the client to download the ICA file from the server. The overall process is as follows:

1. The user clicks a resource (application or desktop) on the Workspace Application.
2. A request from the user is sent to StoreFront through the Citrix Gateway (if configured), which sends the request to the Delivery Controller.
3. The Delivery Controller finds an available machine for the request and sends the machine information and other details to StoreFront. Also, StoreFront requests and receives a one-time ticket from the Secure Ticket Authority.
4. StoreFront generates an ICA File and sends it to the user via Citrix Gateway (if configured).

IFDCD represents the time it takes for the complete process (steps 1–4). The IFDCD duration stops counting when the client receives the ICA file.

LPWD is the StoreFront component of the process.

If IFDCD is high (but LPWD is normal), the server-side processing of the launch was successful, but there were communication issues between the client device and the StoreFront. This results from network issues between the two machines. So you can troubleshoot potential network issues first.

Launch Page Web Server Duration (LPWD)

This is the time taken to process the launch page (launch.aspx) on the StoreFront. If LPWD is high, there might be a bottleneck on the StoreFront.

Possible causes include:

- High load on the StoreFront. Try to identify the cause of slowdown by checking the Internet Information Services (IIS) logs and monitoring tools, Task Manager, Performance Monitor and so on.
- StoreFront is having issues communicating with other components such as Delivery Controller. Check if the network connection between StoreFront and Delivery Controller is slow or some Delivery Controllers are down or overloaded.

Name Resolution Web Server Duration (NRWD)

This is the time taken by the Delivery Controller to resolve the name of a published application/desktop to a VDA Machine IP Address.

When this metric is high, it indicates that the Delivery Controller is taking a long time to resolve the name of a published application to an IP address. Possible causes include:

- a problem on the client
- issues with the Delivery Controller, such as the Delivery Controller being overloaded, or a problem with the network link between them

Ticket Response Web Server Duration (TRWD)

This duration indicates the time it takes to get a ticket (if necessary) from the Secure Ticket Authority (STA) Server or Delivery Controller. When this duration is high, it indicates that the STA server or the Delivery Controller are overloaded.

Session Look-up Client Duration (SLCD)

This duration represents the time taken to query every session to host the requested published application. The check is performed on the client to determine whether an existing session can handle the application launch request. The method used depends on whether the session is new or shared.

Session Creation Client Duration (SCCD)

This duration represents the time taken to create a session, from the moment wfica32.exe (or a similar equivalent file) is launched to the time when the connection is established.

VDA session startup phases

Session Startup VDA Duration (SSVD)

This duration is the high-level server-side connection start-up metric that indicates the time VDA takes to perform the entire start-up operation. When this metric is high, it indicates that there is a VDA issue increasing session start times. This includes the time spent on the VDA performing the entire start-up operation.

Credentials Obtention VDA Duration (COVD)

The time taken for the VDA to obtain the user credentials.

This duration can be artificially inflated if a user fails to provide credentials in a timely manner, and thus, not included in the VDA Startup Duration. This time is likely to be a significant only if manual login is being used and the server side credentials dialog is displayed (or if a legal notice is displayed before login commences).

Credentials Authentication VDA Duration (CAVD)

This is the time taken by the VDA to authenticate the user's credentials against the authentication provider, which can be Kerberos, Active Directory, or a Security Support Provider Interface (SSPI).

Group Policy VDA Duration (GPVD)

This duration is the time taken to apply group policy objects during logon.

Login Script Execution VDA Duration (LSVD)

This is the time taken by the VDA to run the user's login scripts.

You can make the user or group's login scripts asynchronous. Optimize any application compatibility scripts or use environment variables instead.

Profile Load VDA Duration (PLVD)

This is the time taken by the VDA to load the user's profile.

If this duration is high, review your User Profile configuration. Roaming profile size and location contribute to slow session starts. When a user logs on to a session where Terminal Services roaming profiles and home folders are enabled, the roaming profile contents and access to that folder are mapped during logon, which takes extra resources. Sometimes, this can consume significant amount of the CPU usage. Use the **Terminal Services home** folders with redirected personal folders to mitigate this problem. In general, use Citrix Profile Management to manage user profiles in Citrix environments. If you are using Citrix Profile Management and have slow logon times, check if your antivirus software is blocking the Citrix Profile Management tool.

Printer Creation VDA Duration (PCVD)

This is the time taken for the VDA to map the user's client printers synchronously. If the configuration is set for printer creation to be performed asynchronously, no value is recorded for PCVD as it does not impact completion of the session startup.

Excessive time spent in mapping printers is often the result of the printer auto creation policy settings. The number of printers added locally on the users' client devices and your printing configuration can directly affect your session start times. When a session starts, Citrix Virtual Apps and Desktops have to create every locally mapped printer on the client device. Reconfigure your printing policies to reduce the number of printers that get created, specifically when users have many local printers. To do this, edit the Printer Auto creation policy in Delivery Controller and Citrix Virtual Apps and Desktops.

Drive Mapping VDA Duration (DMVD)

This is the time taken by the VDA to map the user's client drives, devices, and ports.

Ensure that your base policies include settings to disable unused virtual channels, such as audio or COM port mapping, to optimize the ICA protocol and improve overall session performance.

Application/Desktop Launch VDA Duration (ALVD/DLVD)

This phase is a combination of userinit and Shell duration. When a user logs on to a Windows machine, Winlogon runs userinit.exe. Usernit.exe runs logon scripts, re-establishes network connections, and then starts explorer.exe, the Windows User interface. userinit represents the duration between the start of userinit.exe to the start of the user interface for the virtual desktop or application. The Shell duration is the time between the initialization of the user interface to the time the user receives keyboard and mouse control.

Session Creation VDA Duration (SCVD)

This time includes miscellaneous delays in session creation on VDA.

Diagnose user logon issues

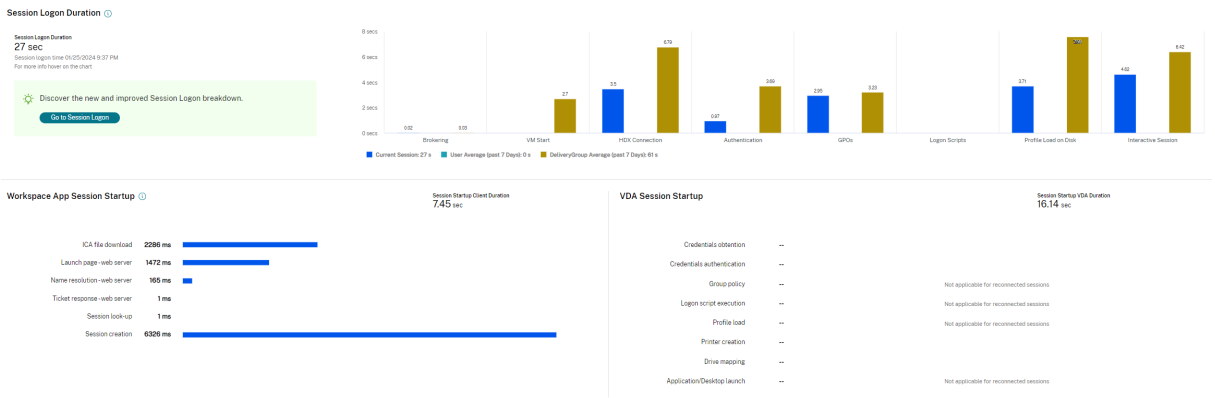
June 14, 2024

Use Logon Duration data to troubleshoot user logon issues.

Logon duration is measured only for initial connections to a desktop or app using HDX. This data does not include users trying to connect with Remote Desktop Protocol or reconnect from disconnected sessions. Specifically, logon duration is not measured when a user initially connects using a non-HDX protocol and reconnects using HDX.

In the User Details view, the duration is displayed as a number value below which the time the logon occurred is displayed and a graph of the phases of the logon process.

As users logon to Citrix Virtual Apps and Desktops, the Monitor Service tracks the phases of the logon process from the time the user connects from Citrix Workspace app to the time when the desktop is ready to use.



The large number on the left is the total logon time and is calculated by combining the time spent establishing the connection and obtaining a desktop from the Delivery Controller with the time spent to authenticate and log on to a virtual desktop. The duration information is presented in seconds (or fractions of seconds).

Prerequisites

Ensure that the following prerequisites are met for logon duration data and drilldowns to appear:

1. Install **Citrix User Profile Manager** and **Citrix User Profile Manager WMI Plugin** on the VDA.
2. Ensure that the Citrix Profile Management Service is running.
3. For XenApp and XenDesktop sites 7.15 and earlier, disable the GPO setting, **Do not process the legacy run list**.
4. Audit process tracking must be enabled for Interactive Session drilldown.
5. For GPO drilldown, increase the size of Group Policy operational logs.

> **Note:**
>
> Logon duration is supported only on the default Windows shell (explorer.exe) and not on custom shells.

Steps to troubleshoot user logon issues

1. From the **User Details** view, troubleshoot the logon state using the Logon Duration panel.
    - If the user is logging on, the view reflects the process of logging on.
    - If the user is logged on, the Logon Duration panel displays the time it took for the user to log on to the current session.
2. Examine the phases of the logon process.

Logon process phases

Brokering

Time taken to decide which desktop to assign to the user.

Machine Start-up

If the session required a machine start, this is the time taken to start the virtual machine. The following sub-section provides breakdown of the time taken to start a virtual machine during different phases:

- Power On - Displays the time taken to power on a virtual machine
- Boot-up and registration - Displays the time taken to boot up and register a virtual machine

You can use the collapsible button to collapse or expand the options under the **Machine Start-up**.

HDX connection

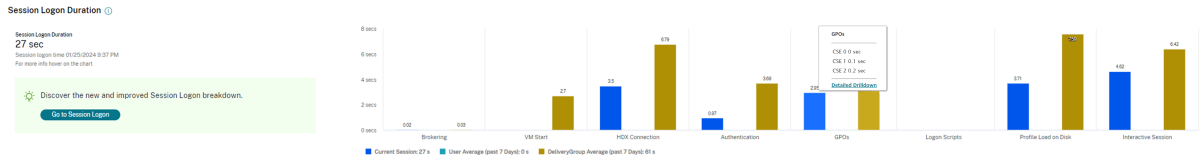
Time taken to complete the steps required in setting up the HDX connection from the client to the virtual machine.

Authentication

Time taken to complete authentication to the remote session.

GPOs

If Group Policy settings are enabled on the virtual machines, this is the time taken to apply group policy objects during logon. The drill-down of the time taken to apply each policy as per the CSEs (Clients-Side Extension) is available as a tooltip when you hover on the GPO bar.



Click **Detailed Drilldown** to see a table with the policy status, and the corresponding GPO name. The time durations in the drilldown represent the CSE processing time only and do not add up to the total GPO time. You can copy the drill-down table for further troubleshooting or use in reports. The GPO time for the policies is retrieved from Event Viewer logs. The logs can get overwritten depending on the memory allocated for the operational logs (default size is 4 MB). For more information about increasing the log size for the operational logs, see the Microsoft TechNet article https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10).

Logon scripts

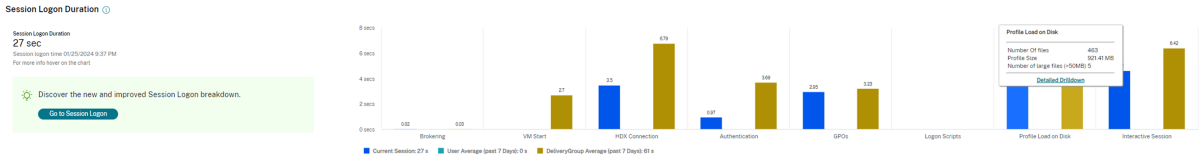
If logon scripts are configured for the session, this is the time taken for the logon scripts to be run.

Profile load

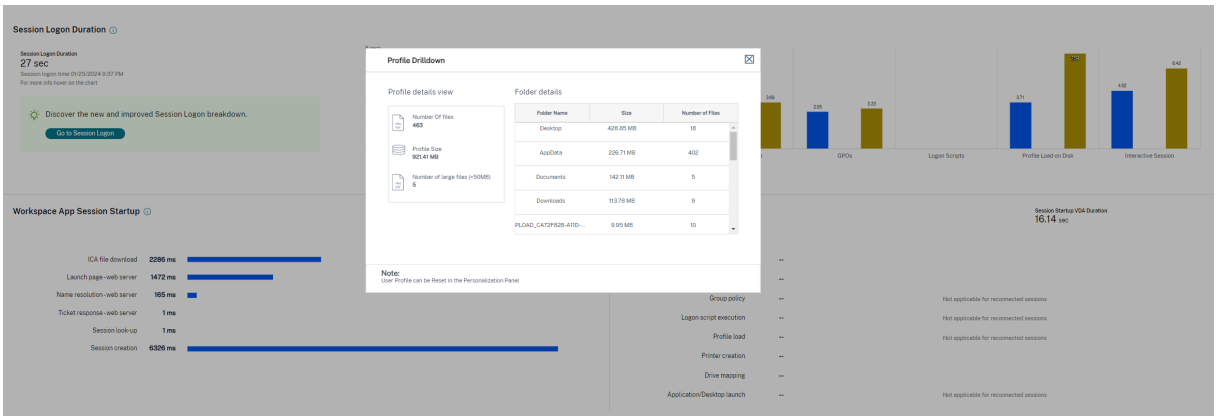
If profile settings are configured for the user or the virtual machine, this is the time taken for the profile to load.

If Citrix Profile Management is configured, the Profile Load bar includes the time taken by Citrix Profile Management to process user profiles. This information helps administrators to troubleshoot high profile processing duration issues. When Profile Management is configured, the Profile Load bar displays an increased duration. This increase is caused by this enhancement and does not reflect a performance degradation. This enhancement is available on VDAs 1903 and later.

Hovering over the Profile Load bar displays a tooltip showing the user profile details for the current session. This additional information can help troubleshoot high profile load issues.



Click **Detailed Drilldown** to drilldown further into each individual folder in the profile root folder (for instance, C:/Users/username), its size, and the number of files (including files inside nested folders).



Profile drilldown is available on VDAs 1811 and later. Using the profile drilldown information, you can resolve issues involving a high profile load time. You can:

- Reset the user profile
- Optimize the profile by removing unwanted large files
- Reduce the number of files to reduce the network load
- Use profile streaming

By default, all folder names are visible. To hide the folder names, edit the registry values on the VDA machine using the following steps:

> **Warning:**
>
> Adding and editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix does not guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure

> to back up the registry before you edit it.

1. On the VDA, add a new registry value **ProfileFoldersNameHidden** at HKEY_LOCAL_MACHINE\Software\Citrix
2. Set the value to 1. This value must be a DWORD (32-bit) value. Folder names visibility is now disabled.
3. To make the folder names visible again, set the value to 0.

> **Note:**
>
> You can use GPO or PowerShell to apply the registry value change on multiple machines. For more information about using GPO to deploy registry changes, see the blog.

Additional information

- Profile drilldown does not consider redirected folders.
- NTUser.dat files in the root folder might not be visible to end users. However, they are included in the profile drilldown and displayed in the list of files in **Root Folder**.
- There are some hidden files in AppData folder which are not included in profile drilldown.
- Number of files and profile size data might not match with the data in the Personalization panel due to certain Windows limitations.

Interactive Session

This is the time taken to "hand off" keyboard and mouse control to the user after the user profile has been loaded. It is normally the longest duration out of all the phases of the logon process and is calculated as **Interactive Session duration = Desktop Ready Event Timestamp (EventId 1000 on VDA) - User Profile Loaded Event Timestamp (EventId 2 on VDA)**. Interactive Session has three subphases: Pre-userinit, Userinit, and Shell. Hover over the Interactive Session to see a tooltip showing the following:

- subphases
- the time taken for each subphase
- the total cumulative time delay between these subphases

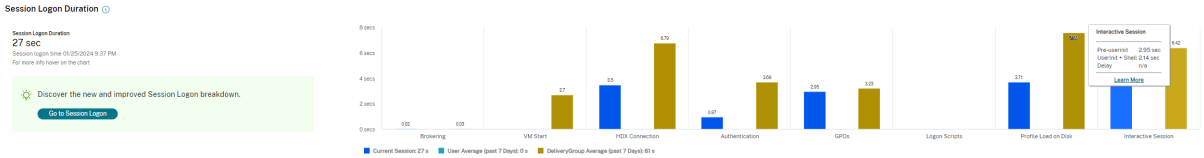
You can use the collapsible button to collapse or expand the options under the Interactive Session.

> **Note:**
>
> This feature is available on VDAs 1811 and later. If you have launched sessions on sites earlier than 7.18 and then upgraded to 7.18, a 'Drilldown unavailable due to server error' message is displayed. However, if you have launched sessions after an upgrade, no error message is displayed.

To view the time duration of each subphase, enable Audit process tracking on the VM (VDA). When the Audit process tracking is disabled (default), the time duration of Pre-userinit and the combined time duration of Userinit and Shell are displayed. You can enable Audit process tracking through a Group Policy Object (GPO) as follows:

1. Create a GPO and edit it using the GPO editor.
2. Go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy**.
3. On the right pane, double-click **Audit process tracking**.
4. Select **Success** and click OK.
5. Apply this GPO to the required VDAs or Group.

For more information about Audit process tracking and enabling or disabling it, see https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10) in the Microsoft documentation.



Logon Duration panel in the User Details view.

- **Interactive Session –Pre-userinit:** This is the segment of Interactive Session which overlaps with Group Policy Objects and scripts. This subphase can be reduced by optimizing the GPOs and scripts.
- **Interactive Session –Userinit:** When a user logs on to a Windows machine, Winlogon runs userinit.exe. Userinit.exe runs logon scripts, re-establishes network connections, and then starts Explorer.exe, the Windows user interface. This subphase of Interactive Session represents the duration between the start of Userinit.exe to the start of the user interface for the virtual desktop or application.
- **Interactive Session –Shell:** In the previous phase, Userinit starts the initialization of Windows user interface. The Shell subphase captures the duration between the initialization of the user interface to the time user receives keyboard and mouse control.
- **Delay:** This is the cumulative time delay between the **Pre-userinit and Userinit** subphases and the **Userinit and Shell** subphases.

The total logon time is not an exact sum of these phases. For example, some phases occur in parallel, and in some phases, extra processing occurs that can result in a longer logon duration than the sum. The total logon time does not include the ICA idle time that is the time between the ICA file download and the ICA file launch for an application.
To enable the automatic opening of ICA file upon application launch, configure your browser for automatic ICA file launch upon download of an ICA file. For more information, see CTX804493.

> **Note:**
>
> The Logon Duration graph shows the logon phases in seconds. Any duration values below one second are displayed as subsecond values. The values above one second are rounded to the nearest 0.5 second. The graph has been designed to show the highest y-axis value as 200 seconds. Any value greater than 200 seconds is shown with the actual value displayed above the bar.

Export data

Along with the default Logon Duration Phases table options, which is Session Logon Phase and Duration, you can also choose the following columns on the Session Logon page:

- Start time
- End time
- Delivery Group - 7d Avg (sec)
- User - 7d Avg (sec)

You can also export the preceding data to a .CSV file.

Troubleshooting tips

To identify unusual or unexpected values in the graph, compare the amount of time taken in each phase of the current session with the average duration for this user for the last seven days, and the average duration for all users in this delivery group for the last seven days.

Escalate as needed. For example, if the **Machine Start-up** is slow, the issue might be in the hypervisor, so you can escalate it to the hypervisor administrator. Or, if the brokering time is slow, you can escalate the issue to the site administrator to check the load balancing on the Delivery Controller.

Examine unusual differences, including:

- Missing (current) logon bars
- Major discrepancy between the current duration and this user's average duration. Causes include:
  - A new application was installed.
  - An operating system update occurred.
  - Configuration changes were made.
  - Profile size of the user is high. In this case, the Profile Load is high.
- Major discrepancy between the user's log on numbers (current and average duration) and the delivery group average duration.

If needed, click **Restart** to observe the user's logon process to troubleshoot issues, such as Machine Start-up or Brokering.

Shadow users

November 9, 2022

Use the shadow user feature to view or work directly on a user's virtual machine or session. You can shadow both Windows or and Linux VDAs. The user must be connected to the machine that you want to shadow. Verify this by checking the machine name listed in the user title bar.

Shadowing is launched in a new tab, update your browser settings to allow pop-ups from the Citrix Cloud URL.

Access the shadowing feature from the **User Details** view. Select the user session, and click **Shadow** in the Activity Manager view or the Session Details panel.

Shadowing Linux VDAs

Shadowing is available for Linux VDAs Version 7.16 or and later running the RHEL7.3 or Ubuntu Version 16.04 Linux distributions.

> **Note:**
>
> - Monitor uses FQDN to connect to the target Linux VDA. Ensure that the Monitor client can resolve the FQDN of the Linux VDA.
> - The VDA must have the python-websockify and x11vnc packages installed.
> - noVNC connection to the VDA uses the WebSocket protocol. By default, **ws://** WebSocket protocol is used. For security reasons, Citrix recommends that you use the secure **wss://** protocol. Install SSL certificates on each Monitor client and Linux VDA.

Follow the instructions in Session Shadowing to configure your VDA for shadowing.

1. After you click **Shadow**, the shadowing connection initializes and a confirmation prompt appears on the user device.
2. Instruct the user to click **Yes** to start the machine or session sharing.
3. The administrator can only view the shadowed session.

Shadowing Windows VDAs

Windows VDA sessions are shadowed using Windows Remote Assistance. Enable User Windows Remote Assistance feature while installing the VDA. For more information, see Enable or Disable features.

1. After you click **Shadow**, the shadowing connection initializes and a dialog box prompts you to open or save the .msrc incident file.

2. Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
3. Instruct the user to click **Yes** to start the machine or session sharing.
4. For more control, ask the user to share keyboard and mouse control.

Streamline Microsoft Internet Explorer browsers for shadowing

Configure your Microsoft Internet Explorer browser to automatically open the downloaded Microsoft Remote Assistance (.msra) file with the Remote Assistance client.

To do this, you must enable the Automatic prompting for file downloads setting in the Group Policy editor:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Automatic prompting for file downloads.

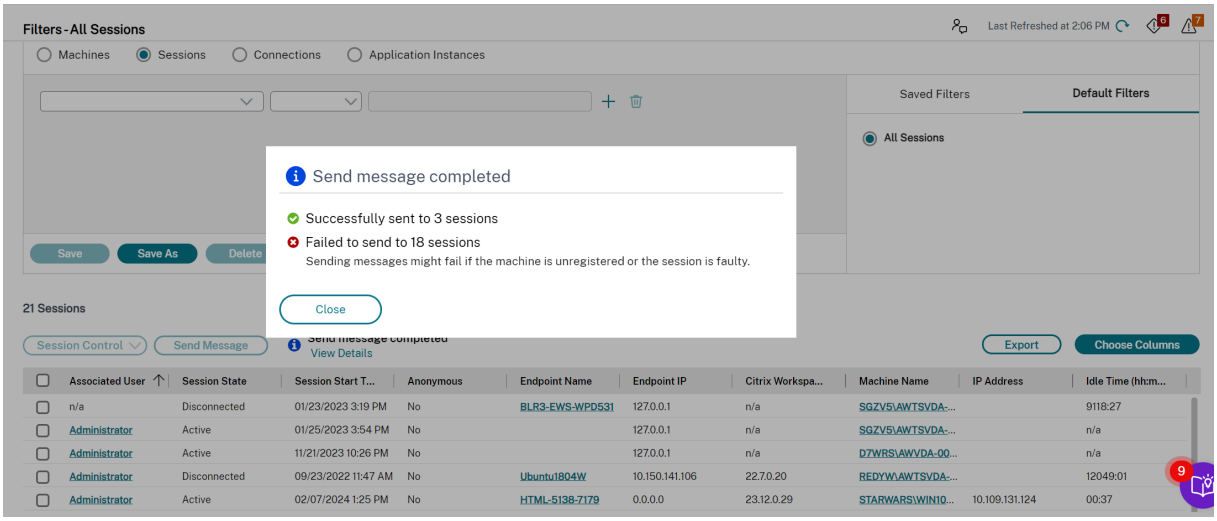
Send messages to users

December 21, 2023

From Monitor, send a message to a user who is connected to one or more machines. For example, use this feature to send immediate notices about administrative actions such as impending desktop maintenance, machine logoffs and restarts, and profile resets.

To send a message to a user, follow these steps:

1. Go to **Monitor** > **Filters** > **Machines** > **All Machines**.
2. Select a machine to which you want to send a message and click **Send Message**.
3. Type your message and click **Send**.



Sending messages can fail if the machines are unregistered or if the sessions are faulty.

If the message is sent successfully, a confirmation message appears. If the user's machine is connected, the message appears there.

If the message is not sent successfully, an error message appears. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click **Try again**.

If you choose to send bulk messages to all connected sessions, the progress of the operation is displayed in percentage. Once the operation is completed, the number of messages that were successfully sent and the number that have failed are displayed. Send message status is specifically helpful when you are administering large sites. It helps understand if the message needs to be resent to certain users.

Resolve application failures

February 8, 2023

In the **Activity Manager** view, click the **Applications** tab. You can view all the applications on all machines to which this user has access, including local and hosted applications for the currently connected machine, and the status of each.

The list includes only those applications that were launched within the session.

For Multi-session OS machines and Single session OS machines, applications are listed for each disconnected session. If the user is not connected, no applications are displayed.

Action	Description
End the application that is not responding	Choose the application that is not responding and click **End Application**. Once the application is terminated, ask the user to launch it again.
End processes that are not responding	If you have the required permission, click the **Processes** tab. Select a process that is related to the application or using a high amount of CPU resources or memory, and click **End Process**. However, if you do not have the required permission to terminate the process, attempting to end a process fails.
Restart the user's machine	For Single session OS machines only, for the selected session, click **Restart**. Alternatively, from the Machine Details view, use the power controls to restart or shut down the machine. Instruct the user to log on again so that you can recheck the application. For Multi-session OS machines, the restart option is not available. Instead, log off from the user and let the user log on again.
Put the machine into maintenance mode	If the machine's image needs maintenance, such as a patch or other updates, put the machine into maintenance mode. From the Machine Details view, click **Details** and turn on the maintenance mode option. Escalate to the appropriate administrator.

Disable the visibility of running applications

By default, the Activity Manager displays a list of all running applications for a user's session. This information can be viewed by all administrators that have access to the Activity Manager feature. For Delegated Administrator roles, this includes Full Administrator, delivery group Administrator, and Help Desk Administrator.

To protect the privacy of users and the applications that they are running, you can disable the Applications tab to list running applications. To do this, on the VDA, modify the registry key at HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information is not collected from the VDA and hence

not displayed in the Activity Manager.

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Restore desktop connections

March 23, 2022

From Monitor, check the user's connection status for the current machine in the user title bar.

If the desktop connection failed, the error that caused failure is displayed and can help you decide how to troubleshoot.

Action	Description
Ensure that the machine is not in maintenance mode	On the User Details page, make sure maintenance mode is turned off.
Restart the user's machine	Select the machine and click **Restart**. Use this option if the user's machine is unresponsive or unable to connect, such as when the machine is using an unusually high amount of CPU resources, which can make the CPU unusable.

Restore sessions

March 23, 2022

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

In the User Details view, troubleshoot session failures in the **Session Details** panel. You can view the details of the current session, indicated by the session ID.

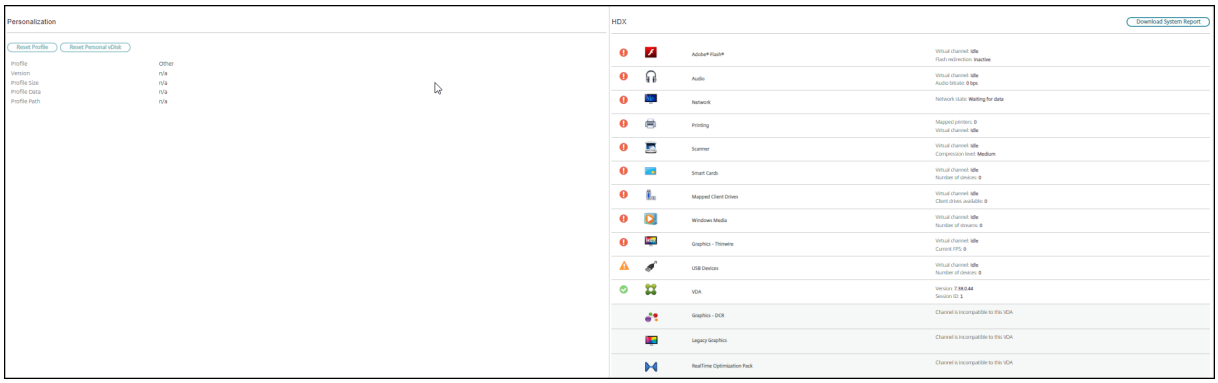
Action	Description
End applications or processes that are not responding	Click the **Applications** tab. Select any application that is not responding and click **End Application**. Similarly, select any corresponding process that is not responding and click **End Process**. Also, end processes that are consuming an unusually high amount of memory or CPU resources, which can make the CPU unusable.
Disconnect the Windows session	Click **Session Control** and then select **Disconnect**. This option is available only for brokered Multi-session OS machines. For non-brokered sessions, the option is disabled.
Log off the user from the session	Click **Session Control** and then select **Log Off**.

To test the session, the user can attempt to log back on to it. You can also shadow the user to more closely monitor this session.

Run HDX channel system reports

November 7, 2023

In the **User Details** view, check the status of the HDX channels on the user's machine in the HDX panel. This panel is available only if the user machine is connected using HDX.



If a message appears indicating that the information is not currently available, wait for one minute for the page to refresh, or select the **Refresh** button. HDX data takes a little longer to update than other data.

Click an error or warning icon for more information.

> Tip:
>
> You can view information about other channels in the same dialog box by clicking the left and right arrows in the left corner of the title bar.

HDX channel system reports are used mainly by Citrix Support to troubleshoot further. To do this, in the HDX panel, click **Download System Report**.

Reset a user profile

March 24, 2022

> **Caution:**
>
> When a profile is reset, although the user's folders and files are saved and copied to the new profile, most user profile data is deleted (for example, the registry is reset and application settings might be deleted).

1. From Monitor, search for the user whose profile you want to reset and select this user's session.
2. Click **Reset Profile**.
3. Instruct the user to log off from all sessions.
4. Instruct the user to log back on. The folders and files that were saved from the user's profile are copied to the new profile.

   > **Important:**
   >
   > If the user has profiles on multiple platforms (such as Windows 8 and Windows 7), instruct the user to log back on first to the same desktop or app that the user reported as a problem. This ensures that the correct profile is reset. For a Citrix user profile, the profile is already reset by the time the user's desktop appears. For a Microsoft roaming profile, the folder restoration might still be in progress for a brief time. The user must stay logged on until the restoration is complete.

The preceding steps assume you are using Citrix Virtual Desktops (Desktop VDA). If you are using Citrix Virtual Desktops (Server VDA) you need to be logged on to perform the profile reset. The user then needs to log off, and log back on to complete the profile reset.

If the profile is not successfully reset (for example, the user cannot successfully log back on to the machine or some of the files are missing), you must manually restore the original profile.

The folders (and their files) from the user's profile are saved and copied to the new profile. They are copied in the listed order:

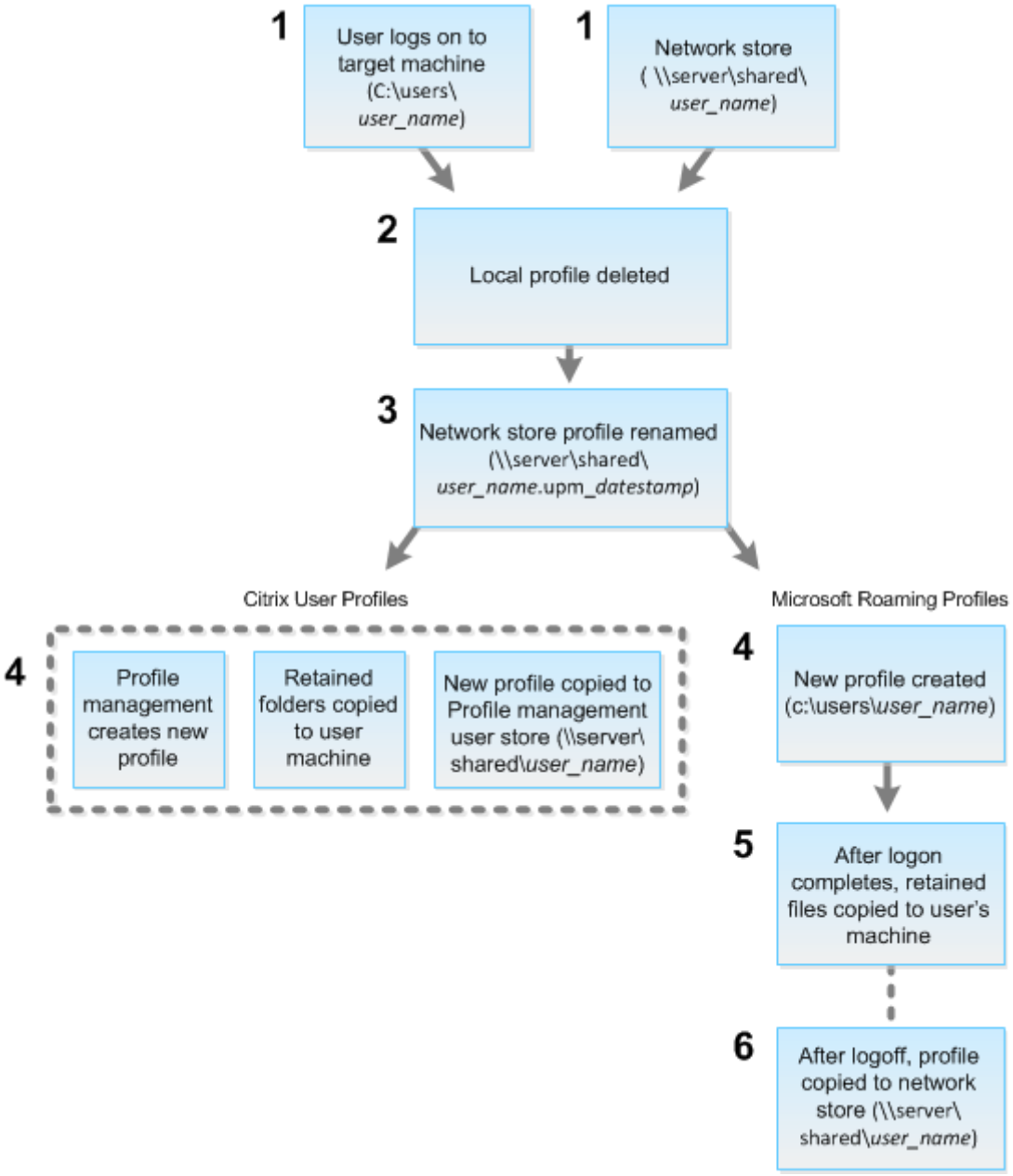
- Desktop
- Cookies
- Favorites
- Documents
- Pictures
- Music
- Videos

> **Note:**
>
> In Windows 8 and later, cookies are not copied when profiles are reset.

How reset profiles are processed

Any Citrix user profile or Microsoft roaming profile can be reset. After the user logs off and you select the reset command (either in Monitor or using the PowerShell SDK), Monitor first identifies the user profile in use and issues an appropriate reset command. Monitor receives the information through Profile Management, including information about the profile size, type, and logon timings.

This diagram illustrates the process following the user log on, when a user profile is reset.



The reset command issued by Monitor specifies the profile type. The Profile Management service then attempts to reset a profile of that type and looks for the appropriate network share (user store). If Profile Management processes the user, but receives a roaming profile command, it is rejected (or the opposite way).

1. If a local profile is present, it is deleted.
2. The network profile is renamed.
3. The next action depends on whether the profile being reset is a Citrix user profile or a Microsoft roaming profile.

For Citrix user profiles, the new profile is created using the Profile Management import rules, and the folders are copied back to the network profile, and the user can log on normally. If a roaming profile is used for the reset, any registry settings in the roaming profile are preserved in the reset profile. You can configure Profile management so that a template profile overrides the roaming profile, if necessary.

For Microsoft roaming profiles, Windows creates a new profile, and when the user logs on, the folders are copied back to the user device. When the user logs off again, the new profile is copied to the network store.

To manually restore a profile after a failed reset

1. Instruct the user to log off from all sessions.
2. Delete the local profile if one exists.
3. Locate the archived folder on the network share that contains the date and time appended to the folder name, the folder with a .upm_datestamp extension.
4. Delete the current profile name. That is, the one without the upm_datestamp extension.
5. Rename the archived folder using the original profile name. That is, remove the date and time extension. You have returned the profile to its original, pre-reset state.

Record sessions

June 6, 2024

You can record ICA sessions using the Session Recording controls from the **User Details** and **Machine Details** screen in Monitor. This feature is available for customers on **Premium** sites.

Dynamic Session Recording

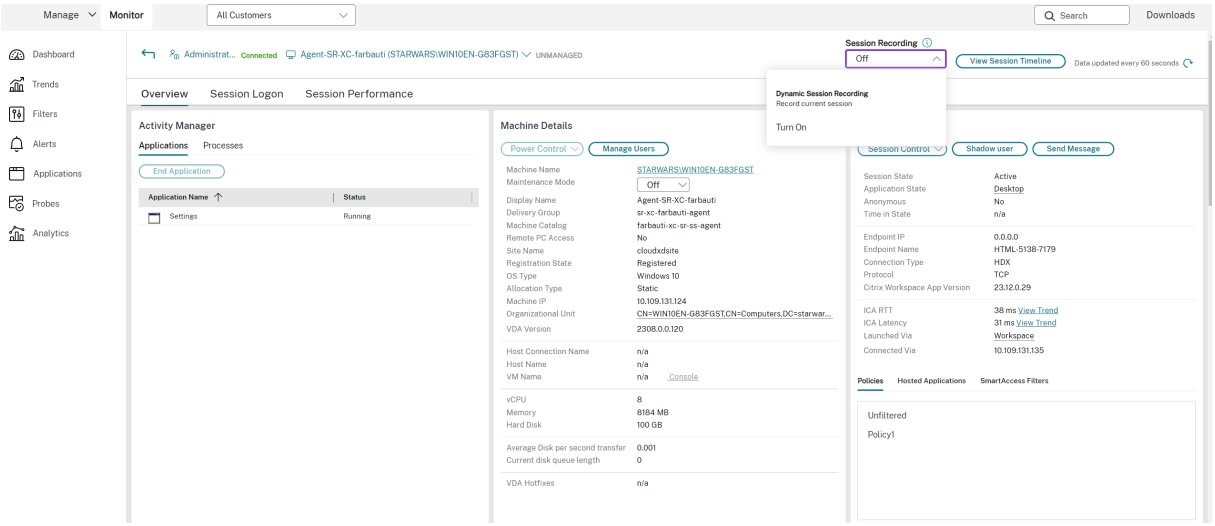
You can record the current active session using the Session Recording controls from the **User Details** screen. For more information about Dynamic Session Recording, see the Session Recording service article.

Session Recording controls in Monitor

You can use the **User Details** > **Session Recording** actions to record the current or subsequent sessions.

- Turn ON Dynamic Session Recording - the current session is recorded.
- Turn OFF - disable recording of sessions for the user.

The **Policies** Panel displays the name of the active Session Recording policy.



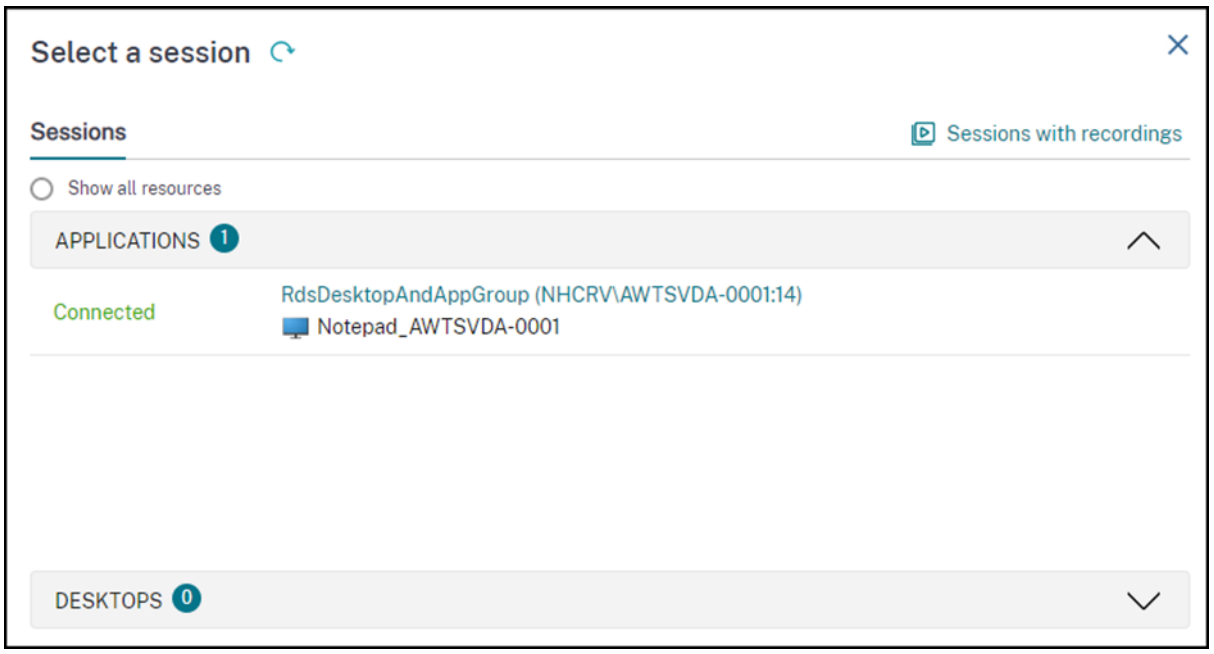
The **Machine Details** panel displays the status of the Session Recording policy for the machine.

Play back live and recorded sessions

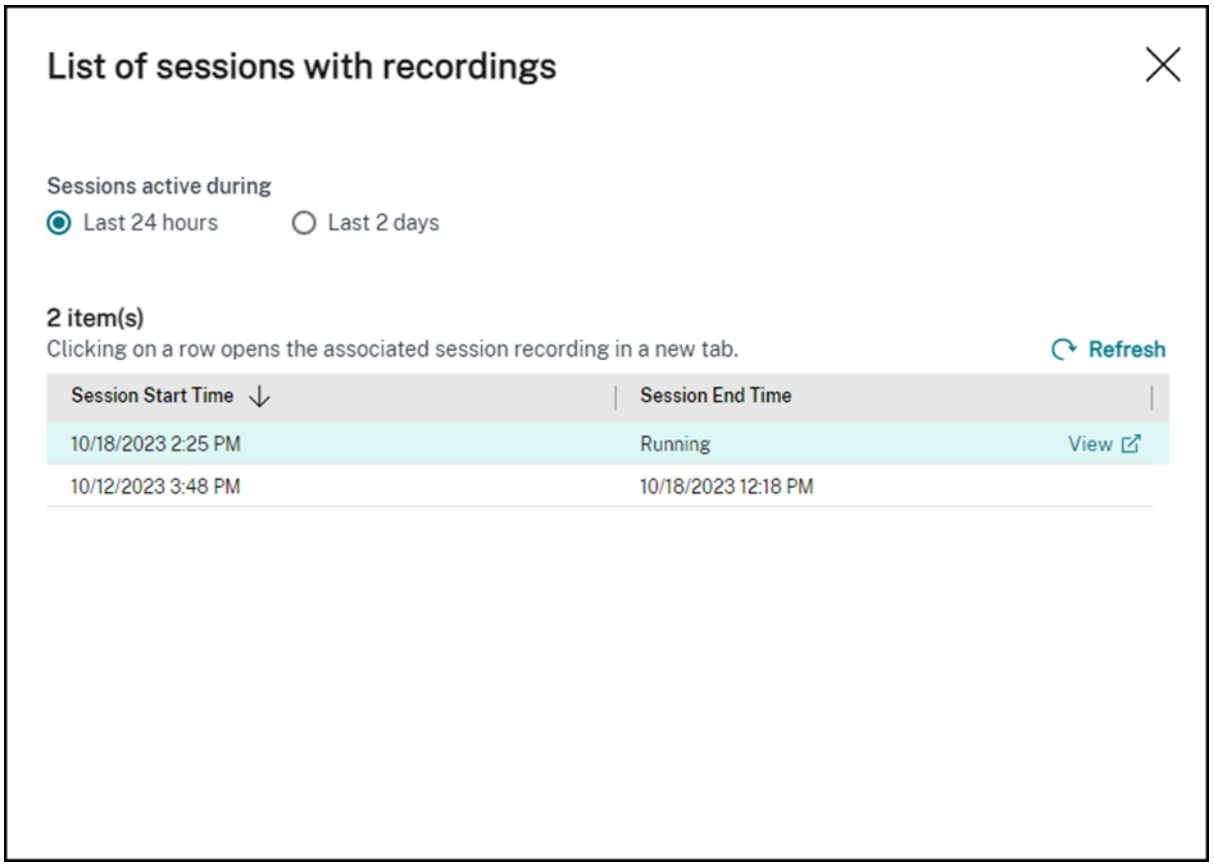
You can play back recorded and live user sessions to understand the issues encountered by the user. Ready access to recordings and session related metrics within the Monitor console eliminates the requirement of searching for the recordings across multiple session recording servers or looking for third-party apps to view the recordings. It helps corelate the issues discovered in the recordings with the performance metrics.

This feature requires VDA and the Session Recording servers version 2308 or later.

Monitor stores session recordings in a centralized repository. The list of recordings belonging to the user are displayed on clicking the **Session Selector** modal > **Sessions with recordings** link.



You can choose to view recordings of sessions that were active during the last 24 hours or the last 2 days. Live recordings of currently active sessions are marked with **Session End Time** as **Running**.



Click the **View** link to play back the recording on a new tab using the Citrix Session Recording playback

server.

Feature compatibility matrix

May 27, 2024

Citrix Monitor supports three Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) editions. They are **Premium**, **Citrix DaaS Advanced**, and **Citrix DaaS Advanced Plus**. Specific Citrix Monitor features, VDA versions, dependent components, and their respective license editions are listed in the following table.

Feature	Dependencies - min version required	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Real-time GPU Utilization available for AMD GPUs	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Access Citrix Analytics for Performance-Session Details	Citrix Analytics for Performance entitlement	Yes	Yes	Yes
Session Auto Reconnect	VDA 1906	Yes	Yes	Yes
Session Startup Duration	VDA 1903	Yes	Yes	Yes
Desktop Probing	Citrix Probe Agent 1903	Yes	No	No
Citrix Profile Management Duration in Profile Load	VDA 1903	Yes	Yes	Yes
Profile Drilldown	VDA 1811	Yes	Yes	Yes
Hypervisor Alerts Monitoring	None	Yes	No	No

Feature	Dependencies - min version required	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Application Probing	Citrix Application Probe Agent 1811	Yes	No	No
Microsoft RDS License Health	VDA 7.16	Yes	Yes	Yes
Access to machine console from Monitor	XenServer Hypervisor 7.3	Yes	Yes	Yes
Export of Filters Data	None	Yes	Yes	Yes
Interactive Session Drill Down	VDA 1808	Yes	Yes	Yes
GPO Drill Down	VDA 1808	Yes	Yes	Yes
Machine Historical Data Available Using OData API	None	Yes	Yes	Yes
Smart Alert Policies	None	Yes	No	No
Health Assistant Link	None	Yes	Yes	Yes
Interactive Session Drill-down	None	Yes	Yes	Yes
Application Analytics	VDA 7.15	Yes	Yes	Yes
OData API V.4	None	Yes	Yes	Yes
Shadow Linux VDA Users	VDA 7.16	Yes	Yes	Yes
Machine Console Access	None	Yes	Yes	Yes

Feature	Dependencies - min version required	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Application Failure Monitoring	VDA 7.15	Yes	Yes	Yes
Application-centric Troubleshooting	VDA 7.13	Yes	Yes	Yes
Disk Monitoring	VDA 7.14	Yes	Yes	Yes
GPU Monitoring	VDA 7.14	Yes	Yes	Yes
Transport Protocol on Session Details Panel	VDA 7.13	Yes	Yes	Yes
User-friendly Connection and Machine Failure Descriptions	VDA 7.x	Yes	Yes	Yes
Historical Data Retention	VDA 7.x	Yes	No	No
Custom Reporting	VDA 7.x	Yes	No	No
Resource Utilization Reporting	VDA 7.11	Yes	Yes	Yes
Alerting Extended for CPU, Memory and ICA RTT Conditions	VDA 7.11	Yes	No	No
Export Report Improvements	VDA 7.x	Yes	Yes	Yes
Logon Duration Breakdown	VDA 7.x	Yes	Yes	Yes

Feature	Dependencies - min version required	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Proactive Monitoring and Alerting	VDA 7.x	Yes	No	No
Hosted Applications Usage	VDA 7.x	Yes	No	No
Single-session and Multi-session OS Usage	VDA 7.x	Yes	No	No
Support for Framehawk Virtual Channel	VDA 7.6	Yes	Yes	Yes

Delegated administration and monitoring

March 23, 2022

Delegated administration uses three concepts: administrators, roles, and scopes. Permissions are based on an administrator's role and the scope of this role. For example, an administrator might be assigned a Help Desk administrator role where the scope involves responsibility for end-users at one site only.

Administrative permissions determine the monitoring interface presented to administrators and the tasks they can perform. Permissions determine:

- The views the administrator can access, collectively referred to as a view.
- The desktops, machines, and sessions that the administrator can view and interact with.
- The commands the administrator can perform, such as shadowing a user's session or enabling maintenance mode.

Monitoring now supports delegated administrator roles that allow you to assign custom defined or built-in roles to administrators. The role determines the available permissions and hence, how an administrator uses monitoring. You can also define the scope applicable for those roles. The scope defines the objects for which the role is applicable.

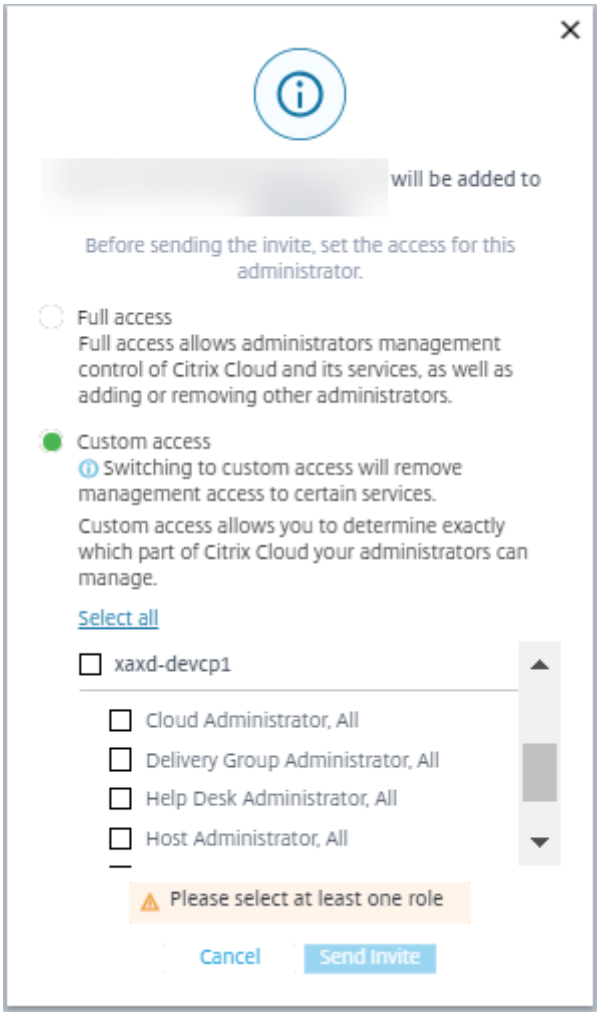
For information about creating delegated administrators, see the main Delegated administration article.

The built-in roles and permissions determine how administrators use **Monitor**:

Administrator Role	Permissions in Monitor
Full Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Delivery group Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Read Only Administrator	Can access all views and see all objects in specified scopes in addition to global information. Can download reports from HDX channels and can export Trends data using the Export option in the Trends view. Cannot perform any other commands or change anything in the views.
Help Desk Administrator	Can access only the Help Desk and User Details views and can view only objects that the administrator is delegated to manage. Can shadow a user's session and perform commands for that user. Can perform maintenance mode operations. Can use power control options for Single session OS Machines. Cannot access the Dashboard, Trends, Alerts, or Filters views. Cannot use power control options for Multi-session OS machines.
Machine catalog Administrator	Can access only the Machine Details page (Machine-based search).
Host Administrator	No access. This administrator is not supported for Monitor and cannot view data.
Probe Agent Administrator	Read-only access to Applications page, cannot access any other view. Meant to run the Citrix Probe Agent on endpoint machines.
Monitoring Full Administrator	Has full access to all views and commands in the **Monitor** tab.

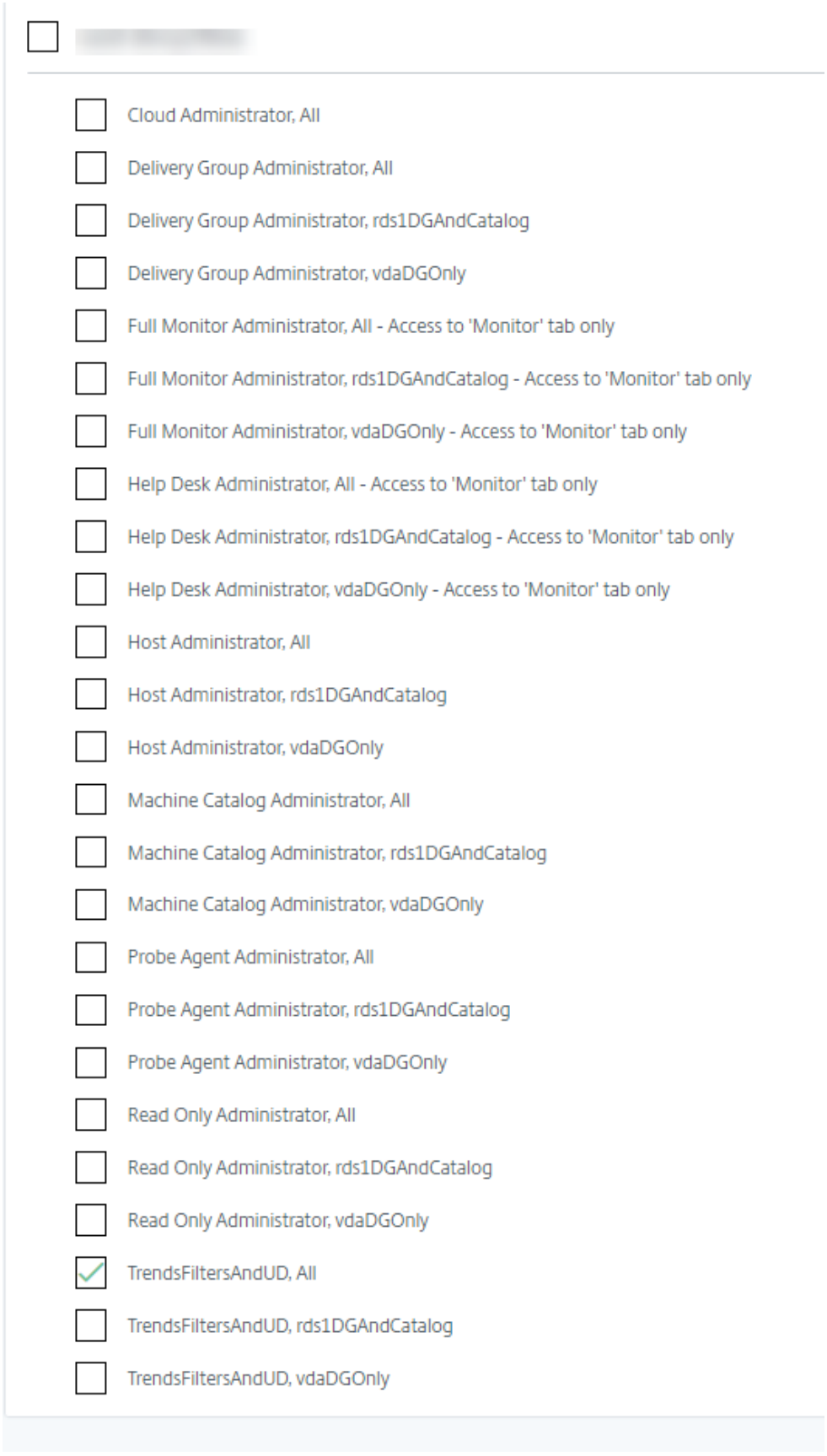
Administrator Role	Permissions in Monitor
Session Administrator	Can view Delivery Groups and manage their associated sessions and machines on the **Filters** page of the **Monitor** tab.

To assign a role (built-in or custom) to a user, from the Citrix Cloud menu, go to **Identity and Access Management** > **Administrators**. Here, when you add or edit the access of an administrator, you can select **Custom Access** and one of the listed roles.



You can define custom roles and scopes in **Full Configuration > Administrators > Administrators**.

The built-in roles and custom roles are listed for selection with custom scope.



Data granularity and retention

June 13, 2024

Aggregation of data values

The Monitor Service collects various data, including user session usage, user logon performance details, session load balancing details, and connection and machine failure information. Data is aggregated differently depending on its category. Understanding the aggregation of data values presented using the OData Method APIs is critical to interpreting the data. For example:

- Connected Sessions and Machine Failures occur over a period. Therefore, they are exposed as maximums over a time period.
- Logon Duration is a measure of the length of time, therefore is exposed as an average over a time period.
- Logon Count and Connection Failures are counts of occurrences over a period, therefore are exposed as sums over a time period.

Concurrent data evaluation

Your sessions must be overlapping to be considered concurrent. However, when the time interval is 1 minute, all sessions in that minute (whether they overlap) are considered concurrent. The size of the interval is so small that the performance overhead involved in calculating the precision is not worth the value added. If the sessions occur in the same hour, but not in the same minute, they are not considered to overlap.

Correlation of summary tables with raw data

The data model represents metrics in two different ways:

- The summary tables represent aggregate views of the metrics in per minute, hour, and day time granularities.
- The raw data represents individual events or current state tracked in the session, connection, application, and other objects.

When attempting to correlate data across API calls or within the data model itself, it is important to understand the following concepts and limitations:

- **No summary data for partial intervals.** Metrics summaries are designed to meet the needs of historical trends over long periods. These metrics are aggregated into the summary table

for complete intervals. There is no summary data for a partial interval at the beginning (oldest available data) of the data collection nor at the end. When viewing aggregations of a day (Interval=1440), this means that the first and most recent incomplete days have no data. Although raw data might exist for those partial intervals, it is never summarized. Pull the min and max SummaryDate from a particular summary table to determine the earliest and latest aggregate interval for a particular data granularity. The SummaryDate column represents the start of the interval. The Granularity column represents the length of the interval for the aggregate data.

- **Correlating by time.** Metrics are aggregated into the summary table for complete intervals as described in the preceding section. They can be used for historical trends, but raw events might be more current in the state than what has been summarized for trend analysis. Any time-based comparison of summary to raw data must take into account that there is no summary data for partial intervals that might occur or for the beginning and ending of the time period.
- **Missed and latent events.** Metrics that are aggregated into the summary table might be slightly inaccurate if events are missed or latent to the aggregation period. Although the Monitor Service attempts to maintain an accurate current state, it does not go back in time to recompute aggregation in the summary tables for missed or latent events.
- **Connection High Availability.** During connection HA, there are gaps in the summary data counts of current connections, but the session instances are still running in the raw data.
- **Data retention periods.** Data in the summary tables is retained on a different grooming schedule from the schedule for raw event data. Data might be missing because it has been groomed away from summary or raw tables. Retention periods might also differ for different granularities of summary data. Lower granularity data (minutes) is groomed more quickly than higher granularity data (days). If data is missing from one granularity due to grooming, it might be found in a higher granularity. Since the API calls only return the specific granularity requested, receiving no data for one granularity does not mean that the data doesn't exist for a higher granularity for the same time period.
- **Time zones.** Metrics are stored with UTC time stamps. Summary tables are aggregated on hourly time zone boundaries. For time zones that don't fall on hourly boundaries, there might be some discrepancy as to where data is aggregated.

Granularity and retention

The granularity of aggregated data retrieved by Monitor is a function of the time (T) span requested. The rules are as follows:

- 0 < T <= 30 days use per-hour granularity
- T > 31 days use per-day granularity

Requested data that does not come from aggregated data comes from the raw Session and Connection information. This data tends to grow fast, and therefore has its own grooming setting. Grooming

ensures that only relevant data is kept long term. This ensures better performance while maintaining the granularity required for reporting.

	Setting name	Affected grooming	Retention days for Premium	Retention days for Advanced
1	GroomSessionsRetentionDays	Session and Connection records retention after Session termination	90	31
2	GroomFailuresRetentionDays	MachineFailureLog and Connection-FailureLog records	90	31
3	GroomLoadIndexesRetentionDays	LoadIndex records	3	3
4	GroomDeletedRetentionDays	Machine, Catalog, DesktopGroup, and Hypervisor entities that have a LifecycleState of 'Deleted'. This also deletes any related Session, SessionDetail, Summary, Failure, or LoadIndex records.	90	31

	Setting name	Affected grooming	Retention days for Premium	Retention days for Advanced
5	GroomSummariesRetentionDays	Desktop Group Summary, FailureLog-Summary, and LoadIn-dexSummary records. Aggregated data - daily granularity.	365	31
6	GroomMachineHotfixLogRetentionDays	Hotfixes applied to the VDA and Controller machines	90	31
7	GroomHourlyRetentionDays	Aggregated data - hourly granularity	32	31
8	GroomApplicationInstanceRetentionDays	Application Instance history	90	Not applicable
9	GroomNotificationLogRetentionDays	Notification Log records	90	Not applicable
10	GroomResourceUsageRawDataRetentionDays	Resource utilization data - raw data	3	3
11	GroomResourceUsageHourDataRetentionDays	Resource utilization summary data - hour granularity	30	30
12	GroomResourceUsageDayDataRetentionDays	Resource utilization summary data - day granularity	365	31

	Setting name	Affected grooming	Retention days for Premium	Retention days for Advanced
13	GroomProcessUsageRawDataRetentionDays	Process utilization data - raw data	1	1
14	GroomProcessUsageHourDataRetentionDays	Process utilization data - hour granularity	7	7
15	GroomProcessUsageDayDataRetentionDays	Process utilization data - day granularity	30	30
16	GroomSessionMetricsDataRetentionDays	Session metrics data	1	1
17	GroomMachineMetricDataRetentionDays	Machine metrics data	3	3
18	GroomMachineMetricDaySummaryDataRetentionDays	Machine metrics summary data	395	31
19	GroomApplicationErrorRetentionDays	Application error data	1	1
20	GroomApplicationFailureRetentionDays	Application failure data	1	1

> **Caution:**
>
> You cannot modify the values on the Monitor Service database.

Retaining data for long periods has the following implications on table sizes:

- **Hourly data.** If hourly data is allowed to stay in the database for up to two years, a site of 1000 delivery groups can cause the database to grow as follows:

  1000 delivery groups x 24 hours/day x 365 days/year x 2 years = 17,520,000 rows of data. The performance impact of such a large amount of data in the aggregation tables is significant. Given that the dashboard data is drawn from this table, the requirements on the database server might be large. Excessively large amounts of data can have a dramatic impact on performance.

- **Session and event data.** This is the data that is collected every time a session is started and a connection/reconnection is made. For a large site (100 K users), this data grows fast. For example, two years' worth of these tables would gather more than a TB of data, requiring a high-end enterprise-level database.

Session launch diagnostics

March 11, 2024

> **Note:**
>
> Session launch diagnostics is currently under preview.

Session launches involve multiple Citrix components. To diagnose session launch failures, use Citrix Monitor (that is, Citrix Director service) to narrow down to the exact component and stage where the problem occurred. Apply the recommended actions to resolve the issue. Citrix Workspace app generates a 32-digit (8-4-4-4-12) Transaction ID which can be used in diagnosing session launch failures.

> **Note:**
>
> This feature is available only for cloud customers in the US, AP-S, and EU regions. It is not available in Japan and Government regions.

Prerequisites

If you are using Citrix DaaS, onboarding is automatic. Cloud customers using on-premises StoreFront must ensure that a supported StoreFront version is onboarded.

- If you are using Citrix Analytics for Performance, see Data sources for the steps to onboard on-premises StoreFront.
- If you are not using Citrix Analytics for Performance:
  1. Go to `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.
  2. Click **Connect to StoreFront deployment**, enter the details, and download the configuration file. For more information, see Onboarding on-premises sites using StoreFront.

  > **Note:**
  >
  > Administrators with Cloud Administrator roles are permitted to onboard StoreFront deployments, while administrators with Full Monitor Administrator roles can only view the

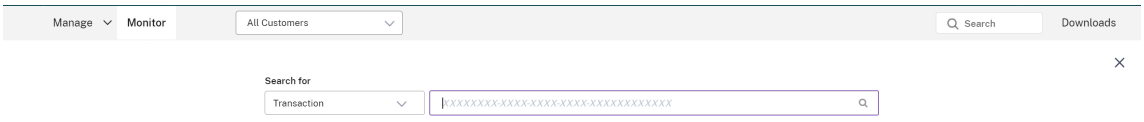
> StoreFront deployments.

Minimum supported versions of other components are as follows:

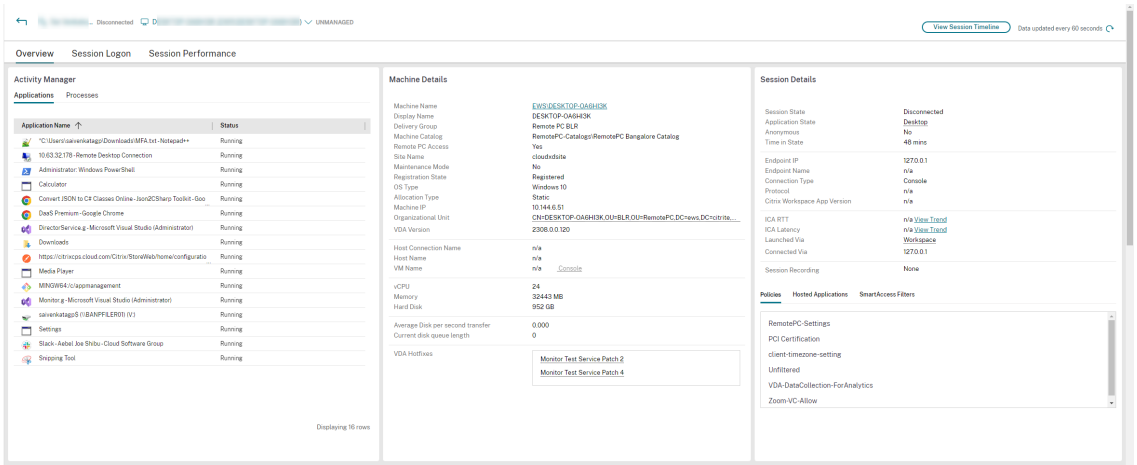
- Citrix Workspace app for Windows 2109
- Citrix Workspace app for Mac 2112
- Citrix Workspace app for Linux 2112
- Citrix Workspace app for HTML5 2110
- Citrix Workspace app for Chrome 2110
- Citrix Workspace app for Android 2110
- VDA version Citrix Virtual Apps and Desktops 2112
- Citrix StoreFront 1912 LTSR CU4

Steps to diagnose session launch failure

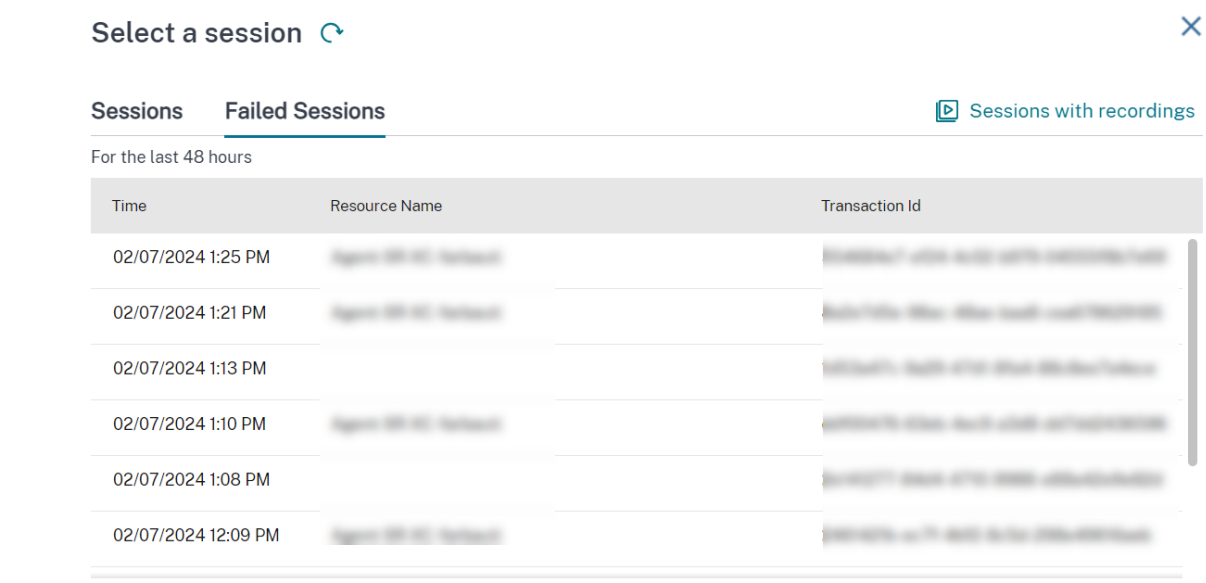
1. Copy Transaction ID of the failed session launch from Citrix Workspace app.
2. In the Monitor UI, search for the 32-digit transaction ID and click **Details**.



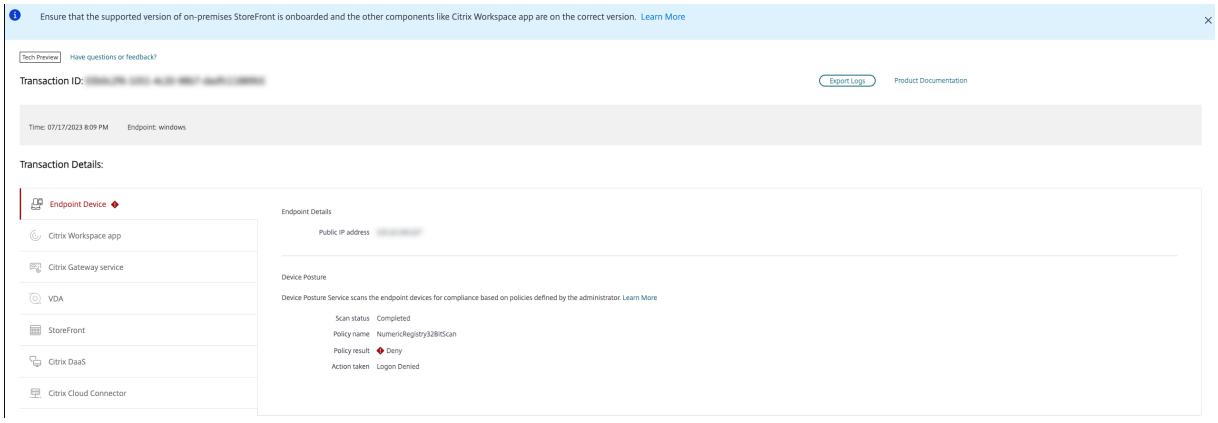
3. If Transaction ID is not available, search using the user name. The Activity Manager of the user is displayed.



4. Click the session selector. Go to the **Failed Sessions** tab. A list of sessions that have failed during the last 48 hours is displayed. Click the selected session.



5. Citrix Monitor displays key information regarding the transaction such as the User Name, Time stamp and the Application or Desktop on which the failure occurred.
6. The Transaction Details panel contains a list of components indicating the failure occurrence.
7. Click **Endpoint Device** in the list of components to view the Device Posture scan status. Device Posture Service scans the endpoint device for compliance based on policies defined by the administrator.



The Scan status, Policy name, Policy result, and Action taken is displayed. Ensure that the Device Posture service is configured with DaaS as described in the Device Posture article. Errors logged by Device Posture are described in Device Posture Error Logs.

1. Click the other component names to check the Component Details and the Last known failure details.
2. The Failure Reason and Error Code are displayed. Click the **Learn more about the error** link to see the specific error code in the Error codes section that contains the detailed description and recommended action.

3. You can export the logs to view them. The log file lists the session launch steps in chronological order and shows the exact component and its stage where the failure occurred.
4. In case more than one failure has occurred across the components, only the last known failure details are displayed on the Transaction page. The exported logs contain the details of all the failures related to the transaction.

> **Note:**
>
> Client-side error codes and diagnostic information are available only when Citrix StoreFront is onboarded and sending data. For more information about onboarding StoreFront, see Prerequisites.

Broker agent

bka.prepare.session.failure.validation

- Description: Failed to validate the prepare session request.
- Recommended Action: Retry action. If failure repeats, check that the connectors are in a healthy state.

bka.prepare.session.failure.rejected

- Description: VDA cannot accept the launch request.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

bka.hdx.prepare.failure.general

- Description: HDX prepares failure.
- Recommended Action: Restart the VDA.

bka.hdx.validate.failure.ticket_not_found

- Description: Referenced ticket or launch not in launch cache.
- Recommended Action: Ensure that VDA can communicate with the connector.

bka.ticketing.validate.failure.unlicensed

- Description: Cannot verify license for launch.
- Recommended Action: Contact Citrix Support.

bka.ticketing.validate.failure.general

- Description: Generic failure while validating a ticket.
- Recommended Action: Gather logs on the VDA and Contact Citrix Support.

bka.set.configuration.failure.policy

- Description: An error occurred during setting policies.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

bka.set.configuration.failure

- Description: An error occurred during setting configuration.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

Broker

brk.validate.credentials.failure.invalid

- Description: Failed to validate credentials due to some issue. The reason can be expanded in the message parameter.
- Recommended Action: Retry action. If failure repeats, check that the connectors are in a healthy state.

brk.resolve.machine.failure.general

- Description: Failed to enumerate or resolve worker. The reason can be expanded in the message parameter.
- Recommended Action: Ensure that machines capable of launching this application are registered with the Broker. Ensure that all available machines have not reached their capacity.

brk.license.check.failure.constraints

- Description: Licensing constraints failed session launch.
- Recommended Action: Ensure that there are licenses available for this type of application or desktop.

brk.resolve.machine.failure.timeout

- Description: Broker timed out while contacting the database.
- Recommended Action: Problems communicating with the site database. Contact Citrix support.

brk.poweron.forlaunch.queued.failure.general

- Description: Queueing power action failed.
- Recommended Action: Problems communicating with the site database. Contact Citrix support.

brk.set.configuration.failure.general

- Description: Unspecified error while setting configuration on target VDA.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

brk.prepare.session.failure.host_unreachable

- Description: Failed to communicate with the VDA.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

brk.prepare.session.failure.general

- Description: Failed to prepare session on VDA, UnsupportedClientType, or ConnectionRefused errors.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

brk.validate.ticket.failure.license

- Description: Failed to retrieve a valid license for this session.
- Recommended Action: Check the health status of the site and ensure all connectors and the Citrix DDC are operational.

brk.validate.ticket.failure.general

- Description: Invalid ticketing call.
- Recommended Action: Contact Citrix support.

brk.reverse.prepare.failure.general

- Description: Generic failure during session launch.
- Recommended Action: Check the health status of the site and ensure all connectors and the Citrix DDC are operational.

brk.reverse.prepare.failure.lease_revoked

- Description: Lease for this session was revoked.
- Recommended Action: Retry action, if failure repeats, check that the connectors are in a healthy state.

brk.reverse.prepare.failure.resource_unavailable

- Description: The resource is already in use or is temporarily unavailable.
- Recommended Action: Retry action, if failure repeats, check that the connectors are in a healthy state.

brk.reverse.prepare.failure.app_protection

- Description: App Protection is missing and is required for this session.
- Recommended Action: Ensure that app protection is enabled on this VDA or remove the App Protection requirement from the application.

HDX VDA Linux

VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Description: Reconnect to a session in pre-logoff state is not allowed.
- Recommended action: Retry to launch the later, this gives time to let the session logoff.

VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Description: Reconnect to a non-exiting session.
- Recommended action: Retry to launch latter. If still fail, contact Citrix support.

VDA_LINUX_ERR_SAME_KEY

- Description: Prepare for a connection, but there is an existing session with the same session key.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_GET_FQDN

- Description: Failed to get the FQDN of this VDA.
- Recommended action: Verify that the DNS configuration on the VDA is correct

VDA_LINUX_ERR_NO_CGP_LISTENER

- Description: There is no a CGP listener running.
- Recommended action: Verify **Session reliability connections** policy is enabled. Verify that the CGP listener is listening on expected port in VDA (default port is 2598, can be changed via **Session reliability port number** policy).

VDA_LINUX_ERR_DTLS_CONNECT

- Description: Failed to establish a DTLS connection to Gateway service.
- Recommended action: Verify that the Gateway service FQDN is reachable from VDA. Verify path `/var/xdl/keystore/cacerts` exists in VDA. Remove `/var/xdl/keystore` and run `/var/xdl/split_ca_bundle.sh` to regenerate CA certificates. Verify that the Gateway service FQDN is trusted by VDA.

VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Description: Failed to accept EDT handshake from client.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_TCP_CONNECT

- Description: Failed to establish a TCP connection to Gateway service.
- Recommended action: Verify that the Gateway service FQDN is reachable from VDA.

VDA_LINUX_ERR_TLS_CONNECT

- Description: Failed to establish a TLS handshake to Gateway service.
- Recommended action: Verify path `/var/xdl/keystore/cacerts` exists in VDA. Remove `/var/xdl/keystore` and run `/var/xdl/split_ca_bundle.sh` to regenerate CA certificates. Verify that Gateway service FQDN is trusted.

VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Description: Failed to establish a rendezvous handshake to Gateway service.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Description: Failed to accept an ICA connection.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- Description: Reconnect to an anonymous session is not allowed.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_CONN_NOT_ALLOWED

- Description: Connection is not allowed.
- Recommended action: If the result code is 3, verify that the license is not expired, otherwise, retry launch later. If you are unable to resolve, contact Citrix support.

VDA_LINUX_ERR_CONN_GENERAL

- Description: Failed to validate connection.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- Description: End user canceled logon.
- Recommended action: This error is expected, when SSO is disabled, and the end user clicks at the ‘Cancel’button in the logon box, otherwise, Contact Citrix support.

VDA_LINUX_ERR_GET_TARGET

- Description: Failed to get the target session.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_START_LOGON_TIMERS

- Description: Failed to start logon timers.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Description: Failed to send command to target session.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Description: Failed to post a reconnect event.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Description: Reconnect to user session timeout.
- Recommended action: Contact Citrix support.

HDX VDA Windows

RENDEZVOUS_CONNECT_FAILED_TCP

- Description: An outbound Rendezvous transport connection attempt over TCP failed.
- Recommended action: Sporadic failures can occur due to poor network conditions. This is expected. Check VDA configuration if this occurs frequently, then contact Citrix support.

RENDEZVOUS_CONNECT_FAILED_EDT

- Description: An outbound Rendezvous transport connection attempt over TCP failed.
- Recommended action: Sporadic failures can occur due to poor network conditions. This is expected. Check VDA configuration if this occurs frequently, then contact Citrix support.

RENDEZVOUS_CONNECT_FAILED_PROXY

- Description: An outbound Rendezvous transport connection attempt failed because of an invalid proxy configuration.
- Recommended action: Check rendezvous proxy configuration, contact Citrix support.

RENDEZVOUS_CONNECT_FAILED_DTLS

- Description: An outbound Rendezvous transport connection attempt failed due to the secure transport handshake failing.
- Recommended action: Check rendezvous configuration, check cryptographic configuration. Contact Citrix support.

RENDEZVOUS_CONNECT_FAILED_TLS

- Description: An outbound Rendezvous transport connection attempt failed due to secure transport handshake failing.
- Recommended action: Check rendezvous configuration, check cryptographic configuration, and contact Citrix support.

RENDEZVOUS_CONNECT_FAILED_CGP

- Description: An outbound Rendezvous transport connection attempt failed due to a CGP configuration issue.
- Recommended action: Check that CGP (Session Reliability) is enabled and CGP ports are being listened on, contact Citrix support.

CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- Description: Network interruption was not resolved due to timing out, session reliability failed to resume the connection.
- Recommended action: Sporadic failures can occur due to poor network conditions. This is expected.

CGP_SR_SUSPEND_RESUME_FAILED

- Description: Network interruption was not resolved due to an unforeseen error, session reliability failed to resume the connection.

- Recommended action: Sporadic failures can occur due to poor network conditions. This is expected.

PREPARE_RECONNECT_REJECTED

- Description: VDA rejected a reconnect request from an incoming ICA connection due to an invalid session key.
- Recommended action: Check VDA configuration, contact Citrix support.

Error: PREPARE_REJECTED

- Description: VDA rejected a connect request from an incoming ICA connection due to an invalid session key.
- Recommended action: Check VDA configuration, contact Citrix support.

PREPARE_LISTENING_FAILED

- Description: VDA failed to start listeners for the incoming ICA connection.
- Recommended action: Check network configuration, verify that listener ports are not in use by other applications, contact Citrix support.

RENDEZVOUSCONNECTIONREQ_FAILED

- Description: VDA failed to notify the ICA Stack to start an outbound Rendezvous connection.
- Recommended action: Check rendezvous configuration, check rendezvous proxy configuration, check CGP (Session Reliability) configuration, contact Citrix support.

RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Description: VDA failed to request the ICA Stack to start an outbound Rendezvous connection due to a proxy configuration error.
- Recommended action: Check rendezvous proxy configuration, contact Citrix support.

ESTABLISH_SESSION_FAILED

- Description: VDA failed to create a session for the incoming ICA connection or failed to connect to an existing session.
- Recommended action: Contact Citrix support.

ICA_ESTABLISH_FAILED

- Description: ICA connections accept or handshake failed.
- Recommended action: Contact Citrix support.

VALIDATE_FAILED

- Description: Broker failed to validate an incoming ICA connection request from the VDA.
- Recommended action: Contact Citrix support.

VALIDATE_TICKETING_FAILED

- Description: Broker failed to validate an incoming ICA connection request from the VDA because of a ticketing issue.
- Recommended action: Contact Citrix support.

MCS

brk.poweron.forlaunch.execution.generalfailure

- Description: General errors.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.insufficientresourcefailure

- Description: A hypervisor operation cannot be completed because of insufficient resources on the hypervisor.
- Recommended action: Check the resource quota in the hypervisor. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.nosuchmanagedmachine

- Description: A machine ID does not exist.
- Recommended action: Check the machine ID in the hypervisor. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- Description: Unable to establish a connection to the hypervisor. For example, the hosting infrastructure address was not found.
- Recommended action: Verify that the hosting infrastructure address is correct. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.invalidcredentialsfailure

- Description: Invalid credentials.
- Recommended action: Check the credentials for the hypervisor connection. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.authorizationfailure

- Description: Insufficient privilege or credentials.
- Recommended action: Check the permission assigned to the credentials for the hypervisor connection. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.sslcertauthfailure

- Description: A connection cannot be established due to an SSL authentication issue.
- Recommended action: Check the hypervisor's connection certificate. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.ratelimitedfailure

- Description: Cloud connection reports that it is rate limiting.
- Recommended action: Retry the connection later if the request is blocked by the hypervisor's rate limitation. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.connectorconnectionfailure

- Description: Errors exist on the cloud connector. For example, a timeout occurs while waiting for the connection. Once the timeout is reached, the cloud connector is disconnected.
- Recommended action: Restart the cloud connector. If that fails contact Citrix support.

brk.poweron.forlaunch.execution.remotehclserverconnectionfailure

- Description: Errors on the HCL/remote proxy plug-in or end point were not found when setting up the connection to the plug-in.
- Recommended action: Restart the connector. If that fails, contact Citrix support.

brk.poweron.forlaunch.execution.expiredcredentialsfailure

- Description: An expired credential was provided.
- Recommended action: Refresh the expired credentials used by the hypervisor connection.

brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure

- Description: Errors during machine creation.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.detachdiskfailed

- Description: The detach disk used by the virtual machine failed.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.createclonefailed

- Description: Create clone disk failed in hypervisor.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.provisionedvmnotfound

- Description: The provisioned VM was not found.
- Recommended action: Remove the provisioned VM from the catalog. If that fails, contact Citrix support.

brk.poweron.forlaunch.execution.invalidvmstate

- Description: The operation cannot proceed due to an invalid VM state.
- Recommended action: Restart the VM first and retry the operation.

brk.poweron.forlaunch.execution.insufficientresources

- Description: Insufficient resources during operation.
- Recommended action: Check the resource quota used by the hypervisor.

brk.poweron.forlaunch.execution.hypervisorinmaintenancemode

- Description: The operation cannot proceed because the hypervisor is in maintenance mode.
- Recommended action: Verify if the hypervisor is in maintenance mode.

brk.poweron.forlaunch.execution.delayed

- Description: Operation is queued.
- Recommended action: Wait for the process to complete. If the operation fails, contact Citrix support.

brk.poweron.forlaunch.execution.recreatevmfailed

- Description: The recreation of the VM failed.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.unknownvirtualmachine

- Description: Unknown virtual machine.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.ratelimitexceed

- Description: The cloud connection is rate limiting.
- Recommended action: Retry the connection later if the request was blocked by the hypervisor's rate limitation.

brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Description: The virtual disk is not stored.
- Recommended action: Retry later. If that fails, contact Citrix support.

Profile Management

xendesktop.upm.userprofile.error.failure

- Description: Citrix Profile Management failed to process the user profile. Use a temporary profile instead.
- Recommended action: This error doesn't cause a logon failure. Citrix Profile Management uses a temporary profile instead. To troubleshoot the error, check the Windows Event logs.

xendesktop.upm.userprofile.error.timeout

- Description: Citrix Profile Management failed to process the user profile within the specified time.
- Recommended action: This error doesn't cause a logon failure. Citrix Profile Management continues processing the user profile. To troubleshoot the error, check the Citrix Profile Management logs.

WEM Agent

wem.agent.userpolicy.error.failure

- Description: The Workspace Environment Management (WEM) agent failed to process group policies for the user. The user logon continues.
- Recommended action: The error does not cause logon failures. For more details, see the WEM product documentation and check the WEM agent service logs.

wem.agent.userpolicy.error.timeout

- Description: The Workspace Environment Management (WEM) agent failed to process group policies for the user within the specified time. The user logon continues.
- Recommended action: The error does not cause logon failures. For more details, see the WEM product documentation and check the WEM agent service logs.

Android Postlaunch

SessionManager.Launch.EngineLoadFailed

- Description: Failed to load or initialize ICA Engine.
- Recommended Action: Contact Citrix support.

SessionManager.Launch.ConnectionFailed

- Description: Engine terminated before connecting.
- Recommended Action: Contact Citrix support.

SessionManager.Launch.LogonFailed

- Description: Session disconnected without completing login.
- Recommended action: Contact Citrix support.

SessionManager.LeaseResolution.Failed

- Description: Unable to attempt lease launch.
- Recommended Action: Contact Citrix support.

SessionManager.clxmtp.SoftDeny

- Description: Engine CLXMTP negotiation failed (soft deny).
- Recommended Action: Contact Citrix support.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: Engine CLXMTP connection failed (implicit soft deny).
- Recommended Action: Contact Citrix support.

Transport.Connect.NoCGP_Fail

- Description: Failed to connect (CGP disabled).
- Recommended Action: Contact Citrix support.

Transport.Connect.FallbackFail

- Description: Failed to connect. Tried the ICA fallback.
- Recommended Action: Contact Citrix support.

Transport.Connect.Fail

- Description: Connection is unavailable.
- Recommended Action: Contact Citrix support.

Android Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: Send ICA request type is incorrect.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00002

- Description: The ICA request is invalid.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00003

- Description: The store is null for the ICA request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00004

- Description: The store URL is null for the ICA request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00005

- Description: The resource parameter is null for the ICA request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00006

- Description: The resource parameter provided for the ICA request isn't a valid resource type.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00007

- Description: The resource parameter provided for the ICA request is null for the ICA launch URL.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00008

- Description: The ICA request is null with authentication manager parameters.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00009

- Description: The ICA request body is null.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000010

- Description: Failed to create an HTTP entity from the ICA request body.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000011

- Description: Failed to download the ICA file because of an exception from creating the authentication manager request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000012

- Description: Failed to download the ICA file because of an exception from running the authentication manager request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000013

- Description: Failed to download the ICA file because of an unexpected response from the authentication manager request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000014

- Description: Failed to download the ICA file when you copy the inputStream from the authentication manager response.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000015

- Description: Failed to parse the ICA document using the inputStream from the authentication manager response.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000016

- Description: The ICA document downloaded is null without any exception.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000017

- Description: Failed to download the ICA file because of an unsuccessful response.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000018

- Description: Resource is unavailable.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000019

- Description: The resource to launch either does not exist, not enabled, or not visible to a user.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000020

- Description: There are no more active sessions.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000021

- Description: The server does not have the required license to do the requested activity.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000022

- Description: There are no workstations available.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000023

- Description: Unable to connect to the workstation. The Server has refused the connection.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000024

- Description: The workstation is under maintenance and is unavailable for use.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000025

- Description: Can't launch the resource because of a `resourceerror` error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000026

- Description: Can't launch the resource because of a `generalapplauncherror` error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000027

- Description: Can't launch the resource because of an unknown error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000028

- Description: Can't launch the resource because of a rebooting error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000029

- Description: Can't launch the resource because of a resuming error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000030

- Description: Can't launch the resource because of an undefined error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_000031

- Description: Can't download the ICA file. However, the error code isn't found in the defined map.
- Recommended Action: Contact Citrix support.

Linux Postlaunch

SessionManager.Launch.EngineLoadFailed

- Description: Failed to load ICA engine.
- Recommended action: Contact Citrix support.

SessionManager.Launch.Failed

- Description: Failed to launch the session.
- Recommended Action: Contact Citrix support.

SessionManager.Launch.ConnectionFailed

- Description: Engine terminated before connecting.
- Recommended Action: Look for other errors associated with the launch attempt.

SessionManager.Launch.LogonFailed

- Description: Session disconnected without completing login.
- Recommended Action: This error indicates login failure, possibly including a failure of the user to manually enter credentials. Investigate how the user attempted to sign into the remote VDA.

SessionManager.LeaseResolution.Failed

- Description: Unable to attempt lease launch.
- Recommended Action: Verify that the leases have been synced to the client machine, and are still valid. User can sign into Citrix Workspace in online mode to trigger the (re-) sync of leases. Look for errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

Transport.Connect.NoCGP_Fail

- Description: Failed to connect (CGP disabled).
- Recommended Action: Investigate why the client isn't able to contact a VDA via TCP or EDT.

Transport.Connect.FallbackFail

- Description: Failed to connect. Tried the ICA fallback.
- Recommended Action: Investigate why the client isn't able to contact a Gateway, Connector, or VDA via either TCP or EDT.

Transport.Connect.Fail

- Description: Citrix Workspace app failed to connect to Gateway, Connector, or VDA through TCP, EDT, or UDP.
- Recommended Action: Investigate why the client isn't able to contact the Gateway, Connector, or VDA through TCP, EDT, or UDP. The firewall between the client and host might not allow the protocols(UDP/TCP) or the required ports.

SessionManager.clxmtp.SoftDeny

- Description: Engine CLXMTP negotiation failed (soft deny).
- Recommended Action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Look for errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: Engine CLXMTP connection failed (implicit soft deny).

- Recommended Action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Investigate why the client can't contact a Connector or Gateway. It might be expected for that host to be inaccessible because of network topology or firewall restrictions.

Linux Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: Unable to connect to store because of no response from the Citrix Workspace app.
- Recommended action: Verify whether Citrix Workspace or StoreFront is down. Also, verify the internet connectivity.

CWA-ICADOWNLOAD_ERR_00002

- Description: User has canceled the session launch.
- Recommended action: Relaunch the session after sometime.

CWA-ICADOWNLOAD_ERR_00003

- Description: Unable to connect to store. Verify that the server certificates are valid.
- Recommended action: Verify if server certificates are installed and active.

CWA-ICADOWNLOAD_ERR_00004

- Description: The resource to launch does not exist, not enabled, or not visible to a user.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00005

- Description: Workstations aren't available for this request.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00006

- Description: Server does not have the required license to do the requested activity.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00007

- Description: Server has refused connection to workstation.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00008

- Description: The requested workstation is under maintenance and is unavailable for use.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00009

- Description: Maximum session limit is reached.
- Recommended action: Reached the maximum session limit that was configured by an admin. Restart the session.

CWA-ICADOWNLOAD_ERR_000010

- Description: General error that cannot be further specified.
- Recommended action: Contact Citrix support.

Mac Postlaunch

Desktop failed to start

- Description: “Desktop name”desktop failed to start. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Viewer failed to start

- Description: Viewer failed to start. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: “Desktop name”desktop is under planned maintenance. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Application failed to start

- Description: “App name”failed to start.
- Recommended action: Contact your admin with the error details.

Application failed to start

- Description: “App name”failed to start. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: “Desktop name”desktop failed to start.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: “Desktop name”desktop failed to start. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Viewer failed to start

- Description: Viewer failed to open “Application name”. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Viewer failed to start

- Description: Viewer failed to open desktop “Desktop name”. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: “Desktop name”desktop is under planned maintenance.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: “Desktop name”desktop is under planned maintenance. Transaction ID - “Transaction ID”.
- Recommended action: Contact your admin with the error details.

Unable to connect to the desktop

- Description: Unable to reach “desktop name”desktop. Transaction ID - “Transaction ID”. Try again later.
- Recommended action: If the problem persists, contact your admin with the error details.

Mac Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: ICA file is invalid.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00002

- Description: Launch request has timed out.
- Recommended action: Verify the internet connection or contact Citrix support.

CWA-ICADOWNLOAD_ERR_00003

- Description: Server did not respond.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00004

- Description: Resource to launch either doesn’t exist, isn’t enabled, or isn’t visible to the user.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00005

- Description: Server isn’t reachable.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00006

- Description: Error while launching the viewer.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00007

- Description: Failed to launch an Apple open event.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00008

- Description: Viewer path isn't reachable.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00009

- Description: User canceled the authentication.
- Recommended action: Ask the user to relaunch the resource.

CWA-ICADOWNLOAD_ERR_000010

- Description: User canceled the LSI Window.
- Recommended action: Ask the user to relaunch the resource.

CWA-ICADOWNLOAD_ERR_000011

- Description: Requested Workstation is under maintenance and unavailable for use.
- Recommended action: Ask the user to try after maintenance is complete, and the workstation is available for use.

CWA-ICADOWNLOAD_ERR_000012

- Description: User login credentials must be changed.
- Recommended action: Ask user to change login credentials.

CWA-ICADOWNLOAD_ERR_000013

- Description: The session connecting the resource is no longer active.
- Recommended action: Ask the user to try again, or contact your Citrix technical support for further assistance.

CWA-ICADOWNLOAD_ERR_000014

- Description: Failed to download ICA file.
- Recommended action: Contact Citrix support.

Windows Postlaunch

SessionManager.Launch.EngineLoadFailed

- Description: The core components for establishing a connection to a remote desktop or application failed to load or initialize properly. Extra details might be provided in the error message.
- Recommended action: Citrix Workspace app isn't functioning as expected. A third-party (non-Citrix) virtual channel DLL or another system component might be causing this problem. It might be necessary to collect and submit CDF traces to determine the nature of the failure.

SessionManager.Launch.ConnectionFailed

- Description: This error is a generic failure indicating that a launch attempt has failed. Other errors sent out might indicate a cause.
- Recommended action: Look for other errors associated with the launch attempt.

SessionManager.Launch.LogonFailed

- Description: This error indicates that a connection to a remote desktop or application was established. However, the session disconnected without completing Windows (or other operating system) login.
- Recommended action: This error indicates some login failure, possibly including a failure of the user to manually enter credentials. Investigate how the user attempted to sign into the remote VDA.

SessionManager.Launch.Cancelled

- Description: The Citrix engine's connect attempt was canceled, most likely by user action.

- Recommended action: This error indicates why a connection wasn't successfully established, but likely indicates correct behavior.

SessionManager.LeaseResolution.Failed

- Description: Indicates that an offline (also called "lease-based") launch failed. This failure is because a valid and required lease for the resource wasn't found on the client machine. Also, the Gateway or Cloud Connector rejected the launch request, or the launch request was somehow invalid.
- Recommended action: Verify that the leases have been synced to the client machine, and are still valid. User can sign into Citrix Workspace in online mode to trigger the (re-) sync of leases. Look for the errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

SessionManager.clxmtp.SoftDeny

- Description: A lease launch was attempted, and a Connector or Gateway informed the client that it can't complete the requested launch. However, the other Connectors or Gateways might be able to help the launch.
- Recommended action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Look for errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: A lease launch was attempted, and a Connector or Gateway was unreachable. However, other Connectors or Gateways might be able to help the launch.
- Recommended action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Investigate why the client can't contact a Connector or Gateway. It might be expected for that host to be inaccessible because of network topology or firewall restrictions.

Transport.Connect.NoCGP_Fail

- Description: The Citrix Workspace app core (engine) components failed to connect to a VDA host through the ICA protocol (port 1494). Attempts to connect to a gateway or VDA via the CGP protocol were not attempted if this event was sent.
- Recommended action: Investigate why the client isn't able to contact a VDA through TCP or EDT.

Transport.Connect.FallbackFail

- Description: The Citrix Workspace app core (engine) components failed to connect to a VDA host through the ICA protocol (port 1494). After this failure, the Citrix Workspace app fails to connect to a Gateway or VDA through the CGP protocol (port 2598).
- Recommended action: Investigate why the client isn't able to contact a Gateway, Connector, or VDA through either TCP or EDT.

Transport.Connect.Fail

- Description: The Citrix Workspace app core (engine) components failed to connect to a Gateway or VDA through the CGP protocol (port 2598). Attempts to connect to a VDA through the ICA protocol were not attempted if this event was emitted.
- Recommended action: Investigate why the client isn't able to contact a Gateway, Connector, or VDA through either TCP or EDT.

Windows Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: Unable to connect to store because of no response from the Citrix Workspace app.
- Recommended action: Verify whether Citrix Workspace or StoreFront is down. Also, verify the internet connectivity.

CWA-ICADOWNLOAD_ERR_00002

- Description: User has canceled the session launch.
- Recommended action: Relaunch the session after sometime.

CWA-ICADOWNLOAD_ERR_00003

- Description: Unable to connect to store. Verify that the server certificates are valid.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00004

- Description: The resource to launch does not exist, not enabled, or not visible to a user.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00005

- Description: Workstations aren't available for this request.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00006

- Description: Server does not have the required license to do the requested activity.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00007

- Description: Server has refused connection to workstation.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00008

- Description: The requested workstation is under maintenance and is unavailable for use.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00009

- Description: Maximum session limit is reached.
- Recommended action: Reached the maximum session limit that was configured by an admin. Restart the session.

CWA-ICADOWNLOAD_ERR_000010

- Description: General error that cannot be further specified.
- Recommended action: Contact your IT admin with the error details.

Workspace

StoreLaunchIcaEndpoint.LaunchFailed

- Description: An error occurred while launching.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

StoreLaunchSessionEndpoint.BadRequest

- Description: The parameters of the launch request were invalid or empty.
- Recommended action: Contact Citrix support.

StoreLaunchSessionEndpoint.FarmUnavailable

- Description: There were no farms available for the launch.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs.

StoreLaunchSessionEndpoint.Error

- Description: There was an internal error while launching.
- Recommended action: Contact Citrix support.

StoreGetIcaFileEndpoint.BadRequest

- Description: There was no launch ticket provided in the request.
- Recommended action: Contact Citrix support.

StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed

- Description: Workspace was unable to retrieve the ICA file.
- Recommended action: Contact Citrix support.

StoreGetIcaFileEndpoint.Error

- Description: Workspace was unable to retrieve the ICA file.
- Recommended action: Contact Citrix support.

WebProxyGetLaunchStatusEndPoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxyGetLaunchStatusEndPoint.LaunchFailed

- Description: There was an internal error while launching the application.
- Recommended action: Contact Citrix support.

WebProxyGetLaunchStatusEndPoint.ResourceNotFound

- Description: The launch failed because the application can't be found.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs and application configuration.

WebProxyLaunchIcaEndpoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxyLaunchIcaEndpoint.LaunchFailed

- Description: There was an internal error while launching the application.
- Recommended action: Contact Citrix support.

WebProxyLaunchIcaEndpoint.ResourceNotFound

- Description: The launch failed because the application can't be found.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs and application configuration.

WebProxySessionsLaunchIcaEndpoint.SessionNotFound

- Description: Workspace was unable to reconnect to the existing HDX session. Your session might be terminated.
- Recommended action: Relaunch the application.

WebProxySessionsLaunchIcaEndpoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed

- Description: Workspace was unable to reconnect to the existing HDX session. Your session might be terminated.
- Recommended action: Contact Citrix support.

WebProxySessionsLaunchIcaEndpoint.Error

- Description: There was an internal error while reconnecting to the session.
- Recommended action: Contact Citrix support.

WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed

- Description: Workspace was unable to reconnect to the HDX session.
- Recommended action: Contact Citrix support.

WebProxySessionsGetLaunchStatusEndpoint.Error

- Description: There was an internal error while reconnecting to the session.
- Recommended action: Contact Citrix support.

DetermineGateway.Error

- Description: Workspace was unable to determine which Gateway to connect to.
- Recommended action: Verify your Gateway configuration. Contact Citrix support.

ConnectionRoutingProviderLaunch.Error

- Description: Workspace was unable to determine which Gateway to connect to.
- Recommended action: Verify your Gateway configuration. Contact Citrix support.

BrokerGetAddressCall.AnonymousPrelaunchNotSupported

- Description: Workspace can't launch the application because the farm doesn't support anonymous launches.
- Recommended action: Contact Citrix support.

BrokerGetAddressCall.LeasingError

- Description: Workspace received an error from the Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.ServiceConnectionError

- Description: Workspace was unable to contact any Citrix Virtual Apps and Desktops broker in the farm.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.BrokerError

- Description: Workspace received an error from a Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.LicensingError

- Description: Workspace was unable to launch the application because of a licensing error.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.Error

- Description: Workspace can't retrieve the VDA details from the Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetLaunchReference.NoAccessToken

- Description: Workspace can't successfully connect to the VDA.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetLaunchReference.BrokerError

- Description: Workspace can't successfully connect to the VDA.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetLaunchReference.Error

- Description: Workspace can't successfully connect to the VDA.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GenerateIcaFile.InvalidIcaSetting

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

StoreIcaFileAndGetTicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetFasVdaLogonTicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GenerateSTATicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetVdaAddress.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetTicket.NoAccessToken

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetTicket.BrokerError

- Description: The Citrix Virtual Apps and Desktops broker was unable to launch the HDX session.
- Recommended action: Verify the ID in the error message and Verify your Citrix Virtual Apps and Desktops logs.

GetTicket.ServiceConnectionError

- Description: Workspace can't contact a Citrix Virtual Apps and Desktops broker.
- Recommended action: Contact Citrix support.

GetTicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetNetscalerConfigurationByCustomer.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

DiscoverMPSServerCapabilities.Error

- Description: There was a problem making a request to the Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetResourceLocationNetScalerConfig.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetCustomerResourceLocations.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetResourceLocationFromResourceProvider.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetNetScalerGatewayInfo.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetCustomerEntitlements.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetResourceLocationForServerFeed.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetResourceInformation.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

Citrix Gateway as a service

CGS-ICASN_ERR_00001

- Description: Application launch failed because of request parsing error.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00002

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00003

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00004

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00005

- Description: Failed to establish connection to the Connector.
- Recommended action: Verify connector health. If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00006

- Description: Connection request to the Connector timed out.
- Recommended action: Verify connector health. Verify if any proxy settings blocks traffic between connector/VDA and NGS. Verify connectivity between VDA and Connector. If the issue persists, Contact Citrix support.

CGS_ICASN_ERR_00007

- Description: Citrix Workspace app closed the connection.
- Recommended action: Verify that the client-side network connectivity is stable. If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00008

- Description: Back-end closed the connection.
- Recommended action: Verify connector health. Verify network stability from Connector/VDA to public network(NGS). If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00009

- Description: Failure in VDA to NGS connection establishment (Rendezvous).
- Recommended action: Verify the connector health. VDA must be able to reach NGS Service. Verify connectivity between VDA and Connector. If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00010

- Description: EDT to TCP fallback. Verify prerequisite for EDT.
- Recommended action: Rendezvous must be enabled and VDA must be able to reach NGS service over UDP. If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00011

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00012

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00013

- Description: Failure in GCT validation.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00014

- Description: Failure in GCT validation.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00015

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00016

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00017

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00018

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00019

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00020

- Description: Error in CGS internal licensing.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00021

- Description: Rendezvous v2 fall back because of disabled feature flag.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00022

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00023

- Description: Timeout in CLXMTP exchange.
- Recommended action: Verify that the connectors are healthy and reachable to NGS service. If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00024

- Description: Failure in CLXMTP VSR validation.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00025

- Description: Failure in CLXMTP VSR validation.
- Recommended action: Contact Citrix support.

CGS_ICASN_ERR_00026

- Description: Connector isn't available in CLXMTP.
- Recommended action: Verify whether the connector is in the healthy state for the resource location. If the issue persists, contact Citrix support.

CGS_ICASN_ERR_00027

- Description: CLXMTP redirect to Connector failed after maximum trials.
- Recommended action: Verify whether the connector is in the healthy state for the resource location. Verify that the `Citrix ClxMtp Service` service is running in all connectors. Contact Citrix support.

CGS_ICASN_ERR_00028

- Description: Failed to communicate with the Controller.
- Recommended action: Contact Citrix support.

Success: CGS_ICASN_SUCCESS_00001

- Description: Session launch request received.
- Recommended action: Not applicable

Success: CGS_ICASN_SUCCESS_00002

- Description: Session launch request completed.
- Recommended action: Not applicable

XAXD proxy

XDPXY_INF_00001

- Description: Broker sends a request to the VDA to prepare for incoming connections.
- Recommended Action: Not applicable

XDPXY_INF_00002

- Description: VDA confirms request for connection by Broker.
- Recommended Action: Not applicable

XDPXY_ERR_00001

- Description: Failed to communicate with the VDA.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00002

- Description: XaxdProxy timed out waiting for a response from VDA.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00003

- Description: Encountered a WCF fault or exception while trying to make the request.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.

  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_INF_00003

- Description: Request for validation for an incoming ICA or RDP connection is called by the stack.
- Recommended Action: Not applicable

XDPXY_INF_00004

- Description: Validation of the incoming ICA or RDP connection is established.
- Recommended Action: Not applicable

XDPXY_ERR_00001

- Description: Failed to communicate with the VDA Proxy.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00002

- Description: XaxdProxy timed out waiting for a response from VDA Proxy.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00003

- Description: Encountered an exception while trying to make the request.

- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_INF_00005

- Description: Request for HDX session traffic direct to VDA is made.
- Recommended Action: Not applicable

XDPXY_INF_00006

- Description: VDA establishes direct connection with Citrix Cloud control plane for HDX session traffic.
- Recommended Action: Not applicable

XDPXY_INF_00007

- Description: Client sends connection request to on-premises StoreFront for a resource.
- Recommended Action: Not applicable

XDPXY_INF_00008

- Description: On-premises StoreFront accepts connection request from client for resource.
- Recommended Action: Not applicable

XDPXY_ERR_00004

- Description: XaxdProxy got an HTTP error response while trying to connect.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Verify network stability from Connector to public network.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00006

- Description: The XML request has an invalid format.
- Recommended Action: Contact Citrix support

XDPXY_ERR_00007

- Description: XML request has invalid credential headers and/or format.
- Recommended Action: Logout, login again, and retry action. if the issue persists, contact Citrix support

XDPXY_INF_00011

- Description: Service continuity launch is requested by the user via WSA.
- Recommended Action: Not applicable

XDPXY_INF_00012

- Description: Service continuity launch is requested by the user via WSA.
- Recommended Action: Not applicable

XDPXY_ERR_00004

- Description: XaxdProxy encountered an HTTP error while trying to connect.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00008

- Description: Service continuity launch failed as XaxdProxy timed out waiting for a response.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00009

- Description: Service continuity launch failed due to the lease being blocked and/or revoked.
- Recommended Action: Contact your Citrix Cloud Administrator with the error details. For more information, see Service continuity documentation.
  - If the issue persists, contact Citrix support.

Citrix DaaS for Citrix Service Providers

January 17, 2024

This article describes how **Citrix Service Providers (CSP)** can set up Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) for tenant customers in Citrix Cloud. For an overview of the features available for Citrix Partners, see Citrix Cloud for Partners.

Requirements

- You are a Citrix Service Provider partner.
- You have a Citrix Cloud account.
- You have a subscription to Citrix DaaS.

Limitations and known issues

Limitations

- Tenant name changes take up to 24 hours to apply across all interfaces.
- When creating a tenant, the email address must be unique.
- Filtering in **Manage > Full Configuration** by scope (similar to Monitor) is not available. To see the resources attached to a scope, select **Administrators** in the left pane. On the **Scopes** tab, select the scope and then select **Edit Scope** in the Action pane.

Known issues

- After scopes are assigned to a resource, you cannot use the management console to remove or unassign them. Those tasks are supported only through PowerShell.
- **Manage > Full Configuration** does not enforce scopes. You are responsible for selecting the appropriate scope when creating machine catalogs, delivery groups, and application groups.

- When more than 15 scopes are created (auto-created and custom), the Citrix Cloud custom access information for an administrator (**Identity and Access Management > Administrators**) does not display correctly. Workaround: Limit scopes to 15 or fewer.

Add a customer

1. Sign in to Citrix Cloud with your CSP credentials. Select **Customers** in the upper left menu.
2. From the Customer Dashboard, select **Invite or Add**. Provide the requested information.
3. If the customer does not have a Citrix Cloud account, adding the customer creates a customer account. Adding the customer also automatically adds you as a full access administrator of that customer's account.
4. If the customer has a Citrix Cloud account:
    a) A Citrix Cloud URL displays, which you copy and send to the customer. For details of this process, see Inviting a customer to connect.
    b) The customer must add you as a full access administrator to their account. See Add administrators to a Citrix Cloud account.

You can add more administrators later and control which customers they can see on the **Manage** and **Monitor** consoles.

Add Citrix DaaS to a customer

1. Sign in to Citrix Cloud with your CSP credentials. Select **Customers** in the upper left menu.
2. From the Customer Dashboard, in the ellipsis menu for the customer, select **Add Service**.
3. In **Select a service to add**, select **Virtual Apps and Desktops**.
4. Select **Continue**.

After you complete this procedure, the customer is onboarded to your Citrix DaaS subscription.

When the onboarding completes, a new customer scope is created automatically in Citrix DaaS. The scope is visible in the **Manage > Full Configuration** display. This scope is unique to that customer. You can rename the scope, but you cannot delete it.

Use this scope to tailor access for other administrators. For example, let's say you have 10 customers and two administrators. Using the unique scope, you can restrict one administrator's access to only three of the customers. The other administrator can access one of those three customers, plus two other customers. For details, see Control administrator access to customers.

Set up a resource location

A resource location holds the machines that deliver apps and desktops for your customers, and infrastructure components such as Citrix Cloud Connectors. For details, see Connect to Citrix Cloud.

Set up catalogs and groups to deliver apps and desktops

> **Note:**
>
> To manage DaaS for a tenant customer, you must switch to the CSP customer's account. To do so, click the customer name in the upper-right menu and click **Change customer**.

A catalog is a group of identical virtual machines. When you create a catalog, an image is used (with other settings) as a template for creating the machines. For details, see Create machine catalogs.

A delivery group is a collection of machines selected from one or more machine catalogs. The delivery group specifies which users can use those machines, plus the applications or desktops available to those users. For details, see Create delivery groups.

Application groups let you manage collections of applications. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups. For details, see Create application groups.

When configuring groups, be sure that:

- The delivery group's scope is a subset of the machine catalog's scope. For example, assume the catalog's scope is A and B. The delivery group's scope can be either A or B, or A and B.
- The application group's scope is a subset of the delivery group's scope. For example, assume the delivery groups associated with an application group have scope A and B. The application group's scope can be either A or B, or A and B.

Federated domains

Federated domains enable customer users to use credentials from a domain attached to your resource location to sign in to their workspace. This allows you to provide dedicated workspaces to your customers that customer users can access using a custom workspace URL (for example, customer.cloud.com), while the resource location is still on your Citrix Cloud account. You can provide dedicated workspaces alongside the shared workspace that customers can access using your CSP workspace URL (for example, csppartner.cloud.com).

To enable customers to access their dedicated workspace, you add them to the appropriate domains that you manage. After configuring the workspace through Workspace Configuration, customers' users can sign in to their workspace and access the apps and desktops that you've made available.

Add a customer to a domain

1. Sign in to Citrix Cloud with your CSP credentials. Select **Customers** in the upper left menu.
2. From the Customer Dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Domains** tab, select **Manage Federated Domain** in the domain's ellipsis menu.
4. On the **Manage Federated Domain** card, in the **Available customers** column, select a customer you want to add to the domain. Select the plus sign next to the customer name. The selected customer now appears in the **Federated customers** column. Repeat to add other customers. When you're done, select **Apply**.

Remove a customer from a domain

When you remove a customer from a domain that you manage, the customer's users can no longer access their workspaces using credentials from your domain.

1. From the Citrix Cloud menu, select **Identity and Access Management**, then select **Domains**.
2. Locate the domain that you want to manage and select the ellipsis button. Select **Manage Federated Domain**.
3. From the list of federated customers, locate or search for the customers you want to remove and select the X button. Select **Remove all** to remove all the customers in the list from the domain. The selected customers move to the list of available customers.
4. Select **Apply**.
5. Review the customers you selected and select **Remove Customers**.

Control administrator access to customers

You can control administrator access to customers by using the unique scope that was created when you added Citrix DaaS to the customer. You can configure access when you add an administrator or later.

To learn about restricting access using roles and scopes in Citrix DaaS, see Delegated administration.

Add an administrator with restricted access

1. Sign in to Citrix Cloud with your CSP credentials. Select **Customers** in the upper left menu.
2. From the Customer Dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, select **Add Administrators From**, and then select **Citrix Identity**.

4. Type the email address of the person you're adding as an administrator, and then select **Invite**.
5. Configure the appropriate access permissions for the administrator. Citrix recommends selecting **Custom access**, unless you want the administrator to have management control of Citrix Cloud and all subscribed services.
6. After selecting **Custom access**, select one or more role and scope pairs for Citrix DaaS, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.
7. When you're done selecting role and scope pairs, select **Send Invite**.

When the administrator accepts the invitation, they have the access that you assigned.

Edit delegated administration permissions for administrators

1. Sign in to Citrix Cloud with your CSP credentials. Select **Customers** in the upper left menu.
2. From the Customer dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, select **Edit Access** from the ellipsis menu for the administrator.
4. Select and clear role and scope pairs for Citrix DaaS, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.
5. Select **Save**.

View customer administrators and their assigned roles and scopes

1. Sign in to Citrix Cloud with your CSP credentials. Select **Customers** in the upper left menu.
2. From the Customer Dashboard, select **My Services > DaaS** in the upper left menu.
3. In Citrix DaaS, select **Manage > Full Configuration**.
4. Select **Administrators** in the left pane.

Information is available on three tabs:

- The **Administrators** tab lists the administrators that have been created, plus their roles and scopes.
- The **Roles** tab lists all roles. To view role details, select the role in the middle pane. The lower portion of that pane lists the object types and associated permissions for the role. Select the **Administrators** tab in the lower pane to display a list of administrators who currently have this role.
- The **Scopes** tab lists all the scopes, including the scopes generated for customers of Citrix partners.

Configure workspaces

The customer has their own workspace with a unique `customer.cloud.com` URL. This workspace is where the customer's users access their published apps and desktops.

The workspace URL is displayed in two places:

- From the Customer dashboard, select **Workspace Configuration** from the menu in the upper left menu.
- From the Citrix DaaS **Welcome** page (the **Overview** tab), the workspace URL appears at the bottom of the page.

You can change access and authentication to a workspace. You can also customize the workspace appearance and preferences. For details, see the following articles:

- Configure workspaces
- Secure workspaces

Monitor a customer's service

The **Monitor** dashboard in a CSP environment is essentially the same as a non-CSP environment. See Monitor for details.

By default, the **Monitor** dashboard displays information about all customers. To display information about one customer, use **Select Customer**.

Keep in mind that the ability to see Monitor displays for a customer is controlled by the administrator's configured access. The access must include a role and scope pair that includes the customer's unique scope.

If you used built-in roles to configure access: The built-in roles control whether the administrator can see the **Manage** and **Monitor** displays. If you select only role and customer-scope pairs that do not include **Monitor** tab visibility, that administrator cannot see the **Monitor** tab for any selected customers. For example, if you give an administrator only **Read Only Administrator,customerABC** access, that administrator cannot see the **Monitor** tab for customer ABC, because read only administrators cannot access Monitor displays.

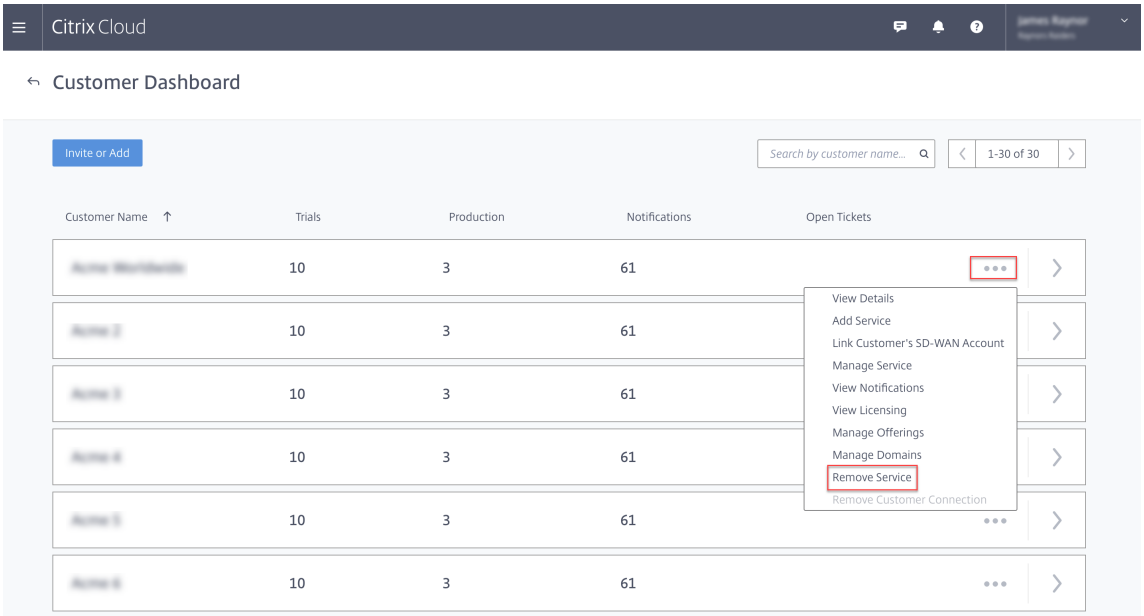
Remove a Service

Prerequisites

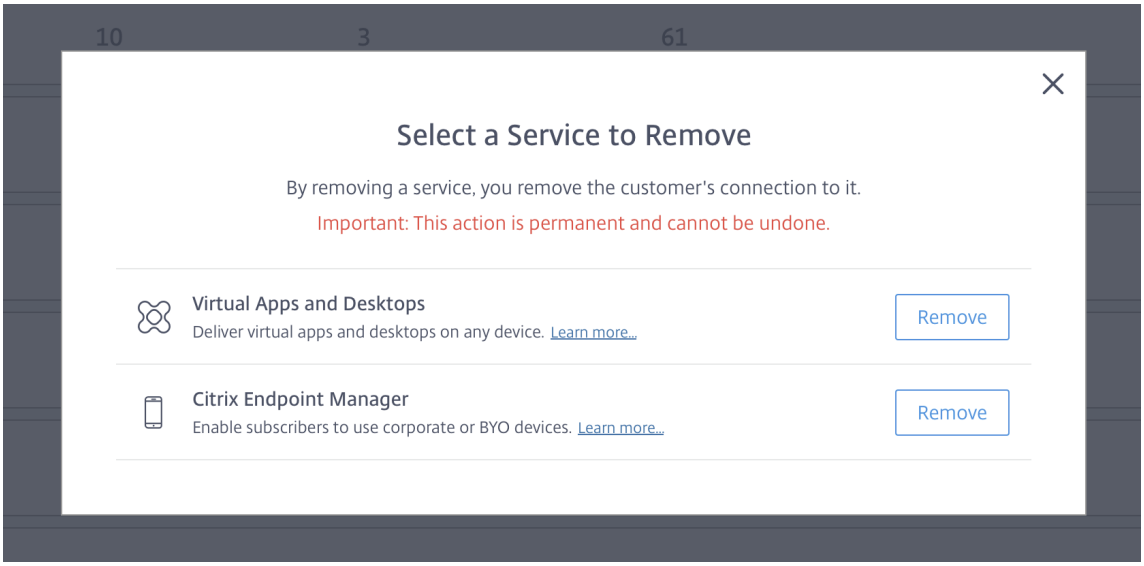
- Ensure that your customer scope is not linked to any Citrix DaaS objects. If they are linked, you cannot remove the service. To unlink scopes, go to **Citrix Studio > Administrators > Scopes** and edit the scope.

- To know your customer scope and manage it, see Create and manage scope.

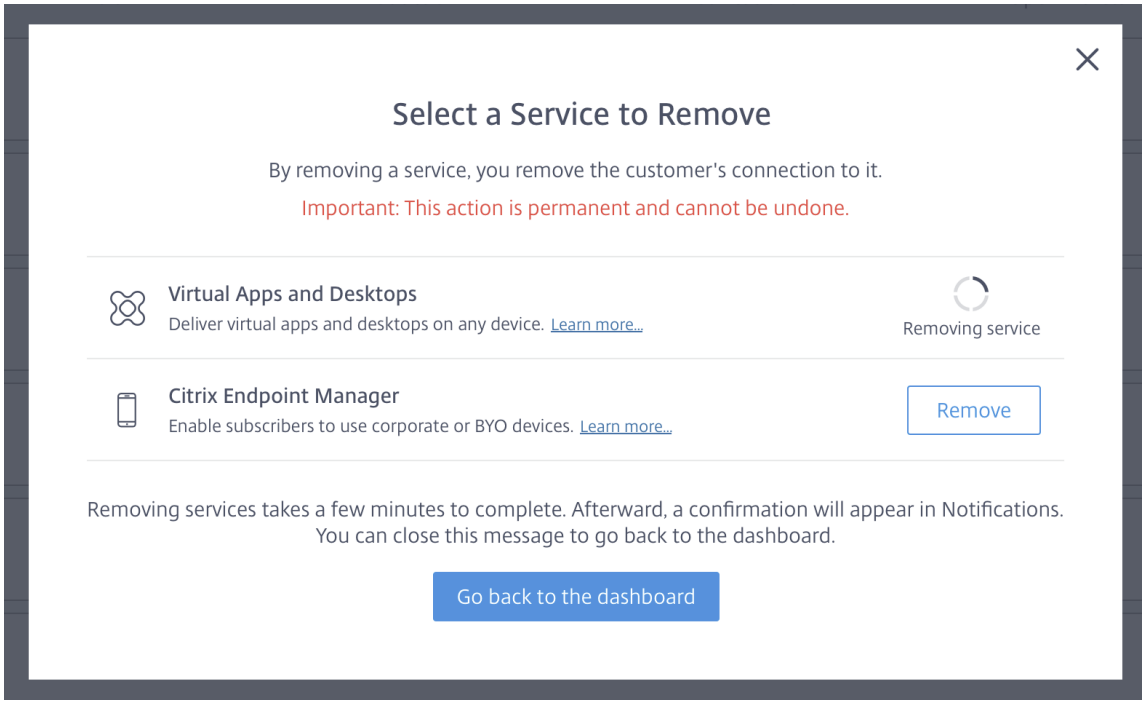
1. Sign in to Citrix Cloud with your Citrix Service Providers credentials.
2. On the **Customer dashboard**, click the **Ellipsis** menu (…) of the customer from where you want to remove a service and select **Remove Service**.



The **Service to Remove** page appears.



3. Click **Remove** to remove the service.



Citrix Gateway service

March 22, 2022

Citrix Gateway provides users with secure access to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) applications.

The Citrix Gateway service enables secure, remote access to those applications, without having to deploy Citrix Gateway in the DMZ or reconfigure your firewall. The infrastructure overhead of using Citrix Gateway moves to Citrix Cloud.

For more information about the Citrix Gateway service, see the product documentation. That content includes how to enable the Citrix Gateway service and known issues for the version you're using.

Citrix ADC is an application delivery controller that analyses application-specific traffic to distribute, optimize, and secure Layer 4-Layer 7 (L4–L7) network traffic intelligently for web applications. The Citrix ADC VPX virtual appliance can be hosted on various virtualization and cloud platforms. For details, see Deploy a Citrix ADC VPX instance.

SDKs and APIs

June 18, 2024

Citrix DaaS Remote PowerShell SDK

The Remote PowerShell SDK automates complex and repetitive tasks. It provides the mechanism to set up and manage the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) environment without using the **Manage** user interfaces.

- Cmdlet details are provided in Citrix DaaS SDK.
- The supported modules are listed in Support and limitations. That section also lists the cmdlets that are disabled in this SDK.
- Remote PowerShell SDK is available for download in the Citrix website.

This product supports PowerShell versions 3 through 7.3.

> **Note:**
>
> Currently, the support for Powershell 7.4 version is in preview.

How this SDK differs from the SDK for customer-managed deployments

In a Citrix Virtual Apps and Desktops deployment that is installed and managed by customer administrators, those administrators run cmdlets and scripts in a site containing VDAs and Delivery Controllers within a common domain structure. In contrast, Citrix DaaS splits the VDAs and Controllers into a resource location and the control plane, respectively. This split means that the original Citrix Virtual Apps and Desktops PowerShell SDK does not work in a Citrix DaaS environment. It cannot cross the secure boundary from the resource location to the control plane.

The solution is the Citrix DaaS Remote PowerShell SDK. When running in the resource location, the Remote PowerShell SDK accesses the control plane as if it is local. This provides the same functionality as a single Citrix Virtual Apps and Desktops site. There is only the lowest non-visible communication layer, enhanced to work either in a single local site or in the cloud environment. The cmdlets are the same, and most existing scripts remain unchanged.

The `Get-XdAuthentication` cmdlet provides the authorization to cross the secure resource location to control plane boundary. By default, `Get-XdAuthentication` prompts users for CAS credentials, and must be done once per PowerShell session. Alternatively, the user can define an authentication profile using an API-access Secure Client, created in the Citrix Cloud console. In both cases, the security information persists for use in subsequent PowerShell SDK calls. If this cmdlet is not explicitly run, it is called by the first PowerShell SDK cmdlet.

Prerequisites

To use the Citrix DaaS Remote PowerShell SDK, whitelist the following URLs:

Commercial

- https://accounts.cloud.com
- https://[service].citrixworkspacesapi.net/[customerid]
- https://[customerid].xendesktop.net:443

Japan

- https://accounts.citrixcloud.jp
- https://[service].citrixworkspacesapi.jp/[customerid]
- https://[customerid].apps.citrixworkspacesapi.jp:443

Government

- https://accounts.cloud.us
- https://[service].citrixworkspacesapi.us/[customerid]
- https://[customerid].xendesktop.us:443

Install and use the Remote PowerShell SDK

Requirements and considerations:

> **Note:**
>
> Do not install the Remote PowerShell SDK on a Citrix Cloud Connector machine. It can be installed on any domain-joined machine within the same resource location.
>
> Citrix does not support running this SDK's cmdlets on Cloud Connectors. The SDK's operation does not involve the Cloud Connectors.
>
> If you also have a Citrix Virtual Apps and Desktops deployment (in addition to the Citrix DaaS deployment), do not install the Remote PowerShell SDK on an on-premises Delivery Controller machine.

- Install **Microsoft Edge WebView2**.
- Ensure that PowerShell 3.0, 4.0, or 5.0 is available on the machine.
- The SDK installer downloads and installs .NET Framework 4.8 if it (or a later supported version) is not already installed.

- If the machine already has the Citrix Virtual Apps and Desktops SDK installed, remove that SDK (from Windows Programs and Features) before installing the Remote PowerShell SDK.
- For an automated environment, use the `-quiet` parameter to install the SDK without user input.

To install the Remote PowerShell SDK:

1. From the download page, download the Virtual Apps and Desktops Remote PowerShell SDK.
2. Install and run the SDK.

Installation logs are created in `%TEMP%\CitrixLogs\CitrixPoshSdk`. Logs can help resolve installation issues.

Run the SDK on a domain-joined computer within that resource location:

- Open a PowerShell command prompt. You do not need to run as an administrator.
- If you want to use the snap-in (rather than the module), add the snap-in using the `Add-PSSnapin` (or `asnp`) cmdlet.
- You can explicitly authenticate by using the `Get-XdAuthentication` cmdlet. Alternatively, run your first Remote PowerShell SDK command, which prompts you for the same authentication as `Get-XdAuthentication`. If you are using a proxy, you must authenticate to the proxy to be able to use the `Get-XdAuthentication` cmdlet. For more information, see Use the Remote PowerShell SDK with a proxy.
- To bypass the authentication prompt, you can use the `Set-XdCredentials` cmdlet to create a default authentication profile, using a Secure Client created in the Citrix Cloud console.
- Continue running PowerShell SDK cmdlets or PowerShell SDK automation scripts. See an example.

To uninstall the Remote PowerShell SDK, from the Windows feature for removing or changing programs, select **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Right-click and select **Uninstall**. Follow the dialog.

Use the Remote PowerShell SDK with a proxy If you are using a proxy, you might be unable to use the `Get-xdAuthentication` cmdlet because of the proxy blocking the HTTP requests that the cmdlet makes.

There are two ways to authenticate to the proxy. You can either use the `ProxyUseDefault` parameter or the `ProxyUsername` and `ProxyPassword` parameters:

- The `ProxyUseDefault` parameter enables authentication to the proxy by using the default proxy credentials. For example:

```
Get-XdAuthentication -ProxyUseDefault
<!--NeedCopy-->
```


- The `ProxyUsername` and `ProxyPassword` parameters enable authentication to the proxy within the PowerShell session. For example:

```
$secureString = ConvertTo-SecureString -String "password" -
    AsPlainText -Force

Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
    $secureString
<!--NeedCopy-->
```

Example activities

Common activities include setting up machine catalogs, applications, and users. A sample script is shown below.

```
    $users = "xd.local\Domain Users"

    $TSVDACatalogName = "TSVDA"

    $TSVDADGName = "TSVDA"

    $TSVDAMachineName = "xd\ds-tsvda2"

    #Create TSVDA Catalog

    $brokerUsers = New-BrokerUser -Name $users

    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
        AllocationType "Random" -Description $TSVDACatalogName -
        PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
        SessionSupport "MultiSession" -MachinesArePhysical $true

    #Add TSVDA Machine to Catalog

    $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
         -CatalogUid $catalog.uid

    #Create new desktops & applications delivery group

    $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
        $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
        " -DeliveryType DesktopsAndApps -Description $TSVDADGName

    #Create notepad application

    New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
        Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg

    #Assign users to desktops and applications

```



```
29      New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
            $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31      New-BrokerAccessPolicyRule -Name $TSVDADGName -
            IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
            DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33      New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
            DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
            $TSVDADGName
34
35      #Add machine to delivery group
36
37      Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38  <!--NeedCopy-->
```

Support and limitations

The following operating systems are supported by the Remote PowerShell SDK:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

The following Citrix Virtual Apps and Desktops PowerShell modules are supported in this release:

- Broker
- Active Directory (AD) Identity
- Machine creation
- Configuration
- Configuration logging
- Host
- Delegated administration
- Analytics

For details about cmdlets, see Citrix Virtual Apps and Desktops SDK.

After authentication, remote access remains valid in the current PowerShell session for 24 hours. After that time, you must enter your credentials.

The Remote PowerShell SDK must be run on a computer within the resource location.

The following cmdlets are disabled in remote operations to maintain the integrity and security of the Citrix Cloud control plane.

Citrix.ADIdentity.Admin.V2:

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

Citrix.Analytics.Admin.V1:

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

Citrix.DelegatedAdmin.Admin.V1:

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight

- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

Citrix.Broker.Admin.V2:

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript

- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

Citrix.ConfigurationLogging.Admin.V1:

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore

- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

Citrix.MachineCreation.Admin.V2:

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

Citrix.EnvTest.Admin.V1:

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

Citrix.Monitor.Admin.V1:

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata

- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

Citrix.Storefront.Admin.V1:

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

Citrix DaaS discovery module for App-V packages and servers

Citrix DaaS can deliver applications contained in App-V packages to your endpoints using either of the following methods:

- Single admin management method (accessing packages from a network share)
- Dual admin management method (accessing packages from a Microsoft App-V Management Server)

The process of registering App-V packages, Microsoft App-V Management, and Publishing Servers with the Application Library using Citrix DaaS differs slightly from registering packages using an on-premises deployment. However, the process of assigning applications to users and launching them on a user's endpoint is identical.

The Citrix DaaS management console in Citrix Cloud cannot view files in a resource location. Also, it cannot directly discover App-V packages or Microsoft App-V servers in your infrastructure. The discovery module provides functions that discover App-V package information in your on-premises infrastructure and uploads the package information to your Citrix DaaS. Package information includes App-V packages, Microsoft App-V servers, and the apps that the packages contain.

The discovery module uses the Virtual Apps and Desktops Remote PowerShell SDK. It can discover package information from either a network share or a Microsoft App-V Management Server. You use the discovery module on a machine in your resource location.

Prerequisites for using the discovery module:

- Verify that PowerShell 3.0 or later is available on the machine.

- Verify that the Citrix Virtual Apps and Desktops Remote PowerShell SDK is installed on the machine.
- Verify that you have access to the network share containing the App-V packages.
- Verify that you have access to the server where the Citrix Cloud Connectors are installed and the Microsoft App-V Management Server is hosted.

Add App-V packages to the Application Library in Citrix Cloud

The following procedure is valid for adding App-V packages from network shares (single admin management) and adding all published App-V packages from the Microsoft App-V Management Server (dual admin management). With the dual admin management method, you must manage the added App-V packages just as you do when using the single admin management method.

1. Download the discovery module from the Citrix DaaS downloads page https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html. Extract the zip file `Citrix.Cloud.AppLibrary.Admin.v1.psm1` to a convenient folder.

   > **Note:**
   >
   > This file is also provided on the Citrix Virtual Apps and Desktops ISO in `Support\Tools\Scripts`. You can copy it locally or reference it directly from the CD drive.

2. Verify that the Virtual Apps and Desktops Remote PowerShell SDK is installed on your machine
3. Navigate to the folder containing the discovery module. In the PowerShell window, type the full path of the folder containing the discovery module and then press **Enter**.
4. Import the discovery module with the command `Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1`.
5. Add the App-V packages to the Application Library in Citrix Cloud using either of the following methods.

   - To add App-V packages from a network share, run the PowerShell cmdlet: `Import-AppVPackageToCloud`.

     For example: `Import-AppVPackageToCloud –PackagePath \\AppVSrv\share\Notepad++.appv`

     For cmdlet help, type `Get-Help Import-AppVPackageToCloud`.

   - To add App-V packages from a Microsoft App-V Management Server, run the PowerShell cmdlet: `Import-AppVPackagesFromManagementServerToCloud`

     For example: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

For cmdlet help, type `Get-Help Import-AppVPackagesFromManagementServerToCloud`

This command imports all published App-V packages from the Microsoft App-V Management Server to Citrix Cloud.

After adding the App-V packages to Citrix Cloud, you must manage them as you do using the single admin management method.

6. Sign in to Citrix Cloud. Select the target customer. After the script runs successfully, the App-V packages are added to the Application Library in Citrix Cloud.

High-level PowerShell functions

The module contains the following high-level functions that you can call from your own PowerShell script:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Discovers and uploads to Citrix DaaS all the information necessary to publish applications from a single App-V Package.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Discovers the UNC paths of packages published by the Management Server and calls **Import-AppVPackageToCloud** for each one in turn.

  Packages discovered in this way are loaded to Citrix DaaS using the single admin management method. Citrix DaaS cannot deliver packages using the dual admin management method.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Discovers Microsoft App-V Management and Publishing Servers and imports the content to the Application Library. This cmdlet imports all the packages managed using Microsoft App-V Management Server and related information. Servers can be added and removed through PowerShell.

  This cmdlet adds App-V packages in dual admin mode. Only App-V packages that are published on the Microsoft App-V Management Server, and which have AD groups added, are imported. If you make changes to the Microsoft App-V Management Server, rerun this cmdlet to synchronize the Application Library with the Microsoft App-V Management Server.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Removes the Microsoft App-V Management and Publishing Servers added to Application Library.

  This cmdlet removes the specified Microsoft App-V Management and Publishing Servers, plus all the associated App-V packages.

Run the discovery module for App-V packages and servers on a domain-joined computer within that resource location. Follow the guidance in Install and use the Remote PowerShell SDK to get started. Continue running PowerShell cmdlets or scripts. See the following examples.

Example activities

Import the Citrix DaaS App-V package discovery module.

```
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
<!--NeedCopy-->
```

Loop through the App-V Package store directory and upload each package.

```
Get-ChildItem -Path "\\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName
 }

<!--NeedCopy-->
```

Discover and upload packages registered with a Microsoft App-V management server.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
<!--NeedCopy-->
```

Discover Microsoft App-V Management and Publishing Servers and add the configuration to the Application Library. This also imports all the packages managed by the Microsoft App-V Management Server in dual admin mode.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer.domain.net  – PublishingServerUrl http://AppVManagementServer.domain.net:8001
<!--NeedCopy-->
```

Read the PowerShell help documentation included in the module.


```
Get-Help Import-AppVPackageToCloud
<!--NeedCopy-->
```

Limitations

- You cannot discover App-V packages on your resource location infrastructure directly from the Citrix DaaS management console in Citrix Cloud. For more information on Citrix Cloud, see the Citrix Cloud documentation.
- Citrix DaaS management console in Citrix Cloud does not have a live connection to the Microsoft App-V Management server. Changes to Packages and other configuration in the Microsoft App-V Management server are not reflected in the Citrix DaaS management console until `Import-AppVDualAdminCloud` is rerun.

Monitor Service OData API

In addition to using the Monitor functions to display historical data, you can query data using the Monitor Service's API. Use the API to:

- Analyze historical trends for planning
- Perform detailed troubleshooting of connection and machine failures
- Extract information for feeding into other tools and processes; for example, using Microsoft Excel's PowerPivot tables to display the data in different ways
- Build a custom user interface on top of the data that the API provides

For details, see Monitor Service OData API. To access the Monitor Service API, see Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Citrix DaaS APIs

The Citrix DaaS APIs are available at https://developer.cloud.com/citrixworkspace/citrix-daas.

Disclaimer

This software / sample code is provided to you "AS IS"with no representations, warranties, or conditions of any kind. You may use, modify, and distribute it at your own risk. CITRIX DISCLAIMS ALL WARRANTIES WHATSOEVER, EXPRESS, IMPLIED, WRITTEN, ORAL OR STATUTORY, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. Without limiting the generality of the foregoing, you acknowledge and agree that (a) the software / sample code might exhibit errors, design flaws or other problems, possibly

resulting in loss of data or damage to property; (b) it might not be possible to make the software / sample code fully functional; and (c) Citrix may, without notice or liability to you, cease to make available the current version and/or any future versions of the software / sample code. In no event must the software / code be used to support of ultra-hazardous activities, including but not limited to life support or blasting activities. NEITHER CITRIX NOR ITS AFFILIATES OR AGENTS WILL BE LIABLE, UNDER BREACH OF CONTRACT OR ANY OTHER THEORY OF LIABILITY, FOR ANY DAMAGES WHATSOEVER ARISING FROM USE OF THE SOFTWARE / SAMPLE CODE, INCLUDING WITHOUT LIMITATION DIRECT, SPECIAL, INCIDENTAL, PUNITIVE, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. You agree to indemnify and defend Citrix against any claims arising from your use, modification, or distribution of the code.