Citrix Virtual Apps and Desktops 7 1912 LTSR

Contents

Citrix Virtual Apps and Desktops 7 1912 Long Term Service Release (LTSR)

May 2, 2024

> **Important:**
>
> The product lifecycle strategy for Current Releases (CR) and Long Term Service Releases (LTSR) is described in Lifecycle Milestones.

Citrix Virtual Apps and Desktops is a virtualization solution that give IT control of virtual machines, applications, licensing, and security, while providing access anywhere for any device.

The Long Term Service Release (LTSR) program for Citrix Virtual Apps and Desktops provides stability and long-term support for Citrix Virtual Apps and Desktops releases.

Cumulative Update 9 (CU9) is the most recent update to the 1912 LTSR. LTSRs are also available for XenApp and XenDesktop Version 7.15. If you are new to the LTSR program, there is no need for you to install the 1912 LTSR initial release. Instead, we recommend that you begin right with the 1912 LTSR CU9.

- For use case information, see https://www.citrix.com/products/citrix-virtual-apps-and-desktops/.
- To learn about components and technologies in Citrix Virtual Apps and Desktops deployments, see the Technical overview.

Earlier releases

Documentation for other currently available releases is located in Citrix Virtual Apps and Desktops.

For even earlier releases, documentation is archived in Legacy Documentation.

Citrix Virtual Apps and Desktops in Citrix Cloud

The Citrix Cloud Virtual Apps and Desktops offering is the Citrix DaaS. For service documentation, see Citrix DaaS.

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

Helpful links

- Citrix Supportability Pack
- LTSR Frequently Asked Questions (FAQs)
- Citrix Virtual Apps and Desktops servicing options
- Product Lifecycle dates
- LTSR Program for Receiver for Windows

Citrix product name and number changes

For information about product name and version number changes that were introduced in 2018, see New names and numbers.

What's new

April 23, 2024

About this release

About Cumulative Update 9 (CU9)

About Cumulative Update 8 (CU8)

About Cumulative Update 7 (CU7)

About Cumulative Update 6 (CU6)

About Cumulative Update 5 (CU5)

About Cumulative Update 4 (CU4)

About Cumulative Update 3 (CU3)

About Cumulative Update 2 (CU2)

About Cumulative Update 1 (CU1)

About 1912 LTSR (initial release)

Cumulative Update 9 (CU9)

April 30, 2024

Release date: April 30, 2024

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 9 (CU9) fixes more than 15 issues reported since the release of 1912 LTSR CU8.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.17.2.0_BUILD_40000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU9 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU9 - using the CU9 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU9 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU9. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU9. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.9000.9299	
Multi-session VDA	1912.0.9000.9299	
Delivery Controller	1912.0.9000.9299	
Citrix Studio	1912.0.9000.85	
Citrix Director	1912.0.9000.14	
Citrix Group Policy Management	7.24.9000.0	
Citrix Group Policy Client-Side Extension	7.24.9000.0	
Citrix StoreFront	1912.0.9000.17	
Citrix Provisioning	1912.80.iso	
Universal Print Server	1912.0.9000.15	
Session Recording	1912.0.9000	
Linux VDA	1912.0.9000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.9000.3	
Citrix Federated Authentication Service	1912.0.9000.14	
Browser Content Redirection	15.19.9000.16	

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	22.11
App protection policies	1912 LTSR CU8
HDX RealTime Optimization Pack	2.9 LTSR CU7
License Server	11.17.2.0 Build 47000
User personalization layer	23.12.4
Session Recording web player	1912.0.9000
Self-Service Password Reset	1912.0.8000
Windows 10 32-bit	Refer to initial release documentation
Workspace Environment Management	2305
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of appli-

cations and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

June 7, 2024

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU8:

Citrix Provisioning

Citrix Provisioning 1912 CU9 documentation provides specific information about the updates in this release.

Delivery Controller

- Create\Update machine catalog task fails in Availability Zone B but works fine for Availability Zone A and C because a volume service instance could not be launched in your cloud connection. Run the below command to update the Site Database table to use the new VolumeWorkerTemplate on the SQL server.

  ```
  UPDATE HostingUnitServiceSchema.VolumeServiceConfigurationBaseTemplate
  SET TemplateId = 'ami-09b42976632b27e9b'
  WHERE RegionName = 'ap-southeast-2'
  ```


> **Note:** Availability Zone may be different for different customers.

[CVADHELP-24094]

- Updates on the `MonitorData.ResourceUtilization` table in the monitoring database are delayed. [CVADHELP-22724]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU9 documentation contains no fixed issues.

Metainstaller

- Upload authorization: If you plan to upload diagnostic collections to Citrix, you must have a Citrix or Citrix Cloud account. (These are the credentials you use to access Citrix downloads or access the Citrix Cloud Control Center.) After your account credentials are validated, a token is issued.
  If you authenticate with a Citrix account or a Citrix Cloud account, click a link to access Citrix Cloud using HTTPS with your default browser. After you enter your Citrix Cloud credentials, the token is displayed. Copy the token and then paste it into Scout. You can then continue in the Scout wizard.
  The token is stored locally on the machine where you're running Scout. To enable use of that token the next time you run Collect or Trace & Reproduce, select the Store token and skip this step in the future check box.
  You must reauthorize each time you select Schedule on the Scout opening page. You cannot use a stored token when creating or changing a schedule.
  [CVADHELP-24415]

Profile Management

Profile Management 1912 CU9 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU9 documentation provides specific information about the updates in this release.

StoreFront

StoreFront 1912 CU9 documentation provides specific information about the updates in this release.

Universal Print Server

Printing

- Printers connected to Universal Print Server might not appear in sessions for printing. The issue occurs when the `httpd.conf` file in Universal Print Server is updated. [CVADHELP-21139]
- When you use VDA version 1912 CU5 and OS version 2012 R2, various print jobs are failing from the production Citrix UPS print server with the following error message:
  `CCgpStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenSt : Failed to Open Stream. Abort Job.`
  [CVADHELP-22354]

VDA for single-session OS

Printing

- Attempt to print a file through local printers using Citrix Workspace app for Mac running macOS Sonoma might fail with the following error message:

  `Error: Printer not activated. Error code -41`

  [CVADHELP-23839]
- When you restart a VDA with the Universal Print Server policies enabled, load balancing for Universal Print Servers might fail to start. [CVADHELP-23714]
- Local printers might not get redirected to the session during the first launch. However, the local printers are redirected during subsequent launches. [CVADHELP-23334]

Session/Connection

- `CtxSvcHost` (`CtxSmartCardSvc`) might exit unexpectedly when you log off from the VDA. [CVADHELP-23172]
- The Microsoft Teams redirection key MSTeamsRedirSupport under the registry `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` might be missing when you reconnect to a user device through a user session. The issue occurs when an RDP session is still existing. [CVADHELP-19993]

- If printers or print servers are unreachable, session logon and logoff might take a lot of time to respond. [CVADHELP-23637]
- The `WebSocketService.exe` process fails to start after a VDA reboot on the leap day. [CVADHELP-24771]
- Microsoft Teams 2.1 is not optimized by default on the VDA. [CVADHELP-24767]

VDA for multi-session OS

Printing

- Attempt to print a file through local printers using Citrix Workspace app for Mac running macOS Sonoma might fail with the following error message:

  ```
  Error: Printer not activated. Error code -41
  ```

  [CVADHELP-23839]
- When you restart a VDA with the Universal Print Server policies enabled, load balancing for Universal Print Servers might fail to start. [CVADHELP-23714]
- Local printers might not get redirected to the session during the first launch. However, the local printers are redirected during subsequent launches. [CVADHELP-23334]

Session/Connection

- If the Session Recording agent is not installed on the VDA and you run `Get-BrokerSessionRecordingS` , `Start-BrokerSessionRecording`, and `Stop-BrokerSessionRecording` PowerShell commands, then the VDA deregisters and registers again with the Delivery Controller within a few seconds. This action has no impact on the existing sessions. If the Session Recording agent is installed on the VDA, the PowerShell commands work without issue. [CVADHELP-23686]
- The `WebSocketService.exe` process might consume more memory than expected on the VDAs. [CVADHELP-23870]
- `CtxSvcHost` (`CtxSmartCardSvc`) might exit unexpectedly when you log off from the VDA. [CVADHELP-23172]
- The `WebSocketService.exe` process fails to start after a VDA reboot on the leap day. [CVADHELP-24771]

System Exceptions

- When you upgrade a VDA from 1912 LTSR CU5 to CU6, a fatal exception occurs on Wdica.sys, and a blue screen with a bug check code, 0x000000CE is displayed. [CVADHELP-22365]

Cumulative Update 8 (CU8)

October 30, 2023

Release date: September 11, 2023

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 8 (CU8) fixes more than 50 issues reported since the release of 1912 LTSR CU7.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.17.2.0_BUILD_40000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU8 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU8 - using the CU8 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU8 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU8. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU8. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU8 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.8000	
Multi-session VDA	1912.0.8000	
Delivery Controller	1912.0.8000	
Citrix Studio	1912.0.8000	
Citrix Director	1912.0.8000	
Citrix Group Policy Management	7.24.8000	
Citrix Group Policy Client-Side Extension	7.24.8000	
Citrix StoreFront	1912.0.8000	
Citrix Provisioning	1912.80.iso	
Universal Print Server	1912.0.8000	
Session Recording	1912.0.8000	
Linux VDA	1912.0.8000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.8000	
Citrix Federated Authentication Service	1912.0.8000	

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Browser Content Redirection	15.19.8000	

Citrix Virtual Apps and Desktops 7 1912 LTSR CU8 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	22.11
App protection policies	1912 LTSR CU8
HDX RealTime Optimization Pack	2.9 LTSR CU7
License Server	11.17.2.0 Build 44000
User personalization layer	23.6.2
Session Recording web player	1912.0.8000
Self-Service Password Reset	1912.0.8000
Windows 10 32-bit	Refer to initial release documentation
Workspace Environment Management	2305
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU8 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

April 18, 2024

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU7:

Citrix Director

- Once a session is established, the display name of the machine in the Machine Details page on Citrix Director reverts to the Delivery Group name. [CVADHELP-18746]

Citrix Policy

- The CseEngine.exe service might consume higher memory than expected on the VDAs. [CVADHELP-19226]

- The virtual channel policy value **VirtualChannelWhiteList** in the HKEY_LOCAL_MACHINE\SOFTWARE\Policie setting might become corrupt and fail to apply on the VDA after restart. This issue occurs when you delete files from the C:\ProgramData\Citrix\GroupPolicy folder or cut the contents in the folder and paste them in a different location. [CVADHELP-21420]
- Group Policy Modeling value shows the disabled value instead of the actual value. For example, the **Display memory unit** value is displayed as disabled instead of the actual value, 65536 KB. [CVADHELP-22484]
- Attempts to apply Citrix user policies on different domains might fail when you upgrade a VDA to version LTSR CU7. [CVADHELP-22992]

Citrix Provisioning

Citrix Provisioning 1912 CU8 documentation provides specific information about the updates in this release.

Citrix Studio

- When you attempt to add machines to a delivery group, the machine allocation page might disappear. As a result, users are not assigned in the Machine Allocation page and the machines are set to **Unassigned**. [CVADHELP-20000]
- When you add an App-V application, the **Delivered As** field might be blank. This issue occurs when you add the application and change the name of the application from its default. [CVADHELP-21138]

Delivery Controller

- If Site aggregation or delivery groups with specific broker policies are enabled, starting an application or a desktop creates a new session instead of reconnecting to an existing one. [CVADHELP-19879]
- When the reserved memory is lesser than the configured memory, attempts to power on a virtual machine might fail with this error message:

  Invalid memory setting: Memory reservation (sched.mem.min) should be equal to memsize (94208). The virtual machine failed to start. Failed to turn on the MemSched module. Error parsing scheduler-specific configuration parameters.

  [CVADHELP-21052]

- Attempts to create a new hosting connection on the XenServer pool master might fail with this error message:

  The host server cannot be contacted. check that the connection has a valid host address and that the host server is powered on and working properly.

  Failed to obtain XenServer host list.

  [CVADHELP-21320]

- Citrix Broker Service (Brokerservice.exe) might exit unexpectedly after disconnecting from the License Server. [CVADHELP-21615]
- There might be a mismatch in the number of sessions displayed on Citrix Studio and Citrix Director. Citrix Studio shows fewer active sessions than Citrix Director. [CVADHELP-21727]
- Certain Citrix XML performance counters might not be added to the performance monitor graph. [CVADHELP-21785]
- Attempts to import Local Host Cache (LHC) might fail with an Event ID, 505. The issue occurs if you have added the registry value, **XmlStaTicketLifetimeInSeconds** to the **Set-BrokerServiceConfigurationData** command. [CVADHELP-22967]
- With this fix, Machine Creation Services supports vSAN 8. [CVADHELP-23415]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU8 documentation provides specific information about the updates in this release.

Metainstaller

- When you install VDA for multi-session OS with the **Enable connections to a server machine** option enabled and upgrade the VDA, **Additional Components for Master MCS Image** text is displayed in the upgrade wizard instead of **Additional Components for Enable Brokered Connections to a Server**.

  > **Note:**
  >
  > This fix is applicable from Citrix Virtual Apps and Desktops 1912 LTSR CU8 and upgrades from 1912 LTSR CUs to 1912 LTSR CU8 and above. However, the fix is not applicable for XenApp and XenDesktop 7.15 LTSR CUs and Upgrades from XenApp and XenDesktop 7.15 LTSR to Citrix Virtual Apps and Desktops 1912 LTSR CUs.

  [CVADHELP-21557]

Microsoft Teams Optimization

- Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might exit unexpectedly while using Microsoft Teams. [CVADHELP-22561]

Profile Management

Profile Management 1912 CU8 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU8 documentation contains no fixed issues.

StoreFront

StoreFront 1912 CU8 documentation provides specific information about the updates in this release.

VDA for single-session OS

Installing, Uninstalling, Upgrading

- After you upgrade a VDA to 1912 LTSR CUx or 2203 LTSR CUx, the value of **ApplicationLaunchWaitTimeoutMS** under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\v might not be restored. [CVADHELP-22758]

Keyboard

- On VDA version 1912 CU5 running on Microsoft Windows 10 version 21H1 or 21H2, the keyboard might not be synchronized with the endpoint correctly in the HDX session. [CVADHELP-21534]

Session/Connection

- Attempts to enable SSL on VDAs might fail when the certificate template is created with **Key Storage Provider** as the **Cryptography** provider. [CVADHELP-21485]
- Internal websites of certain third-party applications with VDA installed might not allow access without a prompt. [CVADHELP-22081]

- With the Enlightened Data Transport (EDT) protocol enabled, Citrix sessions might freeze when you update the VDA from version 1912 LTSR CU6 to version 1912 LTSR CU7. [CVADHELP-23370]
- If the Session Recording agent is not installed on the VDA and you run **Get-BrokerSessionRecordingStatus**, **Start-BrokerSessionRecording**, and **Stop-BrokerSessionRecording** PowerShell commands, then the VDA deregisters and registers again with the Delivery Controller within a few seconds. This action has no impact on the existing sessions. If the Session Recording agent is installed on the VDA, the PowerShell commands work without issue. [CVADHELP-23491]

Smart Cards

- When you start a session using a smart card and try to unlock a locked session, you might receive a prompt to enter a password instead of a smart card PIN. This issue occurs when you have installed the Microsoft patch, KB5018410. [CVADHELP-21665]

System Exceptions

- VDAs might encounter a bug check code, 000000CA if a USB device is inserted and removed quickly. [CVADHELP-21459]
- During session launch, VDAs might experience a fatal exception on ControlUP Custom Virtual Channel Initialization and display a blue screen. [CVADHELP-21885]
- The HTML5 Video Redirection Service (CtxHdxWebSocketService) might exit unexpectedly. [CVADHELP-22012]
- The Citrix PDF Universal Printer driver might exit unexpectedly because of the faulting acfpdfuamd64.dll module. [CVADHELP-22085]
- VDAs might experience a fatal exception on Wdica.sys and display a blue screen. [CVADHELP-22482]
- The graphics status indicator process, GfxStatusIndicator.exe might exit repeatedly. [CVADHELP-23142]

VDA for multi-session OS

Keyboard

- When you open 2 instances of an application and set the **DisableToggler** setting to five seconds, you might have to wait for about 30 seconds before typing in the second application. [CVADHELP-22491]

Session/Connection

- The recording status in the Session Recording Player might not change from **Live** to **Complete** after recording complete and even after logging off. The issue occurs on Microsoft Windows 10 or a published application. [CVADHELP-17556]
- Attempts to enable SSL on VDAs might fail when the certificate template is created with Key Storage Provider as the Cryptography provider. [CVADHELP-21485]
- Attempts to open PDF files using Adobe Acrobat Reader DC in Citrix Servers might fail with this error message:

  Werfault.exe - Application Error

  The application was unable to start correctly (0xc0000142). Click Ok to close the application.

  [CVADHELP-21779]
- Session Recording might continue to record even after you log off from the session or if the session is disconnected. [CVADHELP-22097]
- The user session might refresh continuously when you start a Linux session running Ubuntu through Windows Subsystem for Linux GUI (WSLg). [CVADHELP-22198]
- When you open 2 instances of an application and set the **DisableToggler** setting to five seconds, you might have to wait for about 30 seconds before typing in the second application. [CVADHELP-22679]
- After you upgrade a VDA from 1912 LTSR CU5 to CU6 or CU7, the **LogoffCheckerStartupDelayInSeconds** and **SeamlessFlags** values under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS might not be restored. [CVADHELP-22783]
- When you reconnect to a session after changing the client's DPI value, the new value might not be applied to the session. [CVADHELP-23007]
- With the Enlightened Data Transport (EDT) protocol enabled, Citrix sessions might freeze when you update a VDA from version 1912 LTSR CU6 to version 1912 LTSR CU7. [CVADHELP-23370]

Smart Cards

- When you start a session using a smart card and try to unlock a locked session, you might receive a prompt to enter a password instead of a smart card PIN. This issue occurs when you have installed the Microsoft patch, KB5018410. [CVADHELP-21665]

System Exceptions

- The Terminal Services process might exit unexpectedly because of the faulting module, RPM.dll. [CVADHELP-21108]
- The Service Host (svchost.exe) process might consume higher memory than expected on a VDA for multi-session OS when the UiPath Remote Runtime component is installed. [CVADHELP-21678]
- During session launch, VDAs might experience a fatal exception on ControlUP Custom Virtual Channel Initialization and display a blue screen. [CVADHELP-21885]
- The HTML5 Video Redirection Service (CtxHdxWebSocketService) might exit unexpectedly. [CVADHELP-22012]
- The Citrix PDF Universal Printer driver might exit unexpectedly because of the faulting acfpdfuamd64.dll module. [CVADHELP-22085]
- When you upgrade a VDA from 1912 LTSR CU5 to CU6, a fatal exception occurs on Wdica.sys, and a blue screen with a bug check code, 0x000000CE is displayed. [CVADHELP-22365]
- VDAs might experience a fatal exception on Wdica.sys and display a blue screen. [CVADHELP-22482]

Cumulative Update 7 (CU7)

April 11, 2023

Release date: March 15, 2023

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 7 (CU7) fixes more than 55 issues reported since the release of 1912 LTSR CU6.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.17.2.0_BUILD_40000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU7 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU7 - using the CU7 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU7 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU7. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU7. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU7 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.7000	
Multi-session VDA	1912.0.7000	
Delivery Controller	1912.0.7000	
Citrix Studio	1912.0.7000	
Citrix Director	1912.0.7000	

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Citrix Group Policy Management	7.24.7000	
Citrix Group Policy Client-Side Extension	7.24.7000	
Citrix StoreFront	1912.0.7000	
Citrix Provisioning	1912.37.iso	
Universal Print Server	1912.0.7000	
Session Recording	1912.0.7000	
Linux VDA	1912.0.7000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.7000	
Citrix Federated Authentication Service	1912.0.7000	
Browser Content Redirection	15.19.7000	

Citrix Virtual Apps and Desktops 7 1912 LTSR CU7 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	22.11
App protection policies	1912 LTSR CU7
HDX RealTime Optimization Pack	2.9 LTSR CU6
License Server	11.17.2.0 Build 40000
User personalization layer	22.11.3
Session Recording web player	1912.0.7000
Teams optimization	1912.12.0
Self-Service Password Reset	1912.0.7000

Compatible components and features	Version as shown in Programs and Features
Windows 10 32-bit	Refer to initial release documentation
Workspace Environment Management	2212
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU7 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk

Excluded components and features
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

June 13, 2023

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU6:

Citrix Director

- When a VDA and a Delivery Controller are installed on the same machine, the VDA might not be visible in the **Filter > Machines > All Machines** view of Citrix Director. [CVADHELP-20271]

Citrix Policy

- With this fix, multiple memory issues have been fixed. [CVADHELP-19916, CVADHELP-20908, CVADHELP-20909]
- The policy setting value might appear as **Kpbs** instead of **Kbps**. [CVADHELP-21527]

Citrix Provisioning

Citrix Provisioning 1912 CU7 documentation provides specific information about the updates in this release.

Citrix Studio

- Attempts to create a new Citrix Virtual Apps and Desktops site with the DBCreator, Securityadmin, and Public permissions from the Citrix Studio console might fail. [CVADHELP-20594]

Delivery Controller

- Citrix Studio might display Security Identifiers (SID) of machines instead of account names if some domain controllers are shut down. [CVADHELP-19312]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU7 documentation provides specific information about the updates in this release.

Licensing

- The Citrix Studio (Licensing Admin PowerShell snap-in) might fail to communicate with the Licensing servers only when strong cipher suites are allowed. [CVADHELP-20056]

Microsoft Teams Optimization

- Microsoft Teams calls might disconnect shortly after initial connection. [CVADHELP-20042]
- The HTML5 Video Redirection Service (CtxHdxWebSocketService) might exit unexpectedly. [CVADHELP-21074]

Profile Management

Profile Management 1912 CU7 documentation provides specific information about the updates in this release.

Security Issues

- This fix addresses a security issue. For more information, see Knowledge Center article CTX559370.

Session Recording

Session Recording 1912 CU7 documentation contains no fixed issues.

StoreFront

StoreFront 1912 CU7 documentation provides specific information about the updates in this release.

Universal Print Server

Server

- Attempts to print a document from Citrix Universal Print Server on the shared session printers might fail. The issue occurs after upgrading to Citrix Virtual Apps and Desktops 1912 LTSR CU4. [CVADHELP-19431]

VDA for single-session OS

Keyboard

- The virtual keyboard might not appear automatically in a published application when you place the cursor in an editable field. [CVADHELP-21419]

Session/Connection

- With the Virtualization Based Security feature turned on, when you access a workstation using Remote PC Access through a user device and then disconnect, a black screen might appear when you physically reach the workstation and log on to the system. [CVADHELP-20342]
- Attempts to reconnect to a session might fail. [CVADHELP-20439]
- The Citrix software graphics process (Ctxgfx.exe) might exit unexpectedly when the **session watermark** policy is enabled on the VDA. [CVADHELP-20607]
- When you take over your currently connected user session from a local console of a physical VDA, all or some displays that are attached to the physical VDA might remain in power saving mode. [CVADHELP-20619]
- During session reconnection, the battery status indicator might disappear if the power cord is plugged in. [CVADHELP-20768]
- When you plug in a monitor, the seamless window might disappear. [CVADHELP-21084]
- With the latest version of Chrome, the browser content redirection extension might fail and cause the Optimized Microsoft Teams call to disconnect. [CVADHELP-21336]

System Exceptions

- VDAs might experience a fatal exception and display a blue screen when a session that is utilizing the Enlightened Data Transport (EDT) protocol disconnects or reconnects. [CVADHELP-20293]

- The wfshell.exe process might exit unexpectedly due to the faulting CtxUiMon.dll module. [CVADHELP-20312]
- If Microsoft Azure Information Protection (AIP) is installed and Citrix Hook is enabled, Microsoft 365 applications might exit unexpectedly. [CVADHELP-20642]
- The CseEngine.exe service might consume high memory than expected on the VDAs. [CVADHELP-20909]
- When you start a published desktop, open **File Explorer** and click the redirected local C drive under **Network > \Client**, the **File Explorer** might exit unexpectedly. [CVADHELP-21089]
- VDAs might experience a fatal exception on tdica.sys and display a blue screen. The issue occurs when you are attempting to reconnect to a session. [CVADHELP-21318]

User Experience

- When you sign in from Citrix Gateway and **LDAP SSO Name Attribute** is set to **UserPrincipalName**, the Citrix watermark might display the sign-in name incorrectly. [CVADHELP-21815]

VDA for multi-session OS

Keyboard

- The virtual keyboard might not appear automatically in a published application when you place the cursor in an editable field. [CVADHELP-21419]

Printing

- On Mac clients, the printer's default paper size might not be retained after you log off and log back in. [CVADHELP-21161]

Session/Connection

- When you start an application from a VDA as an anonymous user, this error message might appear:

  Incorrect username and password.

  [CVADHELP-19802]
- The screen saver might appear in a session reconnected from a seamless published app through a VDA that has the screen saver enabled. [CVADHELP-20431]

- With this fix, you can use wildcards in the process path while adding virtual channels to the allow list. For more information, see the Virtual channel security documentation. [CVADHELP-20478]
- During session reconnection, the battery status indicator might disappear if the power cord is plugged in. [CVADHELP-20768]
- VDAs might become unresponsive when the RPM is holding up a logoff process by not releasing a lock as expected. [CVADHELP-20892]
- The Virtual Channel Allow List feature might not work in Microsoft Teams. [CVADHELP-21287]
- With the latest version of Chrome, the browser content redirection extension might fail and cause the Optimized Microsoft Teams call to disconnect. [CVADHELP-21336]

System Exceptions

- The wfshell.exe process might exit unexpectedly due to the faulting CtxUiMon.dll module. [CVADHELP-20312]
- The CseEngine.exe service might consume high memory than expected on the VDAs. [CVADHELP-20909]
- When you start a published desktop, open **File Explorer** and click the redirected local C drive under **Network > \Client**, the **File Explorer** might exit unexpectedly. [CVADHELP-21089]

User Experience

- When you sign in from Citrix Gateway and **LDAP SSO Name Attribute** is set to **UserPrincipalName**, the Citrix watermark might display the sign-in name incorrectly. [CVADHELP-21815]

Cumulative Update 6 (CU6)

December 13, 2022

Release date: October 31, 2022

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 6 (CU6) fixes more than 35 issues reported since the release of 1912 LTSR CU5.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.17.2.0_BUILD_37000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU6 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU6 - using the CU6 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU6 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU6. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU6. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU6 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.6000	
Multi-session VDA	1912.0.6000	
Delivery Controller	1912.0.6000	
Citrix Studio	1912.0.6000	
Citrix Director	1912.0.6000	
Citrix Group Policy Management	7.24.6000	
Citrix Group Policy Client-Side Extension	7.24.6000	
Citrix StoreFront	1912.0.6000	
Citrix Provisioning	1912.31.iso	
Universal Print Server	1912.0.6000	
Session Recording	1912.0.6000	
Linux VDA	1912.0.6000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.6000	
Citrix Federated Authentication Service	1912.0.6000	
Browser Content Redirection	15.19.6000	
Citrix Probe Agent	2009	Download

Citrix Virtual Apps and Desktops 7 1912 LTSR CU6 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	22.08
App protection policies	1912 LTSR CU6

Compatible components and features	Version as shown in Programs and Features
HDX RealTime Optimization Pack	2.9 LTSR CU5
License Server	11.17.2.0 Build 40000
User personalization layer	22.6.1
Session Recording web player	1912.0.6000
Teams optimization	1912.0.0
Self-Service Password Reset	1912.0.6000
Windows 10 32-bit	Refer to initial release documentation
Workspace Environment Management	2206
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU6 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.

- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

March 15, 2023

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU5:

Citrix Director

- On Citrix Director, the **Session Details** page might display applied policies twice if the policies have both computer and user settings defined. [CVADHELP-19205]

Citrix Policy

- After you upgrade Citrix Virtual Apps and Desktops from version 1912 LTSR CU3 to version CU4 or CU5, VDAs might not register with Delivery Controller and remain unregistered. [CVADHELP-19834]
- An incorrect DNS query might be generated when the CseEngine.exe is fetching Group Policy Object (GPO). [CVADHELP-20361]

Citrix Provisioning

Citrix Provisioning 1912 CU6 documentation provides specific information about the updates in this release.

Citrix Studio

- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. [CVADHELP-18741]

- Operations involving machine catalogs in Citrix Studio, such as accessing, creating, removing, or enumerating catalogs might be slow. This issue occurs if a Nutanix hypervisor is used to host the connection. [CVADHELP-19652]

Delivery Controller

- The Citrix Broker Service (Brokerservice.exe) might become unresponsive and go offline. [CVADHELP-16352]
- After you upgrade XenApp and XenDesktop 7.6 to XenApp and XenDesktop 7.15 LTSR CU6 or later, or Citrix Virtual Apps and Desktops 1912 LTSR and create a Machine Creation Services (MCS) catalog, the option **Disk cache size (GB)** might be disabled and cannot be enabled. To enable the fix, restart the Host service and reopen Citrix Studio after the DBschema upgrade. [CVADHELP-17705]
- While updating a Machine Creation Services catalog, if you select the virtual machine and then the relevant snapshot, this error message might appear:

  An unexpected error occurred. Contact Citrix Technical Support.

  [CVADHELP-17794]
- Attempts to power on a machine might fail after the connection to System Center Virtual Machine Manager (SCVMM) is restored. [CVADHELP-18400]
- Citrix Broker Service (Brokerservice.exe) might exit unexpectedly due to the faulting LicPolEng.dll module. [CVADHELP-19674]
- When you use a static IP address to create a VDA version 2203 LTSR machine from a master image, Machine Creation Services (MCS) might not enable DHCP during image preparation. [CVADHELP-19892]
- During a virtual machine upgrade from version 1912 LTSR to version 1912 LTSR CU2, logging on to the machine using the domain credentials fails after the first reboot. However, log on succeeds after the subsequent reboot. [CVADHELP-19900]
- With this fix, unique names are assigned to base disks. [CVADHELP-19938]
- Delivery Controller might experience high CPU usage. As a result, the power status of VDAs is displayed as unknown. [CVADHELP-20061]
- After upgrading Delivery Controller to version 1912 CU5, scheduled reboot might not work correctly with VDAs that are not power managed. [CVADHELP-20138]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU6 documentation contains no fixed issues.

Profile Management

Profile Management 1912 CU6 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU6 documentation contains no fixed issues.

StoreFront

StoreFront 1912 CU6 documentation provides specific information about the updates in this release.

VDA for single-session OS

Keyboard

- The keyboard shortcut, Ctrl+Break might not work in sessions opened using Citrix Workspace app for Linux. [CVADHELP-19043]
- A left-handed mouse with the primary button set to **Left** on the user device and the VDA might not work as expected. [CVADHELP-19444]

Session/Connection

- When the Windows Media Player moves from the current track to the next track in the playlist, audio might not play at the beginning of the next track. The issue occurs if Windows Media redirection is enabled. [CVADHELP-17876]
- Machines might unregister because of a deadlock in Broker Agent and remain unregistered. [CVADHELP-18952]
- When you plug in or unplug a monitor, the seamless window might be positioned incorrectly. [CVADHELP-19168]
- Two VDAs instead of one might be assigned to a single user. [CVADHELP-19700]
- HDX Insights data might not get updated for user sessions on Remote PC Access VDA after reconnection. As a result, the Citrix ADM reports fewer connections than the actual number. [CVADHELP-19762]

- Attempts to launch a session while using the **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384** cipher suite might fail. [CVADHELP-19796]
- When you exit a session, the server might become unresponsive. The issue occurs because of the infinite loop present in icausbb.sys. [CVADHELP-19814]
- The Windows Audio service might not start automatically when you install Virtual Delivery Agent using the `servervdi` command line parameter. This error message appears in the notification area:

  The Audio Service is not running.

  [CVADHELP-19823]
- Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might cause a session leak while using Citrix HDX optimized Microsoft Teams. [CVADHELP-20058]
- Upon reconnecting to a published application, two published applications might be launched and Delivery Controller might show the application state as Application not running. [CVADHELP-20476]

System Exceptions

- An error in CTXCDF might cause Windows Management Instrumentation Provider Service (WMIPRVSE.exe) to stop and generate Event ID 5612 in the Event log. [CVADHELP-17425]
- The WebSocketService.exe process might exit unexpectedly causing Microsoft Teams calls to fail with the following error message:

  Still connecting to remote devices. Calling isn't available yet.

  [CVADHELP-17758]
- The PicaVcHost.exe process might experience an access violation and exit unexpectedly. [CVADHELP-18387]
- Session launches might fail displaying a gray screen. [CVADHELP-19232]

VDA for multi-session OS

Keyboard

- A left-handed mouse with the primary button set to **Left** on the user device and the VDA might not work as expected. [CVADHELP-19444]

Session/Connection

- Machines might unregister because of a deadlock in Broker Agent and remain unregistered. [CVADHELP-18952]
- While playing a video using Windows Media Player, the Custom Virtual Channel event logs might not be displayed in Event Viewer. This might happen when the Virtual channel allow list policy is set to enabled and the value set is empty. [CVADHELP-19525]
- The TermService permission on the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Session might not be restored during the installation of a VDA on Citrix Virtual Apps and Desktops 1912 CU resulting in sessions failures. [CVADHELP-19546]
- **HDX Insights** data might not get updated for user sessions on Remote PC Access VDA after reconnection. As a result, the Citrix ADM reports fewer connections than the actual number. [CVADHELP-19762]
- When you exit a session, the server might become unresponsive. The issue occurs because of the infinite loop present in icausbb.sys. [CVADHELP-19814]
- Upon reconnecting to a published application, two published applications might be launched and Delivery Controller might show the application state as Application not running. [CVADHELP-20476]

System Exceptions

- An error in CTXCDF might cause Windows Management Instrumentation Provider Service (WMIPRVSE.exe) to stop and generate Event ID 5612 in the Event log. [CVADHELP-17425]
- Session launches might fail displaying a gray screen. [CVADHELP-19232]
- When using Auto Client Reconnect (ACR) on multi-session OS VDAs, Citrix Audio Redirection Service might exit unexpectedly. [CVADHELP-19694]
- VDAs might experience a fatal exception on picavc.sys or picadm.sys and display a blue screen. [CVADHELP-19897]

Virtual Desktop Components –Other

- Attempts to launch App-V applications might fail on non-persistent machines if the App-V cache is redirected to the persistent drive. [CVADHELP-19125]
- Creating App-V applications using the single admin management method in Citrix Studio results in duplicate applications in the App-V packages. This slows down application enumeration. The issue occurs after upgrading Citrix Virtual Apps and Desktops 1912 LTSR from version CU2 to CU4.

Creating App-V applications using the single admin management method in Citrix Studio results in duplicate applications in the App-V packages. This slows down application enumeration. The issue occurs after upgrading Citrix Virtual Apps and Desktops 1912 LTSR from version CU2 to CU4. [CVADHELP-19603]

Cumulative Update 5 (CU5)

March 8, 2022

Release date: March 09, 2022

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 5 (CU5) fixes more than 60 issues reported since the release of 1912 LTSR CU4.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.17.2.0_BUILD_37000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU5 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU5 - using the CU5 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU5 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU5. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU5. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU5 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.5000	
Multi-session VDA	1912.0.5000	
Delivery Controller	1912.0.5000	
Citrix Studio	1912.0.5000	
Citrix Director	1912.0.5000	
Citrix Group Policy Management	7.24.5000	
Citrix Group Policy Client-Side Extension	7.24.5000	
Citrix StoreFront	1912.0.5000	
Citrix Provisioning	1912.0.25	
Universal Print Server	1912.0.5000	
Session Recording	1912.0.5000	
Linux VDA	1912.0.5000	See the Linux VDA documentation for supported platforms

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Profile Management	1912.0.5000	
Citrix Federated Authentication Service	1912.0.5000	
Browser Content Redirection	15.19.5000	
Citrix Probe Agent	2006	Download

Citrix Virtual Apps and Desktops 7 1912 LTSR CU5 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	21.07.0
App protection policies	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR CU4
License Server	11.17.2.0 Build 37000
User personalization layer	21.12.2
Session Recording web player	1912.0.0
Teams optimization	1912.0.0
Self-Service Password Reset	1.1
Windows 10 32-bit	Refer to initial release documentation
Workspace Environment Management	2112
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008

> R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU5 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

March 8, 2022

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU4:

Citrix Provisioning

Citrix Provisioning 1912 CU5 documentation provides specific information about the updates in this release.

Citrix Director

- Once a session is established, the display name of the machine in the Machine Details page on Citrix Director reverts to the Delivery Group name. [CVADHELP-18746]
- When accessed from a VDA which has system language set to Spanish, Citrix Director might display incorrect text. [CVADHELP-18864]

Citrix Studio

- When you add the StoreFront server address through Citrix Studio and assign it to a Delivery Group, the store is set to **OFF** by default. As a result, the store cannot be accessed. [CVADHELP-17980]
- Delivery Controller shows a delayed response when you add, create, or remove policies using the **Policies** tab in Citrix Studio. The typical response time is 10 to 15 minutes. [CVADHELP-18743]

Delivery Controller

- In a power managed environment, connections might continue to be brokered to VDAs which have failed to power on. [CVADHELP-18374]
- Attempts to add new administrators using PowerShell commands on Citrix Studio might fail. [CVADHELP-18573]
- Attempts to enumerate or launch sessions in Citrix Studio might fail when SQLs utilize high CPU. The following error message is displayed:

  Event 1201: The connection between Citrix Broker Service and the Database has been lost.

  [CVADHELP-18875]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU5 documentation provides specific information about the updates in this release.

Profile Management

Profile Management 1912 CU5 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU5 documentation contains no fixed issues.

StoreFront

StoreFront 1912 CU5 documentation provides specific information about the updates in this release.

VDA for single-session OS

Keyboard

- When you use a Russian keyboard layout on a macOS device connected to a VDA running Windows, the hotkeys might not work. [CVADHELP-17788]
- On an Android device connected to a VDA running version 1912 LTSR CU3, when you activate a text entry field, the on-screen keyboard might not appear automatically. [CVADHELP-18613]
- When you launch user sessions, the generic client Input Method Editor (IME) might not be set automatically. As a result, the keyboard does not automatically synchronize with the endpoint. [CVADHELP-18776]

Printing

- When you add a policy to the generic universal printer, the default printer might change from the main printer of the client to the generic Citrix Universal Printer. [CVADHELP-18157]
- The session printers might disappear during session reconnection, making the VDAs inaccessible from a Remote Desktop (RDP). [CVADHELP-19062]

Session/Connection

- Audio output quality from a microphone might be poor when connected through Citrix Gateway. [CVADHELP-16863]
- When you close a session launched from a published desktop with the VDAs hosted on Google Cloud Platform, the session might remain active on the VDA and not be marked disconnected. [CVADHELP-17923]
- The following steps performed on a published Microsoft Outlook app with the local IME enabled, might lead to a random string entered in the email window:

  - Open the email window.
  - Press the **Esc** key to display the **Want to save your changes?** dialog and type some random text.
  - Press the **Esc** key to close the dialog.

  [CVADHELP-18379]

- When Citrix IME is enabled, certain third-party applications might not respond and application launches in a user session might fail. The issue occurs because of the faulting CtxIme module. [CVADHELP-18511]
- When you upgrade your VDA from XenApp and XenDesktop version 7.15 CU3 to CU4, or to Citrix Virtual Apps and Desktops Version 1912 LTSR, the **LogoffCheckSysModules** registry value under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI registry key is reset to its default value. [CVADHELP-19214]

User Experience

- A left-handed mouse with the primary button set to **Left** on the user device and the VDA might not work as expected. [CVADHELP-17908]

User Interface

- In a multi-monitor environment, if you set the main monitor to portrait mode, SAS notifications might appear rotated by 90 degrees. [CVADHELP-17779]

VDA for multi-session OS

Keyboard

- When Japanese Input Method Editor (IME) is set to the **Best Experience mode**, input strings might be duplicated. [CVADHELP-18259]
- On an Android device connected to a VDA running version 1912 LTSR CU3, when you activate a text entry field, the on-screen keyboard might not appear automatically. [CVADHELP-18613]

Printing

- When you add a policy to the generic universal printer, the default printer might change from the main printer of the client to the generic Citrix Universal Printer. [CVADHELP-18157]
- The session printers might disappear during session reconnection, making the VDAs inaccessible from a Remote Desktop (RDP). [CVADHELP-19062]

Session/Connection

- Within a published instance of Microsoft Edge or Internet Explorer, signature applied digitally in the web browser using the signature feature might not be clearly visible when you launch certain third-party applications.

  To enable the option, set the following registry key:

  HKEY_LOCAL_MACHINE\Software\Citrix\MultiTouch

  Name: PressureValue

  Type: REG_DWARD

  Value: 32000 (Decimal)

  [CVADHELP-18325]

- When Citrix IME is enabled, certain third-party applications might not respond and application launches in a user session might fail. The issue occurs because of the faulting CtxIme module. [CVADHELP-18511]
- When licenses are exhausted on License Server and the **supplement grace period** feature is disabled, a black screen frozen with the **Access Denied** error message might appear. [CVADHELP-18712]
- If you reconnect to a session running on VDA version 2109 or later using Auto client reconnect, audio devices might not be mapped into the session. [CVADHELP-18888]
- When you exit from a Citrix virtual session, one or more of the following issues might occur:
  - The VDA still lists the terminated session and the logonui.exe process. The logonui.exe process can be forcefully terminated.
  - The session appears with a blank username in Citrix Studio.
  - You might not be able to launch further sessions.

  [CVADHELP-19182]

System Exceptions

- When you configure BCR proxy with a PAC file, Browser Content Redirection might fail. As a result, the HdxBrowserCef.exe process exits unexpectedly. [CVADHELP-16463]
- When you launch Remote Desktop Connection (mstsc.exe) as a published application, the CredentialUIBroker.exe process might exit unexpectedly. [CVADHELP-18694]
- Citrix Stack Control Service (SCService64.exe) might exit unexpectedly. [CVADHELP-18707]

- Microsoft might incorrectly send the **WTS_REMOTE_CONNECT** message before sending the connection notification **ConnectNotify**. As a result, one or more of the following functional issues might occur:
  - Sessions might exit unexpectedly.
  - Session reconnections might fail.
  - RPM Package Manager might crash.

  [CVADHELP-18980]
- When the Auto client reconnect option is selected, the session might close unexpectedly. [CVADHELP-19268]

User Interface

- In a user session launched through the Citrix Workspace app, you might not be able to hide the language bar even after setting the **No, hide the language bar** option. [CVADHELP-18239]
- Status messages might not appear when launching published resources. [CVADHELP-19070]

Cumulative Update 4 (CU4)

March 3, 2022

Release date: November 3, 2021

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 4 (CU4) fixes more than 70 issues reported since the release of 1912 LTSR CU3.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.16.3.0 Build 30000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU4 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU4 - using the CU4 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU4 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU4. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU4. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU4 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.4000	
Multi-session VDA	1912.0.4000	
Delivery Controller	1912.0.4000	
Citrix Studio	1912.0.4000	
Citrix Director	1912.0.4000	

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Citrix Group Policy Management	7.24.4000	
Citrix Group Policy Client-Side Extension	7.24.4000	
Citrix StoreFront	1912.0.4000	
Citrix Provisioning	1912.0.19	
Universal Print Server	1912.0.4000	
Session Recording	1912.0.4000	
Linux VDA	1912.0.3000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.4000	
Citrix Federated Authentication Service	1912.0.4000	
Browser Content Redirection	15.19.4000	
Citrix Probe Agent	2006	Download

Citrix Virtual Apps and Desktops 7 1912 LTSR CU4 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	21.07.0
App protection policies	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR CU4
License Server	11.17.2.0 Build 36000
User personalization layer	21.02.0
Session Recording web player	1912.0.0
Teams optimization	1912.0.0

Compatible components and features	Version as shown in Programs and Features
Self-Service Password Reset	1.1
Windows 10 32-bit	Refer to initial release documentation
Workspace Environment Management	2109
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU4 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack

Excluded components and features
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.

- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

June 30, 2022

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU3:

Citrix Policy

- When creating a policy in a Citrix Cloud environment and filter using the organizational unit for domain A, the user in domain B might not have the ability to log on. The issue occurs when accessing a published application or desktop. [CVADHELP-17179]

Citrix Provisioning

Citrix Provisioning 1912 CU4 documentation provides specific information about the updates in this release.

Citrix Director

- On-premises Citrix Director and the Citrix Virtual Apps and Desktops service **Monitor** tab might display the following message even when the RDS license is working as expected.

  RDS licensing has exceeded its grace period.

  [CVADHELP-17469]

- Assigning the VDA to a Delivery Group and enabling the **VdaDataCollection** setting on the Delivery Controller might cause the VDA data collection engine to restart intermittently. The issue occurs when any group policy settings have been updated. [CVADHELP-18361]
- Searching a user by selecting an assigned or a static desktop with no active sessions might fail with the following error message displayed in Citrix Director:

  Cannot retrieve machines

  [CVADHELP-18327]

Citrix Studio

- Clicking the **Find a solution** link on the error message displayed in Citrix Studio might open an incorrect link. [CVADHELP-17800]

Delivery Controller

- When licensing breaks, a session might continue to work a grace period for 30 days. After 30 days, the grace period ends and the connection fails. [CVADHELP-16487]
- Upgrading Citrix Virtual Apps and Desktops to version 1912 LTSR might not update the Citrix.AzureRmPlugin.dll.config configuration file and the connection to Microsoft Azure Resource Manager might fail. [CVADHELP-16839]
- The Delivery Controller might fail to connect to the database with the following error message. The error results in performance issues.

  Event 1201 The connection between Citrix Broker Service and the Database has been lost.

  This error occurs when a multi-line table function in SQL like, **DAGetSessionUidsInCatalogScope** or **DesktopGroupScope** is called in an environment that is running a large number of sessions. For example, if 100k sessions are running and 100K Uid entries are made in a single table, the performance gets affected and the connection fails.

  [CVADHELP-17021]
- The **MonitorData.[Machine]** table present in the Monitoring database might include duplicate entries. [CVADHELP-17025]
- Attempts to disable the Hypervisor Health alerts in Citrix Director might fail.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Monitor\Service\Toggles

  Name: HypervisorMonitoring

  Type: DWORD

  Value: 00000000

  [CVADHELP-17218]
- The site test might fail when the network connectivity among Delivery Controllers in different satellite zones is blocked. [CVADHELP-17273]
- A Delivery Group administrator assigned with custom scope might not be able to retrieve the list of reboot schedules or manage them. [CVADHELP-17683]

- Attempts to update catalogs with names containing special characters, such as & and $, might fail when the updated master image is not promoted to the VDAs. [CVADHELP-17686]
- With both multi-site aggregation functionality configured and the "SessionReconnection"property set to **SameEndPointOnly** in the entitlement policy rule, a new session might be launched instead of reconnecting to the active session. [CVADHELP-17692]
- When you upgrade Citrix Virtual Apps and Desktops to version 1912 LTSR and reboot the XenServer, the virtual machines might get stuck in the Unknown power state and fail to refresh in Citrix Studio. [CVADHELP-17750]
- Adding a hosting unit on the Delivery Controller with the Fully Qualified Domain Name (FQDN) written in upper case characters as HTTPS URL or HTTP URL, might fail. [CVADHELP-17862]
- Attempting to update the hosting connection password for the Microsoft System Center Virtual Machine Manager (SCVMM) based hypervisor might result in a timeout error. [CVADHELP-17909]
- Starting or restarting the Citrix Monitoring service during an upgrade might result in database connectivity failure and loss of old data. To prevent this, set the default retention in accordance with the Platinum edition (PLT). [CVADHELP-18069]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU4 documentation provides specific information about the updates in this release.

Metainstaller

- When installing or upgrading a VDA, the SetDisplayRequiredMode value under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics might be deleted. [CVADHELP-17031]
- The user personalization layer is not installed. [CVADHELP-17672]

Microsoft Teams Optimization

- Microsoft Teams optimized calls might fail with the ctxsvchost.exe process exiting unexpectedly because of the faulting CtxTeamsSvc.dll module. [CVADHELP-16918]
- The HTML5 Video Redirection Service (txHdxWebSocketService) might exit unexpectedly. [CVADHELP-17146]
- When using Microsoft Teams in HDX optimized mode within a published desktop, audio calls might disconnect. [CVADHELP-17341]

- While attempting to join a call, the Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might exit unexpectedly causing the call to fail. [CVADHELP-17424]

Profile Management

Profile Management 1912 CU4 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU4 documentation provides specific information about the updates in this release.

StoreFront

StoreFront 1912 CU4 documentation provides specific information about the updates in this release.

VDA for single-session OS

Content Redirection

- A black patch might appear on the screen when using Explorer. The issue occurs when connected to endpoints using certain AMD GPU models. [CVADHELP-17057]
- When using some third-party applications, the Websocketagent.exe might use a high percentage of the CPU. The issue occurs when the **Browser Content Redirection** or **HTML5 video redirection** policy is enabled. [CVADHELP-17067]
- This fix is an enhancement to HdxWebProxy to interoperate with its Blue Coat web proxies. [CVADHELP-18078]

Keyboard

- EDT MTU Discovery might calculate an incorrect MTU when paths between the VDA and the client are asymmetrical. As a result, the session launch is successful. However, the keyboard and the mouse are unresponsive. [CVADHELP-16654]

Session/Connection

- VDAs might unregister intermittently when IPv6 is enabled. [CVADHELP-14847]
- The VDAs might unregister and remain so. [CVADHELP-16445]
- After launching a session, the audio running on Microsoft Windows might display a red X that cannot be removed. [CVADHELP-16815]
- Clipboard mapping might be blocked when you initially connect from a virtual desktop session to a client and vice versa. Upon disconnect and reconnect, the clipboard mapping works only from the virtual desktop session to the client. [CVADHELP-17039]
- To update custom text in a watermark, log off and then connect back to the session. [CVADHELP-17056]
- When setting the **DPI** to a value other than 100% within a VDA, the **DPI** value might reset to 100%. The issue occurs when attempting to lock a desktop. [CVADHELP-17276]
- With the Multi-stream policy enabled, sessions launched on Linux endpoints might disconnect. The issue occurs with VDA Version 1912 LTSR. [CVADHELP-17301]
- When using Microsoft Teams in HDX optimized mode within a published desktop, audio calls might disconnect. [CVADHELP-17341]
- Reconnecting to a session with the user personalization layer policy enabled, might fail. [CVADHELP-17369]
- Usage of the AMD graphics card on a single session VDI desktop might fail. [CVADHELP-17757]
- Citrix connection licenses are consumed when you disconnect user sessions that were connected through a physical machine VDA. [CVADHELP-17802]
- When using an NVIDIA GPU, the frequency of frames in full-screen mode might not exceed 60 fps (frames per second) even after configuring the screen to maximum frequency. [CVADHELP-17904]
- The table copy option might be disabled or unavailable in certain third-party applications. To enable the option, set the following registry key:

  HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Citrix\wfshell\virtual Clipboard

  Name: DisableFileSupport

  Type: DWORD

  Value: 00000001

  [CVADHELP-17986]
- This fix enables logging of the Virtual Channel Allow List. For more information, see Virtual channel security. [CVADHELP-18129]

Smart Cards

- Accessing smart cards using the Microsoft Edge browser with **SFRhook** enabled, might cause the msedge.exe process to exit unexpectedly. [CVADHELP-17956]

System Exceptions

- The Citrix Desktop Service (BrokerAgent.exe) might generate a large number of ID 1010 events when using OU based Controller discovery through a direct access VPN tunnel. [CVADHELP-16754]
- Microsoft Teams might fail to optimize when one of the CtxSvcHost.exe processes exits unexpectedly. The issue occurs because of the faulting Citrix HDX Teams Redirection system service. [CVADHELP-16946]
- The Citrix Desktop Service (BrokerAgent.exe) might experience an access violation and exit unexpectedly. [CVADHELP-17055]
- The HTML5 Video Redirection Service (CtxHdxWebSocketService) might exit unexpectedly. [CVADHELP-17146]
- The wfshell.exe process might exit unexpectedly, causing new application launches from published applications to fail. [CVADHELP-17310]
- The VDAs might experience a fatal exception on icausbb.sys and display a blue screen with bug check code, 0x3B. [CVADHELP-17339]
- While attempting to join a call, the Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might exit unexpectedly causing the call to fail. [CVADHELP-17424]
- The winlogon.exe process might exit unexpectedly. The issue occurs because of the faulting module, PicaWinlogonHook64.dll. [CVADHELP-17651]
- Audio and video in a Microsoft Teams optimized video conference call might disconnect and the HdxRtcEngine.exe process might exit. [CVADHELP-17741]

VDA for multi-session OS

Content Redirection

- A black patch might appear on the screen when using Explorer. The issue occurs when connected to endpoints using certain AMD GPU models. [CVADHELP-17057]
- This fix is an enhancement to HdxWebProxy to interoperate with its Blue Coat web proxies. [CVADHELP-18078]

Keyboard

- EDT MTU Discovery might calculate an incorrect MTU when paths between the VDA and the client are asymmetrical. As a result, the session launch is successful. However, the keyboard and the mouse are unresponsive. [CVADHELP-16654]

Printing

- When using the **Save Print Output As** option to print to a file in a seamless session, the print window might not display correctly. [CVADHELP-16614]

Session/Connection

- VDAs might unregister intermittently when IPv6 is enabled. [CVADHELP-14847]
- The VDAs might unregister and remain so. [CVADHELP-16445]
- When using certain third-party applications, a black screen might appear when the application opens another window. [CVADHELP-16956]
- Clipboard mapping might be blocked when you initially connect from a virtual desktop session to a client and vice versa. Upon disconnect and reconnect, the clipboard mapping works only from the virtual desktop session to the client. [CVADHELP-17039]
- Setting the value of **HideStatusMessages** to **1** to hide the Starting bar might cause the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ to not work as expected. [CVADHELP-17138]
- With the Multi-stream policy enabled, sessions launched on Linux endpoints might disconnect. The issue occurs with VDA Version 1912 LTSR. [CVADHELP-17301]
- When using Microsoft Teams in HDX optimized mode within a published desktop, audio calls might disconnect. [CVADHELP-17341]
- Certain third-party applications might become unresponsive in a seamless session. [CVADHELP-17309]
- Starting an SSL session on Citrix Virtual Apps and Desktops LTSR version CU1, CU2, or CU3 might fail with the following error message:

  Your session ‘delivery group name’did not launch successfully due to error code 3500. Please contact your administrator for more information about the error.

  [CVADHELP-17421]
- The Hooking driver, CtxUvi might unload when using docker containers. [CVADHELP-17614]

- This fix provides enhancements to the Virtual Channel Allow List feature. As a result, you can only open Citrix virtual channels in the virtual apps and desktops sessions. You can also add custom virtual channels to the allow list using the **Virtual Channel Allow List** policy settings. [CVADHELP-17918]
- After upgrading Citrix Workspace app to version 1909 or later, you might not be able to move the language bar smoothly in a seamless session. [CVADHELP-18118]
- The table copy option might be disabled or unavailable in certain third-party applications. To enable the option, set the following registry key:

  HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Citrix\wfshell\virtual Clipboard

  Name: DisableFileSupport

  Type: DWORD

  Value: 00000001

  [CVADHELP-17986]
- This fix enables logging of the Virtual Channel Allow List. For more information, see Virtual channel security. [CVADHELP-18129]

Smart Cards

- Accessing smart cards using the Microsoft Edge browser with **SFRhook** enabled, might cause the msedge.exe process to exit unexpectedly. [CVADHELP-17956]

System Exceptions

- The Citrix Desktop Service (BrokerAgent.exe) might generate a large number of ID 1010 events when using OU based Controller discovery through a direct access VPN tunnel. [CVADHELP-16754]
- Microsoft Teams might fail to optimize when one of the CtxSvcHost.exe processes exits unexpectedly. The issue occurs because of the faulting Citrix HDX Teams Redirection system service. [CVADHELP-16946]
- The Citrix Desktop Service (BrokerAgent.exe) might experience an access violation and exit unexpectedly. [CVADHELP-17055]
- The HTML5 Video Redirection Service (CtxHdxWebSocketService) might exit unexpectedly. [CVADHELP-17146]
- The wfshell.exe process might exit unexpectedly, causing new application launches from published applications to fail. [CVADHELP-17310]

- While attempting to join a call, the Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might exit unexpectedly causing the call to fail. [CVADHELP-17424]
- When you launch a published application, winlogon.exe might exit unexpectedly and the user session might disconnect. [CVADHELP-17602]
- Published Universal Windows applications (UWA) might fail to launch with the following exception:

  System.Runtime.InteropServices.COMException (0x80270134)

  [CVADHELP-18116]

Cumulative Update 3 (CU3)

September 21, 2021

Release date: May 12, 2021

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 3 (CU3) fixes more than eighty issues reported since the release of 1912 LTSR CU2.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.16.3.0 Build 30000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU3 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU3 - using the CU3 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU3 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU3. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU3. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU3 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.3000	
Multi-session VDA	1912.0.3000	
Delivery Controller	1912.0.3000	
Citrix Studio	1912.0.3000	
Citrix Director	1912.0.3000	
Citrix Group Policy Management	7.24.3000	
Citrix Group Policy Client-Side Extension	7.24.3000	
Citrix StoreFront	1912.0.3000	
Citrix Provisioning	1912.0.13	
Universal Print Server	1912.0.3000	

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Session Recording	1912.0.3000	
Linux VDA	1912.0.3000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.3000	
Citrix Federated Authentication Service	1912.0.3000	
Browser Content Redirection	15.19.3000	
Citrix Probe Agent	2006	Download

Citrix Virtual Apps and Desktops 7 1912 LTSR CU3 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	19.11.0
App protection policies	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR
License Server	11.16.6.0 Build 34000
User personalization layer	19.11.0
Session Recording web player	1912.0.0
Teams optimization	1912.0.0
Self-Service Password Reset	1.1
Windows 10 32-bit	
Workspace Environment Management	2003.0.0 and later
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU3 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

August 13, 2021

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU2:

Citrix Director

- After uninstalling a VDA, the namespaces for Citrix Windows Management Instrumentation (WMI) might remain. [CVADHELP-14965]
- Citrix Director might intermittently display the following alert on the Delivery Controller:

  The `System.ServiceModel.ChannelFactory1 communication object _[<object name>_]` cannot be changed while its state is Opening.

  [CVADHELP-15801]
- On the **Historic Machine Utilization** page, data in the **Top 10 Processes** table might not be displayed. This message appears:

  Process data collection is disabled on this machine. Enable process monitoring policy to start collection.

  [CVADHELP-15893]
- On the **Director > Trends > Logon Performance > Export Report** page, when you generate and export a report, incorrect brokering time values might appear in the report. The issue occurs with the German language report where `.` is replaced with `,`. [CVADHELP-16097]
- On the **Director > Filters > All Machines** page, if you select a machine and then perform maintenance operations, check marks might not be retained for the selected machines. [CVADHELP-16469]
- When extracting process data from the Monitor API, invalid data might appear. The process creation time (**ProcessCreationDate**) appears after the process collection time (**CollectionDate**) instead of appearing before. [CVADHELP-17092]

Citrix Policy

- When you upgrade the Citrix Group Policy Engine from Version 1.7 to Version 1912 LTSR, the **Printer assignments** policy under **Citrix User Policies** might not be displayed. [CVADHELP-15608]

Citrix Provisioning

Citrix Provisioning 1912 CU3 documentation provides specific information about the updates in this release.

Delivery Controller

- Attempts to restart a Delivery Controller might cause all connected VDAs to unregister in multiple domains. [CVADHELP-12840]
- This fix addresses performance issues you might experience with Delivery Controller (XML service) in slow active directory environments.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer

  Or

  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\DesktopServer

  Name: DisableGetPasswordExpiryInfo

  Type: DWORD

  Value: 1

  [CVADHELP-15536]
- With this fix, the preparation machine does not use the default cache expiration time (five minutes). The fix provides the following:

  - Reduces the expiration time of a machine with an unknown power state (one minute).
  - Reduces the expiration time of a preparation machine that is transitioning power (five seconds)
  - Reduces the expiration time of a preparation machine that is not transitioning power (one minute).
  - Reduces the expiration time of a non-preparation machine that is transitioning power (30 seconds).

  [CVADHELP-15678]
- When you use PowerShell to perform a power action, the action might be processed successfully, but the action is logged as failed in **Citrix Studio > Logging**. [CVADHELP-15807]
- When you delete machines or catalogs associated with an AWS hosting connection, EBS root devices might not be automatically deleted. The issue occurs because the flag **DeleteOnTermination** on the base image changes from `$true` to `$false` on disks created for those catalogs during machine catalog creation. [CVADHELP-16096]
- In a multi-zone environment with high latencies, attempts to upgrade XenApp and XenDesktop version 7.15 LTSR CU5 to Citrix Virtual Apps and Desktops version 1912 CU1 might fail with the following exception:

  NullReferenceException

[CVADHELP-16236]

- On a Delivery Controller, the following error message might appear frequently in **Event Viewer > Windows Logs > Application**:

  Event ID 505: The Citrix Config Sync Service failed an import

  [CVADHELP-16322]

- Signing in to an unbrokered RDP session with a UPN credential might result in an uncaught exception. In 1912 LTSR CU2, a name translation for usernames provided as UPN was introduced. The truncation of the username due to the limit imposed in RDS data structures produces an incorrect username, resulting in the uncaught exception. [CVADHELP-16510]
- When you launch a VM hosted app and then attempt to launch a second VM hosted app from the same VDA, the launch might fail. The issue occurs when the machine catalog uses the static allocation. [CVADHELP-16829]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU3 documentation provides specific information about the updates in this release.

Metainstaller

- When installing or upgrading a VDA, the SetDisplayRequiredMode value under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics might be deleted. [CVADHELP-17031]

Profile Management

Profile Management 1912 CU3 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU3 documentation provides specific information about the updates in this release.

StoreFront

StoreFront 1912 CU3 documentation provides specific information about the updates in this release.

VDA for single-session OS

Keyboard

- With the clipboard redirection policy enabled, attempts to use the **Copy shortcut** option from the right-click menu to copy and paste content between a published application and an endpoint might fail. The issue occurs with Internet Explorer. [CVADHELP-15647]

Printing

- Attempting to print a PDF file from a session launched through Citrix Workspace app for Chrome might fail. [CVADHELP-15318]
- When using a Remote PC Access VDA to print through Citrix Workspace app for Mac, the printer settings might be ignored. [CVADHELP-15320]
- Changes made to the **Local Settings** under **Printer Preferences** might be lost when you do not save the changes within 54 seconds. [CVADHELP-15725]
- When you attempt to print a file using Citrix Universal Printer Driver (UPD), incorrect images might appear in the printed file. The issue occurs when you upgrade a VDA from Version 7.15.5000 to Version 1912.1000 and enable heavyweight compression. [CVADHELP-15813]
- Client printers might fail to redirect when connecting to a hosted HDX session. [[CVADHELP-16279]
- When attempting to print a PDF file from a session launched through Citrix Workspace app for HTML5, the file might not print correctly. [CVADHELP-16809]

Session/Connection

- After upgrading a VDA from Version 7.15.2000 to Version 1912.2000, the data values for **EnableReadImageFileExecOptionsExclusionList** might disappear from the registry keys: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\ and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Noc [CVADHELP-15090]
- Even though the VDA time zone policy is configured to use the server-side time zone, the client-side time zone might still be used. [CVADHELP-15395]
- Surface Pro built-in webcams might fail. [CVADHELP-15567]
- The Citrix HDX HTML5 Video Redirection Agent Service (WebSocketAgent.exe) might stop intermittently. As a result, incoming calls are not displayed under Microsoft Teams. Also, the called party does not receive any notifications. [CVADHELP-15611]

- After installing a VDA, when attempting to view the **Private Key** tab under **Certificate Properties**, this error message might appear:

  One or more of the objects properties are missing or invalid.

  [CVADHELP-15703]

- When you connect a physical monitor to a RemotePC with NVIDIA Physical GPU through a DisplayPort, the monitor might display a blank screen. [CVADHELP-16022]
- When connecting from a touch enabled endpoint to a VDA version 1912, the on-screen keyboard might not work. The issue occurs for non-administrative users with the UAC enabled on a VDA. [CVADHELP-16045]
- VDAs might deregister when the console session reconnects immediately after the user session disconnects. [CVADHELP-16152]
- Attempts to launch a VDA session on a laptop that uses an Intel UHD Graphics card might result in a gray screen. [CVADHELP-16519]
- On Server VDI VDAs, the power button on the **Start** menu might not offer the **Disconnect** option. [CVADHELP-16595]
- When using Generic IME for Microsoft Windows 10 20H2 with KB4586853 update, the application might exit unexpectedly. [CVADHELP-16664]
- When attempting to take a screenshot using the snipping tool or perform complex calculations such as a pivot table, you might experience performance issues. The issue occurs when you set the value of **CursorShapeChangeMinInterval** to 50 under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics. [CVADHELP-16718]
- With this fix, you can now set different input methods for each application window available under advanced keyboard settings. [CVADHELP-16731]
- When using the Remote PC Access on Windows 10 with NVIDIA graphics card adapter in a headless configuration, reconnect issues might occur. [CVADHELP-16848]
- When a non-English VDA goes idle, a timeout message might display with meaningless code. [CVADHELP-16880]
- This fix is an enhancement to **HdxWebProxy**. A BCR component, to the extent that HTTP traffic originating at the overlay, can be routed through web proxies that are configured to authorize the HTTP traffic. [CVADHELP-17044]

System Exceptions

- When you attempt to view embedded Windows Media files from a web application, Internet Explorer might exit unexpectedly. The issue occurs because of the faulting module, HostMM-

Transport.dll. [CVADHELP-15598]

- VDAs might experience a fatal exception on wdica.sys and display a blue screen. [CVADHELP-16055]
- If Terminal Services exits unexpectedly, VDAs might unregister. The issue occurs because of the faulting module, RPM.dll. [CVADHELP-16110]
- VDAs might experience a fatal exception, displaying a blue screen, during remote access. The issue occurs when you install a VDA on a new machine and attempt to restart it. [CVADHELP-16284]
- VDAs might experience a fatal exception and display a blue screen with the bug check code 0x0000010D (WDF_VIOLATION). [CVADHELP-16773]

VDA for multi-session OS

Keyboard

- Japanese keyboard mapping might not work when connected to a non-Windows endpoint. [CVADHELP-15273]
- With the clipboard redirection policy enabled, attempts to use the **Copy shortcut** option from the right-click menu to copy and paste content between a published application and an endpoint might fail. The issue occurs with Internet Explorer. [CVADHELP-15647]

Printing

- Attempting to print a PDF file from a session launched through Citrix Workspace app for Chrome might fail. [CVADHELP-15318]
- When using a Remote PC Access VDA to print through Citrix Workspace app for Mac, the printer settings might be ignored. [CVADHELP-15320]
- Changes made to the **Local Settings** under **Printer Preferences** might be lost when you do not save the changes within 54 seconds. [CVADHELP-15725]
- When you attempt to print a file using Citrix Universal Printer Driver (UPD), incorrect images might appear in the printed file. The issue occurs when you upgrade a VDA from Version 7.15.5000 to Version 1912.1000 and enable **heavyweight compression**. [CVADHELP-15813]
- When you attempt to print a large Microsoft Excel file using Citrix Universal Printer Driver (UPD), the print might fail during the **Spooling** –**Printing process**. [CVADHELP-16153]
- When attempting to print a PDF file from a session launched through Citrix Workspace app for HTML5, the file might not print correctly. [CVADHELP-16809]

Session/Connection

- In certain scenarios, Citrix product license usage shown in Citrix Studio does not match license usage shown in the Citrix License Manager. [CVADHELP-14950]
- After upgrading a VDA from Version 7.15.2000 to Version 1912.2000, the data values for **EnableReadImageFileExecOptionsExclusionList** might disappear from the registry keys: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\ and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Noc [CVADHELP-15090]
- Even though the VDA time zone policy is configured to use the server-side time zone, the client-side time zone might still be used. [CVADHELP-15395]
- After installing a VDA, when attempting to view the **P**rivate Ke**y** tab under **Certificate Properties**, this error message might appear:

  One or more of the objects properties are missing or invalid.

  [CVADHELP-15703]
- When reconnecting to a session, the Citrix Audio Redirection Service (CtxAudioSvc) might fail. The issue occurs when running a VDA for a multi-session OS on Microsoft Windows 10 Version 2004 and later. [CVADHELP-15804]
- When connecting from a touch enabled endpoint to a VDA version 1912, the on-screen keyboard might not work. The issue occurs for non-administrative users with the UAC enabled on a VDA. [CVADHELP-16045]
- An invalid XenApp session on a VDA for Server OS might start when disconnecting and reconnecting a remote desktop session. The invalid session remains until you restart the VDA. [CVADHELP-16453]
- Watermark policy changes such as **Include VDA Host name** and **Include VDA IP address**, might not be in effect during the next session.

  To enable the fix, set this registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\Watermark

  Name: PolicyInterval

  Type: DWORD

  Value: Desired value in seconds (for example, 2 seconds)

  [CVADHELP-16485]
- When applying Fix CVADHELP-12886 and then using a snipping tool, the memory consumption might increase to 4 GB, causing sessions to eventually become unresponsive. [CVADHELP-16542]

- When attempting to take a screenshot using the snipping tool or perform some complex calculations such as a pivot table, you might experience performance issues. The issue occurs when you set the value of **CursorShapeChangeMinInterva**l to 50 under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics. [CVADHELP-16718]
- With this fix, you can now set different input methods for each application window available under advanced keyboard settings. [CVADHELP-16731]
- When you disconnect the initial session launched from a Desktop Viewer on a device, the fast reconnect feature might be bypassed, slowing the session. [CVADHELP-16953]

System Exceptions

- With the **HDX Adaptive Transport** policy enabled, the Terminal service might not end when terminating the service manually. [CVADHELP-15524]
- When you attempt to view embedded Windows Media files from a web application, Internet Explorer might exit unexpectedly. The issue occurs because of the faulting module, HostMM-Transport.dll. [CVADHELP-15598]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen. [CVADHELP-16055]
- If Terminal Services exits unexpectedly, VDAs might unregister. The issue occurs because of the faulting module, RPM.dll. [CVADHELP-16110]

Virtual Desktop Components –Other

- Attempting to launch an executable with a single quote in the file name, might fail. [CVADHELP-16104]

Cumulative Update 2 (CU2)

September 21, 2021

Release date: November 2020

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 2 (CU2) fixes more than 100 issues reported since the release of 1912 LTSR CU1.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

> **Important:**
>
> The Citrix License Administration Console reached end of life and end of support in License Server 11.16.3.0 Build 30000. Use the Citrix Licensing Manager.

New deployments

How do I deploy CU2 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU2 - using the CU2 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU2 provides updates to baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU2. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU2. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU2 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.2000	
Multi-session VDA	1912.0.2000	
Delivery Controller	1912.0.2000	
Citrix Studio	1912.0.2000	
Citrix Director	1912.0.2000	
Citrix Group Policy Management	7.24.2000	
Citrix Group Policy Client-Side Extension	7.24.2000	
Citrix StoreFront	1912.0.2000	
Citrix Provisioning	1912.0.7	
Universal Print Server	1912.0.2000	
Session Recording	1912.0.2000	
Linux VDA	1912.0.2000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.2000	
Citrix Federated Authentication Service	1912.0.2000	
Browser Content Redirection	15.19.2000	
Citrix Probe Agent	2006	Download

Citrix Virtual Apps and Desktops 7 1912 LTSR CU2 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	19.11.0
App protection policies	1912.0.0

Compatible components and features	Version as shown in Programs and Features
HDX RealTime Optimization Pack	2.9 LTSR
License Server	11.16.6.0 Build 32000
User personalization layer	19.11.0
Session Recording web player	1912.0.0
Teams optimization	1912.0.0
Self-Service Password Reset	1.1
Windows 10 32-bit	
Workspace Environment Management	2003.0.0 and later
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU2 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.

- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

List of fixes present in 7.15 LTSR CU7 but not in 1912 LTSR CU2

If you're considering an upgrade from 7.15 LTSR CU7 to 1912 LTSR CU2, be advised that a small subset of fixes that are included in 7.15 LTSR CU7 are not present in 1912 LTSR CU2. If your deployment depends on specific fixes included in 7.15 LTSR CU7, Citrix recommends that you review this list before you upgrade.

- CVADHELP-13287
- CVADHELP-13993
- CVADHELP-14249
- CVADHELP-14428
- CVADHELP-14515
- CVADHELP-14640
- CVADHELP-14740
- CVADHELP-14847
- CVADHELP-14865
- CVADHELP-14870
- CVADHELP-14905
- CVADHELP-14935
- CVADHELP-14950
- CVADHELP-14959
- CVADHELP-14965
- CVADHELP-15248
- CVADHELP-15298
- CVADHELP-15326
- CVADHELP-15536
- CVADHELP-15568
- CVADHELP-15572
- CVADHELP-15598
- CVADHELP-15608
- CVADHELP-15628

- CVADHELP-15724
- CVADHELP-15749
- CVADHELP-15792
- CVADHELP-15893
- CVADHELP-16036
- CVADHELP-16096
- CVADHELP-16097
- CVADHELP-16410
- CVADHELP-16453

Fixed issues

February 10, 2022

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR CU1:

Citrix Director

- In Citrix Director, when you pull the report for a Delivery Group without a failed connection on the **Failure** tab under **Trends**, the details populate correctly. But details of all the Delivery Groups, including the Delivery Group that has no failed connections, might appear as failed connections when you export the report. [CVADHELP-14392]
- When you attempt to configure an email server on a standalone server using Citrix Director, this error message might appear:

  Invalid Email Server.

  The issue occurs when you configure the email server for alerts and notifications. [CVADHELP-14648]
- Citrix Director might not display all the rows of records. Only the top 50 entries are exported to the .CSV file even though the **Application Instances** filter page lists several application instances. [CVADHELP-14783]
- In Citrix Director, when you pull the report for a Delivery Group on the **Load Evaluator Index** tab, the details might appear incorrectly. The report displays the details of all Delivery Groups rather than the selected Delivery Group. [CVADHELP-14869]
- In Citrix Director, when you check machine usage for a selected Deliver Group by navigating to **Director console > Trends > Machine Usage**, the value appears as 0 (Zero). The issue occurs

when you select a Delivery Group under **Multi-session OS Machines**. The issue occurs only with the In Use column. [CVADHELP-15136]

- The integration of NetScaler Management and Analytics System (MAS) with Citrix Director might fail. As a result, the command C:\inetpub\wwwroot\Director\bin..\DisplayConfig\HdxInsightPlugin\HdxInsig fails with the following exception:

  Could not perform the logon operation and inner exception: The remote server returned an error: (400) Bad Request.

  [CVADHELP-15219]

- When you shadow a session on version 1912 LTSR or 1912 LTSR CU1 of the VDA, Microsoft Remote Assistance process (msra.exe) might exit unexpectedly. [CVADHELP-15230]
- The Session Activity consolidation task might time out, affecting the user experience. [CVADHELP-15305]
- On the **Capacity Management > Hosted Applications Usage** tab, when you view a table that displays application-based usage for a delivery group over a time period, the usage data might be incorrect. [CVADHELP-15368]

Citrix Policy

- The **Policies > Assigned to** tab might incorrectly display Citrix policies you assign to one or more delivery groups. For example, you assign a policy to two delivery groups and enable the assignment for only one of them. When you navigate to the **Assigned to** tab, both delivery groups are displayed. When you disable the policy, it becomes unassigned. But the **Assigned to** tab still displays the policy as assigned. [CVADHELP-15233]
- After you upgrade a VDA from Cumulative Update version 2005 to version 2006, the Group Policy engine (CseEngine.exe) service might exit unexpectedly with an exception code 0xc0000409. [CVADHELP-15363]
- In Citrix Studio, when you attempt to create or modify a Citrix policy, this error message appears on the Logging tab:

  Error while attempting to determine the policy change details.

  The policy is applied correctly, but you cannot find out who modified the settings. The issue occurs after you upgrade Citrix Virtual Apps and Desktops to Version 1912 LTSR CU1 from Version 1912 LTSR. [CVADHELP-15726]

Citrix Provisioning

Citrix Provisioning 1912 CU2 documentation provides specific information about the updates in this

release.

Citrix Studio

- When you start a dedicated desktop session, a logon failure might occur and the logoff process might get stuck. Citrix Studio shows the session as connected, but you cannot log off until you manually restart the machine. [CVADHELP-10932]
- When you run Studio as a published app, Studio might become unresponsive. [CVADHELP-14207]
- On the **Machine Allocation** page, certain check boxes might be missing. The issue occurs when you are attempting to add machines to a delivery group or a machine catalog that has one or more user-assigned machines. [CVADHELP-15684]
- This fix replaces the following registry settings with a Studio policy:
  - **Client keyboard layout synchronization and IME improvement**. Enables or disables dynamic keyboard layout synchronization and IME.
  - **Enable Unicode keyboard layout mapping**. Enables or disables Unicode keyboard layout mapping.
  - **Hide keyboard layout switch pop-up message box**. Hides or shows the keyboard layout switch notification dialog message.

  [CVADHELP-15706]
- While you are creating a hosting connection to Azure, attempts to create a service principal might fail with an **ADSTS700016** error. [CVADHELP-16219]

Delivery Controller

- When you generate a License Server report using the **udadmin** command, the report might show that the licenses are issued to the same device multiple times. The issue occurs when different devices with the correct hardware IDs are updated against duplicate names. The issue does not impact the license consumption, but only the report. [CVADHELP-13763]
- When you update machine catalogs using Machine Creation Services, the previous base disk folder might not be deleted from the **VMware Storage**. [CVADHELP-14264]
- The **MonitorData.[User]** table present in the Monitoring database might fail to synchronize data with Active Directory. Also, the user name, display name, and the UPN information present in the table become obsolete. [CVADHELP-14700]
- Attempts to launch applications might fail. Many access requests to the **Chb_State.Sessions** table are blocked. [CVADHELP-14876]

- When you select Machine Catalogs in the Studio navigation pane, Studio might fail to display the list of catalogs. This error message appears:

  You cannot see any catalogs.

  The issue occurs because Studio cannot retrieve the list of objects by using the **Get-ProvSchemeMasterVMImageHistory** PowerShell command. [CVADHELP-15211]

- Attempts to create a Machine Creation Services (MCS) catalog using VMware vSphere 7.0 might fail. [CVADHELP-15237]
- This fix adds support for NV4as_v4 machine types in Azure. [CVADHELP-15317]
- With this fix, the v1 key references to the Director and Monitor Service are removed. [CVADHELP-15327]
- After upgrading a VDA to Version 1912 LTSR CU1, the user name of an untrusted user logging on to the machine appears as **Domain\UPN** instead of **Domain\User name**. [CVADHELP-15440]
- With Citrix Analytics for Performance enabled in Citrix Director, a memory leak might occur in the Monitor Service. [CVADHELP-15607]
- When a table storage account is missing, you can still read the individual records for each machine every 20 seconds in 15 minutes. After that, the power state becomes unresponsive. [CVADHELP-15677]
- Attempts to download snapshots might fail when using Microsoft Azure. [CVADHELP-15679]
- This fix provides Microsoft System Center Virtual Machine Manager (SCVMM) 2019 support for Machine Creation Services (MCS)

  [CVADHELP-15779]

- Changes to the `DefaultInstall` parameter allow you to use Microsoft System Center Configuration Manager (SCCM) to install the Machine Creation Services I/O (MCSIO) under a system account. [CVADHELP-15593]
- Attempts to launch a desktop might fail when the power action is sent from the Delivery Controller. The power action fails with the following exception:

  System.Runtime.Remoting.RemotingException

  [CVADHELP-15835]

- This fix provides the following benefits:

  - **Provides Azure Standard SSD support**. When creating a catalog, you, Citrix Virtual Apps and Desktops administrators, can select Standard SSD as the disk type for both pooled and persistent catalog types.

  - **Allows Azure support for secure transfer in Azure Storage**. The Secure transfer required option enhances the security of storage accounts by allowing access to the accounts only from secure connections.
  - **Resolves a power state caching issue**. A power state synchronization reduces from 20 to 5 minutes.
  - **Supports removing power management constraints**. You can power on 1,000 VMs in 12 minutes. Previously, that took 1 hour.
  - With this fix, Azure Resource Manager throttles requests for subscriptions and tenants, routing traffic based on defined limits, tailored to the specific need of the provider

  [CVADHELP-15392]

- The power state of virtual machines that the Citrix Broker Service obtains might be incorrect, causing session launch failures. The issue occurs when the Controller cannot power cycle the virtual machines correctly. [CVADHELP-15864]
- When you manage or power cycle many machines using a Microsoft Azure plug-in, remoting exceptions might occur. [CVADHELP-16103]

Linux VDA

Linux VDA 1912 CU2 documentation provides specific information about the updates in this release.

Metainstaller

- When you attempt to run the VDAServerSetup_1912.exe installer, an exception might occur. [CVADHELP-14457]
- When upgrading a VDA, you cannot disable the **Optimize performance** feature on the **Features** page. Also, you cannot enable other features on that page. [CVADHELP-14560]

Profile Management

Profile Management 1912 CU2 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU2 documentation provides specific information about the updates in this release.

StoreFront

StoreFront 1912 CU2 documentation provides specific information about the updates in this release.

Third-party issues

- An issue in Microsoft Windows 10 version 1809 might cause slight erratic behavior when using the Surface Pro and Surface Book pen. [HDX-17649]

VDA for single-session OS

Installing, Uninstalling, Upgrading

- When you upgrade a VDA, the **MaxVideoMemoryBytes** registry key might revert to the default value. [CVADHELP-13629]

Keyboard

- When you press Windows **Key + P** to display the projection sidebar, all the connected monitors might display a black background until you click the Esc key. The issue occurs with **Transparent key pass-through** enabled in a seamless session. [CVADHELP-14949]
- For Remote PC Access deployments, keyboard input might not work in sessions running on non-Windows devices. [CVADHELP-15291]
- With the F5 key configured as the keyboard shortcut to the **Activate Terminal Node** function in CATIA V5 Digital Mockup (DMU), reconnecting to a session might trigger the corresponding function. [CVADHELP-15402]

Session/Connection

- When you start a dedicated desktop session, a logon failure might occur and the logoff process might get stuck. Citrix Studio shows the session as connected, but you cannot log off until you manually restart the machine. [CVADHELP-10931]
- When several USB devices are redirected to a session, one of them might not work correctly. [CVADHELP-12516]
- When audio devices are added to a user session, you cannot hear sounds from any of the devices except the sounds of Skype for Business. This error message appears:

Error - no more device slots available - failed to add the device.

The issue occurs when more than eight playback or record devices are attached to an endpoint. [CVADHELP-12760]

- When you configure the **High DPI** setting to use the native resolution instead of high DPI, DPI scaling between the VDA and the user device might not match. The issue occurs during the initial connection. [CVADHELP-13205]
- The default audio device in a session might not be the same as the default one on a user device. In the session, the first device on the audio device list becomes the default. [CVADHELP-13324]
- After you restart a VDA, hardware-based encrypted USB redirection might not work. [CVADHELP-13336]
- In a multi-monitor environment, applications might not display consistently on the same monitor. The issue occurs when you move to a new workstation. [CVADHELP-13657]
- When you use HDX RealTime Webcam Video Compression, a webcam might show a black image instead of a live image. [CVADHELP-13877]
- Some portions of an application window might become transparent, causing the application to run in the background instead of in the foreground. The issue occurs in seamless mode. [CVADHELP-13903]
- In a site where XenApp and XenDesktop Version 7.15 LTSR Cumulative Update 4 runs on Microsoft Windows Server 2016, when you attempt to launch a published application, the application session might become unresponsive. This error message appears:

  Please wait for Local Session Manager

  [CVADHELP-13967]
- During the initial launch of a VDI session on a 4K monitor, the session might display at a lower resolution. Also, a gray border might appear around the session window. The issue occurs with devices using certain third-party graphics cards. [CVADHELP-14401]
- The Citrix software graphics process (Ctxgfx.exe) might constantly consume available memory within a session. [CVADHELP-14509]
- When you install VDA Version 1912 or Version 7.15 CU5 on a physical machine, Windows Management Instrumentation (WMI) records that machine as a virtual machine instead of a virtual physical machine. Microsoft System Center Configuration Manager (SCCM) records that machine as a virtual machine instead of a physical machine. The issue occurs when the Microsoft policy **Turn on Base Virtualization Based Security** is set to **ON**.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XdMonitor

Name: IsVDARunningOnVM

Type: DWORD

Value: 00000000

[CVADHELP-14597]

- On a VDA, when you reconnect to a single-monitor thin client from a multi-monitor thin client, the monitor layout might not be updated. [CVADHELP-14646]
- Some third-party 32-bit scanning applications might not work on a VDA when they are redirected to the VDA using Generic USB redirection. The issue occurs when the scanning applications on the VDA use TWAIN DSM. The issue can also occur on a Remote PC Access VDA. [CVADHELP-14698]
- When a user uses Remote PC Access to access the office PC, the remote session might be viewed from the office PC. As a result, session activities are exposed. [CVADHELP-14893]
- Optimization for Microsoft Teams might fail to work in Microsoft Teams. The issue occurs when Citrix HDX is not connected. [CVADHELP-14967]
- This fix provides a timer to send a small datagram over a UDP connection to keep the connection alive between the host and the client.

  To enable the fix, create the registry setting as follows:

  - *For 32-bit systems*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    Name: KeepAliveTimer

    Type: DWORD

    Value: Indicates the wait time interval (in seconds) between keep-alive messages. If left empty or set to 0, no keep-alive packets are sent and the keep-alive feature does not work. The recommended value is 15.

  - *For 64-bit systems*

    HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

    Name: KeepAliveTimer

    Type: DWORD

    Value: Indicates the wait time interval (in seconds) between keep-alive messages. If left empty or set to 0, no keep-alive packets are sent and the keep-alive feature does not work. The recommended value is 15.

    [CVADHELP-15122]

- A session might disconnect when you maximize, minimize, or resize the desktop. The issue occurs with VDA for single-session OS Version 1912 CU1 running on Microsoft Windows 10 Version 1809. [CVADHELP-15200]
- With the CtxUvi Hooking driver disabled, event logs might not be generated. The issue occurs when available system resources are low. [CVADHELP-15241]
- When you attempt to reconnect to a new virtual machine, the following Microsoft .NET Framework error message might appear:

  Error Unhandled exception has occurred in your application

  [CVADHELP-15267]
- The newest virtual channels might not be added to the internal hardcoded whitelist. When you enable whitelisting, this new virtual channel stops working unless they themselves are added to the user configured whitelist. [CVADHELP-15296]
- With this fix, a warning message appears for a workstation VDA before the session gets disconnected due to an idle time out. [CVADHELP-15319]
- This fix provides support to a new feature that lets you configure multiple forest deployments without enabling NTLM authentication on VDAs. However, the previous feature for enabling NTLM authentication is reserved for other deployments without trusts. A registry entry named **SupportMultipleForestDdcLookup** is added to avoid unwanted enabling of NTLM authentication on VDAs. (NTLM is less secure than Kerberos.) You can use **SupportMultipleForestDdcLookup** instead of the **SupportMultipleForest** entry. You can continue to use **SupportMultipleForest** for backward compatibility. The **SupportMultipleForestDdcLookup** registry key determines how VDAs perform delivery controller lookups. For more information, see Deploy in a multiple Active Directory forest environment. [CVADHELP-15467]
- When a VDA attempts to register with a Delivery Controller, the broker agent performs an initial DNS lookup in the local domain. This lookup ensures that the Delivery Controller is reachable. When the DNS lookup fails, the broker agent falls back to performing top-down queries in Active Directory, repeatedly performing searches in all domains. If the address of the Delivery Controller is invalid (for example, the administrator typed the FQDN incorrectly when installing the VDA), the query operations can cause DDoS-like results on the domain controller. For more information, see Controller search during VDA registration. [CVADHELP-15484]
- With the legacy graphics mode policy enabled, a gray screen might appear when you launch a session. This issue occurs with VDA version 7.15.6000. [CVADHELP-15841]
- With this fix, the WTS Hook is enabled by default when you set the flag to 0x80000000. [CVADHELP-15929]
- The following issues can be observed with Microsoft Teams:

- When you reconnect to a session, the HdxTeams.exe process might fail to start. The issue occurs on a VDA running Microsoft Windows Server.
- The Citrix HDX Teams Redirection Service (TeamsSvcs) might fail to get a user session ID. As a result, the Microsoft Teams redirection registry key is not updated.
- When you reconnect to a session, the Citrix HDX Teams Redirection Service (TeamsSvcs) might exit unexpectedly.

[CVADHELP-16213]

Smart Cards

- With this fix, you can track the number of times a smart card has been inserted or removed from a reader using the **SCardGetStatusChange** function. [CVADHELP-15463]

System Exceptions

- The Citrix Audio Redirection ServiceÂ (CtxAudioSvc) might exit unexpectedly with an Event ID 1000 and an exception code 0x0c0000005. The issue occurs because of the faulting module, CtxVorbisDmo64.dll. [CVADHELP-14898]
- The PicaShell.exe process might exit unexpectedly when there is heap corruption in the clipboard virtual channel DLL. [CVADHELP-14945]
- The Internet Explorer browser add-on (Citrix HDXJsInjector) required for Browser Content Redirection might cause a webpage error when you use the developer tools. The InjectorScript.js intermittently experiences a runtime exception when accessing the HTML document.head. This error message appears:

  Error: Unable to get property 'appendChild'of undefined or null reference

  [CVADHELP-14960]
- VDAs might experience a fatal exception on tdica.sys and display a blue screen with bug check code 0x1000007e. The issue occurs when you launch a session through Citrix Workspace app for HTML5. [CVADHELP-15220]

User Experience

- When certain third-party applications are running within a user session, the mouse pointer might change to a spinning circle. The issue occurs when you drag an object in the session or perform a zoom operation. [CVADHELP-14247]

VDA for multi-session OS

Keyboard

- When you press Windows **Key + P** to display the projection sidebar, all the connected monitors might display a black background until you click the Esc key. The issue occurs with **Transparent key pass-through** enabled in a seamless session. [CVADHELP-14949]

Session/Connection

- When several USB devices are redirected to a session, one of them might not work correctly. [CVADHELP-12516]
- When attempting to highlight text in a user session, you might experience performance issues. The issue occurs when you do that in Microsoft Outlook Version 2016 running in a published desktop.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: CursorShapeChangeMinInterval

  Type: DWORD

  Value: Possible values: 10 through 100. Recommended value: 50. The default is 0, which means disabled.

  [CVADHELP-12886]
- After you restart a VDA, hardware-based encrypted USB redirection might not work. [CVADHELP-13336]
- In a multi-monitor environment, applications might not display consistently on the same monitor. The issue occurs when you move to a new workstation. [CVADHELP-13657]
- When you use HDX RealTime Webcam Video Compression, a webcam might show a black image instead of a live image. [CVADHELP-13877]
- Some portions of an application window might become transparent, causing the application to run in the background instead of in the foreground. The issue occurs in seamless mode. [CVADHELP-13903]
- In a site where XenApp and XenDesktop Version 7.15 LTSR Cumulative Update 4 runs on Microsoft Windows Server 2016, when you attempt to launch a published application, the application session might become unresponsive. This error message appears:

  Please wait for Local Session Manager

[CVADHELP-13967]

- The Citrix software graphics process (Ctxgfx.exe) might constantly consume available memory within a session. [CVADHELP-14509]
- When you attempt to upload a file (such as .crx, .exe, or zip file) through Citrix Workspace app for HTML5 session), session reliability might cause the session to disconnect. [CVADHELP-14513]
- After a VDA reports a full load due to high memory usage, the load index value might remain at 10,000 even if the memory usage drops to a low level. [CVADHELP-14563]
- Microsoft Windows winlogon.exe might exit unexpectedly. The issue occurs when you close a seamless session launched through a server. The issue occurs because of the faulting module, icagfxstack.dll. [CVADHELP-14579]
- When you lock a seamless session, the logon window might cover the entire screen, regardless of the size of the session window. As a result, you cannot access the endpoint's desktop and other applications. [CVADHELP-14589]
- Some third-party 32-bit scanning applications might not work on a VDA when they are redirected to the VDA using Generic USB redirection. The issue occurs when the scanning applications on the VDA use TWAIN DSM. The issue can also occur on a Remote PC Access VDA. [CVADHELP-14698]
- This fix addresses a security vulnerability in an underlying component. For more information, see Knowledge Center article CTX285059. [CVADHELP-14755]
- With the **Allow the audio sandbox to run** policy enabled, audio might not work in Google Chrome you open through Citrix Virtual Apps and Desktops. [CVADHELP-14784]
- Optimization for Microsoft Teams might fail to work in Microsoft Teams. The issue occurs when Citrix HDX is not connected. [CVADHELP-14967]
- This fix provides a timer to send a small datagram over a UDP connection to keep the connection alive between the host and the client.

  To enable the fix, create the registry setting as follows:

  - *For 32-bit systems*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    Name: KeepAliveTimer

    Type: DWORD

    Value: Indicates the wait time interval (in seconds) between keep-alive messages. If left empty or set to 0, no keep-alive packets are sent and the keep-alive feature does not work. The recommended value is 15.

- *For 64-bit systems*

  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

  Name: KeepAliveTimer

  Type: DWORD

  Value: Indicates the wait time interval (in seconds) between keep-alive messages. If left empty or set to 0, no keep-alive packets are sent and the keep-alive feature does not work. The recommended value is 15.

  [CVADHELP-15122]

- With the CtxUvi Hooking driver disabled, event logs might not be generated. The issue occurs when available system resources are low. [CVADHELP-15241]
- When you attempt to reconnect to a new virtual machine, the following Microsoft .NET Framework error message might appear:

  Error Unhandled exception has occurred in your application

  [CVADHELP-15267]

- The newest virtual channels might not be added to the internal hardcoded whitelist. When you enable whitelisting, this new virtual channel stops working unless they themselves are added to the user configured whitelist. [CVADHELP-15296]
- When you attempt to switch to a window using the taskbar preview, opening that window might take a long time. [CVADHELP-15422]
- This fix provides support to a new feature that lets you configure multiple forest deployments without enabling NTLM authentication on VDAs. However, the previous feature for enabling NTLM authentication is reserved for other deployments without trusts. A registry entry named **SupportMultipleForestDdcLookup** is added to avoid unwanted enabling of NTLM authentication on VDAs. (NTLM is less secure than Kerberos.) You can use **SupportMultipleForestDdcLookup** instead of the **SupportMultipleForest** entry. You can continue to use **SupportMultipleForest** for backward compatibility. The **SupportMultipleForestDdcLookup** registry key determines how VDAs perform delivery controller lookups. For more information, see Deploy in a multiple Active Directory forest environment. [CVADHELP-15467]
- When a VDA attempts to register with a Delivery Controller, the broker agent performs an initial DNS lookup in the local domain. This lookup ensures that the Delivery Controller is reachable. When the DNS lookup fails, the broker agent falls back to performing top-down queries in Active Directory, repeatedly performing searches in all domains. If the address of the Delivery Controller is invalid (for example, the administrator typed the FQDN incorrectly when installing the VDA), the query operations can cause DDoS-like results on the domain controller. [CVADHELP-15484]

- With this fix, the WTS Hook is enabled by default when you set the flag to 0x80000000. [CVADHELP-15929]

Smart Cards

- With this fix, you can track the number of times a smart card has been inserted or removed from a reader using the **SCardGetStatusChange** function. [CVADHELP-15463]

System Exceptions

- The Service Host (svchost.exe) process that hosts the Windows audio service might exit unexpectedly within a user session. The issue occurs because of a memory leak. [CVADHELP-13687]
- The Service Host (svchost.exe) process or the wfshell.exe process might experience an access violation and exit unexpectedly. The issue occurs because of the faulting module, icaendpoint.dll. [CVADHELP-14276]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [CVADHELP-14332]
- The wfshell.exe process might exit unexpectedly. [CVADHELP-14414]
- On a device that has more than nine monitors, attempts to launch a user session might fail with a fatal exception, displaying a blue screen with bug check code 0x3B. [CVADHELP-14775]
- The Citrix Audio Redirection ServiceÂ (CtxAudioSvc) might exit unexpectedly with an Event ID 1000 and an exception code 0x0c0000005. The issue occurs because of the faulting module, CtxVorbisDmo64.dll. [CVADHELP-14898]
- The PicaShell.exe process might exit unexpectedly when there is heap corruption in the clipboard virtual channel DLL. [CVADHELP-14945]
- The Internet Explorer browser add-on (Citrix HDXJsInjector) required for Browser Content Redirection might cause a webpage error when you use the developer tools. The InjectorScript.js intermittently experiences a runtime exception when accessing the HTML document.head. This error message appears:

  Error: Unable to get property 'appendChild'of undefined or null reference

  [CVADHELP-14960]
- VDAs might experience a fatal exception on tdica.sys and display a blue screen with bug check code 0x1000007e. The issue occurs when you launch a session through Citrix Workspace app for HTML5. [CVADHELP-15220]
- When you attempt to reconnect to a multiport-enabled TCP session launched from Citrix Workspace app for Linux, the VDA might exit unexpectedly. [CVADHELP-15674]

Virtual Desktop Components –Other

- When you launch an App-V application using a shortcut that is located outside of the application package, the **appve** argument might be added to the command line. This **appve** argument is unnecessary. [CVADHELP-14369]
- Attempts to launch an App-V application using a shortcut located within the **AppData** folder might fail. [CVADHELP-14691]
- This fix addresses a security vulnerability in an underlying component. For more information, see Knowledge Center article CTX285059. [CVADHELP-14989]
- If you create App-V applications by using the single admin management method in Citrix Studio, application enumeration might become slow. The issue occurs when duplicate applications are present in the App-V packages. [CVADHELP-15427]
- This fix addresses a security vulnerability in an underlying component. For more information, see Knowledge Center article CTX285059. [CVADHELP-15612]

Cumulative Update 1 (CU1)

September 21, 2021

Release date: May 7, 2020

About this release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 1 (CU1) fixes more than 70 issues reported since the initial release of the 1912 LTSR.

1912 LTSR (general information)

1912 LTSR (features and upgrade information)

Issues fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

> **Important:**
>
> This release has changes in how to install and upgrade StoreFront. In earlier releases, when you clicked the **Get Started** tile in the full-product installer's main page, the **Core Components** page included StoreFront. You can select StoreFront and other core components to install on the same machine.
>
> As of this release, the **Core Components** page no longer contains a StoreFront check box. To install or upgrade StoreFront, click **Citrix StoreFront** in the **Extend Deployment** panel on the main page. This launches `CitrixStoreFront-x64.exe` from the installation media.
>
> In the `XenDesktopServerSetup.exe` command, you can no longer specify `/components storefront`. If you do, the command fails. To install StoreFront from the command line, run `CitrixStoreFront-x64.exe`, which is available in the Citrix Virtual Apps and Desktops installation media's `x64` folder.

New deployments

How do I deploy CU1 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU1 - using the CU1 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU1 provides updates to 15 baseline components of the 1912 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU1. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU1. If Citrix Provisioning is not part of your deployment, you do not need to install or update it.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU1 baseline components

1912 LTSR baseline component	Version as shown in Programs and Features	Notes
Single-session VDA	1912.0.1000	
Multi-session VDA	1912.0.1000	
Delivery Controller	1912.0.1000	
Citrix Studio	1912.0.1000	
Citrix Director	1912.0.1000	
Citrix Group Policy Management	7.24.1000	
Citrix Group Policy Client-Side Extension	7.24.1000	
Citrix StoreFront	1912.0.1000	
Citrix Provisioning	1912.0.1	
Universal Print Server	1912.0.1000	
Session Recording	1912.0.1000	
Linux VDA	1912.0.1000	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.1000	
Citrix Federated Authentication Service	1912.0.1000	
Browser Content Redirection	15.19.1000	

Citrix Virtual Apps and Desktops 7 1912 LTSR CU1 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version as shown in Programs and Features
App Layering	19.11.0
App protection policies	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR

Compatible components and features	Version as shown in Programs and Features
License Server	11.16.3.0 Build 30000
User personalization layer	19.11.0
Session Recording web player	1912.0.0
Teams optimization	1912.0.0
Self-Service Password Reset	1.1
Windows 10 32-bit	
Workspace Environment Management	2003.0.0 and later
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Citrix Virtual Apps and Desktops 7 1912 LTSR CU1 notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.

- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

July 9, 2020

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1912 LTSR (initial release):

Citrix Director

- When a Delivery Controller is powered off, Citrix Director displays the status of the Delivery Controller incorrectly. As a result, false alerts appear on the *Infrastructure* tab in Citrix Director. [CVADHELP-13835]

Citrix Policy

- Servers might disconnect and become unresponsive unless you restart the Group Policy engine (CseEngine.exe) service. [CVADHELP-12987]

Citrix Provisioning

Citrix Provisioning 1912 CU1 documentation provides specific information about the updates in this release.

Citrix Studio

- When you upgrade Citrix Studio from Version 7.6 to Version 7.15, the time it takes to open some wizards (such as Machine Catalog and Delivery Group) might increase. [CVADHELP-13267]
- When you add App-V packages to Citrix Studio, some packages might show default icons instead of customized icons. [CVADHELP-13338]

Delivery Controller

- Some published applications might cause application enumeration to fail. The issue occurs when a corrupted application icon is present in an .exe file. [CVADHELP-13133]
- After daylight saving time ended for the year 2019 and with the restart schedule configured, an unexpected scheduled restart occurred only for the Delivery Group. [CVADHELP-13486]
- When you add administrators of other domains to Citrix Studio, Studio might display the following error message:

  Error: Failed to validate the Central Configuration Service Location.

  You do not have sufficient permissions to administer the Site using Studio, or there is a problem with the Delegated Administration service.

  The issue occurs if a domain controller in any one of the domains is unreachable. [CVADHELP-13651]
- With this fix, Machine Creation Services (MCS) supports the following new Citrix Hypervisor features: Guest UEFI boot and Secure Boot. [CVADHELP-14210]
- On Citrix Hypervisor, attempts to add machines to an existing Machine Creation Services (MCS) catalog might fail. [CVADHELP-14212]

Federated Authentication Service

- In the properties of the Citrix_SmartcardLogon certificate template, the description of the Key Usage extension should contain 'Digital signature'and 'Key encipherment'only, but lists additional items. However, the certificates issued using this template are correct. [CVADHELP-14040]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 1912 CU1 documentation provides specific information about the updates in this release.

Metainstaller

- When you attempt to launch a desktop, a gray screen might appear. The issue occurs after you upgrade a VDA from Version 7.6 LTSR Cumulative Update to Version 1912. [CVADHELP-13969]

Profile Management

Profile Management 1912 CU1 documentation provides specific information about the updates in this release.

Session Recording

Session Recording 1912 CU1 documentation provides specific information about the updates in this release.

StoreFront

StoreFront 1912 CU1 documentation provides specific information about the updates in this release.

Universal Print Server

Client

- When you attempt to launch an application, the Citrix Print Manager Service (CpSvc.exe) might exit unexpectedly. [CVADHELP-13945]
- The Print Spooler service might exit unexpectedly. [CVADHELP-13954]

Server

- Due to an access violation, the Universal Print Server (UPServer.exe) might exit unexpectedly. [CVADHELP-10627]

VDA for single-session OS

Installing, Uninstalling, Upgrading

- When you upgrade a VDA, the `MaxVideoMemoryBytes` registry key might revert to the default value. [CVADHELP-13629]

Printing

- When you attempt to launch an application, the Citrix Print Manager Service (CpSvc.exe) might exit unexpectedly. [CVADHELP-13945]
- PDF printers automatically created might not be deleted. The issue occurs if they are created under HKEY_LOCAL_MACHINE\SOFTWARE instead of HKEY_CURRENT_CONFIG. [CVADHELP-14280]

Session/Connection

- When the Windows Media Player moves from the current track to the next track in the playlist, audio might not play at the beginning of the next track. The issue occurs if Windows Media redirection is enabled. [CVADHELP-11639]
- When you reconnect to an active session on another machine, redirected printers and client drives might be missing. The issue occurs when you move from one machine to another without locking or disconnecting the active user session. [CVADHELP-13035]
- Reading data from a client drive might take a long time after you change the value of the following registry key to 1 on a VDA:

  To enable the fix, create the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  Name: PacketIntegrityChecks

  Type: DWORD

  Value: 1

  [CVADHELP-13063]
- Attempts to launch a session on a VDA might fail when you use some third-party vulnerability scanners. [CVADHELP-13306]
- Attempts to reconnect to a session might fail with the following error message:

  Cannot start desktop.

  [CVADHELP-13320]
- When you attempt to resize the window of a published desktop, hardware encoding might be disabled. [CVADHELP-13818]
- A VDA might become unresponsive after restart. The issue occurs when security software such as Symantec SEP enforces security scans. [CVADHELP-13832]

- With the **Automatic keyboard display** policy enabled, when you click on the **Google search** box, the keyboard might not pop up automatically. The issue occurs when a session is running on the Internet Explorer, Firefox, or Chrome browsers. [CVADHELP-14065]
- When you right-click the user icon in the Start menu, the context menu fails to display the **Shut down** or **Log off** options. Instead, the context menu displays the same options as the context menu that appears after you right-click a tile. [CVADHELP-14149]
- With the time zone policy set to **Use local time of the client**, the time zone might be redirected incorrectly when you launch a session through Citrix Workspace app for HTML5. For example, the time is set to **UTC+01:00** instead of **UTC+00:00**. As a result, the **Automatically adjust clock for Daylight Saving** setting is cleared instead of being checked. [CVADHELP-14471]
- In a double-hop scenario, a single user might consume two Citrix Concurrent User (CCU) licenses. Double hop is when a user launches the HDX session within another HDX session (for example, when you launch a published application within a virtual desktop session). [CVADHELP-14409]
- When you attempt to move small objects on the screen, corruption might occur on a single pixel. The issue occurs when the **Visual quality** policy is set to **Build to Lossless**. [CVADFIX-8214]

Smart cards

- After you configure smart card authentication on Windows 10, smart card pass-through authentication might fail if you launch a desktop in a user session. The issue occurs when you launch a desktop from a thin client. [CVADHELP-11757]
- When you use a fast smart card to log on to a session, the PIN prompt might appear twice. [CVADHELP-12949]

System Exceptions

- USB redirection can cause VDAs to experience a fatal exception, displaying a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. Also, global lock for USB redirection might not be released, thus blocking other redirections. [CVADHELP-9237]
- VDAs might experience a fatal exception on ctxdvcs.sys and display a blue screen with bug check code 0xc0000409. [CVADHELP-13102]
- An application that uses the Electron framework might exit unexpectedly with the following error message:

  {EXCEPTION} Illegal Instruction An attempt was made to execute an illegal instruction.

  [CVADHELP-13440]

- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [CVADHELP-14431]

User Experience

- Desktop sessions might display artifacts that obscure screen contents and other portions of the display. [CVADHELP-13301]

User Interface

- The **Devices** tab might be missing from the **Citrix Workspace** –**Preferences** window (**Desktop Viewer toolbar** > **Preferences**). The issue occurs with a VDI desktop that runs on Microsoft Windows Server through a Server VDI switch. [CVADHELP-14158]

VDA for multi-session OS

Content Redirection

- When you configure the browser content redirection policy in **Server Fetch** and **Client Render** mode, you route traffics only through a statically configured web proxy. [CVADHELP-14134]

Printing

- Attempts to print documents to a different output printer tray might fail. The print job uses the default tray to print documents even if you choose a different tray in the Print dialog box. [CVADHELP-13492]
- When you attempt to launch an application, the Citrix Print Manager Service (CpSvc.exe) might exit unexpectedly. [CVADHELP-13945]
- PDF printers automatically created might not be deleted. The issue occurs if they are created under HKEY_LOCAL_MACHINE\SOFTWARE instead of HKEY_CURRENT_CONFIG. [CVADHELP-14280]

Session/Connection

- When the Windows Media Player moves from the current track to the next track in the playlist, audio might not play at the beginning of the next track. The issue occurs if Windows Media redirection is enabled. [CVADHELP-11639]

- When you launch a published application on a multi-session VDA, the Windows RunOnce registry key might not execute. [CVADHELP-11991]
- Attempts to launch an application might fail. As a result, session details under **Task Manager** cannot be found and the following application status in Citrix Studio appears: **application not running**. When the issue occurs, the VDA might reregister and the following error message appears:

  Event ID 1048: WCF Failure or Rejection by Broker

  [CVADHELP-12856]
- Reading data from a client drive might take a long time after you change the value of the following registry key to 1 on a VDA:

  To enable the fix, create the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  Name: PacketIntegrityChecks

  Type: DWORD

  Value: 1

  [CVADHELP-13063]
- Attempts to reconnect to a session might fail with the following error message:

  Cannot start desktop.

  [CVADHELP-13320]
- When you attempt to reconnect to a session, the desktop might fail to load and a gray window might appear. The issue occurs with VDA Version 1909 running on Microsoft Windows Server 2019. [CVADHELP-13376]
- A VDA might become unresponsive after restart. The issue occurs when security software such as Symantec SEP enforces security scans. [CVADHELP-13832]
- A user session might close unexpectedly. The issue occurs with unauthenticated (anonymous) users when they launch a second application in windowed mode. [CVADHELP-13917]
- After you upgrade a VDA to Version 1909.1, some third-party applications such as `RemoteScan` might fail to scan a document and become unresponsive. The issue occurs because of the faulting module, twnhook.dll. [CVADHELP-13937]
- The virtual keyboard might fail to appear automatically within a published application. [CVADHELP-14012]
- When you attempt to reconfigure Version 1912 of the VDA to use a custom VDA port from the command line, this error message might appear:

The process could not be completed …Cannot find Ica Configuration file …IcaConfigConsole.exe.

[CVADHELP-14052]

- With the **Automatic keyboard display** policy enabled, when you click on the **Google search** box, the keyboard might not pop up automatically. The issue occurs when a session is running on the Internet Explorer, Firefox, or Chrome browsers. [CVADHELP-14065]
- This fix introduces a policy setting that configures virtual channels using multi-stream ICA through a Citrix policy rather than through a registry key. [CVADHELP-14136]
- If you connect a USB microphone to a user device and launch a session, the USB microphone might fail to redirect. The USB device displays as **Optimized, Policy Restricted**. [CVADHELP-14301]
- In a double-hop scenario, a single user might consume two Citrix Concurrent User (CCU) licenses. Double hop is when a user launches the HDX session within another HDX session (for example, when you launch a published application within a virtual desktop session). [CVADHELP-14409]
- When you attempt to move small objects on the screen, corruption might occur on a single pixel. The issue occurs when the **Visual quality** policy is set to **Build to Lossless**. [CVADFIX-8214]

Smart cards

- When you use a fast smart card to log on to a session, the PIN prompt might appear twice. [CVADHELP-12949]

System Exceptions

- USB redirection can cause VDAs to experience a fatal exception, displaying a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. Also, global lock for USB redirection might not be released, thus blocking other redirections. [CVADHELP-9237]
- VDAs might experience a fatal exception on ctxdvcs.sys and display a blue screen with bug check code 0xc0000409. [CVADHELP-13102]
- An application that uses the Electron framework might exit unexpectedly with the following error message:

  {EXCEPTION} Illegal Instruction An attempt was made to execute an illegal instruction.

  [CVADHELP-13440]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [CVADHELP-14431]

User Experience

- Desktop sessions might display artifacts that obscure screen contents and other portions of the display. [CVADHELP-13301]

User Interface

- When you move a seamless window, graphic content for an application might be distorted. The issue occurs when you move some parts of the window outside of the desktop area. [CVADHELP-14209]

Virtual Desktop Components –Other

- When you launch an App-V application from a VDA hosting many App-V applications, the VDA might deregister. The issue occurs when the time it takes to process associated policy files is long. [CVADHELP-12592]
- When you open a file with the associated published App-V application, the application opens. But the file fails to open in the associated application. [CVADHELP-13971]

1912 LTSR (initial release)

April 24, 2023

About this release

The Long Term Service Release (LTSR) program for Citrix Virtual Apps and Desktops provides stability and long-term support for Citrix Virtual Apps and Desktops releases.

LTSRs are currently available for Citrix Virtual Apps and Desktops 7 1912 (this release), and for XenApp and XenDesktop Versions 7.6 and 7.15. If you are new to the LTSR program, you can install Citrix Virtual Apps and Desktops 7 1912 from scratch. If you are on one of the earlier LTSRs, you can upgrade from there, including from any Cumulative Update (CU). For additional information about supported upgrade paths, see the Upgrade Guide.

In addition, Citrix also recommends specific versions of Citrix Workspace app and other components. While not required for LTSR compliance, upgrading to the recommended versions of those components ensures further ease of maintenance and the availability of the latest fixes in your deployment.

For an overview of the features in Citrix Virtual Apps and Desktops 7 1912 that have been added since earlier releases, see the Citrix Virtual Apps and Desktops Feature Summary Comparison table.

This Citrix Virtual Apps and Desktops release includes new versions of the Windows Virtual Delivery Agents (VDAs) and new versions of several core components. You can:

- **Install or upgrade a site**

  Use the ISO for this release to install or upgrade core components and VDAs. Installing or upgrading to the latest version allows you to use all the latest features.

- **Install or upgrade VDAs in an existing site**

  If you already have a deployment, and aren't ready to upgrade your core components, you can still use several of the latest HDX features by installing (or upgrading to) a new VDA. Upgrading only the VDAs is often helpful when you want to test enhancements in a non-production environment.

  After upgrading your VDAs to this version (from version 7.9 or later), you do not need to update the machine catalog's functional level. The **7.9 (or later)** value remains the default functional level, and is valid for this release. For more information, see VDA versions and functional levels.

For instructions:

- If you are building a new site, follow the sequence in Install and configure.
- If you are upgrading a site, see Upgrade a deployment.

Citrix Virtual Apps and Desktops 7 1912 LTSR

Important notice about upgrading VDAs

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.

Learn if you're affected How PvD 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.

If you don't know whether your VDA has PvD installed, run the installer for the new VDA (1912 LTSR or later) on the machine or image.

- If PvD is installed, a message appears, indicating there is an incompatible component.
  - For the graphical interface, click **Cancel** on the page containing the message, and then confirm that you want to close the installer.
  - From the CLI, the command simply fails with the displayed message.
- If PvD is not installed, the upgrade proceeds.

What to do If the VDA does not have PvD installed, follow the usual upgrade procedure.

If the VDA has PvD installed:

1. Uninstall the current VDA. For details, see Remove components.
2. Install the new VDA.

If you want to continue using PvD on your Windows 7 or Windows 10 (1607 and earlier, without updates) machines, VDA 7.15 LTSR is the latest supported version.

Install and upgrade: New user personalization layer component in single-session VDAs

When installing or upgrading a single-session VDA, you can include the user personalization layer component. This feature is powered by Citrix App Layering, On non-persistent machines, the feature preserves users' data and locally installed applications across sessions.

This feature replaces Personal vDisk, which has been deprecated. If you are upgrading a VDA that previously had PvD installed, see Important notice about upgrading VDAs.

For details about the new feature, see the user personalization layer documentation. For VDA installation guidance, see Install VDAs.

Install and upgrade: Microsoft Visual C++ Runtime 2017 prerequisite

When installing a Delivery Controller or Windows VDA, Microsoft Visual C++ Runtime 2017 is installed automatically if it (or a later supported version) is not already installed. This is a newer Visual C++ Runtime version than the version installed in earlier Citrix Virtual Apps and Desktops releases.

Install and upgrade: SQL Server Express version

When installing the first Delivery Controller, you can choose to have Citrix install Microsoft SQL Server Express on the same machine, for use as the site database. As of this release, for new installations,

we install SQL Server Express 2017 with Cumulative Update 16. This is a newer version than in earlier Citrix Virtual Apps and Desktops releases. For upgrades, we do not upgrade any SQL Server Express version that is already installed.

When you install a Controller, Microsoft SQL Server Express LocalDB is installed automatically for use with Local Host Cache. (This installation is separate from the SQL Server Express used for the site database.) For a new installation, we install SQL Server Express LocalDB 2017 with Cumulative Update 16. This is a newer version than in earlier Citrix Virtual Apps and Desktops releases. For upgrades, we do not upgrade any SQL Server Express LocalDB version that is already installed.

Install and upgrade: Supported Windows 10 versions for VDAs

This release supports Windows 10 32-bit (x86) and 64-bit (x64) OSs. Windows 10 32-bit is supported only for 18 months from the initial release of the 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC. For Windows 10 machines, Citrix recommends using 64-bit (x64).

Install and upgrade: Prevent pending reboot check

When installing or upgrading core components, the installer stops if it detects that a restart is pending from a previous Windows installation on the machine. Now, when using the command-line interface, you can prevent the check for a pending restart by including the `/no_pending_reboot_check` option in the command. For more information, see During installation of any component.

VDAs and machine catalogs: Operating system name changes

Operating system names for VDAs and machine catalogs 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.

Component version number: Change to on-premises value

In a product and component version number (*YYMM.c.m.b*), the value of *c* is **0** for an on-premises release. For example, in **Apps & features**, this version appears as 1912.0.0.*build number*.

In earlier on-premises releases, and in Citrix Cloud releases, the value of *c* is **1**.

For more information, see Product and component version numbers.

Citrix Studio

Support for provisioning Linux machines on Amazon Web Services

Citrix Studio now supports using Machine Creation Services (MCS) to provision Linux machines on Amazon Web Services (AWS). For more information, see Use MCS to create Linux VMs.

Virtual Delivery Agents (VDAs) 1912

Version 1912 of the VDA for Multi-session OS and the VDA for Single-session OS includes the following enhancements (in addition to the VDA installation and upgrade items listed previously in this article):

> **Note:**
>
> Although VDA version number displays indicate "Citrix Virtual Apps and Desktops 7 1912 LTSR", the VDAs are supported for LTSR and CR deployments.

Support for Local Security Authority (LSA) protection

We now support the use of Local Security Authority (LSA) protection on a multi-session server OS and a single-session desktop OS for standard authentication, Federated Authentication Service (FAS) authentication, and Smart Card authentication. For more information about LSA protection, see the Microsoft article Configuring Additional LSA Protection.

App protection

This release introduces an add-on feature that enhances security when using Citrix Workspace app. New policies provide anti-keylogging and anti-screen-capturing capabilities in a session. The new policies along with Citrix Workspace app 1912 or later for Windows can help protect data from keyloggers and screen scrapers. For more information, see App protection.

Citrix Licensing 11.16.3.0 Build 29000

Citrix Licensing 11.16.3.0 Build 29000 contains new features and fixed and known issues.

Citrix Federated Authentication Service 1912

Citrix Federated Authentication Service (FAS) 1912 contains new features.

More information

- Be sure to check Deprecation for any changes to announcement and removal versions.
- For information about product name and version number changes that were introduced in 2018, see New names and numbers.

Baseline components

1912 LTSR baseline component	Version	Notes
Single-session VDA	1912.0	
Multi-session VDA	1912.0	
Delivery Controller	1912.0.0	
Citrix Studio	7.24.0	
Citrix Director	7.24.0	
Group Policy Management Experience	7.24.0	
StoreFront	19.12.0.0	
Provisioning Services	1912	
Universal Print Server	7.24.0	
Session Recording	1912.0.0	
Linux VDA	1912.0.0	See the Linux VDA documentation for supported platforms
Profile Management	1912.0.0	
Federated Authentication Service	7.24.0	
Browser Content Redirection	15.19.0	

Compatible components

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 1912 LTSR environments.

Compatible components and features	Version
App Layering	19.11.0
App protection policies	1912.0.0
HDX RealTime Optimization Pack	2.8
License Server	11.16.3.0 Build 29000
User personalization layer	19.11.0
Session Recording web player	1912.0.0
Teams optimization	1912.0.0
Self-Service Password Reset	1.1
Windows 10 32-bit	
Workspace Environment Management	1912.0.0
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only

> **Note:**
>
> Windows 10 32-bit is supported only for 18 months from the initial release of 1912 LTSR. Windows 10 32-bit is supported only on Windows 10 Enterprise 2019 LTSC.
>
> * XenApp and XenDesktop 7.15 LTSR VDA support in this case is for Windows 7 and Windows 2008 R2 only. XenApp and XenDesktop 7.15 LTSR support ends on August 2022. Citrix support for Windows 7 and Windows 2008 R2 ends when Microsoft ends support for the OS or when XenApp and XenDesktop 7.15 LTSR support ends, whichever comes first. For more information, see the Citrix Product Matrix.

Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the Citrix Virtual Apps and Desktops 1912 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

For your convenience, consider subscribing to the Citrix Workspace app RSS feed to receive a notification when a new version of Citrix Workspace app becomes available.

Notable exclusions

The following features, components, and platforms are not eligible for 1912 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a site running 1912 LTSR. This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp site.

After you install the XenApp 1912 LTSR core components and create a site, the migration process follows this sequence:

- Run the 1912 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Server OS for use in the new site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new site. By tailoring the files, you can import policy and application settings into your 1912 LTSR site in stages: some now and others later.
- Run PowerShell import cmdlets on the new 1912 Controller, which import settings from the XML files to the new XenApp site.

Reconfigure the new site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

August 11, 2022

The following issues have been fixed since Citrix Virtual Apps and Desktops 7 1909:

Citrix Studio

- Citrix Studio might incorrectly display the icons for some discovered applications when you add applications from the Start menu. The issue occurs with Windows built-in applications on Windows 10 version 1903. As a workaround, select the application, click **Properties**, click **Change** on the Delivery page, and then select an applicable icon for that application. [BRK-4430]

Citrix Provisioning

Citrix Provisioning 1912 documentation provides specific information about the updates in this release.

Delivery Controller

- Attempts to stop the Citrix Broker Service might fail. [CVADHELP-12715]
- In VMware vSAN 6.7 environments, deleting a VM created by Machine Creation Services (MCS) might fail due to the removal of the base disk image. This image is shared among multiple VMs. This issue occurs when the .VMDK file contains the flag `dbb.deletable=false`. [CVADHELP-13127]

- If you attempt to create a machine catalog using Machine Creation Services (MCS) in a VMware environment, catalog creation fails with the following error message:

  FailedToCreateImagePreparationVm

  [CVADHELP-13143]

- Attempts to create or update the Machine Creation Services (MCS) catalogs on Microsoft Azure might fail with the following error message:

  Error, exception of type: "System.OutOfMemoryExceotion"

  [CVADHELP-13146]

HDX RealTime Optimization Pack

HDX RealTime Optimization Pack 1912 documentation provides specific information about the updates in this release.

Licensing

Licensing 1912 documentation provides specific information about the updates in this release.

Linux VDA

Linux VDA 1912 documentation provides specific information about the updates in this release.

Profile Management

Profile Management 1912 documentation provides specific information about the updates in this release.

StoreFront

StoreFront 1912 documentation provides specific information about the updates in this release.

VDA for single-session OS

Printing

- On a VDA for Desktop OS, attempts to print a file with a mapped client printer might fail. The issue occurs when the VDA is installed on Windows 10 version 1903. [CVADHELP-13357]

- With the non-default fonts (for example, the barcode font CCode390) installed on the VDA Version 7.18 or later, a printing issue might occur when you update XenApp and XenDesktop from Version 7.17 to 7.18 or later. As a result, the barcode font might not print when you print a document from a session. [CVADHELP-12454]

Session/Connection

- When you play back audio in a user session, you might hear a popping sound. [CVADHELP-11241]
- On Citrix Receiver for Windows, you might hear sounds intermittently when you play audio. [CVADHELP-11440]
- On some user devices, it might take a long time to launch a second application if you set the graphics cards to ON. [CVADHELP-12387]
- The optimized webcam feature of Media Foundation-based video applications might not work for some APIs. [CVADHELP-12427]
- When you change visual effects within a user session, the `UserPreferencesMask` value under the registry key HKEY_CURRENT_USER\Control Panel\Desktop might not be updated to the new value.

  To enable the fix, create the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\UI Tweak\SystemPropertiesComputerNa

  Name: HookProcess

  Type: REG_DWORD

  Data: 1

  [CVADHELP-12796]
- Attempts to copy text from a published application to an endpoint might fail when using Citrix Workspace app 1902 for Windows or later. [CVADHELP-12945]
- An access violation can cause the wfshell.exe process to exit unexpectedly. As a result, an attempt to launch an application fails. [CVADHELP-13032]

System exceptions

- When you attempt to export video clips on a VDA for Desktop OS, certain third-party applications might exit unexpectedly. [CVADHELP-11303]

- Servers might experience a fatal exception on tdica.sys and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**.

  [CVADHELP-12611]

- The wfshell.exe process might exit unexpectedly on a VDA. [CVADHELP-12819]
- Attempts to launch applications might fail when the wfshell.exe process exits unexpectedly. The issue occurs because of the faulting module, cmpcom.dll. [CVADHELP-13089]

VDA for multi-session OS

Printing

- With the non-default fonts (for example, the barcode font CCode390) installed on the VDA Version 7.18 or later, a printing issue might occur when you update XenApp and XenDesktop from Version 7.17 to 7.18 or later. As a result, the barcode font might not print when you print a document from a session. [CVADHELP-12454]

Session/Connection

- When listening to audio with the audio quality set to high, you might hear a popping or a crackling sound. The issue occurs when you pause the audio for a few seconds and then start the audio again. [CVADHELP-10657]
- On some user devices, it might take a long time to launch a second application if you set the graphics cards to ON. [CVADHELP-12387]
- The optimized webcam feature of Media Foundation-based video applications might not work for some APIs. [CVADHELP-12427]
- When you change visual effects within a user session, the UserPreferencesMask value under the registry key HKEY_CURRENT_USER\Control Panel\Desktop might not be updated to the new value.

  To enable the fix, create the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\UI Tweak\SystemPropertiesComputerNa

  Name: HookProcess

  Type: REG_DWORD

  Data: 1

  [CVADHELP-12796]

- Attempts to copy text from a published application to an endpoint might fail when using Citrix Workspace app 1902 for Windows or later. [CVADHELP-12945]
- An access violation can cause the wfshell.exe process to exit unexpectedly. As a result, an attempt to launch an application fails. [CVADHELP-13032]

System Exceptions

- Microsoft Internet Explorer might exit unexpectedly. The issue occurs because of the faulting module, icaendpoint.dll. [CVADHELP-12171]
- Servers might experience a fatal exception on tdica.sys and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [CVADHELP-12611]
- The wfshell.exe process might exit unexpectedly on a VDA. [CVADHELP-12819]
- Attempts to launch applications might fail when the wfshell.exe process exits unexpectedly. The issue occurs because of the faulting module, cmpcom.dll. [CVADHELP-13089]

User Experience

- When you click the volume control on the taskbar using the left mouse button, the volume control might fail to open. The issue occurs on a non-English version of the Microsoft Windows operating system. [CVADHELP-10739]

Known issues

April 23, 2024

Notes

- Known issues that are described in the 1912 initial release, CU1, CU2, CU3, CU4, CU5, CU6, CU7, and CU8 sections of this article continue to be present in CU9 unless they are included in the list of fixed issues.
- If a known issue has a workaround, it is provided after the description of the issue.
- The following warning applies to any workaround that suggests changing a registry entry:

> **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.

Known issues in 1912 CU9

- You cannot install a VDA on Windows 2012 R2 with Citrix Workspace app during a VDA install or upgrade.

  Workaround: Exclude the Citrix Workspace app during a VDA install or upgrade. See Citrix Workspace app system requirements before you deploy the VDA.
  [LCM-14080]

- When you install CVAD LTSR 1912 CU9 using the command-line install method, and you enter commands in the command prompt, it enters into a new line and initiates the silent installation. However, after the installation is complete, you don't get a message indicating the installation is complete. [LCM-14108]

Known issues in 1912 CU8

- If you install Windows, IIS and Citrix Director in drives other than C:\ and upgrade Citrix Director to release 1912 LTSR CU8, the Citrix Director icon might appear blank. However, you can click the icon to launch the Citrix Director.

  You can use the following workaround to help display the icon correctly.

1. Open the command prompt and run the command echo **%systemdrive%**.
2. Copy the output of the command.
3. Right-click on Citrix Director icon > More > Open file location.
4. Open Notepad and drag the icon from file explorer to Notepad.
5. In the contents, replace "C:"with the output copied in step 2 and save.
6. The Citrix Director icon will now be displayed correctly.

[DIR-21012]

Known issues in 1912 CU7

- Attempts to install Citrix Workspace app might fail on Windows Server 2012 R2. For more information, see Knowledge Center article CTX477888. [LCM-12342]

- Attempts to install Citrix Workspace app along with VDA installation might fail if there is no internet access. As a workaround, you must either skip installing Citrix Workspace app or install Microsoft WebView (which is a prerequisite for Citrix Workspace app) before you install the VDA. [LCM-12992]

Known issues in 1912 CU6

- Microsoft no longer supports the creation of new virtual machines with unmanaged disks on Azure. However, previously created master templates using unmanaged disks are usable. [LCM-10287]
- The command line install parameter, `/IGNORE_DB_CHECK_FAILURE`, is not supported in 1912 LTSR CUs. [LCM-11958]
- Attempts to install Citrix Workspace app might fail on Windows Server 2012 R2. For more information, see Knowledge Center article CTX477888. [LCM-12342]
- Attempts to install Citrix Workspace app along with VDA installation might fail if there is no internet access. As a workaround, you must either skip installing Citrix Workspace app or install Microsoft WebView (which is a prerequisite for Citrix Workspace app) before you install the VDA. [LCM-12992]
- The Virtual Channel Allow List feature might not work in Microsoft Teams. [CVADHELP-21287]

Known issues in 1912 CU5

- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. The issue occurs due to the Microsoft changes made on Azure. A private fix is available at CTX457802. [CVADHELP-18741]
- When using this VDA version, Citrix policies applied to a machine by OU can sometimes fail to apply. [CVADHELP-19826]
- After upgrading Delivery Controller to version 1912 CU5, scheduled reboot might not work correctly with VDAs that are not power managed. [CVADHELP-20138]
- The Virtual Channel Allow List feature might not work in Microsoft Teams. [CVADHELP-21287]

Known issues in 1912 CU4

- When using this VDA version, Citrix policies applied to a machine by OU can sometimes fail to apply. [CVADHELP-19826]

- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. The issue occurs due to the Microsoft changes made on Azure. A private fix is available at CTX457802. [CVADHELP-18741]
- When you exit from a Citrix virtual session, one or more of the following issues might occur:
  - The VDA still lists the terminated session and the logonui.exe process. The logonui.exe process can be forcefully terminated.
  - The session appears with a blank username in Citrix Studio.
  - You might not be able to launch further sessions.

  A private fix is available at CTX340125.

  [CVADHELP-19182]
- The Virtual Channel Allow List feature might not work in Microsoft Teams. [CVADHELP-21287]

Known issues in 1912 CU3

- When attempting to update the Licensing CEIP option using the `Set-LicCEIPOption` cmdlet, the operation fails with a "Communication Error."As a workaround, the CEIP option can be enabled through Citrix Licensing Manager. For more information, see Knowledge Center article CTX220679. [LCM-9169]
- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. The issue occurs due to the Microsoft changes made on Azure. A private fix is available at CTX457802. [CVADHELP-18741]
- The Virtual Channel Allow List feature might not work in Microsoft Teams. [CVADHELP-21287]

Known issues in 1912 CU2

- Configuring your on-premises site with Citrix Analytics for Performance from Director might fail if the Delivery Controller is running a Microsoft .NET Framework version earlier than 4.8. As a workaround, upgrade the .NET Framework in your Delivery Controller to version 4.8. [LCM-9255]
- Signing in to an unbrokered RDP session with a UPN credential might result in an uncaught exception. In 1912 LTSR CU2, a name translation for usernames provided as UPN was introduced. The truncation of the username due to the limit imposed in RDS data structures produces an incorrect username, resulting in the uncaught exception. [CVADHELP-16510]
- If the .NET Framework version is not at least 4.7.2 after upgrading to 1912 LTSR CU2, the Azure Resource Manager fails. [CVADHELP-16533]

- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. The issue occurs due to the Microsoft changes made on Azure. A private fix is available at CTX457802. [CVADHELP-18741]
- Citrix Director might fail to enumerate policy information. The issue occurs when you use an older version of Director to view session details associated with 1912 LTSR CU2 VDA. As a workaround, follow the steps mentioned in the upgrade sequence. [LCM-8201]
- Some file operations executed in a published app or a published desktop session to a client mapped drive might fail with a "permission denied"error message. Users might also see the "File In Use"error on the local client machine. For more information, see Knowledge Center article CTX285248. [HDX-26969]

Known issues in 1912 CU1

In addition to the known issues in the 1912 LTSR initial release, CU1 contains the following, new known issues:

Citrix Provisioning

- When you attempt to downgrade a Citrix Provisioning Target Device from Version 1912 LTSR or 1912 LTSR CU1, the following message might appear:

  Installation failed.

  As a workaround, uninstall the 1912 LTSR or 1912 LTSR CU1 version and then reinstall the earlier version. [LCM-7341]
- When you upgrade a Provisioning Server from Version 7.15 Cumulative Update 5 to Version 1912, a warning message might appear twice. This message appears because of a dependency on the CDF installer (a separate, Citrix Virtual Apps and Desktops component) during the installation of Citrix Provisioning. The provisioning installer cannot suppress the reboot message created by the CDF installer. As a result, the reboot message appears twice. [LCM-7594]

General

- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. The issue occurs due to the Microsoft changes made on Azure. A private fix is available at CTX457802. [CVADHELP-18741]

Logging display

- After a `BrokerHostingPowerAction` PowerShell cmdlet runs, the Studio **Logging** display indicates that the cmdlet failed, although the cmdlet completed successfully. As a workaround, check the result on the host. [BRK-7002]

Content redirection

- With browser content redirection enabled, attempts to open a new tab by right-clicking a hyperlink in Chrome can fail. As a workaround, select `Always allow pop-ups and redirects` in the `Pop-ups blocked` message. [LCM-7480]

Install and upgrade

- With app protection enabled, the imported app protection feature table might be removed when you upgrade from Version 1912 to Version 1912 LTSR CU1. Also, the update of the StoreFront feature might be lost. As a workaround, perform the following steps:

  1. On an upgraded CU1 Controller, reimport the xml feature table available with the CU1 download.
  2. On the StoreFront server, reenable the app protection feature.

  [LCM-7872]

Known issues in 1912 initial release

Install and upgrade

- If you already have Universal Print Server (UPS) version 19061022052 installed, upgrading UPS using the 1906.2 metainstaller does not add any new UPS functionality. After the upgrade, only the Universal Print Server version number, in Programs and Features, is changed to 19062022068. [HDX-20674]
- When you run the Citrix Virtual Apps and Desktops metainstaller, on the Diagnostics page if you click **Connect** without first selecting **Collect diagnostic information**, after you close the Connect to Citrix Insight Services dialog the **Next** button is disabled and you cannot move to next page. To re-enable the **Next** button, select and immediately deselect **Collect diagnostic information**. [XAXDINST-572]
- If you upgrade Studio from XenApp and XenDesktop 7.15 LTSR (7.15 Studio) to Citrix Virtual Apps and Desktops 7 1912 LTSR (1912 Studio), then uninstall 1912 Studio and reinstall 7.15 Studio,

studio fails to launch with error "'Cannot load windows PowerShell snap-in PvsPsSnapIn error' occurred in studio."To solve this issue, before reinstalling 7.15 Studio, manually delete PvsPsSnapIn.dll under `C:\Program Files\Citrix\PowerShell SDK`. [XAXDINST-610]

- If you request a list of valid options for the `XenDesktopServerSetup.exe` command, the `/no_webstudio` option is listed. This option is for internal use only. Do not use it. [STUD-9701]

VDA installation

- After installing a VDA and before restarting the machine, a Citrix Files error message appears: "Incompatible .NET Framework, shutting down. Install one of the KBs listed on this Known Issue page to resolve:.."As a workaround, before VDA installation, install KB4054856 on top of `NDP471-KB4033342-x86-x64-AllOS-ENU.exe`. [LCM-7563]

General

- When MCS creates non-persistent machines in AWS, the DeleteOnTermination flag is set to True. However, upon power cycling, MCS re-creates new EBS volumes and swaps it with the old one which changes the DeleteOnTermination flag to False. [PMCS-4953]
- In Citrix Hypervisor, after installing a new VDA the Citrix Desktop Service erroneously sets the XenTools registry value to UTC. The service does not verify the system time, leading to a connection failure resulting in machines existing in an unregistered state. This issue is temporary. The VDA corrects the system time when it synchronizes from various sources. The current fix sets the XenTools registry value to UTC only if the operating system time is UTC, resulting in no mismatch. [PMCS-5425]
- If you use the hypervisor to delete a virtual machine provisioned using Citrix Virtual Apps and Desktops, you may not be able to add the machine to the catalog because the base disk is also deleted as part the virtual machine deletion process. [PMCS-8591]
- Using a template to provision a catalog is considered an experimental feature. When using this method, virtual machine preparation may fail. As a result, the catalog cannot be published using the template. [PMCS-602]
- If you try to add a protected app to your **Favorites**, this message might appear, "Your apps are not available at this time…"When you then click **OK**, this message appears, "Cannot add app." After you switch to the **Favorites** screen, the protected app is listed there, but you can't remove it from **Favorites**. [WSP-5497]
- Each time you upload a compressed file using Citrix Workspace app for HTML5 on an end-to-end SSL using either Chrome or Safari browser, session reliability might start, eventually creating an

unusable session. To resolve this issue, relaunch the session. To re-enable file transfer, log off from the current session. [HDX-22106]

- After installing the Skype for Business Web App Plug-in, webcams might not be enumerated and meeting pages on Firefox might not refresh automatically. [HDX-13288]
- Upgrading the VDA to version 1906 automatically installs the new MCS I/O driver if it was not previously installed. As a result, target devices fail to boot in read only mode. Citrix recommends that you do not install updated MCS I/O functionality and Citrix Provisioning in the same Windows environment. [PVS-4151]
- When you start an application from StoreFront, the application might not start in the foreground, or the application is in the foreground but might not have focus. As a workaround, click the icon in the task bar to bring the application to the front or in the application screen to bring it to focus. [HDX-10126]
- When you connect to a new session, disconnect, and then reconnect to the same session, your desktop icons might flicker. As a workaround reset the user profile, log off the session, and log on again. [HDX-15926, UPM-1362]
- When using Windows 10 1809 LTSC, VCLibs dependencies fail to install. [HDX-16754]
- The combo box might not display properly when a user selects a combo box that is already in focus on the host. As a workaround, select another UI element and then select the combo box. [HDX-21671]
- When you attempt to reconnect to a session, the desktop might fail to load and a gray window might appear. The issue occurs with VDA Version 1909 running on Microsoft Windows Server 2019. [HDX-21804]
- You have enabled Local App Access. If you start a Windows 2012 R2 VDA session, disconnect and reconnect the session, and then start a local application and maximize it, the VDA taskbar might truncate the application. [HDX-21913]
- When both IPv4 and IPv6 addressing is configured in your network, resources in a delivery group may not be accessible when the delivery group uses a Broker Access Policy rule configured to allow IPv4 address filtering only. To ensure all resource filtering behaves as expected, configure the Broker Access Policy rule to include both client IPv4 and IPv6 addresses. [WADA-7776]

  For example, to set rules allowing IPv4 and IPv6 addresses via 'direct to StoreFront' and 'Citrix Gateway' access, use PowerShell such as:

```
1  Set-BrokerAccessPolicyRule -Name "Apps_Direct" -
       IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
       10.0.0.1","2001::3")
2  Set-BrokerAccessPolicyRule -Name "Apps_AG" -
       IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
       10.0.0.1","2001::3")
```


To confirm a rule, use PowerShell such as:

```
Get-BrokerAccessPolicyRule -Name \"Apps\_Direct\" | Select Name,
    IncludedClientIPFilterEnabled,IncludedClientIPs
```

This returns the following when the rule is correctly set for IPv4 and IPv6 addresses:

```
Name         IncludedClientIPFilterEnabled IncludedClientIPs
--                  -------------------------- -----------------
Apps_Direct                           True {
10.0.0.1/32, 2001::3/128 }
```

- When applications from Microsoft Office 365 build 16.0.7967 and later are published as applications from a Windows Server 2019 host, Office license activation fails. Citrix are working with Microsoft to address this Microsoft limitation. The supported workaround is to install Windows Server 2016 VDAs, which do not have Web Authentication Manager component that is misbehaving. [LCM-7637]
- Citrix Virtual Apps and Desktops does not support the System Center Virtual Machine Manager (SCVMM) delegated administrators with access to multiple top level host groups (without root) and duplicate host group names. The following error message appears when adding an SCVMM hosting connection using the delegated administrator account:

  Unexpected error. Contact Citrix Support

  [CVADHELP-10669]
- Attempts to create a hosting connection to Azure in Citrix Studio might fail with an exception. The issue occurs due to the Microsoft changes made on Azure. A private fix is available at CTX457802. [CVADHELP-18741]

Studio

- In some cases, the virtual machine's power state appears as unknown even if it appears registered. To resolve this issue, edit the registry key `HostTime` value to disable time synchronization with the host:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenTools\HostTime="Local"`

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenTools\HostTime="Local"`

> **Tip:**
>
> The default value is `HostTime="UTC"`. Change this value to something other than UTC, for

> example, `Local`. This change effectively disables time synchronization with the host. [BRK-4187]

Director

- The **Console** link on Citrix Director > Machine Details does not launch the Machine Console in the Microsoft Edge 44 and Firefox 68 ESR browsers. [DIR-8160]
- If you have upgraded to Director 7 1903 or later from any previous releases and not cleared the browser cache (not selected the 'Disable cache'check box), custom reports previously created are lost and Director displays an "Unexpected Server error"on the Custom Reports tab. Differences in UI design between previous and current versions of Director can cause this issue. Disable cache and perform a hard refresh to view old custom reports and create and view new custom reports. [DIR-7634]

Graphics

- Setting the policy **View window contents while dragging** to **Prohibited** does not work on ESXi and Hyper-V. [HDX-22002]
- If you start a video preview using a 64-bit webcam app over Theora compression, the session might crash. [HDX-21443]
- Skype Universal Windows app (UWA) launches with a black background. In some cases, this background occupies the client's entire screen. [HDX-22088]
- In some cases, an application may launch in the background while another application is currently in focus. As a result, local window ordering is lost. [HDX-21569]
- The XenCenter console might display a blank screen after disconnecting a XenDesktop session. As a workaround, send CTLR+ALT+DEL to the XenCenter console to make the console screen appear. [HDX-17261]
- DPI might not match during a session running on Windows Multi-session OS 2016 or 2019 when the DPI is changed on the client and the session is reconnected. As a workaround, resize the session window to match the DPI. [HDX-17313]
- These issues apply to ADM hardware encoding. [HDX-20476]:
  - Pixelation might occur when using Citrix Workspace app for Windows. As a workaround, make the following registry setting on the client that has Citrix Workspace app for Windows installed:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRe
    (32-bit)

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
(64-bit)

Name: MaxNumRefFrames

Type: DWORD

Value: 5

- You might see less than optimal performance when using 4k resolution. This issue causes a frame rate of only 7–10 frames per second. Also, encoding time increases.
- Video stutter might occur for the first two to five seconds of the video when using the Selective H.264 graphics mode. RapidFire SDK is not designed for this use case.

Printing

- Universal Print Server printers selected on the virtual desktop do not appear in the **Devices and Printers** window in Windows Control Panel. However, when users are working in applications, they can print using those printers. This issue occurs only on the Windows Server 2012, Windows 10 and Windows 8 platforms. For more information, see CTX213540. [HDX-5043, 335153]
- The default printer might not be marked correctly in the printing dialog window. This issue does not affect print jobs sent to the default printer. [HDX-12755]

Machine Creation Services

- In AWS environments, launching and terminating volume worker instances fails to remove their associated network interfaces. To resolve this issue, manually delete network interfaces with conditions matching the following state: `Available && Description: "XD NIC"&& tag: "XdConfig : XdProvisioned=true"`. [PMCS-20775]

App-V

- App-V applications may fail to start if more than 100 applications are published in a single Delivery Group. To increase this limit, use the MaxReceivedMessageSize property on the appropriate binding element to increase Max Receivable message size. Do this in the configuration of the Delivery Controller and/or the Broker Agent on the VDA. [APPV-11]

Third-party issues

- Chrome supports UI Automation only for toolbars, tabs, menus, and buttons around a web page. Because of this Chrome issue, the automatic keyboard display feature might not work in

a Chrome browser on touch devices. As a workaround, run `chrome --force-renderer-accessibility` or you can open a new browser tab, type `chrome://accessibility`, and enable **Native accessibility API** support for specific or all pages. In addition, when you publish a seamless app, you can publish Chrome with the `--force-renderer-accessibility` switch. [HDX-20858]

- An issue in Microsoft Windows 10 version 1809 might cause slight erratic behavior when using the Surface Pro and Surface Book pen. [HDX-17649]
- A VDA running on Azure might freeze when using Enlightened Data Transport (EDT), requiring a session reconnect. As a workaround, set edtMSS=1350 and OutbufLength=1350 in Azure environments. For more information, see CTX231821. [HDX-12913]
- In browser content redirection, after starting a YouTube video using the YouTube HTML5 video player, full-screen mode might not work. You click the icon in the lower-right corner of the video, and the video doesn't resize leaving the black background in the full area of the page. As a workaround, click the full screen button, and then select theater mode. [HDX-11294]

Deprecation

October 3, 2023

The announcements in this article are intended to give you advanced notice of platforms, Citrix products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they 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. For information about the Long Term Service Release (LTSR) servicing option, see https://support.citrix.com/article/CTX205549.

Deprecations and removals

The following table shows the platforms, Citrix products, and features that are deprecated or removed.

Deprecated items are not removed immediately. Citrix continues to support them in this Citrix Virtual Apps and Desktops 7 1912 Long Term Service Release (LTSR), but they will be removed in a future release.

Removed items are either removed, or are no longer supported, in Citrix Virtual Apps and Desktops. Dates in **bold** face indicate changes at this release.

Item	Deprecation announced in	Removed in	Alternative
Support for WebRTC SDP format (Plan B)	2308	—	Upgrade the Citrix Workspace App to a supported version.
Support for Single Window mode in Microsoft Teams Optimization	2308	—	Upgrade the Citrix Workspace App to a version that supports MultiWindow mode. For more information, see Feature matrix and version support.
Import Citrix Provisions target devices into Citrix Virtual Apps and Desktops catalogs for management	1912 LTSR	-	Use the Citrix Provisioning Export Devices Wizard.
StoreFront browser support for Microsoft Edge Legacy	1912 LTSR CU2	**1912 LTSR CU3**	Upgrade to Microsoft Edge (based on Chromium).
Citrix License Administration Console (last included in the Windows License Server 11.16.3 build 30000 and removed in the Windows License Server v11.16.6 build 31000).	1912 LTSR CU2	1912 LTSR CU2	Use the Citrix Licensing Manager.

Item	Deprecation announced in	Removed in	Alternative
Citrix SCOM Management Packs for XenApp and XenDesktop, Provisioning Services, and StoreFront. For the product versions that can be monitored, see Citrix SCOM Management Packs documentation.	**1912†**		Use Director for monitoring and managing your deployment. For more information on SCOM EOL and alternatives, see https://support.citrix.com/article/CTX266943.
Support for Microsoft .NET Framework versions prior to version 4.8 for VDAs and core server components. Includes Delivery Controller, Studio, Director, and StoreFront.	**1912**		Upgrade to .NET Framework version 4.8.
VDAs on Windows Server 2012 R2.	**1912**		Install VDAs on a supported operating system.
AppDNA application migration component of Citrix Virtual Apps and Desktops Premium edition.	1909		
Installing Studio on 32-bit (x86) machines.	1909		Install on a supported x64 operating system.
Support for the Excel hook in seamless applications. This was used for creating separate taskbar icons for each Microsoft Excel 2010 workbook.	1909	1909	

Item	Deprecation announced in	Removed in	Alternative
Core server components on Windows Server 2012 R2 (including Service Packs). Includes: Delivery Controller, Studio and Director.	1906		Install on a newer supported operating system.
Support for Site Configuration, Configuration Logging, and Monitoring databases on Microsoft SQL Server versions 2008 R2, 2012, and 2014 (including all Service Packs and editions).	1906		Install databases on a supported Microsoft SQL Server version.
Support for VDAs on Windows 10 on x86 platforms.	1906	1909*	Install VDAs on a supported x64 operating system. **This feature is still supported in Citrix Virtual Apps and Desktops 7 1912 LTSR**.
Removal of Citrix Smart Tools Agent from Citrix Virtual Apps and Desktops installation media.	1903	1906	

Item	Deprecation announced in	Removed in	Alternative
Removal of Delivery Controller options for the following end-of-life products within StoreFront: VDI-in-a-Box, and XenMobile (9.0 and earlier).	1903	1903	
Support for Linux VDA on Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Install Linux VDA on a later version of Red Hat Enterprise Linux.
StoreFront support for users to access desktops on Desktop Appliance sites	1811	**1912**	Use Desktop Lock for nondomain-joined use cases.
Support for Framehawk display remoting technology	1811	1903	Use Thinwire with adaptive transport enabled.
Support for Citrix Smart Scale in all Citrix Virtual Apps and Desktops (and XenApp and XenDesktop) versions. This functionality will reach End of Life on 31 May 2019.	1808	1906	Consider using the Virtual Apps and Desktops Service on Citrix Cloud for improved power management functionality.
Support for Microsoft .NET Framework versions 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, and 4.7 by Citrix StoreFront, Citrix VDAs, Citrix Studio, Citrix Director, and Citrix Delivery Controller.	7.18	1808	Upgrade to .NET Framework version 4.7.1 or later. (The installer automatically installs .NET Framework 4.7.1 if it is not already installed.)

Item	Deprecation announced in	Removed in	Alternative
Support for Linux VDA on Red Hat Enterprise Linux 7.3.	7.18	1808	Install Linux VDA on a later version of Red Hat Enterprise Linux.
StoreFront support for TLS 1.0, and TLS 1.1 protocols between Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) and Citrix Receiver, and Workspace Hub.	7.17		Upgrade Citrix Receivers to a Citrix Workspace app that supports the TLS 1.2 protocol. For more information on Citrix Workspace app, see https://docs.citrix.com/en-us/citrix-workspace-app.
VDA support for policy setting "Automatic installation of in-box printer drivers".	7.16	7.16	None. Policy setting supported with VDAs on earlier OSs only (Windows 7, Windows Server 2012 R2 and earlier).
Support for the Linux VDA on SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Install Linux VDA on supported SUSE version.
Support for Citrix WDDM driver on VDAs	7.16	7.16	The Citrix WDDM driver is no longer installed with VDAs.
Mobility SDK / Mobile SDK (from the former Citrix Labs)	7.16		Superseded by mobile experience policy settings, and native experiences for hosted desktops/apps.

Item	Deprecation announced in	Removed in	Alternative
VDAs on Windows 10 version 1511 (Threshold 2) and earlier Windows Single-session OS releases, including Windows 8.x and Windows 7 (see https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (and 7.12)	7.16	Install Single-session OS VDAs on Windows 10 minimum version 1607 (Redstone 1) or newer Semi-Annual Channels. If using 1607 LTSB, we recommend a 7.15 VDA. See CTX224843.
VDAs on Windows Server 2008 R2 and Windows Server 2012 (including Service Packs)	7.15 LTSR (and 7.12)	7.16	Install VDAs on a supported operating system.
Desktop Composition Redirection (previously known as DirectX Command Remoting) (DCR)	7.15 LTSR	7.16	Use Thinwire.
Citrix Receiver for Web classic experience (“green bubbles”user interface)	7.15 LTSR (and StoreFront 3.12)	1903	Citrix Receiver for Web unified experience.
Core components on Windows Server 2012 and Windows Server 2008 R2 (including Service Packs). Includes: Delivery Controller, Studio, Director, StoreFront, License Server, and Universal Print Server.	7.15 LTSR	7.18	Install components on a supported operating system.

Item	Deprecation announced in	Removed in	Alternative
Self-Service Password Reset (SSPR) feature on Windows Server 2012 and Windows Server 2008 R2 (including Service Packs)	7.15 LTSR	7.18	Install on a newer supported operating system.
Studio on Windows 7, Windows 8, and Windows 8.1 (including Service Packs)	7.15 LTSR	7.18	Install Studio on a supported operating system.
Flash Redirection	7.15 LTSR	**1912**	Create video content as HTML5 Video. Use HTML5 Video Redirection for managed content, and Browser Content Redirection for public web sites. For more information, see the Flash Redirection End of Life note.
Citrix Online Integration (Goto product) with StoreFront	7.14 (and StoreFront 3.11)	StoreFront 3.12	

Item	Deprecation announced in	Removed in	Alternative
The user account, CtxAppVCOMAdmin, which was created during VDA installation and added to the Local Administrators Group on the VDA machine, is no longer created. The underlying "COM" mechanism is also removed.	7.14	7.14	The Windows service CtxAppVService performs the same function. It is automatically installed and configured and requires no user interaction.
Universal Print Server UpsServer component support on Windows Server 2008 32-bit	7.14	7.14	Install on a newer supported operating system.
StoreFront and Receiver for Web on Internet Explorer 8	7.13	7.13	
VDA command line installation option /no_appv to prevent installation of the Citrix App-V components	7.13	7.13	Use the command line installation option /exclude "Citrix Personalization for App-V –VDA".
The full-product installer no longer installs the Citrix.Common.Commands snap-in on new installations and automatically removes it when upgrading existing installations.	7.13	7.13	Some PowerShell commands that were provided by the Citrix.Common.Commands snap-in are still available in the XenApp 6.5 SDK.
Partial functionality to manipulate icon data that was provided by *-CtxIcon cmdlets.	7.13	7.13	Now provided by *-BrokerIcon cmdlets in the Broker Service.

Item	Deprecation announced in	Removed in	Alternative
Legacy Thinwire mode	7.12	7.16	Use Thinwire. If you are using Legacy Thinwire mode on Windows Server 2008 R2, migrate to Windows Server 2012 R2 or Windows Server 2016, and use Thinwire.
In-place upgrades from StoreFront 2.0, 2.1, 2.5, and 2.5.2	7.13	7.16	Upgrade from one of these versions to a later supported version and then to XenApp and XenDesktop 7.16.
In-place upgrades from XenDesktop 5.6 or 5.6 FP1	7.12	7.16	Migrate your XenDesktop 5.6 or 5.6 FP1 deployment to the current XenDesktop version. To do this, first upgrade to XenDesktop 7.6 LTSR (with the latest CU), then upgrade to the latest Citrix Virtual Desktops (formerly XenDesktop) release or LTSR version.
Installing Delivery Controller, Director, StoreFront, or License Server on 32-bit (x86) machines.	7.12	7.16	Install on a supported x64 operating system.
Connection leasing	7.12	7.16	Use Local Host Cache.

Item	Deprecation announced in	Removed in	Alternative
XenDesktop 5.6 used on Windows XP. VDA installations on Windows XP are not supported.	7.12	7.16	Install VDAs on a supported operating system.
CloudPlatform connections	7.12		Use a different supported hypervisor or cloud service.
Azure Classic (also known as Azure Service Management) connections	7.12		Use Azure Resource Manager.
AppDisks functionality (and the AppDNA integration into Studio, which supports it)*	7.13	2003	Use Citrix App Layering.
Personal vDisk functionality*	7.13	2006	Use Citrix App Layering user layer or user personalization layer technology.

† **Important**: after June 2020, you must remove any SCOM Management Pack from your Citrix Virtual Apps and Desktops 7 1912 LTSR site to keep your LTSR support and benefits.

* Feature not covered by the Long Term Service Releases (LTSR) servicing option.

System requirements

November 10, 2022

Introduction

The system requirements in this document were valid when this product version released. Updates are made periodically. System requirements components not covered here (such as host systems, Citrix Workspace app, and Citrix Provisioning) are described in their respective documentation.

Review the Prepare to install article before beginning an installation.

Unless otherwise noted, the component installer deploys software prerequisites automatically (such as .NET and C++ packages) if the required versions are not detected on the machine. The Citrix installation media also contains some of this prerequisite software.

The installation media contains several third-party components. Before using the Citrix software, check for security updates from the third party, and install them.

For globalization information, see Knowledge Center article CTX119253.

For components and features that can be installed on Windows Servers, Nano Server installations are not supported, unless noted. Server Core is supported only for Delivery Controllers and Director.

Hardware requirements

RAM and disk space values are in addition to requirements for the product image, operating system, and other software on the machine. Your performance varies, depending on your configuration. The configuration includes the features you use, plus the number of users, and other factors. Using only the minimum can result in slow performance.

The following table lists the minimum requirements for core components.

Component	Minimum
All core components on one server, for an evaluation only, not a production deployment	5 GB RAM
All core components on one server, for a test deployment or a small production environment	12 GB RAM
Delivery Controller (more disk space required for Local Host Cache)	5 GB RAM, 800 MB hard disk, database: see Sizing guidance
Studio	1 GB RAM, 100 MB hard disk
Director	2 GB RAM, 200 MB hard disk
StoreFront	2 GB RAM, see the StoreFront documentation for disk recommendations
License Server	2 GB RAM; see the Licensing documentation for disk recommendations

Sizing of VMs that deliver desktops and applications

Specific recommendations cannot be provided because of the complex and dynamic nature of hardware offerings, and every deployment has unique needs. Generally, sizing a Citrix Virtual Apps VM is

based on the hardware and not the user workloads. (An exception is RAM. You need more RAM for applications that consume more.)

For more information:

- Citrix Tech Zone contains guidance on VDA sizing.
- Citrix Virtual Apps and Desktops Single Server Scalability discusses how many users or VMs can be supported on a single physical host.

Microsoft Visual C++ 2017 Runtime

Installing the Microsoft Visual C++ 2017 Runtime on a machine that has the 2015 Runtime installed can result in automatic removal of the 2015 version. This action is as designed.

If you've already installed Citrix components that automatically install the Visual C++ 2015 Runtime, those components continue to operate correctly with the Visual C++ 2017 version.

For more information, see the Microsoft article https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html.

Delivery Controller

Supported operating systems:

- Windows Server 2019, Standard and Datacenter Editions, and with the Server Core option
- Windows Server 2016, Standard and Datacenter Editions, and with the Server Core option
- Windows Server 2012 R2, Standard and Datacenter Editions, and Server Core for Windows Server 2012 R2

Requirements:

- Microsoft .NET Framework 4.7.1 is installed automatically if it (or a later version) is not already installed.
- Windows PowerShell 3.0 or later.
- Microsoft Visual C++ 2017 Runtime, 32-bit and 64-bit.

Databases

Supported Microsoft SQL Server versions for the Site Configuration, Configuration Logging, and Monitoring databases:

- SQL Server 2019, Express, Standard, and Enterprise Editions.
- SQL Server 2017, Express, Standard, and Enterprise Editions.

  - For new installations: By default, SQL Server Express 2017 with Cumulative Update 16 is installed when installing the Controller, if an existing supported SQL Server installation is not detected.
  - For upgrades, any existing SQL Server Express version is not upgraded.

- SQL Server 2016 SP1 through SP3, Express, Standard, and Enterprise Editions.
- SQL Server 2014 SP1 through SP3, Express, Standard, and Enterprise Editions.
- SQL Server 2012 through SP4, Express, Standard, and Enterprise Editions.
- SQL Server 2008 R2 SP2 and SP3, Express, Standard, Enterprise, and Datacenter Editions.

The following database high availability solutions are supported (except for SQL Server Express, which supports only standalone mode):

- SQL Server AlwaysOn Failover Cluster Instances
- SQL Server AlwaysOn Availability Groups (including Basic Availability Groups)
- SQL Server Database Mirroring

Windows authentication is required for connections between the Controller and the SQL Server Site database.

When installing a Controller, Microsoft SQL Server Express LocalDB 2017 with Cumulative Update 16 is installed for use with the Local Host Cache feature. This installation is separate from the default SQL Server Express installation for the site database. (When upgrading a Controller, the existing Microsoft SQL Server Express LocalDB version is not upgraded. If you want to upgrade the LocalDB version, follow the guidance in Database actions.)

For more information, see the following articles:

- Databases
- Knowledge Center article CTX114501 lists the most current supported databases
- Database sizing guidance
- Local Host Cache

Citrix Studio

Supported operating systems:

- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows 10

Requirements:

- Microsoft .NET Framework 4.7.1 is installed automatically if it (or a later version) is not already installed.
- Microsoft Management Console 3.0 (included with all supported operating systems).
- Windows PowerShell 3.0 or later.

Citrix Director

Supported operating systems:

- Windows Server 2019, Standard and Datacenter Editions, and with the Server Core option
- Windows Server 2016, Standard and Datacenter Editions, and with the Server Core option
- Windows Server 2012 R2, Standard and Datacenter Editions, and Server Core for Windows Server 2012 R2

Requirements:

- Microsoft .NET Framework 4.7.1 is installed automatically if it (or a later version) is not already installed.
- Microsoft Internet Information Services (IIS) 7.0 and ASP.NET 2.0. Ensure that the IIS server role has the Static Content role service installed. If this software is not already installed, you are prompted for the Windows Server installation media. Then the software is installed for you.

> Note:
>
> To view the event logs on machines where Citrix Director is installed, you must install Microsoft .NET Framework 2.0.

Citrix User Profile Manager:

- Ensure that the Citrix User Profile Manager and Citrix User Profile Manager WMI Plug-in are installed on the VDA (**Additional Components** page in the installation wizard). The Citrix Profile Management Service must be running to view the user profile details in Director.

System Center Operations Manager (SCOM) integration requirements:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Supported browsers for viewing Director:

- Internet Explorer 11. (You can use Internet Explorer 10 only on Windows Server 2012 R2 machines.) Compatibility mode is not supported for Internet Explorer. Use the recommended browser settings to access Director. When you install Internet Explorer, accept the default to use the recommended security and compatibility settings. If you already installed the browser

and chose not to use the recommended settings, go to **Tools > Internet Options > Advanced > Reset** and follow the instructions.
- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

The recommended optimal screen resolution to view Director is 1366 x 1024.

Virtual Delivery Agent (VDA) for single-session OS

Supported operating systems:

- Windows 10 (x64 only), minimum version 1607.
  - For edition support, see Knowledge Center article CTX224843.
  - For Citrix known issues with version 1709, see Knowledge Center article CTX229052.

Requirements:

- Microsoft .NET Framework 4.7.1 is installed automatically if it (or a later version) is not already installed.
- Microsoft Visual C++ 2017 Runtime, 32-bit and 64-bit.

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 on Windows 10.

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 feature is not installed and does 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 single-session 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. For more information, see Prepare to install.

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

To use the Server VDI feature, you can use the command line interface to install a VDA for Windows single-session OS on a Windows Server 2019 or Windows Server 2016 machine. See Server VDI for guidance.

For information about installing a VDA on a Windows 7 machine, see Earlier operating systems.

Virtual Delivery Agent (VDA) for multi-session OS

Supported operating systems:

- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions

The installer automatically deploys the following requirements, which are also available on the Citrix installation media in the **Support** folders:

- Microsoft .NET Framework 4.7.1 is installed automatically if it (or a later version) is not already installed.
- Microsoft Visual C++ 2017 Runtime, 32-bit and 64-bit.

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled.

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 ware 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. For more information, see Prepare to install.

If Media Foundation is not present on the VDA, these multimedia features do not work:

- Windows Media Redirection
- HTML5 Video Redirection
- HDX RealTime Webcam Redirection

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.

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. Knowledge Center article CTX131239 contains current version information, plus links to known issues.

Some features are not supported on all host platforms or versions. See the feature documentation for details.

The Remote PC Access Wake on LAN feature requires Microsoft System Center Configuration Manager minimum 2012.

- **Amazon Web Services (AWS)**
  - You can provision applications and desktops on supported Single-session and Multi-session Windows operating systems.
  - Citrix supports the Amazon Relational Database Service (RDS). See the Citrix Ready marketplace and Citrix and AWS for additional information.
- **Citrix Hypervisor (formerly XenServer)**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Citrix Hypervisor virtualization environments.
- **CloudPlatform** (deprecated)
- **Microsoft Azure Classic** (deprecated)
- **Microsoft Azure Resource Manager**

  For more information, see Microsoft Azure Resource Manager virtualization 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 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.

Active Directory functional levels

The following functional levels for the Active Directory forest and domain are supported:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

Audio

UDP audio for Multi-Stream ICA is supported on Citrix Workspace app for Windows and Citrix Workspace app for Linux 13.

Echo cancellation is supported on Citrix Workspace app for Windows.

See the specific HDX feature support and requirements. For more information on HDX features and Citrix Workspace apps, see the Feature matrix.

HDX Windows Media delivery

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and real-time Windows Media multimedia transcoding: Citrix Workspace app for Windows, Citrix Workspace app for iOS, and Citrix Workspace app for Linux.

To use Windows Media client-side content fetching on Windows 8 devices, set the Citrix Multimedia Redirector as a default program: in **Control Panel > Programs > Default Programs > Set your default programs**, select **Citrix Multimedia Redirector** and click either **Set this program as default** or **Choose defaults for this program**. GPU transcoding requires an NVIDIA CUDA-enabled GPU with Compute Capability 1.1 or higher; see https://developer.nvidia.com/cuda/cuda-gpus.

HDX 3D Pro

The VDA for Windows single-session OS detects the presence of GPU hardware at runtime.

The physical or virtual machine hosting the application can use GPU Passthrough or Virtual GPU (vGPU):

- GPU Passthrough is available with: Citrix XenServer, Nutanix AHV, VMware vSphere, and VMware ESX, where it is referred to as virtual Direct Graphics Acceleration (vDGA). GPU Passthrough is also available with Microsoft Hyper-V in Windows Server 2016, where it is referred to as Discrete Device Assignment (DDA).

- vGPU is available with Citrix Hypervisor, Nutanix AHV, and VMware vSphere; see https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html. HDX 3D Pro is also supported with Cloud instances on the Microsoft Azure NV-series and Amazon {AWS} EC2 G3 offerings.

Citrix recommends that the host computer has at least 4 GB of RAM and four virtual CPUs with a clock speed of 2.3 GHz or higher.

Graphical Processing Unit (GPU):

- For CPU-based compression (including lossless compression), HDX 3D Pro supports any display adapter on the host computer that is compatible with the application being delivered.
- For virtualized graphics acceleration using the NVIDIA GRID API, HDX 3D Pro can be used with supported NVIDIA GRID cards (see NVIDIA GRID). The NVIDIA GRID delivers a high frame rate, resulting in a highly interactive user experience.
- Virtualized graphics acceleration is supported on the Intel Xeon Processor E3 Family of data center graphics platform. For more information, see https://www.citrix.com/intel and https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Virtualized graphics acceleration is supported with AMD RapidFire on the AMD FirePro S-series server cards. See AMD Virtualization Solution).

User device:

- HDX 3D Pro supports all monitor resolutions that the GPU supports on the host computer. For optimum performance with the minimum recommended user device and GPU specifications, Citrix recommends a maximum resolution of 1920 x 1200 pixels for LAN connections, and 1280 x 1024 pixels for WAN connections.
- Citrix recommends that user devices have at least 1 GB of RAM and a CPU with a clock speed of 1.6 GHz or higher. Use of the default deep compression codec, which is required on low-bandwidth connections, requires a more powerful CPU unless the decoding is done in hardware. For optimum performance, Citrix recommends that user devices have at least 2 GB of RAM and a dual-core CPU with a clock speed of 3 GHz or higher.
- For multi-monitor access, Citrix recommends user devices with quad-core CPUs.
- User devices do not need a GPU to access desktops or applications delivered with HDX 3D Pro.
- Citrix Workspace app must be installed.

For more information, see the HDX 3D Pro articles and www.citrix.com/xenapp/3d.

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
- Windows Server 2012 R2

Requirements:

- Microsoft Visual C++ 2017 Runtimes, x86 and x64
- Microsoft .NET Framework 4.7.1 (minimum)

For VDAs for Multi-session OS, 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.

Other

Only Citrix License Server 11.16 and later is supported. For more information, see Licensing.

When using Citrix Provisioning (formerly Provisioning Services) with this release, version 7.x is covered by the XenApp 7.x/XenDesktop 7.x lifecycle and the Citrix Virtual Apps and Desktops lifecycle. See the Product Matrix for more information about version compatibility.

For supported StoreFront versions, see the StoreFront system requirements.

The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the Site Configuration database. If you install `CitrixGroupPolicyManagement_x64.msi` separately (for example, on a machine that does not have a Citrix Virtual Apps and Desktops core component installed), that machine must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.

If you want to edit domain GPOs using GPMC, enable the Group Policy Management feature (in the Windows Server Manager) on all machines containing Delivery Controllers.

Multiple NICs are supported.

By default, the Citrix Workspace app for Windows is not installed when you install a current VDA. For more information, see the Citrix Workspace app for Windows documentation.

See App-V for supported versions of Microsoft App-V.

See Local App Access for supported browser information for that feature.

Mixed DPIs with multi-monitors. The use of different DPIs between monitors is not supported in Citrix Virtual Apps and Desktops environments. You can verify the DPI (% scaling) using the **Windows Control Panel > Display** options. If using a Windows 8.1 or Windows 10 client device, enabling the **Let**

me choose one scaling level for all my displays option in the **Windows Control Panel > Display** options configures the monitors appropriately. For more information, see CTX201696.

This version of Citrix Virtual Apps and Desktops is not compatible with AppDNA 7.8 and AppDNA 7.9. Citrix recommends using the current AppDNA release.

Technical overview

April 23, 2024

Citrix Virtual Apps and Desktops are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

Citrix Virtual Apps and Desktops allow:

- End users to run applications and desktops independently of the device's operating system and interface.
- Administrators to manage the network and control access from selected devices or from all devices.
- Administrators to manage an entire network from a single data center.

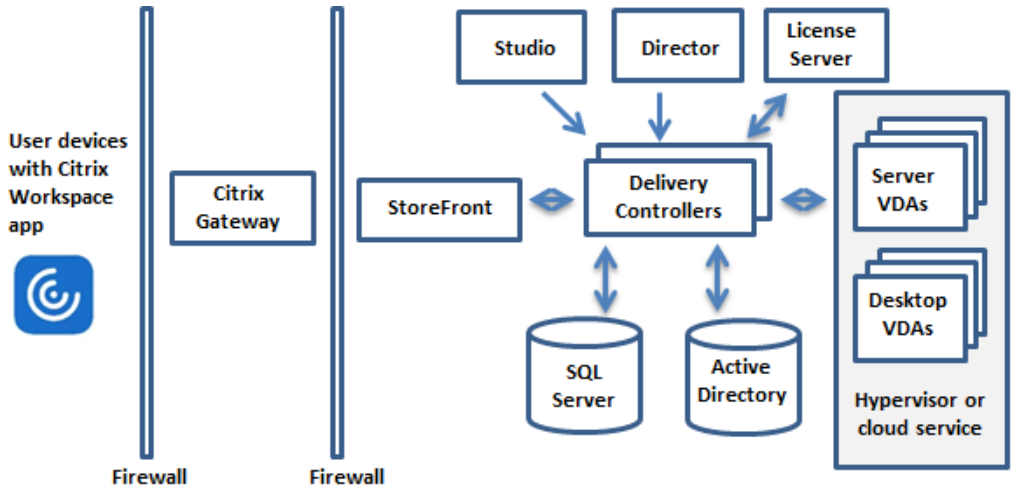
Citrix Virtual Apps and Desktops share a unified architecture called FlexCast Management Architecture (FMA). FMA's key features are the ability to run multiple versions of Citrix Virtual Apps or Citrix Virtual Desktops from a single Site and integrated provisioning.

Learn about product name changes.

Key components

This article is most helpful if you're new to Citrix Virtual Apps and Desktops. If you currently have a 6.x or earlier XenApp farm, or a XenDesktop 5.6 or earlier site, see Changes in 7.x, too.

This illustration shows the key components in a typical deployment, which is called a Site.



Delivery Controller

The Delivery Controller is the central management component of a Site. Each Site has one or more Delivery Controllers. It is installed on at least one server in the data center. For Site reliability and availability, Controllers should be installed on more than one server. If your deployment includes a hypervisor or cloud service, the Controller services communicate with it to distribute applications and desktops, authenticate and manage user access, broker connections between users and their desktops and applications, optimize use connections, and load-balance these connections.

The Controller's Broker Service tracks which users are logged on and where, what session resources the users have, and if users need to reconnect to existing applications. The Broker Service executes PowerShell cmdlets and communicates with a broker agent on the VDAs over TCP port 80. It does not have the option to use TCP port 443.

The Monitor Service collects historical data and places it in the Monitor database. This service uses TCP port 80 or 443.

Data from the Controller services is stored in the Site database.

The Controller manages the state of desktops, starting and stopping them based on demand and administrative configuration. In some editions, the Controller allows you to install Profile Management to manage user personalization settings in virtualized or physical Windows environments.

Database

At least one Microsoft SQL Server database is required for every Site to store configuration and session information. This database stores the data collected and managed by the services that make up the Controller. Install the database within your data center, and ensure it has a persistent connection to the Controller.

The Site also uses a Configuration Logging database and a Monitoring database. By default, those databases are installed in the same location as the Site database, but you can change this.

Virtual Delivery Agent (VDA)

The VDA is installed on each physical or virtual machine in your Site that you make available to users. Those machines deliver applications or desktops. The VDA enables the machine to register with the Controller, which in turn allows the machine and the resources it is hosting to be made available to users. VDAs establish and manage the connection between the machine and the user device. VDAs also verify that a Citrix license is available for the user or session, and apply policies that are configured for the session.

The VDA communicates session information to the Broker Service in the Controller through the broker agent in the VDA. The broker agent hosts multiple plugins and collects real-time data. It communicates with the Controller over TCP port 80.

The word "VDA"is often used to refer to the agent as well as the machine on which it is installed.

VDAs are available for Single-session and Multi-session Windows operating systems. VDAs for Multi-session Windows operating systems allow multiple users to connect to the server at one time. VDAs for Single-session Windows operating systems allow only one user to connect to the desktop at a time. Linux VDAs are also available.

Citrix StoreFront

StoreFront authenticates users and manages stores of desktops and applications that users access. It can host your enterprise application store, which gives users self-service access to the desktops and applications that you make available to them. It also keeps track of users'application subscriptions, shortcut names, and other data. This helps ensure that users have a consistent experience across multiple devices.

Citrix Workspace app

Installed on user devices and other endpoints (such as virtual desktops), Citrix Workspace app provides users with quick, secure, self-service access to documents, applications, and desktops. Citrix Workspace app provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications. For devices that cannot install the device-specific Citrix Workspace app software, Citrix Workspace app for HTML5 provides a connection through an HTML5-compatible web browser.

Citrix Studio

Studio is the management console where you configure and manage your Citrix Virtual Apps and Desktops deployment. Studio eliminates the need for separate management consoles for managing delivery of applications and desktops. Studio provides wizards to guide you through environment setup, creating workloads to host applications and desktops, and assigning applications and desktops to users. You can also use Studio to allocate and track Citrix licenses for your Site.

Studio gets the information it displays from the Broker Service in the Controller, communicating over TCP port 80.

Citrix Director

Director is a web-based tool that enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become system-critical, and perform support tasks for end users. You can use one Director deployment to connect to and monitor multiple Citrix Virtual Apps or Citrix Virtual Desktops Sites.

Director displays:

- Real-time session data from the Broker Service in the Controller, which includes data the Broker Service gets from the broker agent in the VDA.
- Historical Site data from the Monitor Service in the Controller.

Director uses the ICA performance and heuristics data captured by the Citrix Gateway device to build analytics from the data and then presents it to the administrators.

You can also view and interact with a user's sessions through Director, using Windows Remote Assistance.

Citrix License Server

The License Server manages your Citrix product licenses. It communicates with the Controller to manage licensing for each user's session and with Studio to allocate license files. A Site must have at least one license server to store and manage your license files.

Hypervisor or cloud service

The hypervisor or cloud service hosts the virtual machines in your Site. These can be the VMs you use to host applications and desktops, as well as VMs you use to host the Citrix Virtual Apps and Desktops components. A hypervisor is installed on a host computer dedicated entirely to running the hypervisor and hosting virtual machines.

Citrix Virtual Apps and Desktops support various hypervisors and cloud services.

Although many deployments require a hypervisor, you don't need one to provide Remote PC Access. A hypervisor is also not required when you are using Provisioning Services (PVS) to provision VMs.

For more information, see:

- Network ports.
- Databases.
- Windows services in Citrix Virtual Apps and Desktops components: Configure user rights.
- Supported hypervisors and cloud services: System requirements.

Additional components

The following additional components, not shown in the illustration above, can also be included in Citrix Virtual Apps and Desktops deployments. For more information, see their documentation.

Citrix Provisioning

Citrix Provisioning (formerly Provisioning Services) is an optional component that is available with some editions. It provides an alternative to MCS for provisioning virtual machines. Whereas MCS creates copies of a master image, PVS streams the master image to user devices. PVS doesn't require a hypervisor to do this, so you can use it to host physical machines. PVS communicates with the Controller to provide users with resources.

Citrix Gateway

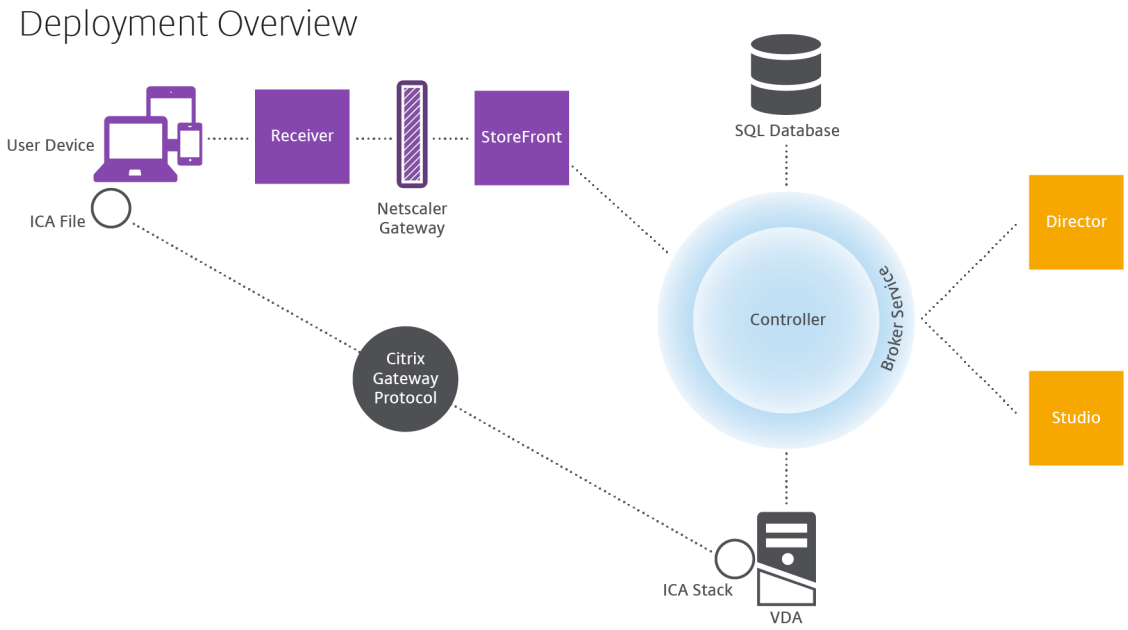
When users connect from outside the corporate firewall, Citrix Virtual Apps and Desktops can use Citrix Gateway (formerly Access Gateway and NetScaler Gateway) technology to secure these connections with TLS. The Citrix Gateway or VPX virtual appliance is an SSL VPN appliance that is deployed in the demilitarized zone (DMZ). It provides a single secure point of access through the corporate firewall.

Citrix SD-WAN

In deployments where virtual desktops are delivered to users at remote locations such as branch offices, Citrix SD-WAN technology can be employed to optimize performance. Repeaters accelerate performance across wide-area networks. With repeaters in the network, users in the branch office experience LAN-like performance over the WAN. Citrix SD-WAN can prioritize different parts of the user experience so that, for example, the user experience does not degrade in the branch location when a large file or print job is sent over the network. HDX WAN optimization provides tokenized compression and data deduplication, dramatically reducing bandwidth requirements and improving performance.

How typical deployments work

A Site is made up of machines with dedicated roles that allow for scalability, high availability, and failover, and provide a solution that is secure by design. A Site consists of VDA-installed servers and desktop machines, and the Delivery Controller, which manages access.



The VDA enables users to connect to desktops and applications. It is installed on server or desktop machines in the data center for most delivery methods, but it can also be installed on physical PCs for Remote PC Access.

The Controller is made up of independent Windows services that manage resources, applications, and desktops, and optimize and balance user connections. Each Site has one or more Controllers. Because sessions are affected by latency, bandwidth, and network reliability, all Controllers ideally should be on the same LAN.

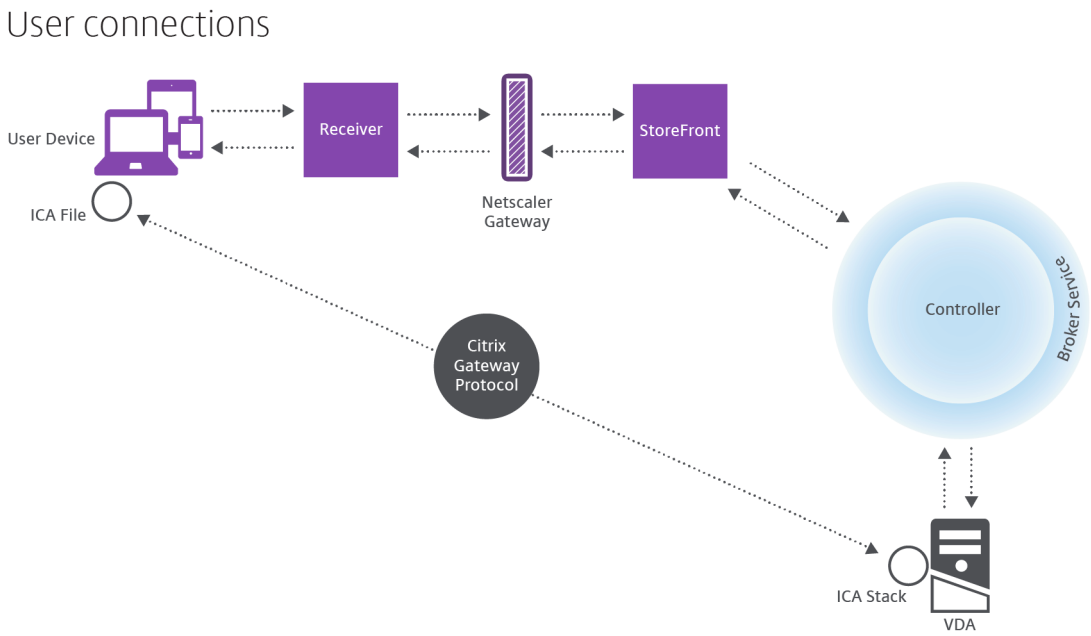
Users never directly access the Controller. The VDA serves as an intermediary between users and the Controller. When users log on using StoreFront, their credentials pass through to the Broker Service on the Controller. The Broker Service then obtains profiles and available resources based on the policies set for them.

How user connections are handled

To start a session, the user connects either through Citrix Workspace app installed on the user's device, or a StoreFront Web site.

The user selects the physical or virtual desktop or virtual application that is needed.

The user's credentials move through this pathway to access the Controller, which determines which resources are needed by communicating with a Broker Service. Citrix recommends that administrators place an SSL certificate on StoreFront to encrypt the credentials coming from Citrix Workspace app.



The Broker Service determines which desktops and applications the user is allowed to access.

After the credentials are verified, information about available applications or desktops is sent back to the user through the StoreFront-Citrix Workspace app pathway. When the user selects applications or desktops from this list, that information goes back down the pathway to the Controller. The Controller then determines the proper VDA to host the specific applications or desktop.

The Controller sends a message to the VDA with the user's credentials, and then sends all the data about the user and the connection to the VDA. The VDA accepts the connection and sends the information back through the same pathways to Citrix Workspace app. A set of required parameters is collected on StoreFront. These parameters are then sent to Citrix Workspace app either as part of the Citrix-Workspace-app-StoreFront protocol conversation, or converted to an Independent Computing Architecture (ICA) file and downloaded. As long as the Site was properly set up, the credentials remain encrypted throughout this process.

The ICA file is copied to the user's device and establishes a direct connection between the device and the ICA stack running on the VDA. This connection bypasses the management infrastructure (Citrix Workspace app, StoreFront, and Controller).

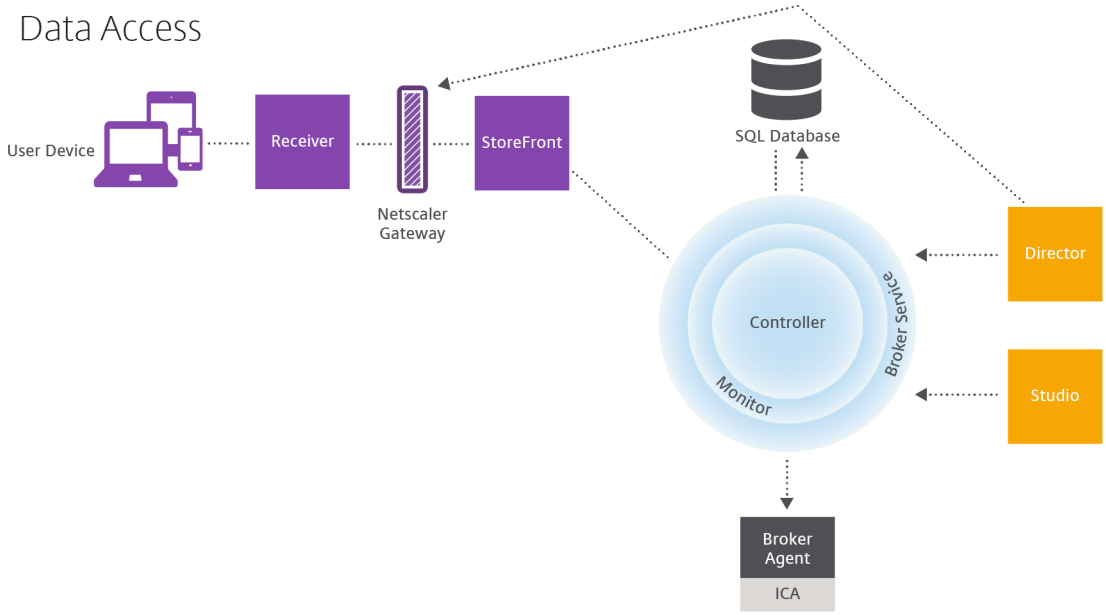
The connection between Citrix Workspace app and the VDA uses the Citrix Gateway Protocol (CGP). If a connection is lost, the Session Reliability feature enables the user to reconnect to the VDA rather than having to relaunch through the management infrastructure. Session Reliability can be enabled

or disabled in Citrix policies.

After the client connects to the VDA, the VDA notifies the Controller that the user is logged on. The Controller then sends this information to the Site database and starts logging data in the monitoring database.

How data access works

Every Citrix Virtual Apps and Desktops session produces data that IT can access through Studio or Director. Using Studio, administrators can access real-time data from the Broker Agent to manage sites. Director accesses the same data plus historical data stored in the Monitoring database. It also accesses HDX data from NetScaler Gateway for help desk support and troubleshooting.



Within the Controller, the Broker Service reports session data for every session on the machine providing real-time data. The Monitor Service also tracks the real-time data and stores it as historical data in the Monitoring database.

Studio communicates only with the Broker Service; it accesses only real-time data. Director communicates with the Broker Service (through a plugin in the Broker Agent) to access the Site database.

Director can also access Citrix Gateway to get information on the HDX data.

Deliver desktops and applications

You set up the machines that will deliver applications and desktops with machine catalogs. Then, you create Delivery Groups that specify the applications and desktops that will be available (using

machines in the catalogs), and which users can access them. Optionally, you can then create Application Groups to manage collections of applications.

Machine catalogs

Machine catalogs are collections of virtual or physical machines that you manage as a single entity. These machines, and the application or virtual desktops on them, are the resources you provide to your users. All the machines in a catalog have the same operating system and the same VDA installed. They also have the same applications or virtual desktops.

Typically, you create a master image and use it to create identical VMs in the catalog. For VMs you can specify the provisioning method for the machines in that catalog: Citrix tools (Citrix Provisioning or MCS) or other tools. Alternatively, you can use your own existing images. In that case, you must manage target devices on an individual basis or collectively using third-party electronic software distribution (ESD) tools.

Valid machine types are:

- **Multi-session OS:** Virtual or physical machines with a multi-session operating system. Used for delivering Citrix Virtual Apps published apps (also known as server-based hosted applications) and Citrix Virtual Apps published desktops (also known as server-hosted desktops). These machines allow multiple users to connect to them at one time.
- **Single-session OS:** Virtual or physical machines with a single-session operating system. Used for delivering VDI desktops (desktops running single-session OSs that can optionally be personalized), VM-hosted apps (applications from single-session OSs), and hosted physical desktops. Only one user at a time can connect to each of these desktops.
- **Remote PC Access:** Enables remote users to access their physical office PCs from any device running Citrix Workspace app. The office PCs are managed through the Citrix Virtual Desktops deployment, and require user devices to be specified in a whitelist.

For more information, see Citrix Virtual Apps and Desktops Image Management and Create machine catalogs.

Delivery Groups

Delivery Groups specify which users can access which applications and/or desktops on which machines. Delivery Groups contain machines from your machine catalogs, and Active Directory users who have access to your Site. You might assign users to your Delivery Groups by their Active Directory group, because Active Directory groups and Delivery Groups are ways to group users with similar requirements.

Each Delivery Group can contain machines from more than one catalog, and each catalog can contribute machines to more than one Delivery Group. However, each individual machine can only belong to one Delivery Group at a time.

You define which resources users in the Delivery Group can access. For example, to deliver different applications to different users, you might install all of the applications on the master image for one catalog and create enough machines in that catalog to distribute among several Delivery Groups. You can then configure each Delivery Group to deliver a different subset of applications that are installed on the machines.

For more information, see Create Delivery Groups.

Application Groups

Application Groups provide application management and resource control advantages over using more Delivery Groups. Using the tag restriction feature, you can use your existing machines for more than one publishing task, saving the costs associated with deployment and managing additional machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a Delivery Group. Application Groups can also be helpful when isolating and troubleshooting a subset of machines in a Delivery Group.

For more information, see Create Application Groups.

More information

Citrix Virtual Apps and Desktops diagrams

Active Directory

October 6, 2022

Active Directory is required for authentication and authorization. The Kerberos infrastructure in Active Directory is used to guarantee the authenticity and confidentiality of communications with the Delivery Controllers. For information about Kerberos, see the Microsoft documentation.

The System requirements article lists the supported functional levels for the forest and domain.

This product supports:

- **Deployments in which the user accounts and computer accounts exist in domains in a single Active Directory forest.** User and computer accounts can exist in arbitrary domains within

a single forest. All domain functional levels and forest functional levels are supported in this type of deployment.

- **Deployments in which user accounts exist in an Active Directory forest that is different from the Active Directory forest containing the computer accounts of the controllers and virtual desktops.** In this type of deployment, the domains containing the Controller and virtual desktop computer accounts must trust the domains containing user accounts. Forest trusts or external trusts can be used. All domain functional levels and forest functional levels are supported in this type of deployment.
- **Deployments in which the computer accounts for Controllers exist in an Active Directory forest that is different from one or more additional Active Directory forests that contain the computer accounts of the virtual desktops.** In this type of deployment a bi-directional trust must exist between the domains containing the Controller computer accounts and all domains containing the virtual desktop computer accounts. In this type of deployment, all domains containing Controller or virtual desktop computer accounts must be at "Windows 2000 native"functional level or higher. All forest functional levels are supported.
- **Writable domain controllers.** Read-only domain controllers are not supported.

Optionally, Virtual Delivery Agents (VDAs) can use information published in Active Directory to determine which Controllers they can register with (discovery). This method is supported primarily for backward compatibility, and is available only if the VDAs are in the same Active Directory forest as the Controllers. For information about this discovery method see Active Directory OU-based discovery and CTX118976.

> **Note:**
>
> Do not change the computer name or the domain membership of a Delivery Controller after the site is configured.

Deploy in a multiple Active Directory forest environment

This information applies to minimum version XenDesktop 7.1 and XenApp 7.5. It does not apply to earlier versions of XenDesktop or XenApp.

In an Active Directory environment with multiple forests, if one-way or two-way trusts are in place you can use DNS forwarders or conditional forwarders for name lookup and registration. To allow the appropriate Active Directory users to create computer accounts, use the Delegation of Control wizard. See the Microsoft documentation for details about this wizard.

No reverse DNS zones are necessary in the DNS infrastructure if appropriate DNS forwarders are in place between forests.

The `SupportMultipleForest` key is necessary if the VDA and Controller are in separate forests,

regardless of whether the Active Directory and NetBIOS names are different. Use the following information to add the registry key:

> **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. Back up the registry before you edit it.

On the VDA, configure : `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`

- Name: `SupportMultipleForest`
- Type: `REG_DWORD`
- Data: `0x00000001 (1)`

On all Delivery Controllers, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Name: `SupportMultipleForest`
- Type: `REG_DWORD`
- Data: `0x00000001 (1)`

You might need reverse DNS configuration if your DNS namespace is different than that of Active Directory.

If external trusts are in place during setup, the ListOfSIDs registry key is required. The ListOfSIDs registry key is also necessary if the Active Directory FQDN is different than the DNS FQDN, or if the domain containing the Domain Controller has a different NetBIOS name than the Active Directory FQDN. To add the registry key, use the following information:

For the VDA, locate the registry key `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`

- Name: `ListOfSIDs`
- Type: `REG\\_SZ`
- Data: Security Identifier (SID) of the Controllers. (SIDs are included in the results of the `Get-BrokerController` cmdlet.)

When external trusts are in place, make the following change on the VDA:

1. Locate the file `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`.
2. Make a backup copy of the file.

3. Open the file in a text editing program such as Notepad.
4. Locate the `text allowNtlm="false"` and change the text to `allowNtlm="true"`.
5. Save the file.

After adding the `ListOfSIDs` registry key and editing the brokeragent.exe.config file, restart the Citrix Desktop Service to apply the changes.

The following table lists the supported trust types:

Trust type	Transitivity	Direction	Supported in this release
Parent and child	Transitive	Two-way	Yes
Tree-root	Transitive	Two-way	Yes
External	Nontransitive	One-way or two-way	Yes
Forest	Transitive	One-way or two-way	Yes
Shortcut	Transitive	One-way or two-way	Yes
Realm	Transitive or nontransitive	One-way or two-way	No

For more information about complex Active Directory environments, see CTX134971.

Databases

November 10, 2022

A Citrix Virtual Apps or Citrix Virtual Desktops site uses three SQL Server databases:

- **Site:** (also known as Site Configuration) stores the running site configuration, plus the current session state and connection information.
- **Configuration Logging:** (also known as Logging) stores information about site configuration changes and administrative activities. This database is used when the Configuring Logging feature is enabled (default = enabled).
- **Monitoring:** stores data used by Director, such as session and connection information.

Each Delivery Controller communicates with the Site database. Windows authentication is required between the Controller and the databases. A Controller can be unplugged or turned off without affecting other Controllers in the site. This means, however, that the Site database forms a single point of failure. If the database server fails, existing connections continue to function until a user either

logs off or disconnects. For information about connection behavior when the Site database becomes unavailable, see Local Host Cache.

Citrix recommends that you back up the databases regularly so that you can restore from the backup if the database server fails. The backup strategy for each database may differ. For instructions, see CTX135207.

If your site contains more than one zone, the primary zone should always contain the Site database. Controllers in every zone communicate with that database.

High availability

There are several high availability solutions to consider for ensuring automatic failover:

- **AlwaysOn Availability Groups (including Basic Availability Groups):** This enterprise-level high availability and disaster recovery solution introduced in SQL Server 2012 enables you to maximize availability for one or more databases. AlwaysOn Availability Groups requires that the SQL Server instances reside on Windows Server Failover Clustering (WSFC) nodes. For more information, see https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?redirectedfrom=MSDN&view=sql-server-ver15.
- **SQL Server database mirroring:** Mirroring the database ensures that, if you lose the active database server, an automatic failover process happens in a matter of seconds, so that users are generally unaffected. This method is more expensive than other solutions because full SQL Server licenses are required on each database server; you cannot use SQL Server Express edition in a mirrored environment.
- **SQL clustering:** The Microsoft SQL clustering technology can be used to automatically allow one server to take over the tasks and responsibilities of another server that has failed. However, setting up this solution is more complicated, and the automatic failover process is typically slower than alternatives such as SQL mirroring.
- **Using the hypervisor's high availability features:** With this method, you deploy the database as a virtual machine and use your hypervisor's high availability features. This solution is less expensive than mirroring because it uses your existing hypervisor software and you can also use SQL Server Express edition. However, the automatic failover process is slower, as it can take time for a new machine to start for the database, which may interrupt the service to users.

The Local Host Cache feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to applications and desktops even when the Site database is not available. For more information, see Local Host Cache.

If all Controllers in a site fail, you can configure the VDAs to operate in high availability mode so that users can continue to access and use their desktops and applications. In high availability mode, the

VDA accepts direct ICA connections from users, rather than connections brokered by the Controller. Use this feature only on the rare occasion when communication with all Controllers fails; it is not an alternative to other high availability solutions. For more information, see CTX 127564.

Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

Install database software

By default, SQL Server Express edition is installed when you install the first Delivery Controller if another SQL Server instance is not detected on that server. That default action is generally sufficient for proof of concept or pilot deployments. However, SQL Server Express does not support Microsoft high availability features.

The default installation uses the default Windows service accounts and permissions. See the Microsoft documentation for details of these defaults, including the addition of Windows service accounts to the sysadmin role. The Controller uses the Network Service account in this configuration. The Controller does not require any additional SQL Server roles or permissions.

If necessary, you can select **Hide instance** for the database instance. When configuring the address of the database in Studio, enter the instance's static port number, rather than its name. See the Microsoft documentation for details about hiding an instance of SQL Server Database Engine.

Most production deployments, and any deployment that uses Microsoft high availability features, should use supported non-Express editions of SQL Server installed on machines other than the server where the first Controller is installed. The System requirements article lists the supported SQL Server versions. The databases can reside on one or more machines.

Ensure the SQL Server software is installed before creating a site. You don't have to create the database, but if you do, it must be empty. Configuring Microsoft high availability technologies is also recommended.

Use Windows Update to keep SQL Server up-to-date.

Set up the databases from the site creation wizard

Specify the database names and addresses (location) on the **Databases** page in the site creation wizard. (See Database address formats.) To avoid potential errors when Director queries the Monitor Service, do not use whitespace in the name of the Monitoring database.

The **Databases** page offers two options for setting up the databases: automatic and using scripts. Generally, you can use the automatic option if you (the Studio user and Citrix administrator) have the required database privileges. (See Permissions required to set up databases.)

You can change the location of the Configuration Logging and Monitoring database later, after you create the site. See Change database locations.

To configure a site to use a mirror database, complete the following and then proceed with the automatic or scripted setup procedures.

1. Install the SQL Server software on two servers, A and B.
2. On Server A, create the database intended to be used as the principal. Back up the database on Server A and then copy it to server B.
3. On Server B, restore the backup file.
4. Start mirroring on server A.

To verify mirroring after creating the site, run the PowerShell cmdlet `get-configdbconnection` to ensure that the Failover Partner has been set in the connection string to the mirror.

If you later add, move, or remove a Delivery Controller in a mirrored database environment, see Delivery Controllers.

Automatic setup

If you have the required database privileges, select the "Create and set up databases from Studio" option on the **Databases** page of the site creation wizard, and then provide the names and addresses of the principal databases.

If a database exists at an address you specify, it must be empty. If databases don't exist at a specified address, you are informed that a database cannot be found, and then asked if you want the database to be created for you. When you confirm that action, Studio automatically creates the databases, and then applies the initialization scripts for the principal and replica databases.

Scripted setup

If you do not have the required database privileges, someone with those permissions must help, such as a database administrator. Here's the sequence:

1. In the site creation wizard, select the **Generate scripts** option. This action generates six scripts: two for each of the three databases (one for each principal database and another for each replica). You can indicate where to store the scripts.
2. Give those scripts to your database administrator. The site creation wizard stops automatically at this point; you'll be prompted when you return later to continue the site creation.

The database administrator then creates the databases. Each database must have the following characteristics:

- Use a collation that ends with "_CI_AS_KS". Citrix recommends using a collation that ends with "_100_CI_AS_KS".

- For optimum performance, enable the SQL Server Read-Committed Snapshot. For details, see CTX 137161.
- Configured high availability features, if desired.
- To configure mirroring, first set the database to use the full recovery model (simple model is the default). Back up the principal database to a file and copy it to the mirror server. On the mirror database, restore the backup file to the mirror server. Then, start mirroring on the principal server.

The database administrator uses the SQLCMD command-line utility or SQL Server Management Studio in SQLCMD mode to run each of the xxx_Replica.sql scripts on the high availability SQL Server database instances (if high availability is configured), and then run each of the xxx_Principal.sql scripts on the principal SQL Server database instances. See the Microsoft documentation for SQLCMD details.

When all the scripts complete successfully, the database administrator gives the Citrix administrator the three principal database addresses.

In Studio, you are prompted to continue the site creation, and are returned to the **Databases** page. Enter the addresses. If any of the servers hosting a database cannot be contacted, an error message is displayed.

Permissions required to set up databases

You must be a local administrator and a domain user to create and initialize the databases (or change the database location). You must also have certain SQL Server permissions. The following permissions can be explicitly configured or acquired by Active Directory group membership. If your Studio user credentials do not include these permissions, you are prompted for SQL Server user credentials.

Operation	Purpose	Server role	Database role
Create a database	Create a suitable empty database	dbcreator	
Create a schema	Create all service-specific schemas and add the first Controller to the site	securityadmin*	db_owner
Add a Controller	Add a Controller (other than the first) to the site	securityadmin*	db_owner

Operation	Purpose	Server role	Database role
Add a Controller (mirror server)	Add a Controller login to the database server currently in the mirror role of a mirrored database	securityadmin*	
Remove Controller	Remove controller from site	**	db_owner
Update a schema	Apply schema updates or hotfixes		db_owner

* While technically more restrictive, in practice, the securityadmin server role should be treated as equivalent to the sysadmin server role.

** When a controller is removed from a site, either directly through Desktop Studio, or using the scripts generated by Desktop Studio or SDK, the controller logon to the database server is not removed. This is to avoid potentially removing a logon being used by non-XenDesktop services on the same machine. The logon must be removed manually if it is no longer required; this requires securityadmin server role membership.

When using Studio to perform these operations, the user account must be a member of the sysadmin server role.

Preferred database rights scripts

In enterprise environments, database setup includes scripts that must be handled by different teams with different roles (rights): `securityadmin` or `db_owner`.

Using PowerShell, you can now specify the preferred database rights. (This feature is not available in Studio, which supports only a single script containing all tasks.)

Specifying a nondefault value results in separate scripts being created. One script contains tasks that need the `securityadmin` role. The other script requires only `db_owner` rights, and can be run by a Citrix administrator without having to contact a database administrator.

In the `get-*DBSchema` cmdlets, the `-DatabaseRights` option has the following valid values:

- `SA`: Generates a script that creates the databases and the Delivery Controller login. These tasks require `securityadmin` rights.
- `DBO`: Generates a script that creates the user roles in the database, adds the logins, and then creates the database schemas. These tasks require `db_owner` rights.
- `Mixed`: (Default) All tasks in one script, regardless of required rights.

For more information, see the cmdlet help.

Database address formats

You can specify a database address in one of the following forms:

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

For an AlwaysOn Availability Group, specify the group's listener in the location field.

Change database locations

After you create a site, you can change the location of the Configuration Logging and Monitoring databases. (You cannot change the location of the Site database.) When you change the location of a database:

- The data in the previous database is not imported to the new database.
- Logs cannot be aggregated from both databases when retrieving logs.
- The first log entry in the new database indicates that a database change occurred, but it does not identify the previous database.

You cannot change the location of the Configuration Logging database when mandatory logging is enabled.

To change the location of a database:

1. Ensure a supported version of Microsoft SQL Server is installed on the server where you want the database to reside. Set up high availability features as needed.
2. Select **Configuration** in the Studio navigation pane.
3. Select the database for which you want to specify a new location and then select **Change Database** in the **Actions** pane.
4. Specify the new location and the database name.
5. If you want Studio to create the database and you have the appropriate permissions, click **OK**. When prompted, click **OK**, and then Studio creates the database automatically. Studio attempts to access the database using your credentials. If that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. The credentials are retained only for the database creation time frame.
6. If you do not want Studio to create the database, or you do not have sufficient permissions, click **Generate script**. The generated scripts include instructions for manually creating the database and a mirror database, if needed. Before uploading the schema, ensure that the database is empty and that at least one user has permission to access and change the database.

More information

- Database sizing tool.
- Sizing the Site database and configuring connection strings when using SQL Server high availability solutions.

Delivery methods

July 24, 2020

Citrix Virtual Apps and Desktops offers various delivery methods. A single delivery method will likely not meet all of your requirements.

Introduction

Choosing the appropriate application delivery 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 and isolated from the base operating system and each other. This isolation 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 (VDA, Citrix Provisioning agent) 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. For details, 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.

- **Remote PC Access:** Remote PC Access enables employees to remotely access their physical office PCs. When users 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 details, see Remote PC Access.

For desktops, consider published desktops or VDI desktops.

Citrix Virtual Apps published apps and desktops

Use multi-session OS machines to deliver Citrix Virtual Apps and Desktops 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. This provides 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.
- 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 same machine, that single machine is now using 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 master image are securely managed, hosted, and run on machines within your data center, providing a more cost-effective application delivery solution.
- On 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' data.

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, a single user can use multiple applications (and is not limited to a single application) because the operating system sees each application as a new session.
- Within a delivery group, when users log on they 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 Apps and 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 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 master 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 master image.) After the first use,

each time a user logs on to use a desktop, 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.

Network ports

February 6, 2020

The following tables list the default network ports used by Delivery Controllers, Windows VDAs, Director, and Citrix License Server. When Citrix components are installed, the operating system's host firewall is also updated, by default, to match these default network ports.

For an overview of communication ports used in other Citrix technologies and components, see CTX101810.

You may need this port information:

- For regulatory compliance purposes.
- If there is a network firewall between these components and other Citrix products or components, so you can configure that firewall appropriately.
- If you use a third-party host firewall, such as one provided with an anti-malware package, rather than the operating system's host firewall.
- If you alter the configuration of the host firewall on these components (usually Windows Firewall Service).
- If you reconfigure any features of these components to use a different port or port range, and then want to disable or block ports that are not used in your configuration. Refer to the documentation for the component for details.
- For port information about other components such as StoreFront and Citrix Provisioning (formerly Provisioning Services), see the component's current "System requirements"article.

The tables list only incoming ports. Outgoing ports are usually determined by the operating system and use unrelated numbers. Information for outgoing ports is not normally needed for the purposes listed above.

Some of these ports are registered with the Internet Assigned Numbers Authority (IANA). Details about these assignments are available at http://www.iana.org/assignments/port-numbers. However, the descriptive information held by IANA does not always reflect today's usage.

Additionally, the operating system on the VDA and Delivery Controller require incoming ports for its own use. See the Microsoft Windows documentation for details.

VDA, Delivery Controller, and Director

Component	Usage	Protocol	Default incoming port	Notes
VDA	ICA/HDX	TCP, UDP	1494	EDT protocol requires 1494 to be open for UDP. See ICA policy settings.
VDA	ICA/HDX with Session Reliability	TCP, UDP	2598	EDT protocol requires 2598 to be open for UDP. If multi-stream and multi-port are enabled, the administrator defines the port numbers for the additional three streams. See ICA policy settings.
VDA	ICA/HDX over TLS/DTLS	TCP, UDP	443	All Citrix Workspace apps
VDA	ICA/HDX over WebSocket	TCP	8008	Citrix Workspace app for HTML5, and Citrix Workspace app for Chrome 1.6 and earlier only
VDA	ICA/HDX audio over UDP Real-time Transport	UDP	16500..16509	

Component	Usage	Protocol	Default incoming port	Notes
VDA	ICA/Universal Print Server	TCP	7229	Used by the Universal Print Server print data stream CGP (Common Gateway Protocol) listener.
VDA	ICA/Universal Print Server	TCP	8080	Used by the Universal Print Server listener for incoming HTTP/SOAP requests.
VDA	Wake On LAN	UDP	9	Remote PC Access power management
VDA	Wake Up Proxy	TCP	135	Remote PC Access power management
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA, StoreFront, Director, Studio	TCP	80	
Delivery Controller	StoreFront, Director, Studio over TLS	TCP	443	
Delivery Controller	Delivery Controller, VDA	TCP	89	Local Host Cache (This use of port 89 might change in future releases.)
Delivery Controller	Orchestration	TCP	9095	Orchestration
Director	Delivery Controller	TCP	80, 443	

Citrix Licensing

The following ports are used for Citrix Licensing.

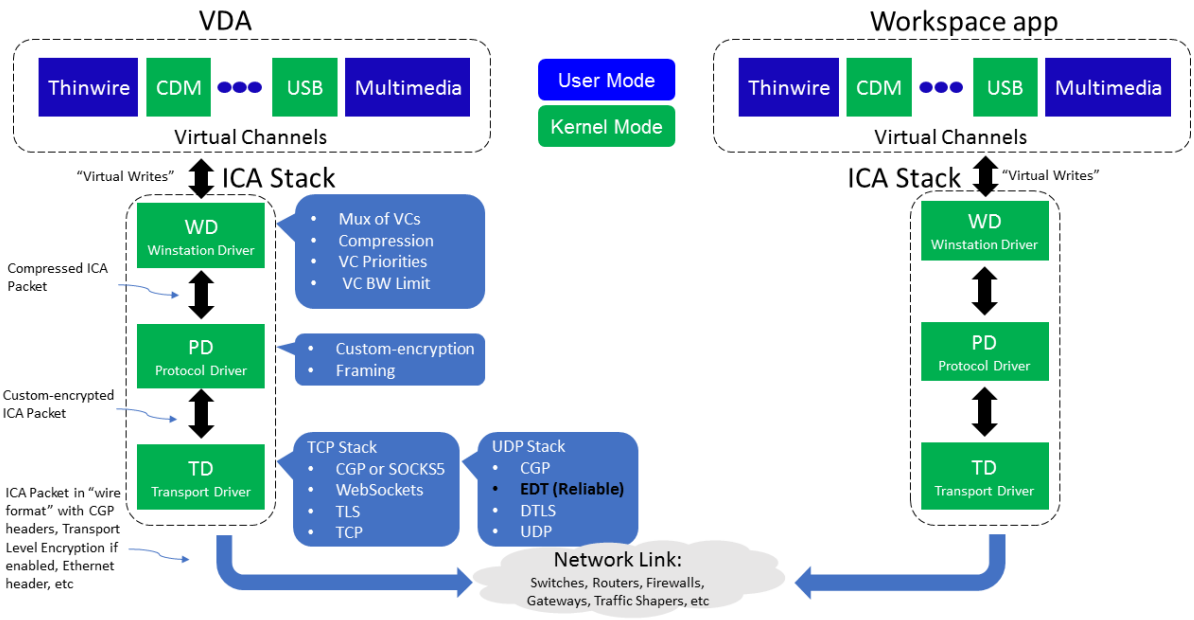
Component	Usage	Protocol	Default incoming port
License Server	License Server	TCP	27000
License Server	License Server for Citrix (vendor daemon)	TCP	7279
License Server	License Administration Console	TCP	8082
License Server	Web Services for Licensing	TCP	8083

HDX

January 26, 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.

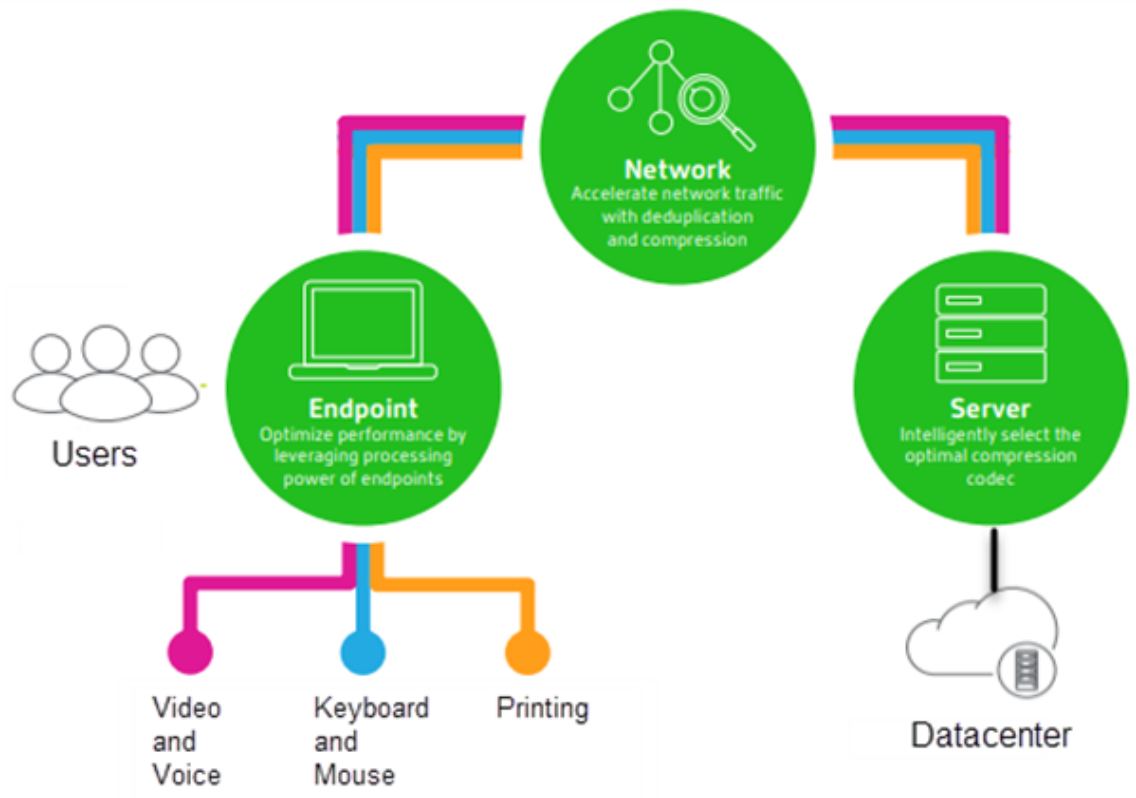


HDX is designed around three technical principles:

- 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.

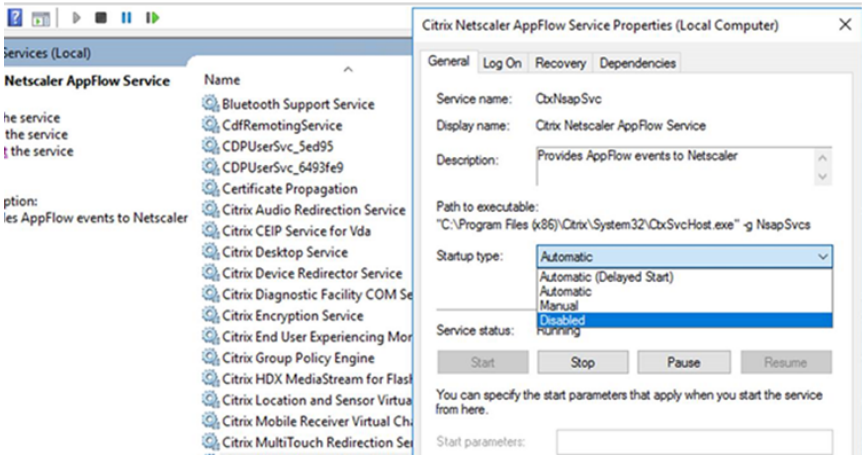
Minimum requirements:

- 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 Virtual Apps and Desktops 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, Windows 8, and Windows 7 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
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.
Under HKEY_LOCAL_MACHINE/SOFTWARE/Citrix, create the CtxKlMap key.
Set the DWORD value of EnableKlMap = 1

To disable this feature, set the DWORD value EnableKlMap = 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.

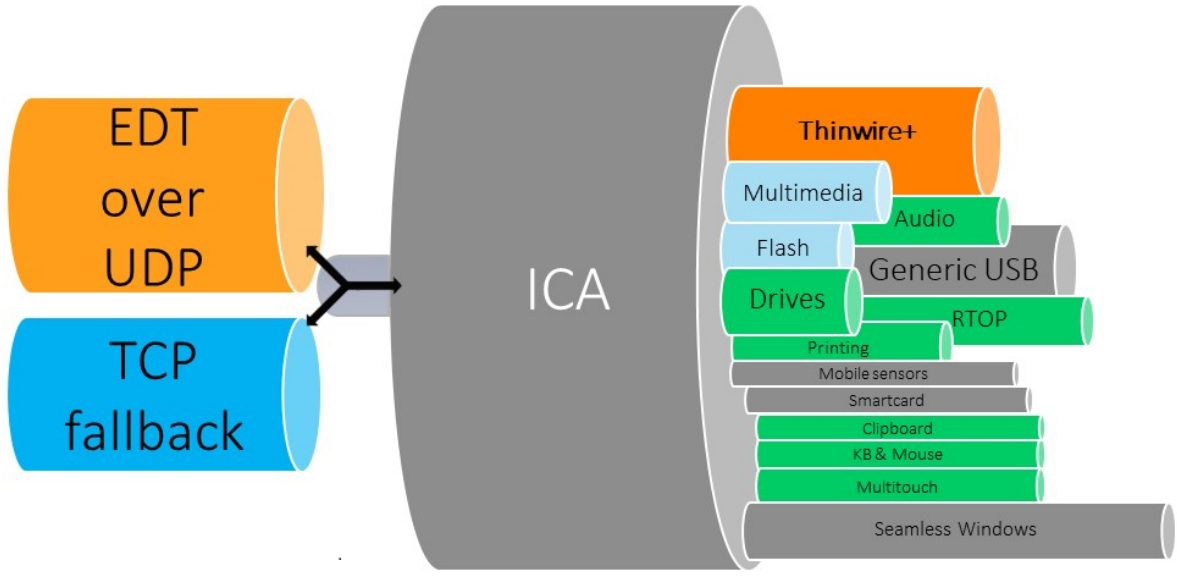
1. Under the HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap key, set the DWORD value DisableWindowHook =1.
2. To use normal Unicode keyboard layout mapping, set DWORD value DisableWindowHook = 0.

Adaptive transport

May 12, 2023

Adaptive Transport is a mechanism in Citrix Virtual Apps and Desktops that provides the ability to use Enlightened Data Transport (EDT) as the transport protocol for ICA connections. Adaptive Transport switches to TCP when EDT is not available.

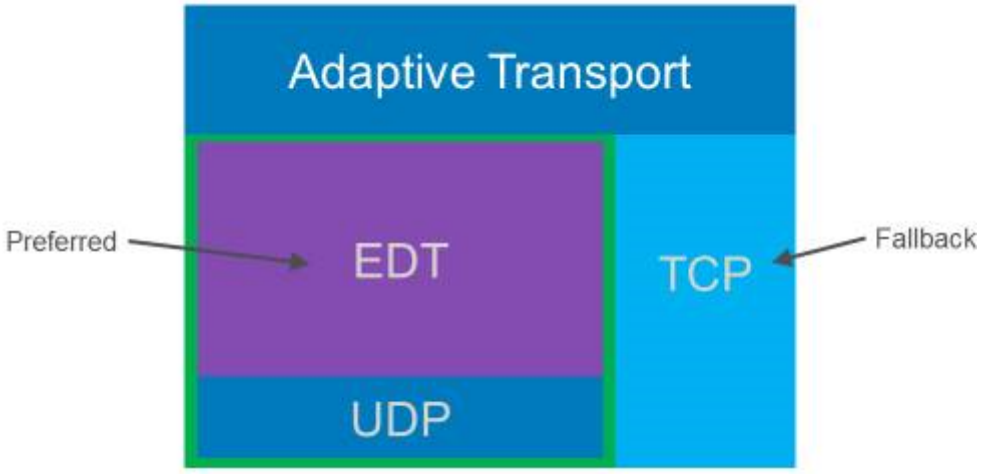
EDT is a Citrix-proprietary transport protocol built on top of User Datagram Protocol (UDP). It delivers a superior user experience on challenging long-haul connections while maintaining server scalability. EDT improves data throughput for all ICA virtual channels on unreliable networks, providing a better and more consistent user experience.



When Adaptive Transport is set to **Preferred**, EDT is used as the primary transport protocol and TCP is used for fallback. By default, Adaptive Transport is set to **Preferred**. You can set Adaptive Transport to **Diagnostic mode** for testing purposes, which only allows EDT and disables the fallback to TCP.

With Citrix Workspace app for Windows, Mac, and iOS, EDT and TCP connections are attempted in parallel during the initial connection, session reliability reconnection, and automatic client reconnection. Doing so reduces the connection time if the underlying UDP transport is unavailable and TCP must be used instead. If Adaptive Transport is set to **Preferred** and the connection is established using TCP, Adaptive Transport continues to attempt to switch to EDT every five minutes.

With Citrix Workspace app for Linux and Android, EDT connections are attempted first. If the connection is unsuccessful, Citrix Workspace app tries to connect using TCP after the EDT request times out.



System requirements

The following are the requirements for using Adaptive Transport and EDT:

- Control plane
  - Citrix Virtual Apps and Desktops Service
  - Citrix Virtual Apps and Desktops 1912 or later
- Virtual Delivery Agent
  - Version 1912 or later (2103 or later recommended)
  - Version 2012 is the minimum required for using EDT with Citrix Gateway Service
- StoreFront
  - Version 3.12.x
  - Version 1912.0.x
- Citrix Workspace app
  - Windows: version 1912 or later (2105 or later recommended)
  - Linux: version 1912 or later (2104 or later recommended)
  - Mac: version 1912 or later (2108 or later recommended)
  - iOS: latest version available in Apple App Store
  - Android: latest version available in Google Play
- Citrix Gateway (ADC)
  - 13.0.52.24 or later
  - 12.1.56.22 or later
- Firewall (from VDA perspective)
  - UDP 1494 inbound –if session reliability is disabled
  - UDP 2598 inbound –if session reliability is enabled
  - UDP 443 inbound –if VDA SSL is enabled for ICA encryption (DTLS)
  - UDP 443 outbound –if using Citrix Gateway Service. For more information, see the Citrix Gateway service documentation.

Considerations

- Enable session reliability to use EDT MTU Discovery and to use EDT with Citrix Gateway and Citrix Gateway service.
- Ensure that the EDT MTU is adequately set to avoid fragmentation. Otherwise, performance can be impacted or sessions might fail to launch in some situations. For more information, see the EDT MTU Discover.

- For details on requirements and considerations for using EDT with Citrix Gateway service, see HDX Adaptive Transport with EDT support for Citrix Gateway service.
- For details on Citrix Gateway configuration to support EDT, see Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight.
- IPv6 is not supported currently.

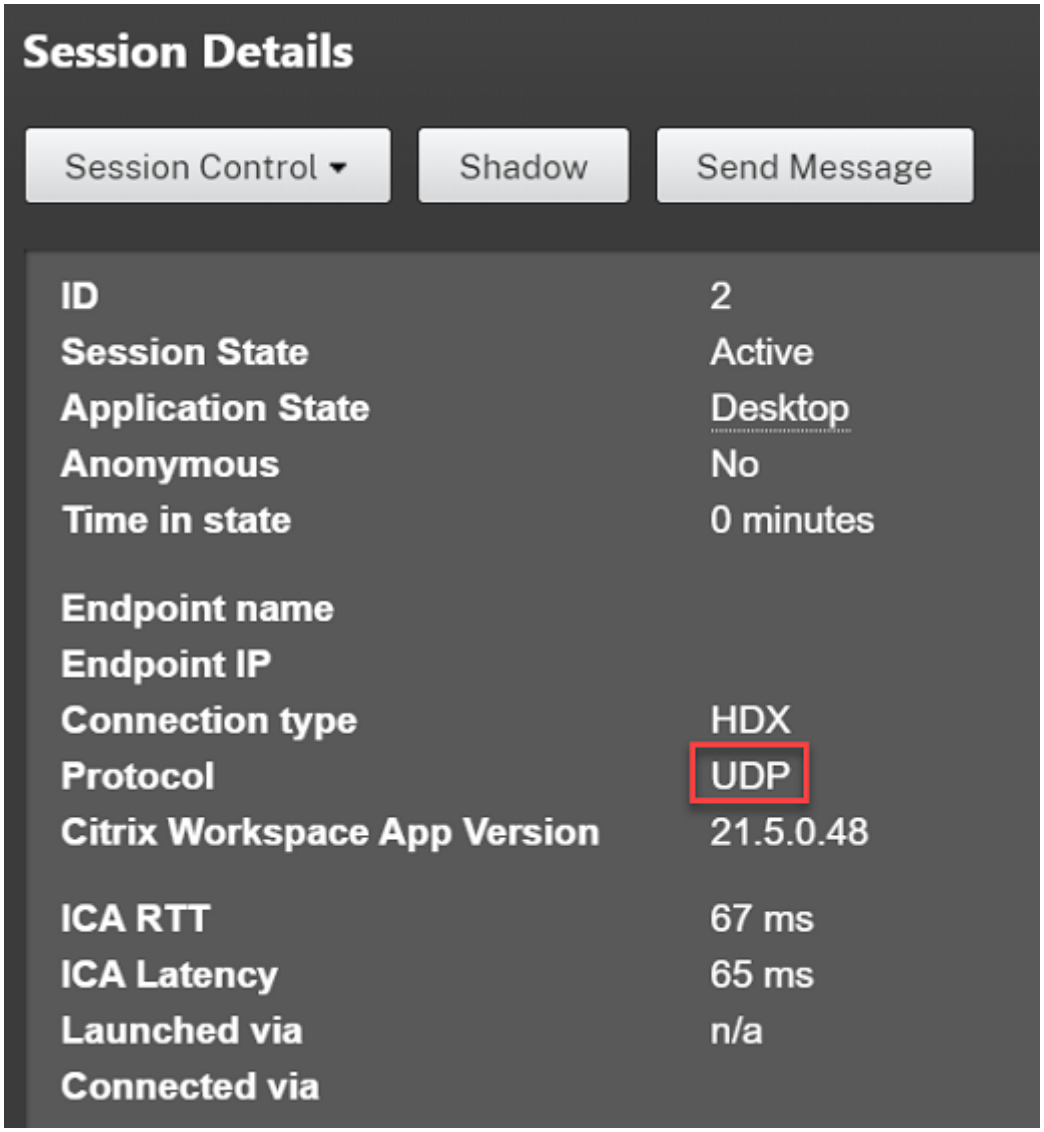
Configuration

Adaptive Transport is enabled by default. You can configure the following options using the **HDX Adaptive Transport** setting in Citrix policy.

- **Preferred**. This is the default setting. Adaptive Transport is enabled, and it uses EDT as the preferred transport protocol, with fallback to TCP.
- **Diagnostic mode**. Adaptive Transport is enabled, and it forces the use of EDT. Fallback to TCP is disabled. This setting is recommended for testing and troubleshooting only.
- **Off**. Adaptive Transport is disabled, and only TCP is used for transport.

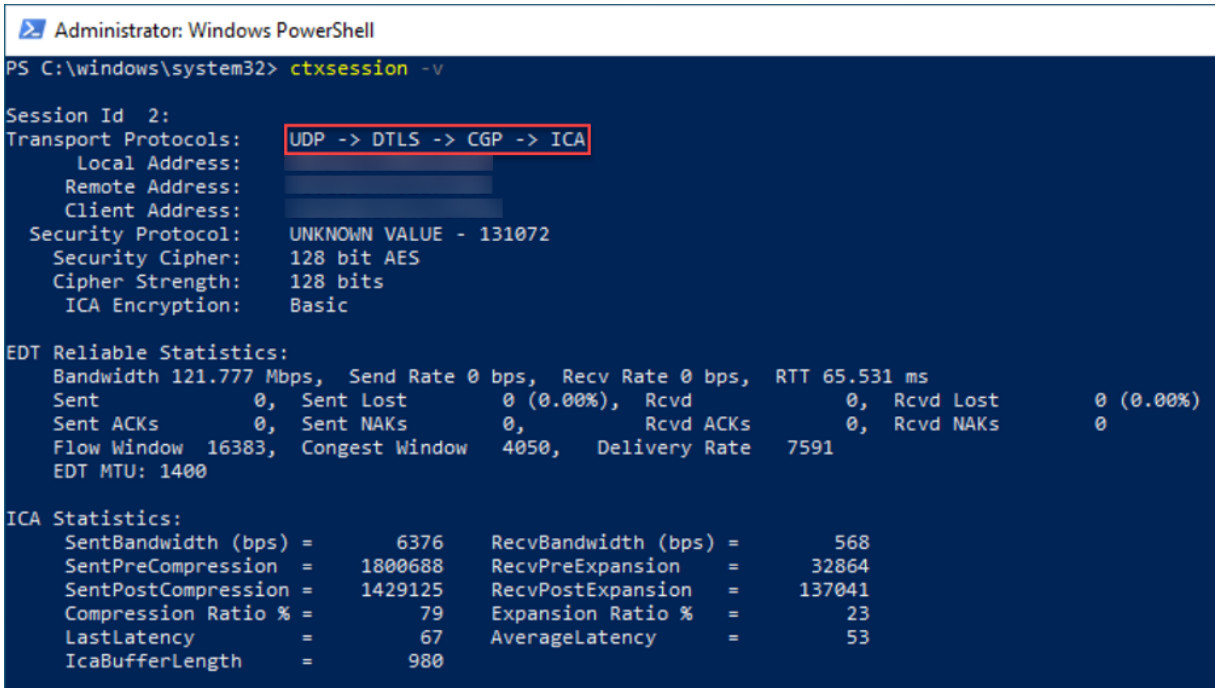
To confirm that EDT is being used as the transport protocol for the session, you can use Director or the CtxSession.exe command-line utility on the VDA.

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. If the **Connection type** is **RDP**, ICA is not in use, and the **Protocol** displays N/A. For more information, see Monitor sessions.



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)



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.

Requirements

- VDA minimum version 1912 (2103 or later recommended)
- Citrix Workspace app
  - Windows: version 1912 or later (2105 or later recommended)
  - Mac: version 2108 or later
  - Android: version 21.5 or later
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Session Reliability must be enabled

If you use client platforms or versions that don't support this feature, see CTX231821 for details about configuring a custom EDT MTU that is appropriate for your environment.

> **Important:**
>
> MTU Discovery is not supported with Multi-Stream ICA.

To enable or disable EDT MTU Discovery on the VDA

Set the following registry key:

- Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- Value name: MtuDiscovery
- Value type: DWORD
- Value data: 00000001

Restart the VDA and wait for the VDA to register.

To disable EDT MTU Discovery, delete this registry value and restart the VDA.

This setting is machine-wide and affects all sessions connecting from a supported client.

> **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.

Requirements

- Citrix Virtual Delivery Agent (VDA) 2003
- Citrix Workspace app 2002 for Windows
- Session reliability enabled. For more information about session reliability, see Session reliability policy settings.

Known issues

Adaptive Transport and EDT contain the following issues:

- Packet fragmentation can cause performance degradation or even failure to launch sessions. You can adjust the EDT MTU to avoid this. Use MTU Discovery or the workaround described in CTX231821.
- A grey or black screen may appear when launching a session from a Windows client if MTU Discovery is enabled. To address this issue, upgrade to Workspace app for Windows 2105 or later or Workspace app for Windows 1912 CU4 or later.

- Fallback to TCP may fail on Linux and Android clients when connecting through Citrix Gateway or Citrix Gateway Service. This happens when there is a successful EDT negotiation between the client and the Gateway, and the EDT negotiation fails between the Gateway and the VDA. To address this issue, upgrade to Workspace app for Linux 2104 or later and Workspace app for Android 21.5 or later.
- Asymmetrical network paths can cause MTU Discovery to fail for connections that do not go through Citrix Gateway or Citrix Gateway Service. To address this issue, upgrade to VDA version 2103 or later. [CVADHELP-16654]
- When using Citrix Gateway or Citrix Gateway Service, 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 not yet available. [CGOP-18438]
- MTU Discovery may 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, these are the available options:
  - Disable packet processing on the user's modem.
  - Disable MTU Discovery and use a hardcoded MTU as described in CTX231821.
  - Disable Adaptive Transport to force sessions to use TCP. If only a subset of users is affected, consider disabling it on the client-side so that other users can continue to use EDT.

Troubleshoot

To troubleshoot Adaptive Transport and EDT, we suggest the following:

1. Thoroughly review and validate the requirements, considerations, and known issues.
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. Launch a direct session internally, bypassing the Citrix Gateway, and check the protocol in use. If the session uses EDT, the VDA is ready to use EDT for external connections through Citrix Gateway.

6. If EDT works for direct internal connections and not for sessions going through Citrix Gateway:
    - Ensure that Session Reliability is enabled
    - Ensure that the Gateway has DTLS enabled
7. Check if the appropriate firewall rules have been configured in both network firewalls and firewalls running on the VDA machines.
8. 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 VPN, some Wi-Fi access points, and mobile networks, such as 4G and 5G. For information on how to address this issue, see the MTU Discovery section.

Interoperability with Citrix SD-WAN

Citrix SD-WAN WAN optimization (WANOP) offers cross-session tokenized compression (data deduplication), including URL-based video caching, providing significant bandwidth reduction. The reduction occurs if two or more people at the office location watch the same client-fetched video or transfer or print significant portions of the same file or document. Furthermore, by running the processes for ICA data reduction and print job compression on the branch office appliance, WANOP offers VDA server CPU offload and enables higher Citrix Virtual Apps and Desktops server scalability.

Currently, SD-WAN WANOP does not support EDT. However, there is no need to disable Adaptive Transport if SD-WAN WANOP is in use. When a user launches a session that goes through an SD-WAN with WANOP enabled, it automatically sets the session to use TCP as the transport protocol. Non-WANOP sessions continue to use EDT whenever possible.

Citrix ICA virtual channels

March 7, 2022

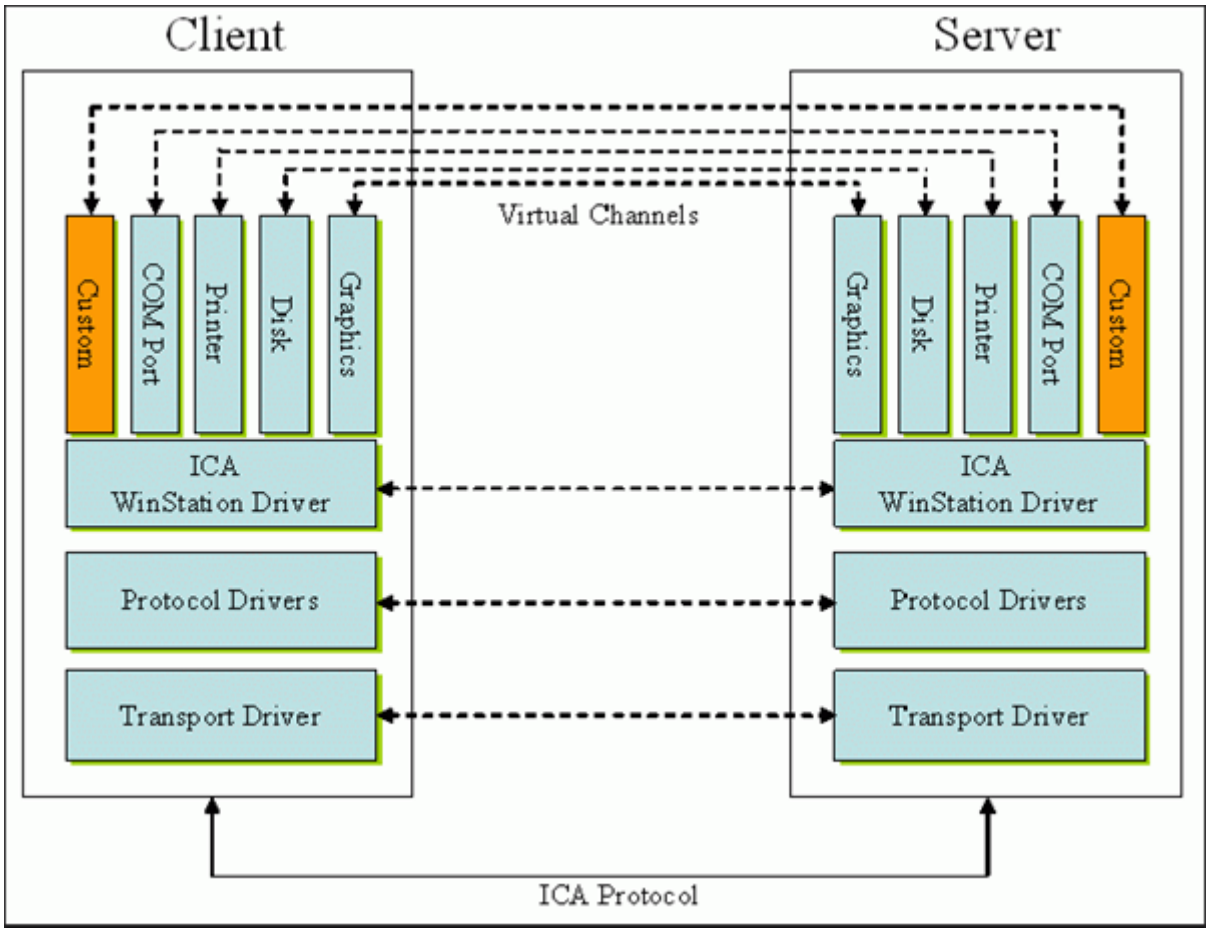
> **Warning**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

What are ICA virtual channels?

A large portion of the functionality and communication between the Citrix Workspace app and the Citrix Virtual Apps and Desktops servers occurs over virtual channels. Virtual channels are a necessary part of the remote computing experience with the Citrix Virtual Apps and Desktops 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 new versions of the Citrix Virtual Apps and Desktops servers 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 Virtual Apps and Desktops ship 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.

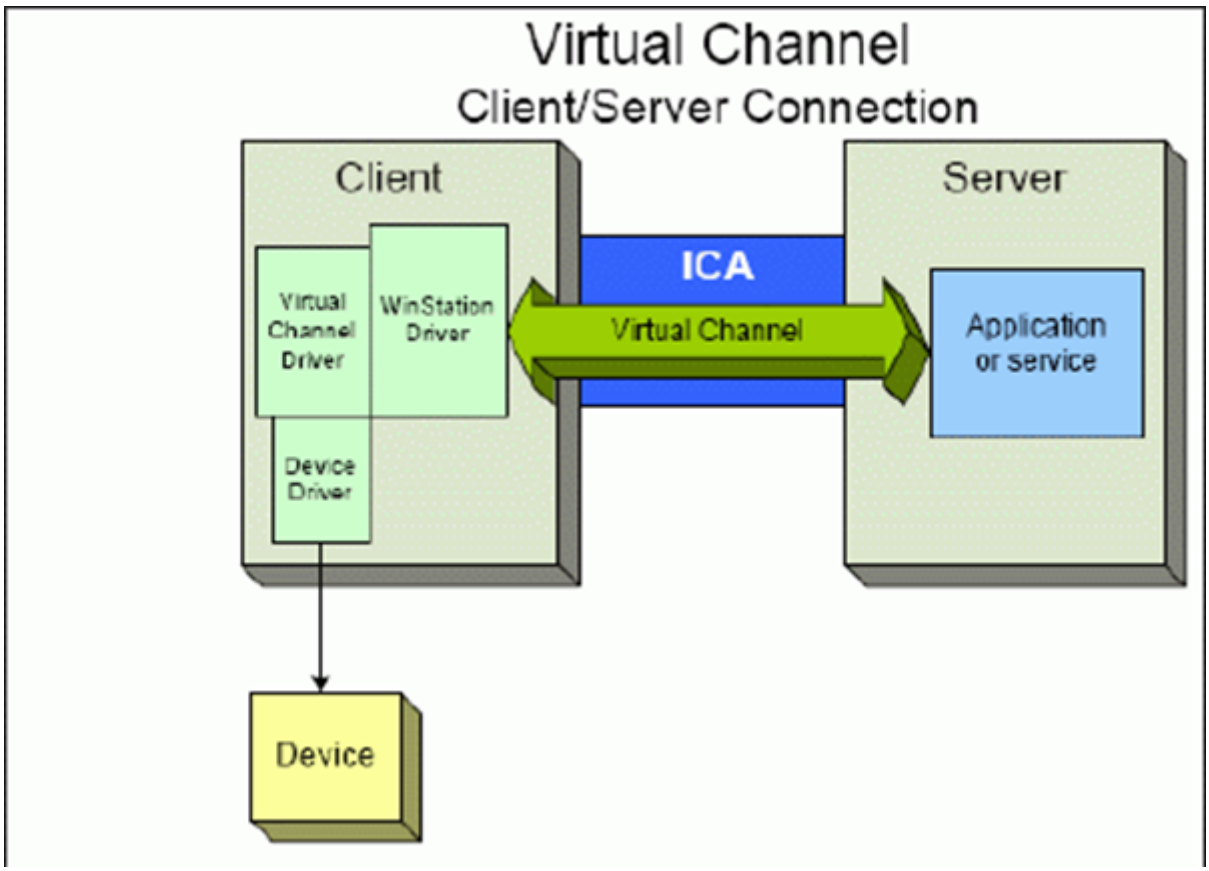
Hosting specialized channels in windows services

On Citrix Virtual Apps and Desktops 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)

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 Virtual Apps and Desktops 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.

> Notes:
>
> - The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.
> - Because of enhanced security for Citrix Virtual Apps and Desktops and Citrix Workspace app for Windows, you must take an extra step when installing a custom virtual channel.

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
Browser Content Redirection	No
CDM	Yes
CEIP	No
Clipboard	Yes
Continuum (MRVC)	No
Control VC	Yes

Virtual Channel	Is double hop supported?
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

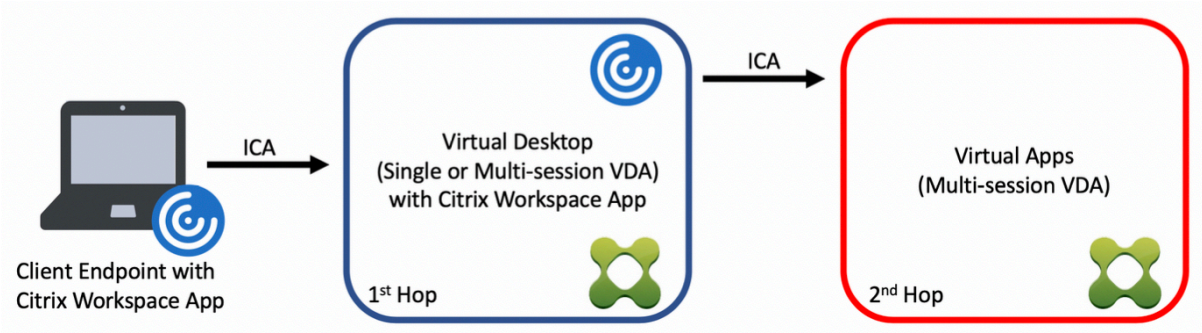
See also

- 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 Virtual Apps and Desktops

August 14, 2020

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 Virtual Apps and Desktop editions including the Citrix Cloud service 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.
Generic	Optimized	While technically possible, it is recommended to use the optimized mode across both hops when device support is available.

First hop (VDI or published desktop)	Second hop (Virtual apps)	Support notes
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

Install and configure

February 6, 2020

Review the referenced articles before starting each deployment step, to learn about what you see and specify during the deployment.

Use the following sequence to deploy Citrix Virtual Apps and Desktops.

Prepare

Review Prepare to install and complete any necessary tasks.

- Where to find information about concepts, features, differences from earlier releases, system requirements, and databases.
- Considerations when deciding where to install core components.
- Permission and Active Directory requirements.
- Information about the available installers, tools, and interfaces.

Install core components

Install the Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server, and Citrix StoreFront. For details, see Install core components or Install using the command line.

Create a Site

After you install the core components and launch Studio, you are automatically guided to create a Site.

Install one or more Virtual Delivery Agents (VDAs)

Install a VDA on a machine running a Windows operating system, either on a master image or directly on each machine. See Install VDAs or Install using the command line. Sample scripts are provided if you want to install VDAs through Active Directory.

For machines with a Linux operating system, follow the guidance in Linux Virtual Delivery Agent.

For a Remote PC Access deployment, install a VDA for Desktop OS on each office PC. If you need only the core VDA services, use the standalone VDAWorkstationCoreSetup.exe installer and your existing Electronic Software Distribution (ESD) methods. (Prepare to install describes the available VDA installers.)

Install optional components

If you plan to use the Citrix Universal Print Server, install its server component on your print servers. See Install core components or Install using the command line.

To allow StoreFront to use authentication options such as SAML assertions, install the Citrix Federated Authentication Service.

To enable end users to have greater control over their user accounts, install Self-Service Password Reset.

Optionally, integrate more Citrix components into your Citrix Virtual Apps and Desktops deployment.

- Citrix Provisioning is an optional component that provisions machines by streaming a master image to target devices.
- Citrix Gateway is a secure application access solution that provides administrators with granular application-level policy and action controls to secure access to applications and data.
- Citrix SD-WAN is a set of appliances that optimize WAN performance.

Create a machine catalog

After you create a Site in Studio, you are guided to create a machine catalog.

A catalog can contain physical or virtual machines (VMs). Virtual machines can be created from a master image. When using a hypervisor or cloud service to provide VMs, you first create a master image on that host. Then, when you create the catalog, you specify that image, which is used when creating VMs.

Create a Delivery Group

After you create your first machine catalog in Studio, you are guided to create a Delivery Group.

A Delivery Group specifies which users can access machines in a selected catalog and the applications available to those users.

Create an Application Group (optional)

After you create a Delivery Group, you can optionally create an Application Group. You can create Application Groups for applications that are shared across different Delivery Groups or used by a subset of users within Delivery Groups.

Prepare to install

May 9, 2024

Deploying Citrix Virtual Apps and Desktops begins with installing the following components. This process prepares for delivery of applications and desktops to users inside your firewall.

- One or more Delivery Controllers
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrix License Server
- One or more Citrix Virtual Delivery Agents (VDAs)
- Optional components and technologies such as the Universal Print Server, the Federated Authentication Service, and Self-Service Password Reset

For users outside your firewall, install and configure an additional component, such as Citrix Gateway. For an introduction, see Integrate Citrix Virtual Apps and Desktops with Citrix Gateway.

You can use the full-product installer on the product ISO to deploy many components and technologies. You can use a standalone VDA installer to install VDAs. All installers offer graphical and command line interfaces. See Installers.

The product ISO contains sample scripts that install, upgrade, or remove VDAs for machines in Active Directory. You can also use the scripts to manage master images used by Machine Creation Services (MCS) and Citrix Provisioning (formerly Provisioning Services). For details, see Install VDAs using scripts.

Learn about product name changes.

Information to review before installation

- Technical overview: If you're unfamiliar with the product and its components.
- Security: When planning your deployment environment.
- Known issues: Issues you might encounter in this version.
- Databases: Learn about the system databases and how to configure them. During Controller installation, you can install SQL Server Express for use as the Site database. You configure most database information when you create a site, after you install the core components.
- Remote PC Access: If you're deploying an environment that enables your users to access their physical machines in the office remotely.
- Connections and resources: If you're using a hypervisor or cloud service to host or provision VMs for applications and desktops. You can configure the first connection when you create a site (after you install the core components). Set up your virtualization environment before then.
- Microsoft System Center Configuration Manager: If you're using ConfigMgr to manage access to applications and desktops, or if you're using the Wake on LAN feature with Remote PC Access.

Where to install components

Review the System requirements for supported platforms, operating systems, and versions. Component prerequisites are installed automatically, except as noted. See the Citrix StoreFront and the Citrix License Server documentation for their supported platforms and prerequisites.

You can install the core components on the same server or on different servers.

- Installing all the core components on one server can work for evaluation, test, or small production deployments.
- To accommodate future expansion, consider installing components on different servers. For example, installing Studio on a different machine than the server where you installed the Controller allows you to manage the site remotely.
- For most production deployments, installing core components on separate servers is recommended.

- To install a supported component on a Server Core OS (such as a Delivery Controller), you must use the command line. That OS type does not offer a graphical interface, so install Studio and other tools elsewhere, and then point them to the Controller server.

You can install both a Delivery Controller and a VDA for multi-session OS on the same server. Launch the installer and select the Delivery Controller (plus any other core components you want on that machine). Then launch the installer again and select the Virtual Delivery Agent for multi-session OS.

Ensure that each operating system has the latest updates. For example, installation of a Controller or VDA on Windows Server 2012 R2 fails if Windows update KB2919355 is not installed.

Ensure that all machines have synchronized system clocks. The Kerberos infrastructure that secures communication between the machines requires synchronization.

Optimization guidance for Windows 10 single-session machines is available in CTX216252.

Where NOT to install components:

- Do not install any components on an Active Directory domain controller.
- Installing a Controller on a node in a SQL Server clustering installation, SQL Server mirroring installation, or on a server running Hyper-V is not supported.
- Do not install Studio on a server running XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2 or any earlier version of XenApp.

If you attempt to install (or upgrade to) a Windows VDA on an OS that is not supported for this product version, a message guides you to an article that describes your options.

Permission and Active Directory requirements

You must be a domain user and a local administrator on the machines where you are installing components.

To use the standalone VDA installer, you must have elevated administrative privileges or use **Run as administrator**.

Configure your Active Directory domain before starting an installation.

- System requirements lists the supported Active Directory functional levels. Active Directory contains more information.
- You must have at least one domain controller running Active Directory Domain Services.
- Do not install any Citrix Virtual Apps and Desktops components on a domain controller.
- Do not use a forward slash (/) when specifying Organizational Unit names in Studio.

The Windows user account used to install the Citrix License Server is automatically configured as a Delegated Administration full administrator on the license server.

For more information:

- Security best practices
- Delegated Administration
- Microsoft documentation for Active Directory configuration

Installation guidance, considerations, and best practice

During installation of any component

- When installing or upgrading core components (Delivery Controller, Studio, Lixense Server, Director, StoreFront) from the full-product ISO, if the Citrix installer detects that a restart is pending from a previous Windows installation on the machine, the installer stops with exit/return code 9. You are prompted to restart the machine.

  This is not a Citrix forced restart. It is due to other components installed earlier on the machine. If this occurs, restart the machine and then launch the Citrix installer again.

  When using the command-line interface, you can prevent the check for the pending restart by including the `/no_pending_reboot_check` option in the command.

- Usually, if a component has prerequisites, the installer deploys them if they are not present. Some prerequisites might require a machine restart.

- When you create objects before, during, and after installation, specify unique names for each object. For example, provide unique names for networks, groups, catalogs, and resources.

- If a component does not install successfully, the installation stops with an error message. Components that installed successfully are retained. You do not need to reinstall them.

- Citrix 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. During installation, you can also choose to participate in other Citrix technologies that collect diagnostics for maintenance and troubleshooting. For information about these programs, see Citrix Insight Services.

- Google Analytics are collected (and later uploaded) automatically when you install (or upgrade) Studio. After installing Studio, you can change this setting with the registry key `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. A value of 1 enables collection and upload, 0 disables collection and upload.

- 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's 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.

During VDA installation

The Citrix Workspace app for Windows is available, but not installed by default when you install a VDA. You or your users can download and install (and 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 your StoreFront server. See the StoreFront documentation.

The Print Spooler Service is enabled by default on supported Windows servers. If you disable this service, you cannot successfully install a VDA for Windows multi-session OS, so ensure that this service is enabled before installing a VDA.

Most supported Windows editions come with Microsoft Media Foundation already installed. If the machine on which you're installing a VDA does not have Media Foundation (such as N editions), several multimedia features will not be installed and will not work. 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` to acknowledge the limitation.

If Media Foundation is not present on the machine with the VDA, these multimedia features do not work:

- Windows Media Redirection
- HTML5 Video Redirection
- HDX RealTime Webcam Redirection

When you install the VDA, a new local user group called Direct Access Users is created automatically. On a VDA for single-session OS, this group applies only to RDP connections. On a VDA for multi-session OS, this group applies to ICA and RDP connections.

The VDA must have valid Controller addresses with which to communicate. Otherwise, sessions cannot be established. You can specify Controller addresses when you install the VDA or later. Just remember that it must be done.

VDA supportability tools

Each VDA installer includes a supportability MSI that contains Citrix tools for checking the VDA 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, you can 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 after and 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 restarts needed during VDA installation:

- Ensure that a supported .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 this with the `/noresume` option.)

> **Note:**
>
> When you're upgrading a VDA to version 7.17 or a later supported version, a restart occurs during the upgrade. This cannot be avoided.

Installers

Full-product installer

Using the full-product installer provided in the ISO, you can:

- Install, upgrade, or remove core components: Delivery Controller, Studio, Director, StoreFront, License Server.

- Install or upgrade Windows VDAs for server or desktop operating systems.
- Install the Universal Print Server UpsServer component on your print servers.
- Install the Federated Authentication Service.
- Install the Self-Service Password Reset Service.

To deliver a desktop from a multi-session OS for one user (for example, for web development), use the full-product installer's command line interface. For details, see Server VDI.

Standalone VDA installers

Standalone VDA installers are available on the Citrix download pages. The standalone VDA installers are much smaller than the full-product ISO. They more easily accommodate deployments that:

- Use Electronic Software Distribution (ESD) packages that are staged or copied locally
- Have physical machines
- Have remote offices

By default, files in the self-extracting standalone VDAs are extracted to the `Temp` folder. More disk space is required on the machine when extracting to the `Temp` folder than when using the full-product installer. However, 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. (They are not available on the full-product installation media.)

VDAServerSetup.exe:

Installs a VDA for multi-session OS. It supports all the VDA for multi-session OS options that are available with the full-product installer.

VDAWorkstationSetup.exe:

Installs a VDA for single-session OS. It supports all the VDA for single-session OS options that are available with the full-product installer.

VDAWorkstationCoreSetup.exe:

Installs a VDA for single-session OS 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 a master image. It installs only the core services necessary for VDA connections such deployments. Therefore, it supports only a subset of the options that are valid with the full-product or `VDAWorkstationSetup` installers.

This installer does not install or contain the components used for:

- App-V.

- Profile Management. Excluding Citrix Profile Management from the installation affects Citrix Director displays. For details, see Install VDAs.
- Machine Identity Service.
- Personal vDisk or AppDisks.
- Citrix Supportability Tools.
- Citrix Files for Windows.
- Citrix Files for Outlook.

The `VDAWorkstationCoreSetup.exe` installer does not install or contain a Citrix Workspace app for Windows.

Using `VDAWorkstationCoreSetup.exe` is equivalent to using the full-product or VDAWorkstationSetup 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 User Profile Manager""Citrix User Profile Manager WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows"`.

You can install the omitted components/features later by running the full-product installer. That action installs all missing components.

The `VDAWorkstationCoreSetup.exe` installer does not automatically install the Browser Content Redirection MSI. (All other VDA installers install that MSI automatically.) To enable use of the browser content redirection feature, install `BCR_x64.msi` on the machine after you install the VDA. The MSI is located in the `x64 > Virtual Desktop Components` folder on the full-product installation media.

Citrix installation return codes

The installation log contains the result of component installations as a Citrix return code, not a Microsoft value.

- 0 = Success
- 1 = Failed
- 2 = PartialSuccess
- 3 = PartialSuccessAndRebootNeeded
- 4 = FailureAndRebootNeeded
- 5 = UserCanceled
- 6 = MissingCommandLineArgument

- 7 = NewerVersionFound
- 8 = SuccessRebootNeeded
- 9 = FileLockReboot
- 10 = Aborted
- 11 = FailedMedia
- 12 = FailedLicense
- 13 = FailedPrecheck
- 14 = AbortedPendingRebootCheck
- -1 = Exit

For example, when using tools such as Microsoft System Center Configuration Manager, a scripted VDA installation might appear to fail when the installation log contains the return code 3. This can occur when the VDA installer is waiting for a restart that you must initiate (for example, after a Remote Desktop Services role prerequisite installation on a server). A VDA installation is considered successful only after all prerequisites and selected components are installed, and the machine is restarted after the installation.

Alternatively, you can wrap your installation in CMD scripts (which return Microsoft exit codes) or change the success codes in your Configuration Manager package.

Microsoft Azure Resource Manager virtualization environments

November 10, 2022

Follow this guidance when using Microsoft Azure Resource Manager to provision virtual machines in your deployment.

Be familiar with the following:

- Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant
- Consent framework: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
- Service principal: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals

Limitations

Consider the following limitation when using Azure Resource Manager:

- This product does not support VDAs in a Windows Virtual Desktop (WVD) environment. For WVD support, use the Citrix Virtual Apps and Desktops service or Citrix Virtual Apps and Desktops Standard for Azure service.

Azure on-demand provisioning

When you use MCS to create machine catalogs in Azure Resource Manager, the Azure on-demand provisioning feature:

- Reduces your storage costs
- Provides faster catalog creation
- Provides faster virtual machine (VM) power operations

For the administrator, on-demand provisioning introduces no differences in the Studio procedures for creating host connections and MCS machine catalogs. The differences lie in how and when resources are created and managed in Azure, and VM visibility in the Azure portal.

When MCS created a catalog, the VMs were created in Azure during the provisioning process.

With Azure on-demand provisioning, VMs are created only when Citrix Virtual Apps and Desktops initiates a power-on action, after the provisioning completes. A VM is visible in the Azure portal only when it is running. (In Studio, VMs are visible, whether they're running.)

When you create an MCS catalog, the Azure portal displays the resource groups, network security group, storage accounts, network interfaces, base images, and identity disks. The Azure portal does not show a VM until Citrix Virtual Apps and Desktops initiates a power-on action for it. Then, the VM's status in Studio changes to **On**.

- For a pooled machine, the operating system disk and write-back cache exist only when the VM exists. Pooled machines result in significant storage savings 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. It remains in storage until the machine is deleted.

Initiating a power-off action for a VM results in Azure deleting it. The VM no longer appears in the Azure portal. In Studio, the VM's status changes to **Off**.

Catalogs created before on-demand provisioning

If you have machine catalogs that were created before Citrix Virtual Apps and Desktops supported the Azure on-demand provisioning feature (mid-2017), VMs in those catalogs are visible in the Azure portal whether they're running. You cannot convert those VMs to on-demand machines.

To take advantage of the performance enhancements and storage cost benefits of on-demand provisioning, create catalogs using MCS.

Azure Managed Disks

Azure Managed Disks is an elastic disk storage system you can use with MCS-created machine catalogs, as an alternative to using conventional storage accounts.

The managed disks feature hides the complexity of creating and managing storage accounts. It provides a simple and highly available solution for creating and managing disks. You can use managed disks as master images, in addition to VMs. Using managed disks can improve machine catalog creation and update time. For more information, see Learn about Managed Disks.

By default, a machine catalog uses managed disks. You can override this default when you create the catalog.

Use managed disks

When you create a machine catalog in Studio, the **Master Image** page of the catalog creation wizard lists managed disks, in addition to VMs and VHDs. Not all Azure regions support the Managed Disks feature. Managed disks appear in the list for any region that's visible to the catalog's host connection.

Catalog creation time is optimized when the image and catalog are in the same region.

The managed disks feature does not currently support copying disks between Azure regions. Selecting an image in a region other than where MCS provisions the catalog copies the image to a VHD in a conventional storage account. The image appears in the catalog's region, and then converted back to a managed disk.

On the **Storage and License Types** page of the catalog creation wizard, you can select a check box to use conventional storage accounts instead of managed disks. You cannot select the check box when you are provisioning in an Azure region that does not support managed disks.

Create a connection to Azure Resource Manager

The Connections and resources article contains information about the wizards that create a connection. The following information covers details specific to Azure Resource Manager connections.

Considerations:

- Service principals must have been granted contributor role for the subscription.

- 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.
- 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.
- You can use an existing Microsoft account by adding it as a member of the subscription's directory. However, there can be complications if the user was previously granted guest access to one of the directory's resources. In this case, a placeholder entry exists in the directory that does not grant the necessary permissions, and an error is returned.

  To resolve the access issue, remove the resources from the directory and add them back explicitly. However, exercise this option carefully, because it has unintended effects for other resources that account can access.
- There is a known issue where certain accounts are detected as directory guests when they are actually members. Accounts detected as guests typically occurs 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 contain resources from regions other than their own region. Resource groups can potentially be confusing if you expect the resources displayed in a resource group's region.
- Ensure your network and subnet are large enough to host the number of machines you require. The network size requires some foresight, but Microsoft helps you specify the right values, with guidance about the address space capacity.

There are two ways to establish a host connection to Azure Resource Manager:

- Authenticate to Azure Resource Manager to create a service principal.
- Use the details from a previously created service principal to connect to Azure Resource Manager.

Authenticate to Azure Resource Manager to create a service principal

Before you start, make sure:

- 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 you want to use for provisioning resources.

In the Site Setup or Add Connection and Resources wizard:

1. On the **Connection** page, select the **Microsoft Azure** connection type. Then select your Azure Cloud environment.
2. On the **Connection Details** page, enter your Azure subscription ID and a name for the connection. The connection name can contain 1–64 characters, and cannot contain only blank spaces or non-alphanumeric characters. After you enter the subscription ID and connection name, the **Create new** button is enabled.
3. Enter the Azure Active Directory account user name and password.
4. Click **Sign in**.
5. Click **Accept** to give Citrix Virtual Apps and Desktops the listed permissions. Citrix Virtual Apps and Desktops creates a service principal that allows it to manage Azure Resource Manager resources on behalf of the specified user.
6. After you click **Accept**, you are returned to the **Connection** page in Studio. When successfully authenticating to Azure, the **Create new** and the **Use existing** buttons are replaced with **Connected**, and a green check mark indicates the successful connection to your Azure subscription.
7. Indicate which tools to use to create the virtual machines, and then click **Next**. (You cannot progress beyond this page in the wizard until you successfully authenticate with Azure and accept giving the required permissions.
8. Resources comprise the region and the network.
    - On the **Region** page, select a region.
    - On the **Network** page, type a 1–64 character resource name to help identify the region and network combination in Studio. A resource name cannot contain only blank spaces, and cannot contain the non-alphanumeric.
    - Select a virtual network and resource group pair. Since you can have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations. Selecting a region on the previous page that does not have any virtual networks, returns you to that page. Select a region that has virtual networks.
9. Complete the wizard.

Use the details from a previously created service principal to connect to Azure Resource Manager

To create a service principal manually, connect to your Azure Resource Manager subscription and use the PowerShell cmdlets provided in the following section.

Prerequisites:

- **$SubscriptionId:** Azure Resource Manager `SubscriptionID` for the subscription where you want to provision VDAs.
- **$AADUser:** Azure AD user account for your subscription's AD tenant. Make the `$AADUser` the co-administrator for your subscription.
- **$ApplicationName:** Name for the application to be created in Azure AD.
- **$ApplicationPassword:** Password for the application. You use this password as the application secret when creating the host connection.

To create a service principal:

1. Connect to your Azure Resource Manager subscription.

   ```
   Login-AzureRmAccount
   ```

2. Select the Azure Resource Manager subscription where you want to create the service principal.

   ```
   Select-AzureRmSubscription -SubscriptionID $SubscriptionId
   ```

3. Create the application in your AD tenant.

   ```
   $AzureADApplication = New-AzureRmADApplication -DisplayName
   $ApplicationName -HomePage "https://localhost/$ApplicationName"-
   IdentifierUris https://$ApplicationName -Password $ApplicationPassword
   ```

4. Create a service principal.

   ```
   New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
   ApplicationId
   ```

5. Assign a role to the service principal.

   ```
   New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
   ServicePrincipalName $AzureADApplication.ApplicationId –scope
   /subscriptions/$SubscriptionId
   ```

6. From the output window of the PowerShell console, note the ApplicationId. You provide that ID when creating the host connection.

In the Site Setup or Add Connection and Resources wizard:

1. On the **Connection** page, select the **Microsoft Azure** connection type and your Azure environment.
2. On the **Connection Details** page, enter your Azure subscription ID and a name for the connection. (The connection name can contain 1–64 characters, and cannot contain only blank spaces or non-alphanumeric characters.

3. Click **Use existing**. Provide the subscription ID, subscription name, authentication URL, management URL, storage suffix, Active Directory ID or tenant ID, application ID, and application secret for the existing service principal. After you enter the details, the **OK** button is enabled. Click **OK**.
4. Indicate which tools to use to create the virtual machines, and then click **Next**. The service principal details you provided are used to connect to your Azure subscription. (You cannot progress beyond this page in the wizard until you provide valid details for the Use existing option.)
5. Resources comprise the region and the network.
    - On the **Region** page, select a region.
    - On the **Network** page, type a 1–64 character resources name to help identify the region and network combination in Studio. A resource name cannot contain only blank spaces, and cannot contain non-alphanumeric characters.
    - Select a virtual network and resource group pair. (Since you can have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If you selected a region on the previous page that does not have any virtual networks, you need to return to that page and select a region that has virtual networks.
6. Complete the wizard.

Create a machine catalog using an Azure Resource Manager master image

This information is a supplement to the guidance in Create machine catalogs.

A master image is the template that is used to create the VMs in a machine catalog. Before creating the machine catalog, create a master image in Azure Resource Manager. For information about master images in general, see the Create machine catalogs article.

When you create a machine catalog in Studio:

- The **Operating System** and **Machine Management** pages do not contain Azure-specific information. Follow the guidance in Create machine catalogs.
- On the **Master Image** page, select a resource group. Navigate through the containers to the Azure VHD you want to use as the master image. The VHD must have a Citrix VDA installed on it. If the VHD is attached to a VM, the VM must be stopped.
- The **Storage and License Types** page appears only when using an Azure Resource Manager master image.

  Select a storage type: standard or premium. The storage type affects which machine sizes are offered on the **Virtual Machines** page. Both storage types make multiple synchronous copies

of your data within a single data center. For details about Azure storage types and storage replication, see the following:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

Select whether to use existing on-premises Windows Server licenses. Doing so with using existing on-premises Windows Server images utilizes Azure Hybrid Use Benefits (HUB). More details are available at https://azure.microsoft.com/pricing/hybrid-use-benefit/.

HUB reduces the cost of running VMs in Azure to the base compute rate. It waives the price of extra Windows Server licenses from the Azure gallery. Bring your on-premises Windows Servers images to Azure to use HUB. Azure gallery images are not supported. On-premises Windows Client licenses are currently not supported.

Check if the provisioned Virtual Machines are successfully utilizing HUB. Run the PowerShell command `Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM` and check 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/.

- On the **Virtual Machines** page, indicate how many VMs you want to create; you must specify at least one. Select a machine size. After you create a machine catalog, you cannot change the machine size. If you later want a different size, delete the catalog and then create a catalog that uses the same master image and specifies the desired machine size.

  Virtual machine names cannot contain non-ASCII or special characters.

- (When using MCS) On the **Resource Groups** page, choose whether to create resource groups or use existing groups.

  If you choose to create resource groups, click **Next**.

  If you choose to use existing resource groups, select groups from the **Available Provisioning Resource Groups** list. Select enough groups to accommodate the machines you're creating in the catalog. Studio displays a message 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(#azure-resource-groups).

- The **Network Cards**, **Computer Accounts**, and **Summary** pages do not contain Azure-specific information. Follow the guidance in Create machine catalogs.

Complete the wizard.

Delete machine catalogs

Deleting an Azure Resource Manager machine catalog results in the removal of the associated machines and resource groups, even if you indicate that they be retained.

Azure resource groups

Azure provisioning resource groups provide a way to provision the VMs that provide applications and desktops to users. Add existing empty Azure resource groups when you create an MCS machine catalog in Studio, or have new resource groups created.

For information about Azure resource groups, see the Microsoft documentation.

Requirements

- Each resource group can hold up to 240 VMs. There must be sufficient available empty resource groups in the region where you're creating the catalog. If you want to use existing resource groups when creating a machine catalog, select enough available groups to accommodate the number of machines created in the catalog. For example, if you specify 500 machines in the catalog creation wizard, select at least three available provisioning resource groups.

  You cannot add resource groups to a machine catalog after the catalog is created. So, consider adding enough resource groups to accommodate machines you might add to the catalog later.
- Create empty resource groups in the same region as your host connection.
- If you want to create resource groups for each MCS catalog, configure the Azure service principal associated with the host connection. This principal must have permission to create and delete resource groups. If you want to use existing empty resource groups, the Azure service principal associated with the host connection must have Contributor permission on those empty resource groups.
- When you create a host connection in Studio using the **Create new** option, the created service principal has subscription scope contribute permissions. Alternatively, you can use the **Use existing** option to create the connection, and provide the details of an existing subscription scope service principal. Use the **Create new** option to create the Service Principal in Studio. The principal has the needed permissions to create and delete new resource groups or provision into existing empty resource groups.
- Narrow scope service principals must be created using PowerShell. Also, when using a narrow scope service principal, you must use PowerShell or the Azure portal to create empty resource groups for each catalog where MCS provisions VMs.

If you are using narrow scope service principal for the host connection and don't see your master image resource group on the **Master Image** page of the catalog creation wizard, it is probably because the narrow scope service principal you are using doesn't have the permission `Microsoft.Resources/subscriptions/resourceGroups/read` to list the master image resource group. Close the wizard, update the service principal with the permission (see the blog post for instructions), and then restart the wizard. The update in Azure can take up to 10 minutes to appear in Studio.

About Azure service principals

To provision machines in Azure Resource Manager, a plug-in must be granted access to your Azure subscription. These permissions are granted via a service principal that has been assigned permissions to the relevant Azure resources. A service principal serves the same basic purpose as a user account. It provides the plug-in with an Azure Active Directory identity that supplies credentials for authentication and permissions on Azure resources. Just like user accounts, service principals are configured using Role Based Access Control (RBAC).

Depending on how permissions are defined, we classify service principals as:

- subscription scope service principals; or
- narrow scope service principals

Subscription scope service principals Subscription scope service principals have *contributor permissions* on all resources in the subscription which makes them easy to create and manage. Citrix Studio automates the process of creating subscription scope service principals or they can be created manually in PowerShell. These principals allow the Azure Resource Manager plug-in to create Azure Resource Groups and completely automate the management of resources. The disadvantage is that the plug-in has permissions to resources in the subscription that are unrelated to the resources that the plug-in is tasked with managing.

Using the *contributor role* allows the plug-in to create, delete, read, and write all resources in the subscription. Permissions do not extend to objects in any Azure Active Directory nor are subscription scope service principals allowed to grant other users or service principals access to resources.

Narrow scope service principals Narrow scope service principals allow the Azure Resource Manager plug-in access to a limited set of resources defined by you. Azure requires subscription scope permissions to create resource groups. The plug-in is unable to create resource groups when using narrow scope service principals. In addition to the service principals, you are required to provide a pool of resource groups for each catalog into which machines are to be provisioned.

Citrix Studio does not support creating narrow scope service principals or catalogs. Both of these tasks must be performed using PowerShell. However, once a catalog has been created, it can be managed like any other catalog in Studio including adding and deleting machines. If at some point you want to use an existing narrow scope service principal with a new pool of resource groups, you must explicitly add permissions to the service principal using PowerShell.

Defining Your Azure subscription access requirements The techniques and examples in the following sections demonstrate common requirements and requires change for your particular circumstances.

Consider using a subscription scope service principal if:

- you want the simplest management experience.
- you want to avoid using PowerShell and manage everything in Citrix Studio.
- your Azure subscription is dedicated to a single Citrix Virtual Apps and Desktops service.
- you are doing a proof of concept Citrix Virtual Apps and Desktops installation.
- your Citrix Virtual Apps and Desktops administrators have contributor access at Azure subscription scope.

Consider using a narrow scope service principal if:

- your Azure subscription is hosting multiple unrelated services.
- your Azure administrators have different subscription permissions depending on their role.
- your company has security standards that require access control at a fine-grained level.
- you have an existing process for creating narrow scope service principals.

> **Tip:**
>
> You can create *child* subscriptions that are billed as part of your primary subscription and refer to the default Azure Active Directory in your primary subscription. This configuration provides another mechanism for controlling access to unrelated resources.

Planning a narrow scope service principal catalog Before creating a narrow scope service principal catalog, decide how many resource groups are required to host the initial and future number of virtual machines. Due to a limitation in Machine Creation Services, it is not possible to add resource groups once a catalog has been created.

Provision one catalog per resource group pool The Azure Resource Manager plug-in creates the necessary infrastructure in each resource group. The resource group consists of storage accounts, security groups, network interfaces, virtual machines, and so forth Storage accounts are created on demand as needed when and if machines are added to the catalog. This means that the size of a catalog can grow to an upper limit set by the size of the resource group pool and Azure subscription quotas. Once a storage account has been created, it is not deleted until the catalog is deleted. Since any virtual machine can be deleted, it is possible to end up with empty storage accounts. This situation is rare because virtual machines tend to be randomly distributed over the available storage accounts. Machines have to be tediously selected by inspecting the content of storage accounts to deliberately empty a storage account.

Azure limits the number of virtual machines in a resource group to 800, but the Azure Resource Manager plug-in uses a different measure. A standard Azure disk has a limit of 500 I/O operations per second (IOPS) and a standard storage account has an IOPS limit of 20,000. For this reason, the plug-in provisions no more than 40 machines to a storage account. This limit is applied to both standard and premium storage. In addition, the plug-in creates no more than 19 storage accounts in a resource group.

The basic formula for calculating the number of resource groups based on the maximum number of machines is therefore:

Number of resource groups = ceiling(Maximum number of machines / (40 * 19))

The Azure Resource Manager plug-in assumes that it has exclusive use of the resource group pool. There is no user created resources in any of the specified resource groups.

Basics of Azure Role Based Access Control (RBAC).

Access to Azure resources are granted by assigning an RBAC role to a service principal at a certain scope. Scope can be a subscription, a resource group or a specific resource. Resources are arranged in a containment hierarchy and the permissions defined by the role apply to all resources below the scope where it is applied. A role applied on a subscription is applied to all resources in the subscription. A role applied to a resource group is applied to all resources contained in the resource group.

An implication of the Azure resource hierarchy is that only service principals with subscription scope permissions are allowed to create resource groups. This is not ideal because it prevents applications like the plug-in from creating resource groups on demand to a logical group and manage resources. Unless they have broad permissions on the full subscription.

Azure has a large selection of built-in roles and also supports the definition of custom roles. Refer to the Custom roles for Azure resources more information on Custom Roles in Azure RBAC.

Creating a subscription scope service principal This example shows how to create a subscription scope service principal. The details can be used to create an Azure connection in Citrix Studio. Select to use an existing service principal or an Azure connection can be created manually in PowerShell.


```
param(
[string]$applicationName = "SubscriptionScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId"

Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Creating a basic narrow scope service principal This section describes the process for creating the simplest possible narrow scope service principal where permissions are assigned at the resource group scope.

The Azure Resource Manager plug-in needs permission to the following resources:

1. The master image VHD
2. The virtual network for the machines
3. The resource groups into which the machines are to be provisioned.

To simplify the script, we assume that contributor access can be granted at resource group scope. The Azure Resource Manager plug-in has contributor permissions on the resource group where the image VHD is stored, the resource group that contains the virtual network and the resource group pool where the machines are provisioned.

```
param(
[string]$applicationName = "BasicNarrowScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string[]]$resourceGroups
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
```



```
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/"

foreach ($rg in $resourceGroups)
{

  New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
     ServicePrincipalName $application.ApplicationId `
  -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
 }


Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Creating a narrow scope service principal using custom roles Azure comes with a large set of built-in RBAC roles. Citrix uses the contributor role in the previous section. As noted, that gave the Azure Resource Manager plug-in slightly broader permissions than strictly required. This section defines a custom role and further tightens access. If desired, access can be locked down using more custom roles and applying roles directly to the image and network resources.

> **Note:**
>
> The required permissions are subject to change.

Use the following permissions to define a custom role for granting access to the virtual network and the master image at the resource group scope.

The master image VHD.

For catalog creation:

- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listKeys/action

For Future Citrix Studio support:

- Microsoft.Resources/subscriptions/resourceGroups/read

The virtual network for the machines:

- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/join/action

The resource groups for provisioned machines.

We can create another custom role with the following permissions, but to keep the example simple, continue to use the Contributor role for the machine resource groups. These resource groups do not contain resources not created by the Azure Resource Manager plug-in. The contributor role makes it less likely that changes to the plug-in require changes to the service principal:

- Microsoft.Compute/virtualMachines/*
- Microsoft.Network/networkInterfaces/*
- Microsoft.Network/networkSecurityGroups/*
- Microsoft.Resources/deployments/*
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Storage/storageAccounts/*
- Microsoft.Storage/storageAccounts/listKeys/action

Citrix Virtual Apps and Desktops Custom Access Roles.

Create a custom role by first defining it in JSON:

```
{

  "Name": "Citrix-Custom-Reader",
  "Description": "Grants access to Citrix XenDesktop images and virtual
      networks.",
  "Actions": [
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/listKeys/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action"
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    "/subscriptions/<YOUR-SUBSCRIPTION-ID>"
  ]
 }

<!--NeedCopy-->
```

Create the role by referencing the **JSON** definition:

```
New-AzureRmRoleDefinition -InputFile citrix-custom-reader.json
<!--NeedCopy-->
```


Use the new custom role when creating a service principal:

```
param(
[string]$applicationName = "NarrowScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string[]]$machineResourceGroups,
[Parameter(Mandatory=$true)][string]$imageResourceGroup,
[Parameter(Mandatory=$true)][string]$networkResourceGroup
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/"

foreach ($rg in $machineResourceGroups)
{

  New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
     ServicePrincipalName $application.ApplicationId `
  -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
 }


New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/resourcegroups/
    $imageResourceGroup"

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/resourcegroups/
    $networkResourceGroup"

Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Creating Citrix Virtual Apps and Desktops Azure Connections.

It is reasonable to create a Citrix Virtual Apps and Desktops Azure connection in Citrix Studio using an existing service principal. It is equally reasonable to create the connection in PowerShell.

The following is an example of creating a connection in PowerShell:


```
param(
[string]$connectionName = "AzureConnection",
[Parameter(Mandatory=$true)][string]$applicationId,
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string]$subscriptionName,
[Parameter(Mandatory=$true)][string]$tenantId
)

Add-PsSnapin Citrix*

$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <Property xsi:type="StringProperty" Name="AuthenticationAuthority" Value="https://login.microsoftonline.com/"/>
 <Property xsi:type="StringProperty" Name="ManagementEndpoint" Value="https://management.azure.com/"/>
 <Property xsi:type="StringProperty" Name="StorageSuffix" Value="core.windows.net"/>
 <Property xsi:type="StringProperty" Name="TenantId" Value="$tenantId" />
 <Property xsi:type="StringProperty" Name="SubscriptionId" Value="$subscriptionId"/>
 <Property xsi:type="StringProperty" Name="SubscriptionName" Value="$subscriptionName"/>
</CustomProperties>
"@

$connection = New-Item -ConnectionType "Custom" -CustomProperties $customProperties -HypervisorAddress @("https://management.azure.com/") `
-Path @("XDHyp:\Connections\$connectionName") -Persist -PluginId "AzureRmFactory" -Scope @() `
-SecurePassword (ConvertTo-SecureString -AsPlainText -Force $applicationPassword) -UserName $applicationId

New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.HypervisorConnectionUid

<!--NeedCopy-->
```

At this point add resources to the connection, using either Studio or in PowerShell.

Create Citrix Virtual Apps and Desktops catalogs.

The following example uses the Citrix PowerShell Snap-ins to create a Citrix Virtual Apps and Desktops catalog.

Because narrow scope service principals do not allow the Azure Resource Manager plug-in to create resource groups, you must:

1. Create a pool of resource groups.
2. Assign the service principal permissions on all the resource groups in the resource group pool.
3. List each resource group in the resource group in a custom property when creating the provisioning scheme.

The custom property is named **ResourceGroups** and the value is a comma separated list of resource group names. An example of how to define this custom property is shown in the following example.

> **Note:**
>
> Only resource groups that are intended for machines are listed in the custom property. One or more resource groups where the image or virtual network is located are not included. If they are specified, the Azure Resource Manager plug-in attempts to provision machines into those resource groups which can cause some unintended behavior.

In this example, machines are provisioned in two resource groups named xd-sales-1 and xd-sales-2:

```
Add-PsSnapin Citrix*

# The hosting unit name is the name of the Azure connection resources that should be used for this catalog
$hostingUnitName = "AzureHostingUnit"
$domain = "citrix.local"
$controllerAddress = ("ddc." + $domain)
$adminAddress = ($controllerAddress + ":80")
$catalogName = "catalog-name"
$network = "network-resource-group.resourcegroup\network-name"
$subnet = "subnet-name"
$serviceOffering = "Standard_A4"
$template = "image-resource-group.resourcegroup\imagestorage.storageaccount\images.container\image-name.vhd"

$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="Standard_LRS" />
    <Property xsi:type="StringProperty" Name="ResourceGroups" Value="xd-sales-1, xd-sales-2" />
</CustomProperties>
"@

$identityPool = New-AcctIdentityPool -AdminAddress $adminAddress -AllowUnicode -Domain $domain `
    -IdentityPoolName $catalogName -NamingScheme "vm-#" -NamingSchemeType "Numeric" -Scope @()

$brokerCatalog = New-BrokerCatalog -AdminAddress $adminAddress -AllocationType "Random" -IsRemotePC $False `
```



```
    -MinimumFunctionalLevel "L7_9" -Name $catalogName -
       PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @()
       `
    -SessionSupport "MultiSession"

Write-Host $brokerCatalog

$provScheme = New-ProvScheme -AdminAddress $adminAddress -CleanOnBoot -
   CustomProperties $customProperties `
    -HostingUnitName $hostingUnitName -IdentityPoolName $catalogName `
    -MasterImageVM "XDHyp:\HostingUnits\$hostingUnitName\image.folder\
       $template.vhd" `
    -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\$hostingUnitName\virtualprivatecloud.folder\
    $network.virtualprivatecloud\$subnet.network" }
  `
    -ProvisioningSchemeName $catalogName -Scope @() -SecurityGroup @()
       `
    -ServiceOffering "XDHyp:\HostingUnits\$hostingUnitName\
       serviceoffering.folder\$serviceOffering.serviceoffering"

Write-Host $provScheme

Set-BrokerCatalog -AdminAddress $adminAddress -Name $catalogName -
   ProvisioningSchemeId $provScheme.ProvisioningSchemeUid

Add-ProvSchemeControllerAddress -AdminAddress $adminAddress.com -
   ControllerAddress $controllerAddress -ProvisioningSchemeName
   $catalogName
<!--NeedCopy-->
```

At this point you can refresh the catalog page in Citrix Studio, add machines and manage machines as with any other catalog.

Configure resource groups for a machine catalog in Studio

The **Resource Groups** page in the catalog creation wizard allows you to choose whether to create resource groups or use existing groups. See Create a machine catalog using an Azure Resource Manager master image.

What happens to resource groups when you delete a machine catalog:

- If you let Citrix Virtual Apps and Desktops create resource groups when you create the machine catalog, and then later delete the catalog, those resource groups and all of the resources in those resource groups are also deleted.
- If you use existing resource groups when you create the machine catalog, and then later delete the catalog, all resources in those resource groups are deleted, but the resource groups are not deleted.

Considerations, limitations, and troubleshooting

When you use existing resource groups, the list of available resource groups on the Resource Groups page in the catalog creation wizard does not auto-refresh. So, if you have that wizard page open and create or add permissions to resource groups in Azure, the changes are not reflected in the wizard's list. To see the latest changes, either go back to the **Machine Management** page in the wizard and reselect the resources associated with the host connection, or close and restart the wizard. It can take up to 10 minutes for changes made in Azure to appear in Studio.

A resource group should be used in only one machine catalog. However, this is not enforced. For example, you select 10 resource groups when creating a catalog, but create only one machine in the catalog. Nine of the selected resource groups remain empty after the catalog is created. You might intend to use them to expand your capacity in the future, so they remain associated with that catalog. You can't add resource groups to a catalog after the catalog is created, so planning for future growth is sound practice. However, if another catalog is created, those nine resource groups appear in the available list. Citrix Virtual Apps and Desktops does not currently keep track of which resource groups are allocated to which catalogs. It's up to you to monitor that.

If your connection uses a service principal that can access empty resource groups in various regions, they will all appear in the available list. Be sure to choose resource groups in the same region where you're creating the machine catalog.

Troubleshooting:

- Resource groups don't appear in the list on the Resource Groups page of the catalog creation wizard.

  The service principal must have appropriate permissions applied to the resource groups you want to appear in the list. See the Requirements section above.

- When adding machines to a previously created machine catalog, not all machines are provisioned.

  After creating a catalog, and later adding more machines to the catalog, do not exceed the machine capacity of the resource groups originally selected for the catalog (240 per group). You cannot add resource groups after the catalog is created. If you attempt to add more machines than the existing resource groups can accommodate, the provisioning fails.

  For example, you create a machine catalog with 300 VMs and 2 resource groups. The resource groups can accommodate up to 480 VMs (240 multiplied by 2). If you later try to add 200 VMs to the catalog, that exceeds the capacity of the resource groups (300 current VMs + 200 new VMs = 500, but the resource groups can hold only 480).

More information

- Connections and resources
- Create machine catalogs
- CTX219211: Set up a Microsoft Azure Active Directory 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

February 6, 2020

Follow this guidance if you use Hyper-V with Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

This release supports the VMM versions listed in System requirements.

You can use Citrix Provisioning (formerly Provisioning Services) and Machine Creation Services to provision:

- Generation 1 Desktop or Server OS VMs
- Generation 2 Windows Server 2012 R2, Windows Server 2019, Windows Server 2016, and Windows 10 VMs (with or without Secure Boot)

Install and configure a hypervisor

> **Important:**
>
> All Delivery Controllers must be in the same forest as the VMM servers.

1. Install Microsoft Hyper-V server and VMM on your servers.
2. Install the System Center Virtual Machine Manager console on all Controllers. 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.
3. Verify the following account information:

   The account you use to specify hosts in Studio is a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account only has the delegated administrator role in VMM, the storage data is not listed in Studio during the host creation process.

The user account used for Studio integration must also be a member of the administrators local security group on each Hyper-V server to support VM life cycle management (such as VM creation, update, and deletion).

Installing a Controller on a server running Hyper-V is not supported.

Create a master VM

1. Install a VDA on the master VM, and select the option to optimize the desktop. This improves performance.
2. Take a snapshot of the master VM to use as a backup.

Create virtual desktops

If you are using MCS to create VMs, when creating a Site or a connection:

1. Select the Microsoft virtualization host type.
2. Enter the address as the fully qualified domain name of the host server.
3. Enter the credentials for the administrator account you set up earlier that has permissions to create new VMs.
4. In **Host Details**, select the cluster or standalone host to use when creating new VMs.

   Browse for and select a cluster or standalone host even if you are using a single Hyper-V host deployment.

MCS on SMB 3 file shares

For machine catalogs created with MCS on SMB 3 file shares for VM storage, ensure that credentials meet the following requirements so that calls from the Controller's Hypervisor 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 life cycle events are performed through the Hyper-V server using the VMM user credentials.

When you use SMB as storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Controller to individual Hyper-V machines when using VMM 2012 SP1 with Hyper-V on Windows Server 2012. For more information, see CTX137465.

Using a standard PowerShell V3 remote session, the HCL 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 and are then sent to the Hyper-V machine to act on the SMB 3.0 storage.

- **Consolidate master image**: A master 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 difference disk:** Creates a difference disk from the master image generated by consolidating the master image. The difference 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 Controller, the HCL must first copy the identity disk through the Hyper-V machine as follows.

  The HCL uploads the Identity to the Hyper-V machine through the administrator share.

  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).

  The HCL deletes the file from the administrator share.

  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 it is deleted so that it is available for reuse.

- **Download identity disks:** As with uploads, the identity disks pass though the Hyper-V machine to the HCL. The following process creates a folder that only has VMM user permissions on the Hyper-V server if it does not exist.

  The Hyper-V machine copies the disk from the SMB storage to local Hyper-V storage through a PowerShell script running in the PowerShell V3 remote session.

  HCL reads the disk from the Hyper-V machine's administrator share into memory.

  HCL deletes the file from the administrator share.

- **Personal vDisk creation:** If the administrator creates the VM in a Personal vDisk machine catalog, you must create an empty disk (PvD).

  The call to create an empty disk does not require direct access to the storage. If you have PvD disks that reside on different storage than the main or operating system disk, then the use remote PowerShell to create the PvD in a directory folder that has the same name of the VM from which it was created. For CSV or LocalStorage, do not use remote PowerShell. Creating the directory before creating an empty disk avoids VMM command failure.

  From the Hyper-V machine, perform a mkdir on the storage.

Citrix Hypervisor virtualization environments

April 16, 2024

Create a connection to Citrix Hypervisor

When you create a connection to Citrix Hypervisor (formerly XenServer), you must provide the credentials for a VM Power Admin or higher-level user.

Citrix recommends using HTTPS to secure communications with Citrix Hypervisor. To use HTTPS, you must replace the default SSL certificate installed on Citrix Hypervisor; see CTX128656.

You can configure high availability if it is enabled on the Citrix Hypervisor server. Citrix recommends that you select all servers in the pool (from Edit High Availability) to allow communication with the Citrix Hypervisor server if the pool master fails.

You can select a GPU type and group, or pass through, if the Citrix Hypervisor supports vGPU. The display indicates if the selection has dedicated GPU resources.

When using local storage on one or more Citrix Hypervisor 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.)

Use IntelliCache for Citrix Hypervisor 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.

- 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, you must enable it in both this product and Citrix Hypervisor.

- When installing Citrix Hypervisor, select **Enable thin provisioning (Optimized storage for Virtual Desktops)**. Citrix does not support mixed pools of servers that have IntelliCache enabled and servers that do not. For more information, see the Citrix Hypervisor documentation.
- In Citrix Virtual Apps and Desktops, IntelliCache is disabled by default. You can change the setting only when creating a Citrix Hypervisor connection; you cannot disable IntelliCache later. When you add a Citrix Hypervisor connection:
  - Select **Shared** as the storage type.
  - Select the **Use IntelliCache** check box.

Required Citrix Hypervisor permissions

The Citrix Hypervisor permissions are role-based (RBAC).

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.

Create a machine catalog using a Citrix Hypervisor connection

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.

More information

- Connections and resources
- Create machine catalogs

Microsoft System Center Configuration Manager environments

March 3, 2021

Sites using Microsoft System Center Configuration Manager (Configuration Manager) to manage access to applications and desktops can extend that use to Citrix Virtual Apps and Desktops using these options:

- Install VDAs using SCCM.
- **Configuration Manager Wake Proxy feature:** The Remote PC Access Wake on LAN feature requires Configuration Manager. For more information, see Remote PC Access - Wake on LAN.
- **Citrix Virtual Apps and Desktops properties:** Properties enable you to identify Citrix Virtual Desktops for management through Configuration Manager. (In some versions, Configuration Manager uses the former name of Citrix Virtual Apps and Desktops: XenApp and XenDesktop.)

Properties

Properties are available to Microsoft System Center Configuration Manager to manage virtual desktops.

Boolean properties displayed in Configuration Manager may appear as `1` or `0`, not true or false.

The properties are available for the `Citrix_virtualDesktopInfo` class in the `Root\Citrix\DesktopInformation` namespace. Property names come from the Windows Management Instrumentation (WMI) provider.

Property	Description
`AssignmentType`	Sets the value of IsAssigned. Valid values are: `ClientIP`, `ClientName`, `None`, and `User` (sets `IsAssigned` to `True`).
`BrokerSiteName`	Site. Returns the same value as `HostIdentifier`.
`DesktopCatalogName`	Machine catalog associated with the desktop.
`DesktopGroupName`	Delivery group associated with the desktop.
`HostIdentifier`	Site. Returns the same value as `BrokerSiteName`.
`IsAssigned`	`True` to assign the desktop to a user, set to `False` for a random desktop
`IsMasterImage`	Allows decisions about the environment. For example, you might install applications on the image and not on the provisioned machines, especially if those machines are in a clean state on boot machines. Valid values are: `True` on a VM that is used as an image (this value is set during installation based on a selection), or cleared on a VM provisioned from that image.
`IsVirtualMachine`	`True` for a virtual machine, **`false`** for a physical machine.
`OSChangesPersist`	`False` if the desktop operating system image is reset to a clean state every time it is restarted; otherwise, **`true`**.
`PersistentDataLocation`	The location where Configuration Manager stores persistent data. This location is not accessible to users.
`PersonalvDiskDriveLetter`	For a desktop with a Personal vDisk, the drive letter you assign to the Personal vDisk.
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	Determined when the desktop registers with the Controller. They are null for a desktop that has not fully registered.

To collect the properties, run a hardware inventory in Configuration Manager. To view the properties, use the Configuration Manager Resource Explorer. In these instances, the names might include spaces or vary slightly from the property names. For example, `BrokerSiteName` might appear as `Broker Site Name`.

- Configure Configuration Manager to collect Citrix WMI properties from the Citrix VDA
- Create query-based device collections using Citrix WMI properties
- Create global conditions based on Citrix WMI properties
- Use global conditions to define application deployment type requirements

You can also use Microsoft properties in the Microsoft class `CCM_DesktopMachine` in the `Root\ccm_vdi` namespace. For more information, see the Microsoft documentation.

VMware virtualization environments

June 7, 2024

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.)

If you plan to use MCS, do not disable the Datastore Browser feature in vCenter Server (described in https://kb.vmware.com/s/article/2101567). If you disable this feature, MCS does not work correctly.

Required privileges

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 Virtual Apps and Desktops operations and the minimum required VMware privileges.

> **Note:**
>
> The permissions list display name, specifically the *User Interface*, is different for some vSphere versions. For example, in vSphere 6.7 the *User Interface* permission is **Change Memory** and

> **Change Settings**, rather than **Settings** and **Memory** as described in the required privileges noted on this page.

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

SDK	User interface
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
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

Image update and rollback

SDK	User interface
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations

SDK	User interface
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
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:

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
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

SDK	User interface
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.

Create AppDisks

Valid for VMware vSphere minimum version 5.5 and XenApp and XenDesktop minimum version 7.8.

SDK	**User interface**
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
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.EditDevice	Virtual machine > Configuration > Modify Device Settings
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On

Delete AppDisks

Valid for VMware vSphere minimum version 5.5 and XenApp and XenDesktop minimum version 7.8.

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

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 Delivery Controller.

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the hosts 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 Delivery Controllers.
   b) On the Controller, 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 may need to 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 on the address bar displaying the certificate error.
   d) View the certificate and click the Details tab.
   e) Select **Copy to file and export in .CER format**, providing a name when prompted to do so.

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.

- Open your web browser and make a secure web connection to the vCenter server (for example https://server1.domain1.com).
- Accept the security warnings.
- Click on the address bar displaying the certificate error.
- View the certificate.

3. Import the certificate into the certificate store on each of your Controllers.

   a) Click **Install certificate**, select **Local Machine**, and then click **Next**.
   b) Select **Place all certificates in the following store**, and then click **Browse**. Select **Trusted People** and then click **OK**. Click **Next** and then click **Finish**.

   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.

Configuration considerations

Create a master VM:

Use a master VM to provide user desktops and applications in a machine catalog. On your hypervisor:

1. Install a VDA on the master VM, selecting the option to optimize the desktop, which improves performance.
2. Take a snapshot of the master VM to use as a back-up.

Create a connection:

In the connection creation wizard:

- Select the VMware connection type.
- Specify the address of the access point for the vCenter SDK.
- Specify the credentials for a VMware user account you set up earlier that has permissions to create new VMs. Specify the username in the form domain/username.

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 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 Virtual Apps and Desktops, even if not by the Controllers.

When creating a vSphere host connection in Studio, a dialog box allows you to view the certificate of the machine you are connecting to. You can then choose whether to trust it.

Nutanix virtualization environments

September 21, 2022

Follow this guidance when using Nutanix Acropolis to provide virtual machines in your Citrix Virtual Apps and Desktops deployment. The setup process includes the following tasks:

- Install and register the Nutanix plugin in your Citrix Virtual Apps and Desktops environment.
- Create a connection to the Nutanix Acropolis hypervisor.
- Create a machine catalog that uses a snapshot of a master image you created on the Nutanix hypervisor.

For more information, see the Nutanix Acropolis MCS Plugin Installation Guide, available at the Nutanix Support Portal.

Prepare to install the Nutanix MCS plugin for the Citrix Cloud connector

Nutanix Acropolis integration prerequisites for the Citrix Virtual Apps and Desktops Delivery Controller include:

- Users running the AHV MCS plugin for the Citrix Cloud Connector installer must have administrator privileges on the Citrix Cloud Connector VM.
- Register the Citrix Cloud Connector VM with a resource location in the Citrix Cloud tenant.
- Install the AHV MCS plugin for the Citrix Cloud Connector on all Cloud Connectors registered with the Citrix Cloud tenant. Perform this installation even if the connectors serve a resource location without the AHV.

Install and register the Nutanix plugin

After you install the Citrix Virtual Apps and Desktops components, complete the following procedure to install and register the Nutanix plugin on the Delivery Controllers. You will then be able to use Studio to create a connection to the Nutanix hypervisor and then create a machine catalog that uses a snapshot of a master image you created in the Nutanix environment.

1. Obtain the Nutanix plugin from Nutanix, and install it on the Delivery Controllers.
2. Verify that a Nutanix Acropolis folder has been created in C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Run `C:\\Program Files\\Common Files\\Citrix\\HCLPlugins\\RegisterPlugins.exe –PluginsRoot "C:\\Program Files\\Common Files\\Citrix\\HCLPlugins\\CitrixMachineCreation\\v1.0.0.0"`.
4. Restart the Citrix Host Service, Citrix Broker Service, and Citrix Machine Creation Services.
5. Run the following PowerShell cmdlets to verify that the Nutanix Acropolis plugin has been registered:

```
Add-PSSnapin Citrix\*
Get-HypHypervisorPlugin
<!--NeedCopy-->
```

Create a connection to Nutanix

See Create a Site or Connections and resources for complete information about all pages in the wizards that create a connection.

In the Site Setup or Add Connection and Resources wizard, select the **Nutanix** connection type on the **Connection** page, and then specify the hypervisor address and credentials, plus a name for the connection. On the **Network** page, select a network for the hosting unit.

Create a machine catalog using a Nutanix snapshot

This information is a supplement to the guidance in the Create machine catalogs article. It describes only the fields that are unique to Nutanix.

The snapshot you select is the template that is used to create the VMs in the catalog. Before creating the catalog, create images and snapshots in Nutanix.

- For information about master images in general, see the Create machine catalogs article.
- For Nutanix procedures for creating images and snapshots, see the Nutanix documentation referenced above.

The **Operating System** and **Machine Management** pages do not contain Nutanix-specific information. Follow the guidance in the Create machine catalogs article.

On the **Container** page, which is unique to Nutanix, select the container where the VMs' disks will be placed.

On the **Master Image** page, select the image snapshot. Acropolis snapshot names must be prefixed with "XD_"to be used in Citrix Virtual Apps and Desktops. Use the Acropolis console to rename your snapshots, if needed. If you rename snapshots, restart the Create Catalog wizard to see a refreshed list.

On the **Virtual Machines** page, indicate the number of virtual CPUs and the number of cores per vCPU.

The **Network Cards**, **Computer Accounts**, and **Summary** pages do not contain Nutanix-specific information. Follow the guidance in the Create machine catalogs article.

Microsoft Azure virtualization environments

April 22, 2022

> **NOTE:**
>
> This article contains Azure (Classic) information. For Azure Resource Manager information, see Microsoft Azure Resource Manager virtualization environments.

Connection configuration

When using Studio to create a Microsoft Azure connection, you need information from the Microsoft Azure Publish Settings file. The information in that XML file for each subscription looks similar to the sample below (your actual management certificate will be much longer):

```
\<Subscription
ServiceManagementUrl="*address*"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl;
   sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
<!--NeedCopy-->
```

The following procedure assumes you are creating a connection from Studio, and have launched either the Site creation wizard or the connection creation wizard.

1. In a browser, go to https://manage.windowsazure.com/publishsettings/index.
2. Click the Cloud Shell icon next to the search box and follow the instructions to download the Publish Settings file.
3. In Studio, on the **Connection** page of the wizard, after you select the Microsoft Azure connection type, click **Import**.
4. If you have more than one subscription, you are prompted to select the subscription you want.

The ID and certificate are automatically and silently imported into Studio.

Power actions using a connection are subject to thresholds. Generally, the default values are appropriate and should not be changed. However, you can edit a connection and change them (you cannot change these values when you create the connection). For details, see Edit connection settings.

Virtual machines

When creating a machine catalog in Studio, selecting the size of each virtual machine depends on the options presented by Studio, the cost and performance of the selected VM instance type, and scalability.

Studio presents all of the VM instance options that Microsoft Azure makes available in a selected region; Citrix cannot change this presentation. Therefore, you should be familiar with your applications and their CPU, memory, and I/O requirements. Several choices are available at difference price and performance points; see the following Microsoft articles to better understand the options.

- Virtual Machine and Cloud Service Sizes for Azure: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-sizes-specs
- Virtual Machine Pricing: http://azure.microsoft.com/en-us/pricing/details/virtual-machines

Basic tier: VMs prefixed with "Basic"represent the basic disk. They are limited primarily by the Microsoft supported IOPS level of 300. These are not recommended for Desktop OS (VDI) or Server OS RDSH (Remote Desktop Session Host) workloads.

Standard tier: Standard tier VMs appear in four series: A, D, DS, and G.

Series	Appear in Studio as
A	Extra small, small, medium, large, extra large, A5, A6, A7, A8, A9, A10, A11. Medium and large are recommended to test using Desktop OS (VDI) or Server OS (RDSH) workloads, respectively.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. These VMs offer SSD for temporary storage.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. These VMs offer local SSD storage for all disks.
G	Standard_G1 –G5. These VMs are for high performance computing.

When provisioning machines in Azure premium storage, be sure to select a machine size that is supported in the premium storage account.

Cost and performance of VM instance types

For US list pricing, the cost of each VM instance type per hour is available at http://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

When working with cloud environments, it is important to understand your actual computing requirements. For proof of concept or other testing activities, it can be tempting to leverage the high-performance VM instance types. It may also be tempting to use the lowest-performing VMs to save on costs. The better goal is to use a VM appropriate for the task. Starting with the best-performing may not get the results you need, and will become very expensive over time - in some cases, within a week. For lower-performing VM instance types with a lower cost, the performance and usability may not be appropriate for the task.

For Desktop OS (VDI) or Server OS (RDSH) workloads, testing results using LoginVSI against its medium workload found that instance types Medium (A2) and Large (A3) offered the best price/performance ratio.

Medium (A2) and Large (A3 or A5) represent the best cost/performance for evaluating workloads. Anything smaller is not recommended. More capable VM series may offer your applications or users the performance and usability they demand; however, it is best to baseline against one of these three instance types to determine if the higher cost of a more capable VM instance type provides true value.

Scalability

Several constraints affect the scalability of catalogs in a hosting unit. Some constraints, such as the number of CPU cores in an Azure subscription, can be mitigated by contacting Microsoft Azure support to increase the default value (20). Others, such as the number of VMs in a virtual network per subscription (2048), cannot change.

Currently, Citrix supports 1000 VMs in a catalog.

To scale up the number of VMs in a catalog or a host, contact Microsoft Azure support. The Microsoft Azure default limits prevent scaling beyond a certain number of VMs; however, this limit changes often, so check the latest information: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits.

A Microsoft Azure virtual network supports up to 2048 VMs.

Microsoft recommends a limit of 40 standard disk VM images per cloud service. When scaling, consider the number of cloud services required for the number of VMs in the entire connection. Also consider VMS needed to provide the hosted applications.

Contact Microsoft Azure support to determine if the default CPU core limitations must be increased to support your workloads.

Install core components

May 7, 2020

The core components on the installation media are the Citrix Delivery Controller, Citrix Studio, Citrix Director, and Citrix License Server.

(In versions before 1912 LTSR CU1, core components included StoreFront. You can still install StoreFront by choosing **Citrix StoreFront** from the **Extend Deployment** section, or by running the command available on the installation media.)

Before you start an installation, review this article and Prepare to install.

This article describes the installation wizard sequence when installing core components. Command-line equivalents are provided. For more information, see Install using the command line.

Step 1. Download the product software and launch the wizard

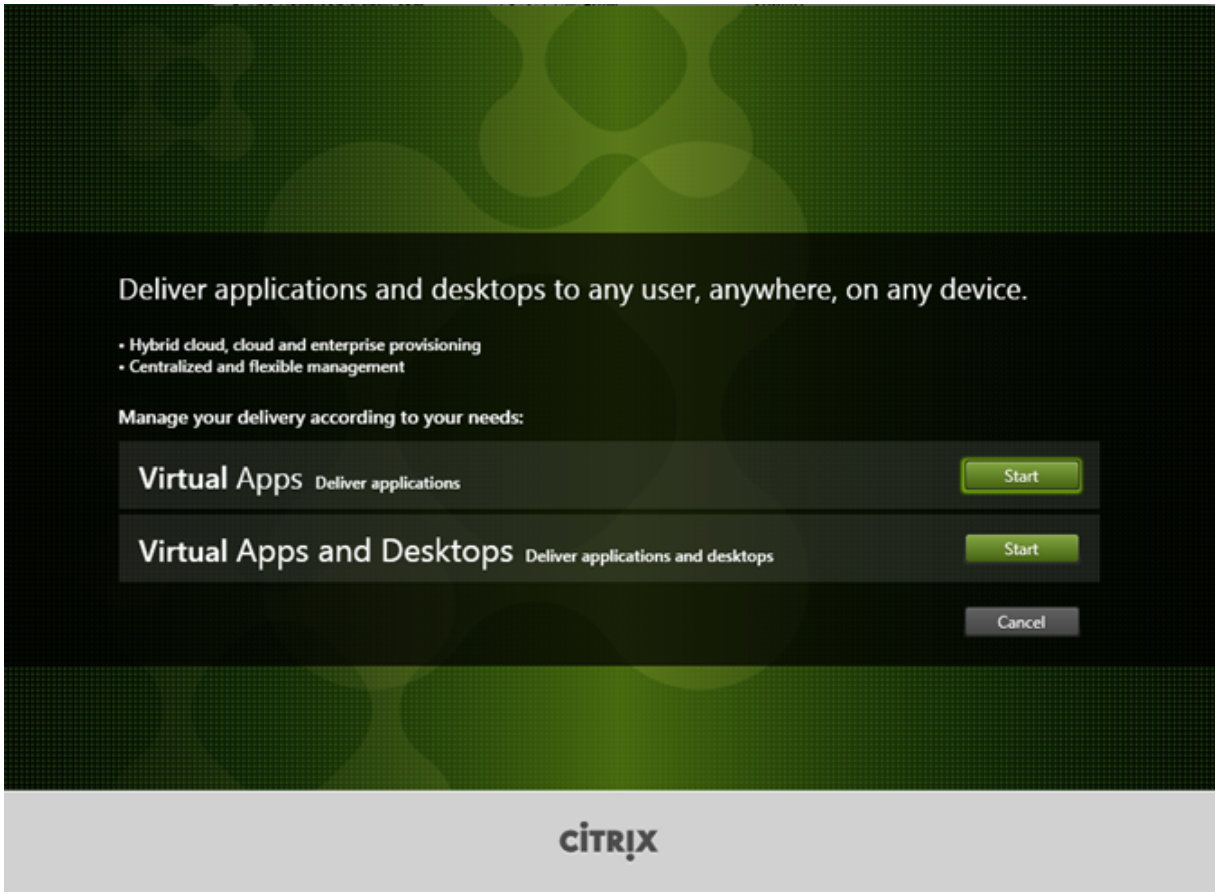
Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page. Download the product ISO file.

Unzip the file. Optionally, burn a DVD of the ISO file.

Log on to the machine where you are installing the core components, using a local administrator account.

Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.

Step 2. Choose which product to install

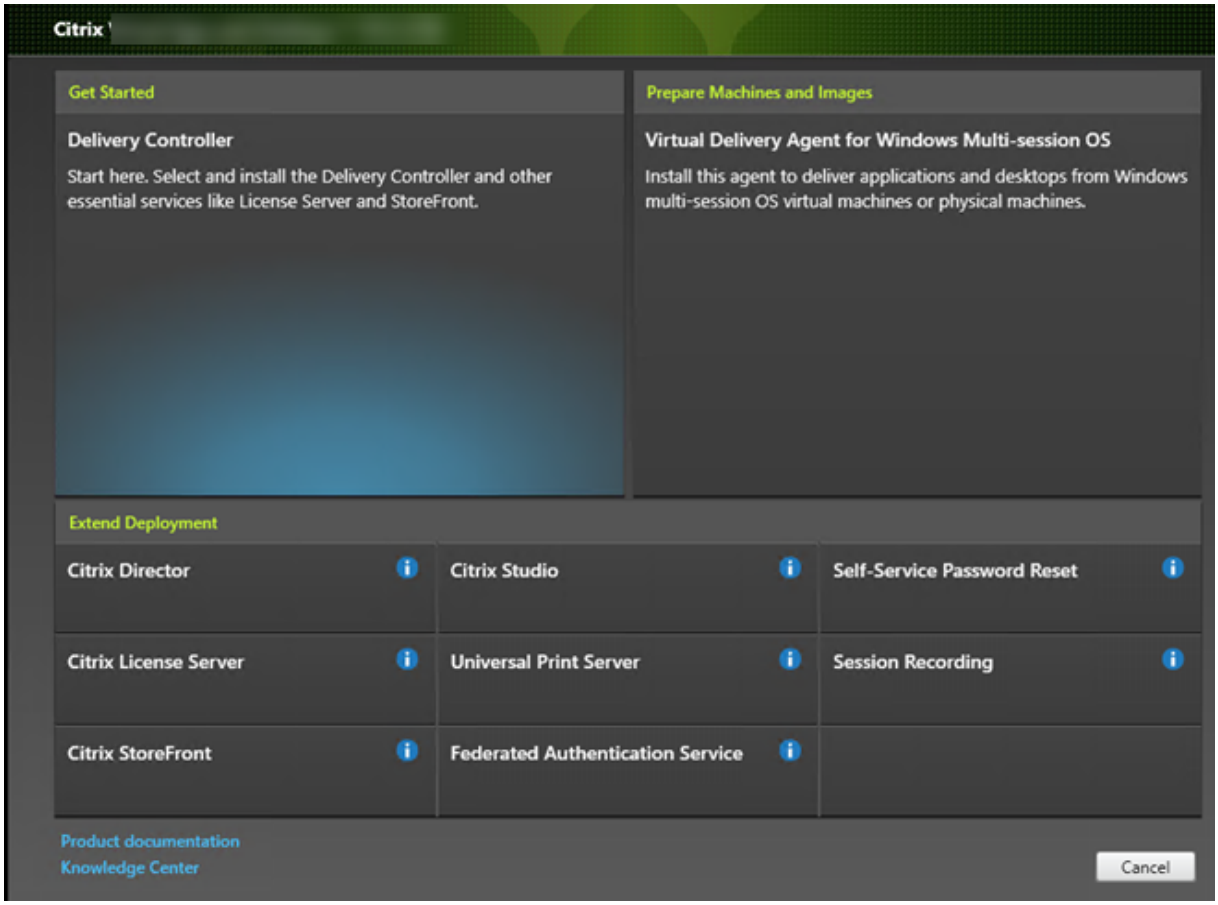


Click **Start** next to the product to install: Virtual Apps or Virtual Apps and Desktops.

(If the machine already has Citrix Virtual Apps and Desktops components installed on it, this page does not appear.)

Command-line option: /xenapp to install Citrix Virtual Apps; Citrix Virtual Apps and Desktops is installed if option is omitted

Step 3. Choose what to install

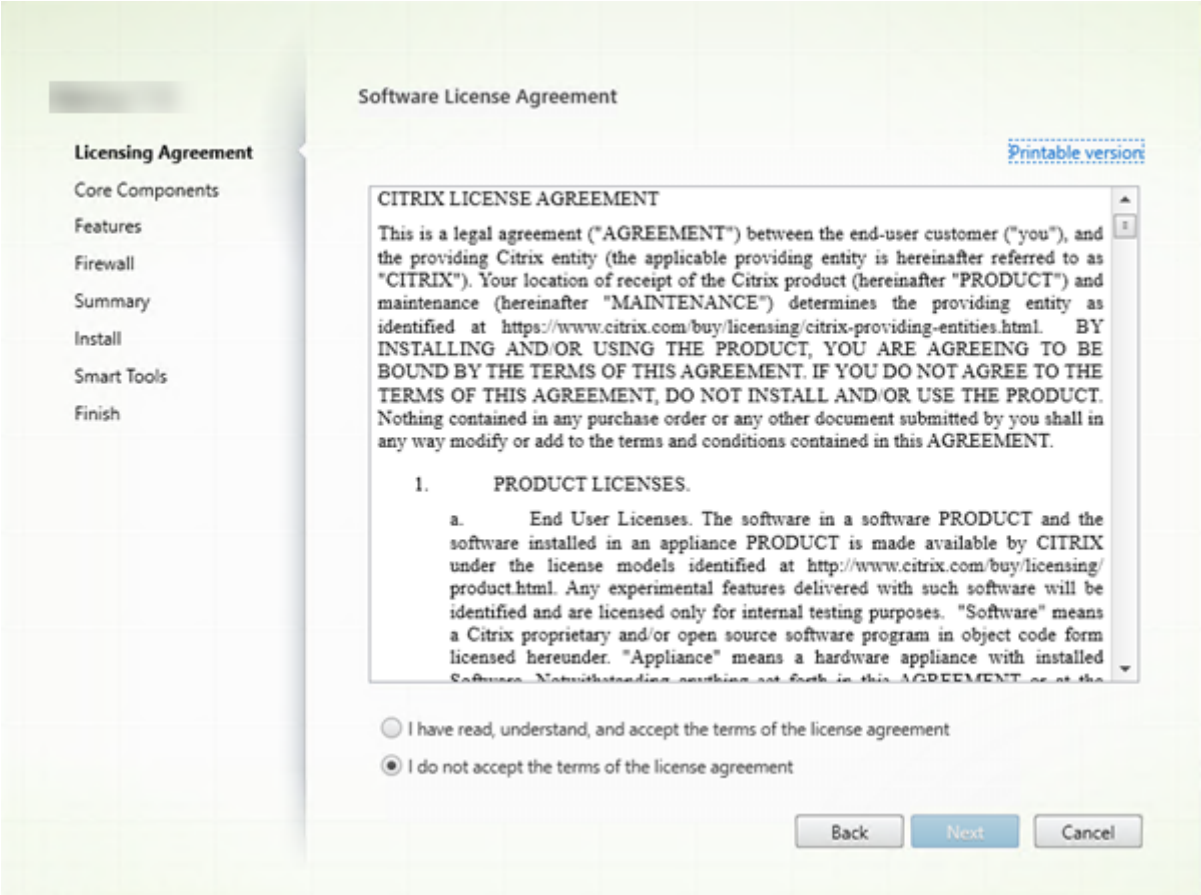


If you're just getting started, select **Delivery Controller**. (On a later page, you select the specific components to install on this machine.)

If you've already installed a Controller (on this machine or another) and want to install another component, select the component from the **Extend Deployment** section.

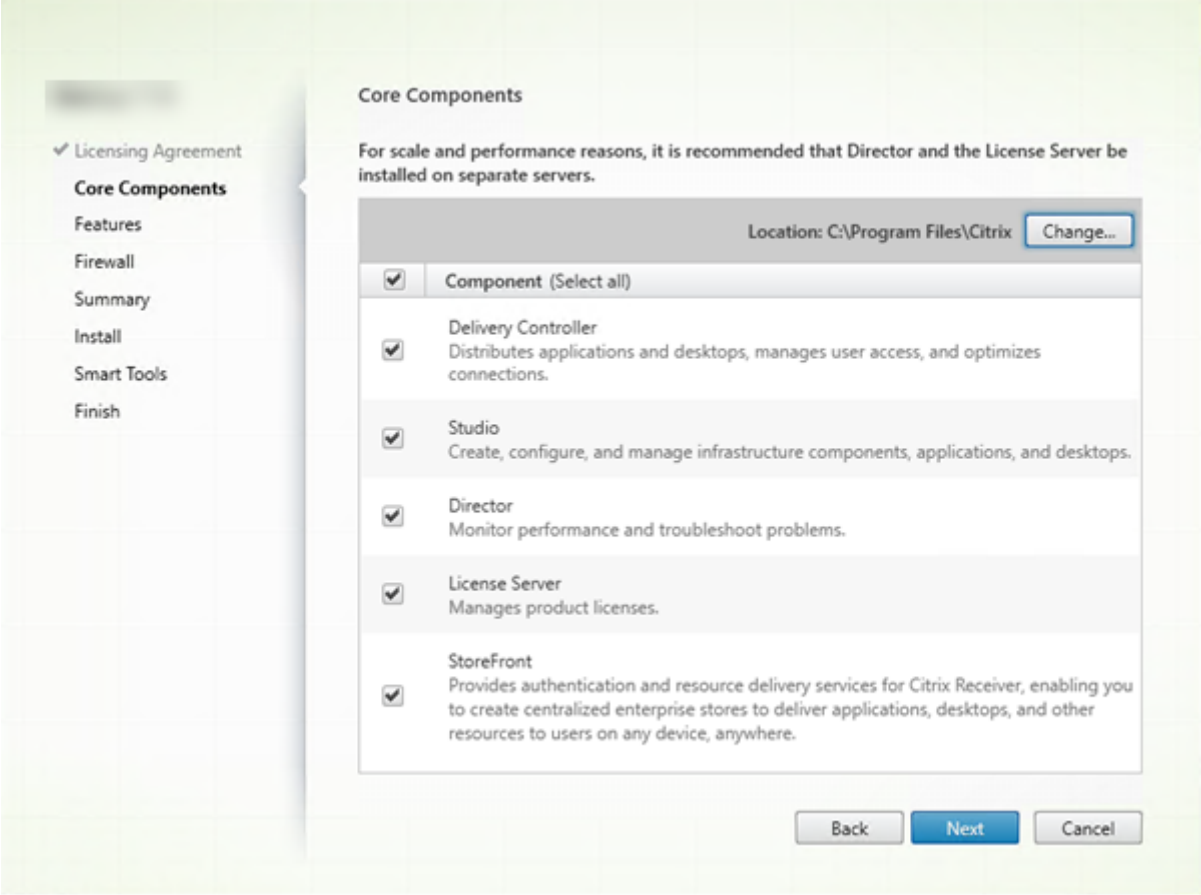
Command-line option: `/components`

Step 4. Read and accept the license agreement



On the **Licensing Agreement** page, after you read the license agreement, indicate that you have read and accepted it. Then click **Next**.

Step 5. 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. The default is fine for most deployments. If you specify a different location, it must have execute permissions for network service.
- **Components:** By default, the check boxes for all core components are selected. Installing all of the core components on one server is fine for proof of concept, test, or small production deployments. For larger production environments, Citrix recommends installing Director, StoreFront, and the License Server on separate servers.

  Select only the components you want to install on this machine. After you install components on this machine, you can run the installer again on other machines to install other components.

  An icon alerts you when you choose not to install a required core component on this machine. That alert reminds you to install that component, although not necessarily on this machine.

Click **Next**.

Command-line options: `/installdir`, `/components`, `/exclude`

Hardware check

When you install or upgrade a Delivery Controller, the hardware is checked. The installer alerts you if the machine has less than the recommended amount of RAM (5 GB), which can affect site stability. (For more information, see Hardware requirements.)

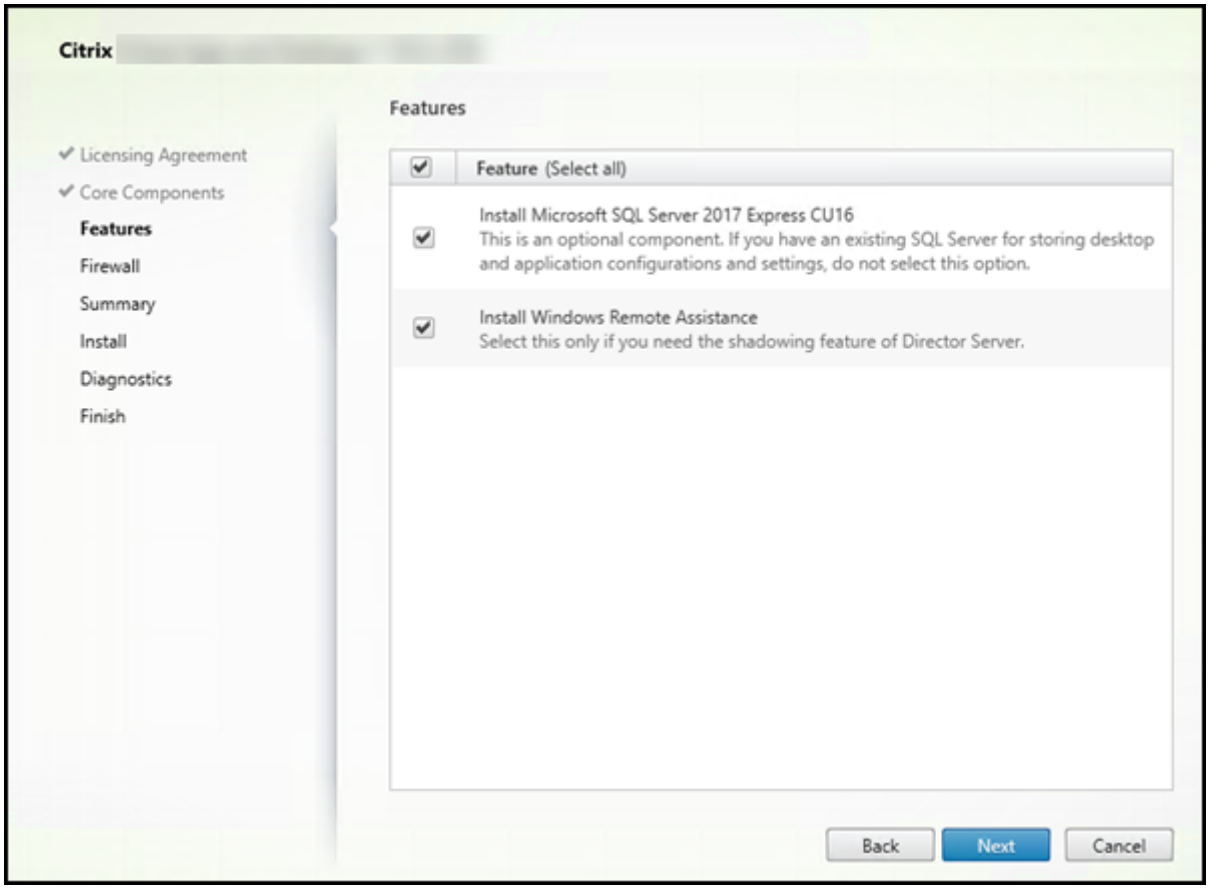
Graphical interface: A dialog box appears.

- Recommended: Click **Cancel** to stop the installation. Add more RAM to the machine and then start the installation again.
- Alternatively, click **Next** to continue with the installation. The site might have stability issues.

Command-line interface: The install/upgrade ends. The install logs contain a message that describes what was found and the available options.

- Recommended: Add more RAM to the machine and then run the command again.
- Alternatively, run the command again with the `/ignore_hw_check_failure` option to override the warning. Your site might have stability issues.

Step 6. Enable or disable features



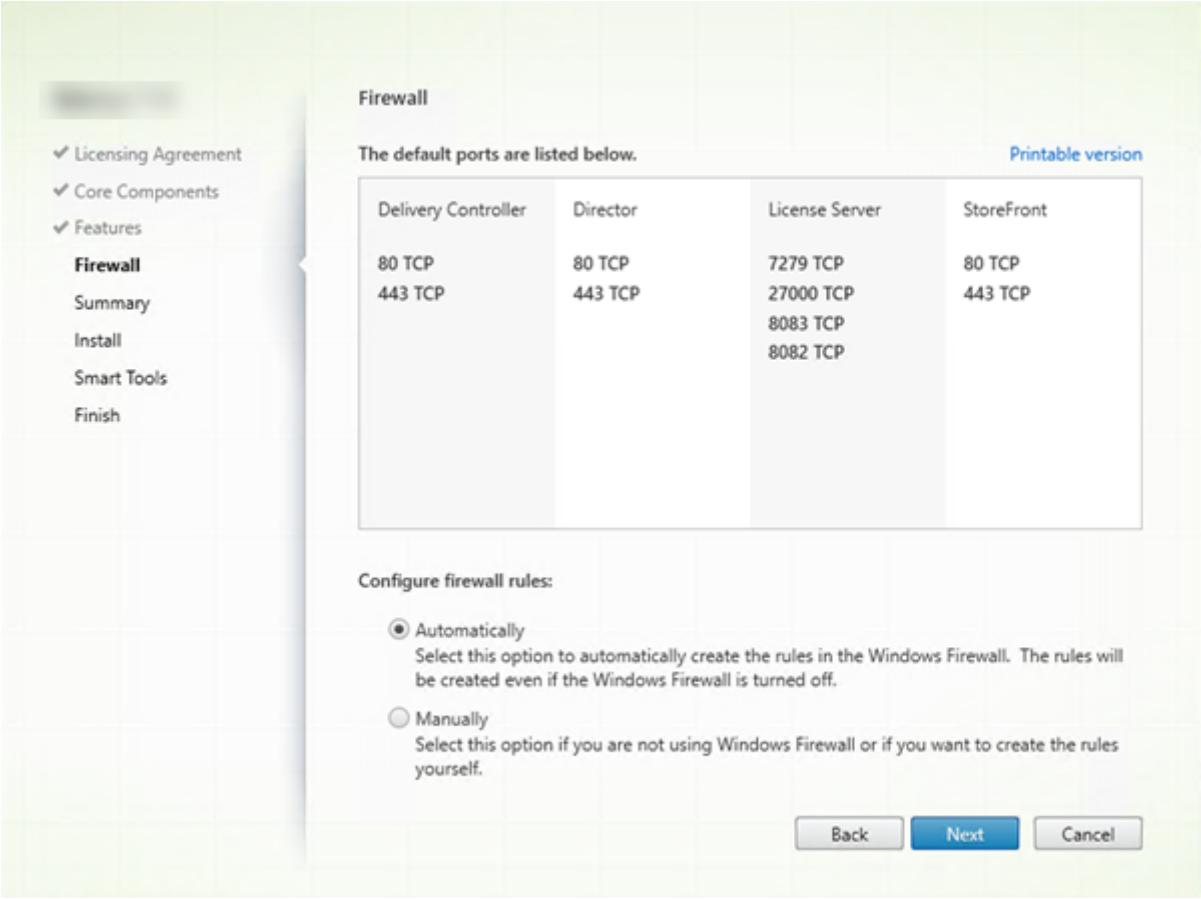
On the **Features** page:

- Choose whether to install Microsoft SQL Server Express for use as the Site database. By default, this selection is enabled. If you're not familiar with the Citrix Virtual Apps and Desktops databases, review Databases.
- When you install Director, Windows Remote Assistance is installed automatically. You choose whether to enable shadowing in Windows Remote Assistance for use with Director user shadowing. Enabling shadowing opens TCP port 3389. By default, this feature is enabled. The default setting is fine for most deployments. This feature appears only when you are installing Director.

Click **Next**.

Command-line options: `/nosql` (to prevent installation), `/no_remote_assistance` (to prevent enabling)

Step 7. Open Windows firewall ports



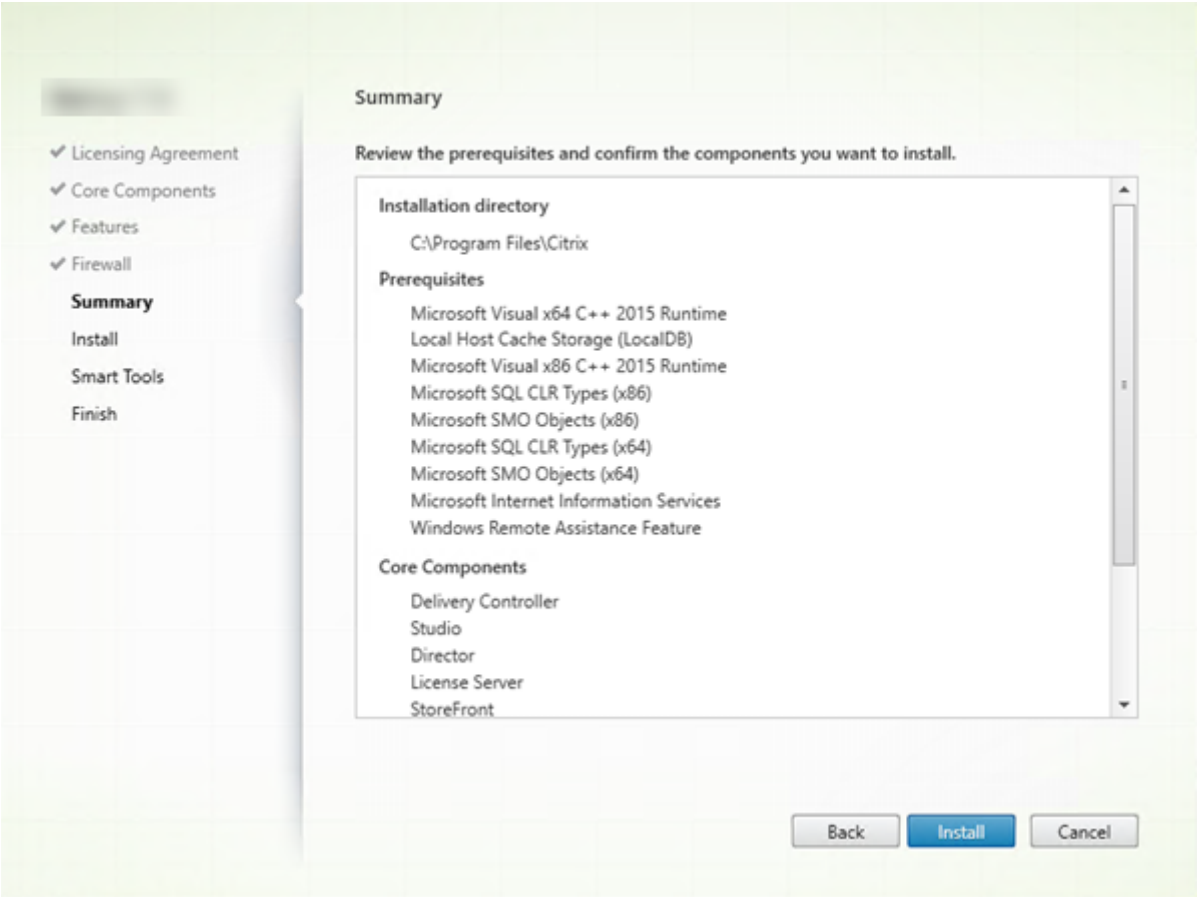
By default, the ports on the **Firewall** page are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. The default setting is fine for most deployments. For port information, see Network ports.

Click **Next**.

(The graphic shows the port lists when you install all the core components on this machine. That type of installation is usually done only for test deployments.)

Command-line option: `/configure_firewall`

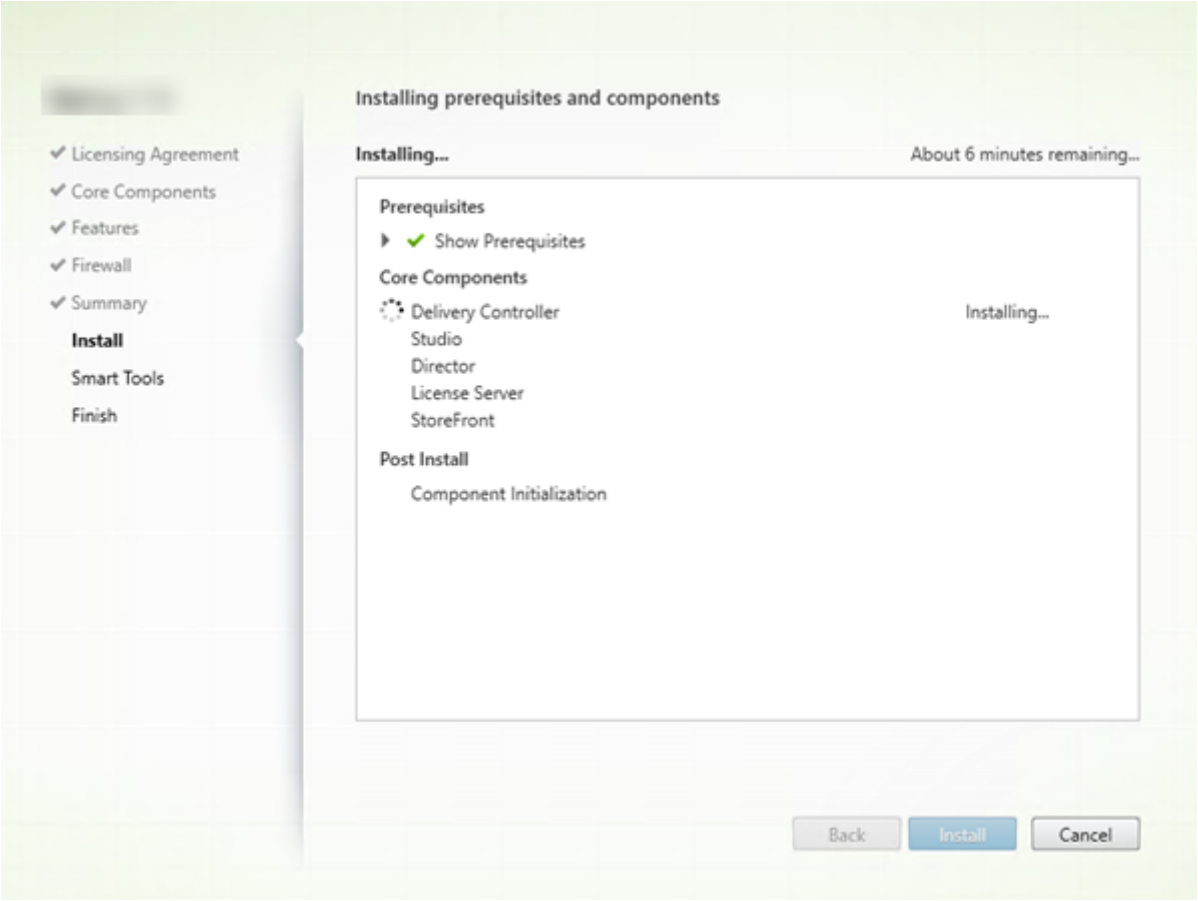
Step 8. Review prerequisites and confirm installation



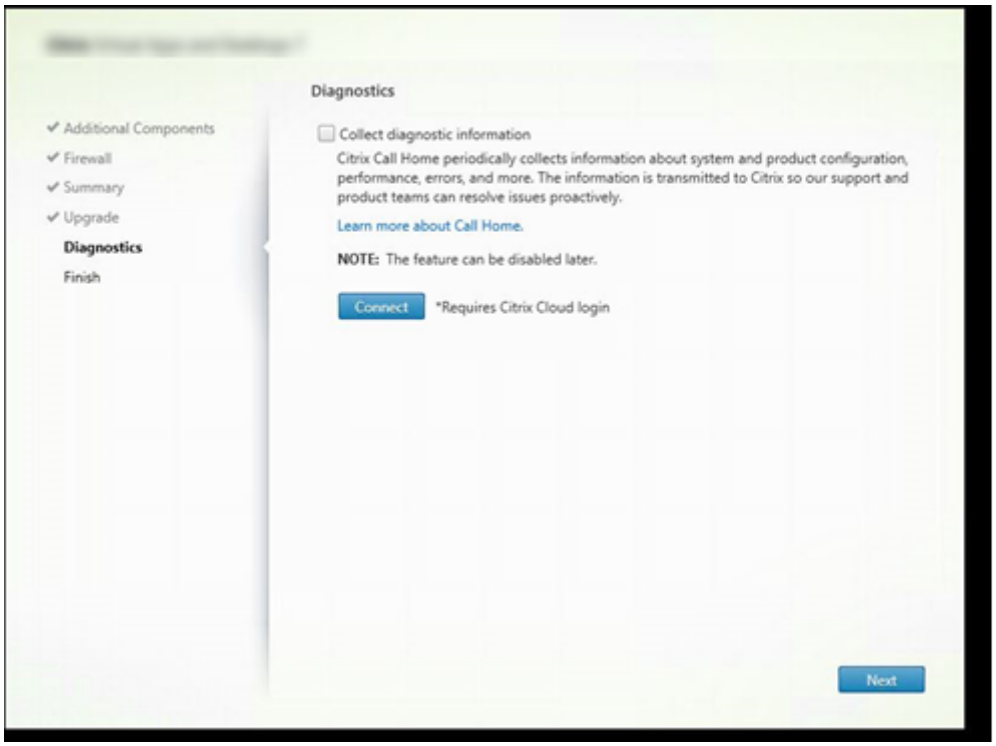
The **Summary** page lists what will be installed. Use the Back button to return to earlier wizard pages and change selections, if needed.

When you're ready, click **Install**.

The display shows the progress of the installation:



Step 9. Diagnostics



On the **Diagnostics** page, choose whether to participate in Citrix Call Home.

This page appears when installing a Delivery Controller using the graphical interface. When you install StoreFront (but not a Controller), the wizard displays this page. When you install other core components (but not a Controller or StoreFront), the wizard does not display this page.

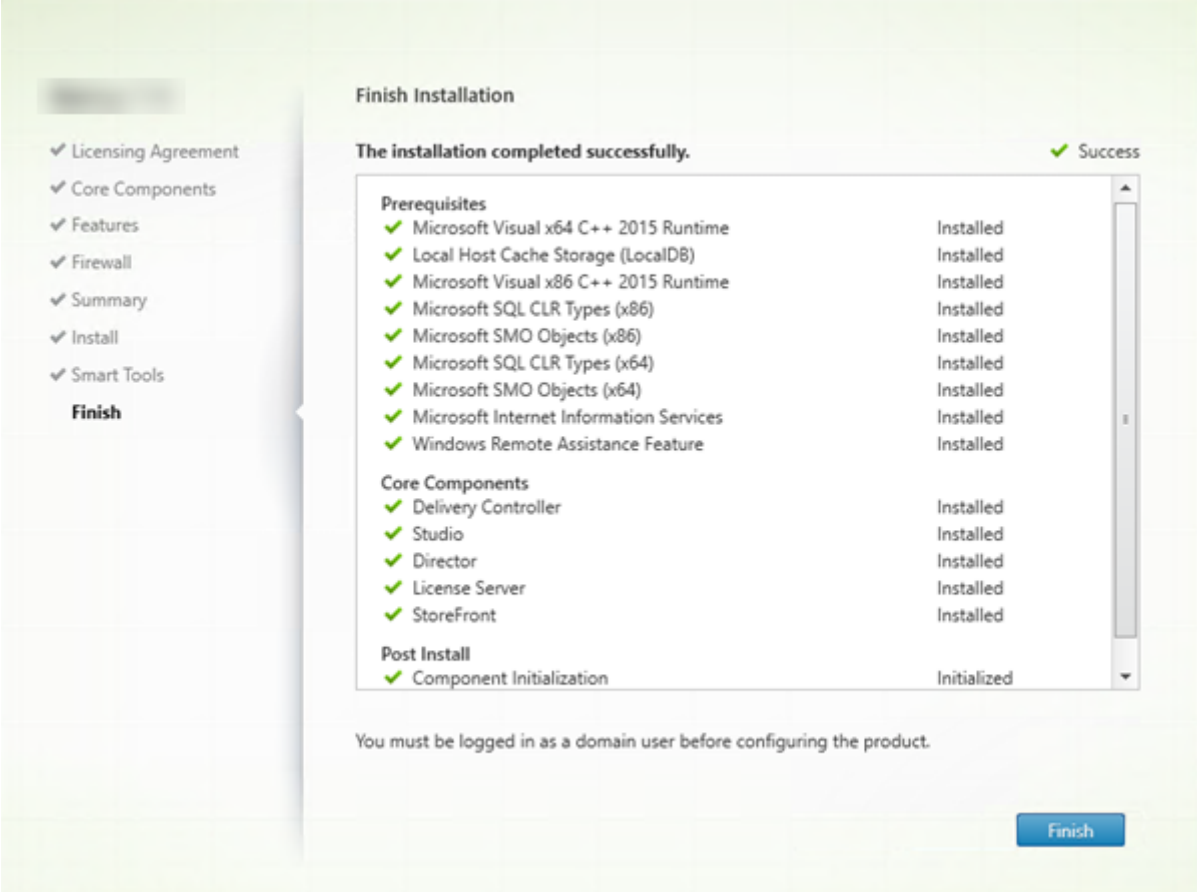
During an upgrade, this page does not appear if Call Home is already enabled or if the installer encounters an error related to the Citrix Telemetry Service.

If you choose to participate (the default), click **Connect**. When prompted, enter your Citrix account credentials. (You can change your enrollment choice later, after installation.)

After your credentials are validated (or if you choose not to participate), click **Next**.

For more information, see Call Home.

Step 10. Finish this installation



The **Finish** page contains green check marks for all prerequisites and components that installed and initialized successfully.

Click **Finish**.

Step 11. Install remaining core components on other machines

If you installed all the core components on one machine, continue with Next steps. Otherwise, run the installer on other machines to install other core components. You can also install more Controllers on other servers.

Next steps

After you install all the required core components, use Studio to create a site.

After creating the site, install VDAs.

At any time, you can use the full-product installer to extend your deployment with the following components:

- **Universal Print Server server component:** Launch the installer on your print server. Select **Universal Print Server** in the **Extend Deployment** section. Accept the license agreement. On the **Firewall** page, by default, TCP ports 7229 and 8080 are opened in the firewall if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable that default action if you want to open the ports manually.

  To install this component from the command line, see Install using the command line.
- Federated Authentication Service.
- Self-Service Password Reset.
- Session Recording.

Install VDAs

November 2, 2022

> **Important:**
>
> If you're upgrading a VDA that has Personal vDisk (PvD) installed, see Upgrade VDAs to 1912 or later.

There are two types of VDAs for Windows machines: VDA for multi-session OS and VDA for single OS. (For information about VDAs for Linux machines, see the Linux Virtual Delivery Agent documentation.)

Before starting an installation, review Prepare to install and complete all preparation tasks.

Before installing VDAs, you should have already installed the core components. You can also create the site before installing VDAs.

This article describes the installation wizard sequence when installing a VDA. Command-line equivalents are provided. For details, see Install using the command line.

Step 1. Download the product software and launch the wizard

If you're using the full-product installer:

1. If you haven't downloaded the product ISO yet:

- Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page. Download the product ISO file.
- Unzip the file. Optionally, burn a DVD of the ISO file.

2. Use a local administrator account on the image or machine where you're installing the VDA. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.

   The installation wizard launches.

If you're using a standalone package:

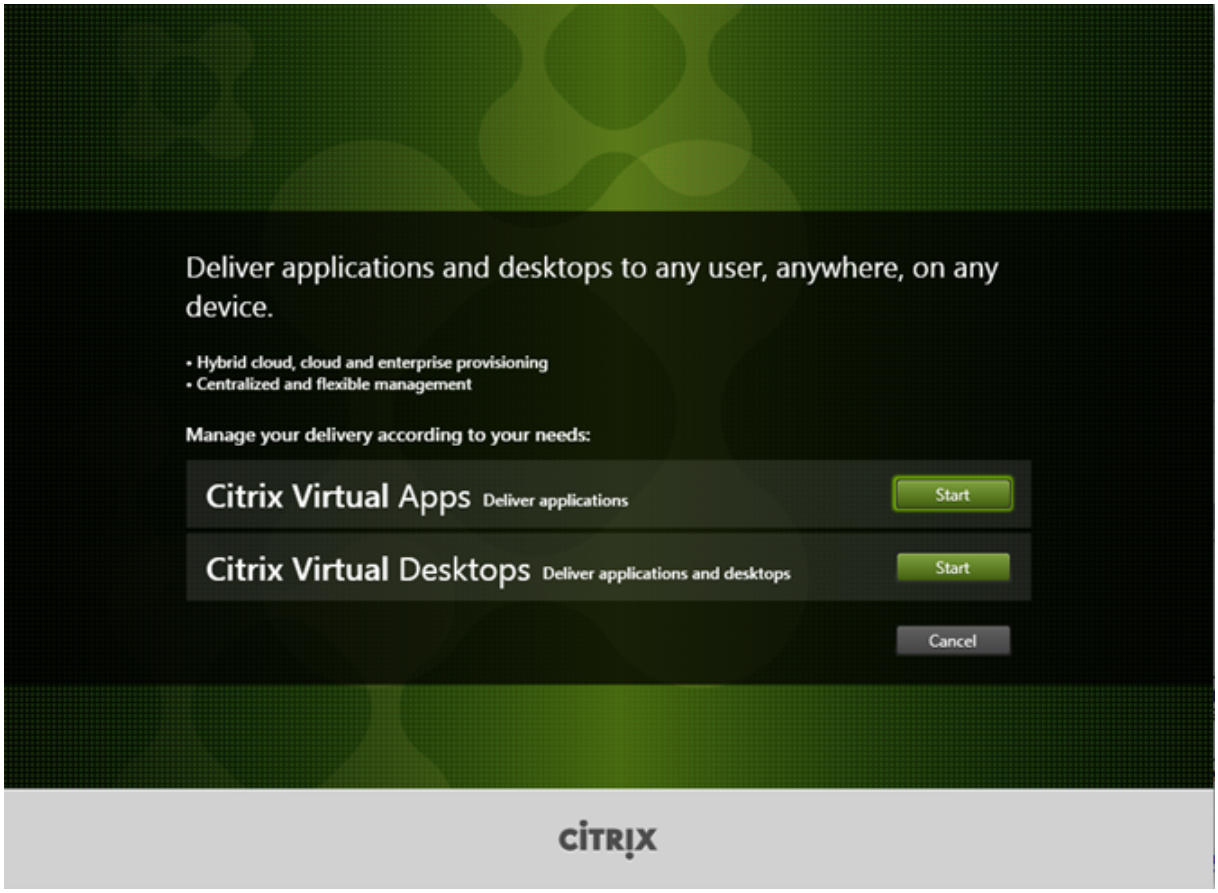
1. Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page. Download the appropriate package:

   - VDAServerSetup.exe: Multi-session OS VDA *version*
   - VDAWorkstationSetup.exe: Single-session OS VDA *version*
   - VDAWorkstationCoreSetup.exe: Single-session OS Core Services VDA *version*

2. Right-click the package and choose **Run as administrator.**

   The installation wizard launches.

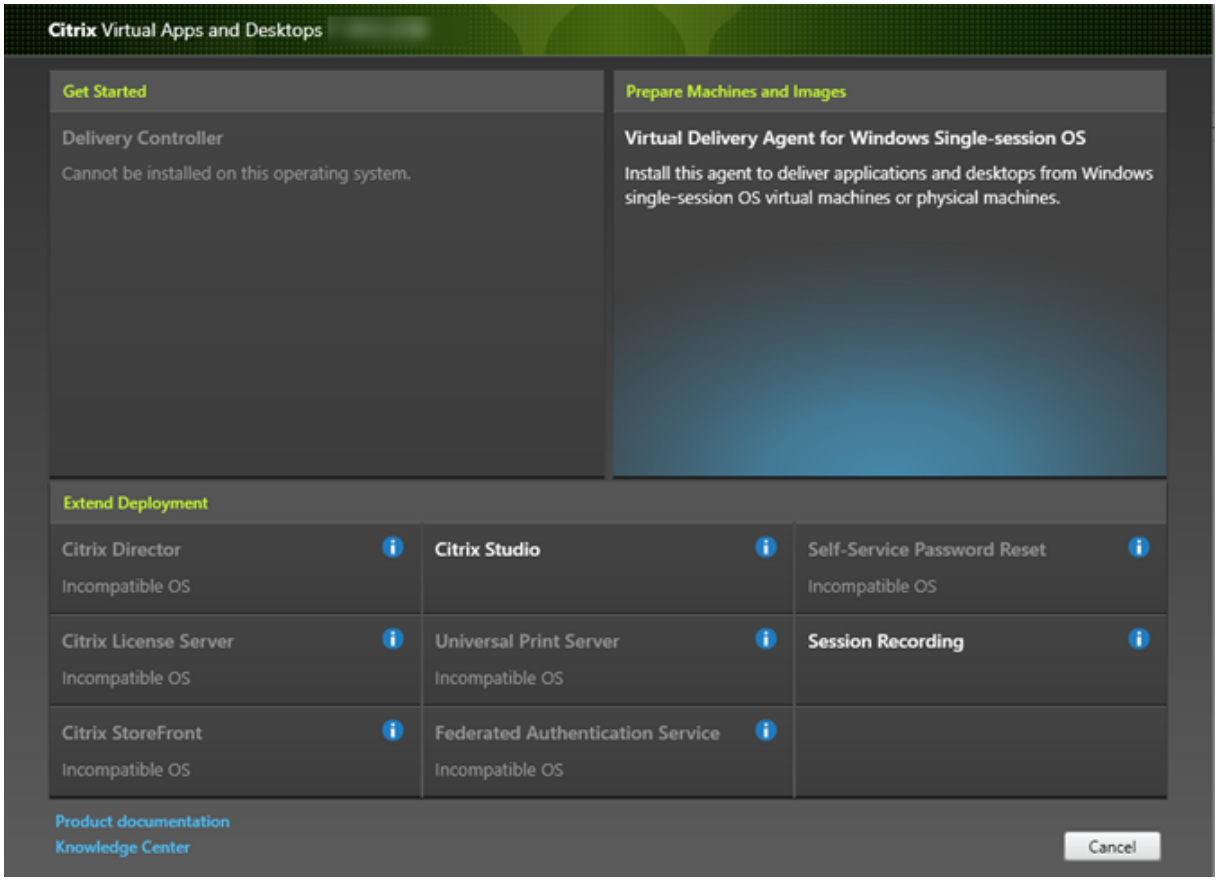
Step 2. Choose which product to install



Click **Start** next to the product to install: Citrix Virtual Apps or Citrix Virtual Desktops. (If the machine already has a Citrix Virtual Apps or Citrix Virtual Desktops component installed, this page does not appear.)

Command-line option: /xenapp to install Citrix Virtual Apps. Citrix Virtual Desktops is installed if option is omitted

Step 3. Select the VDA

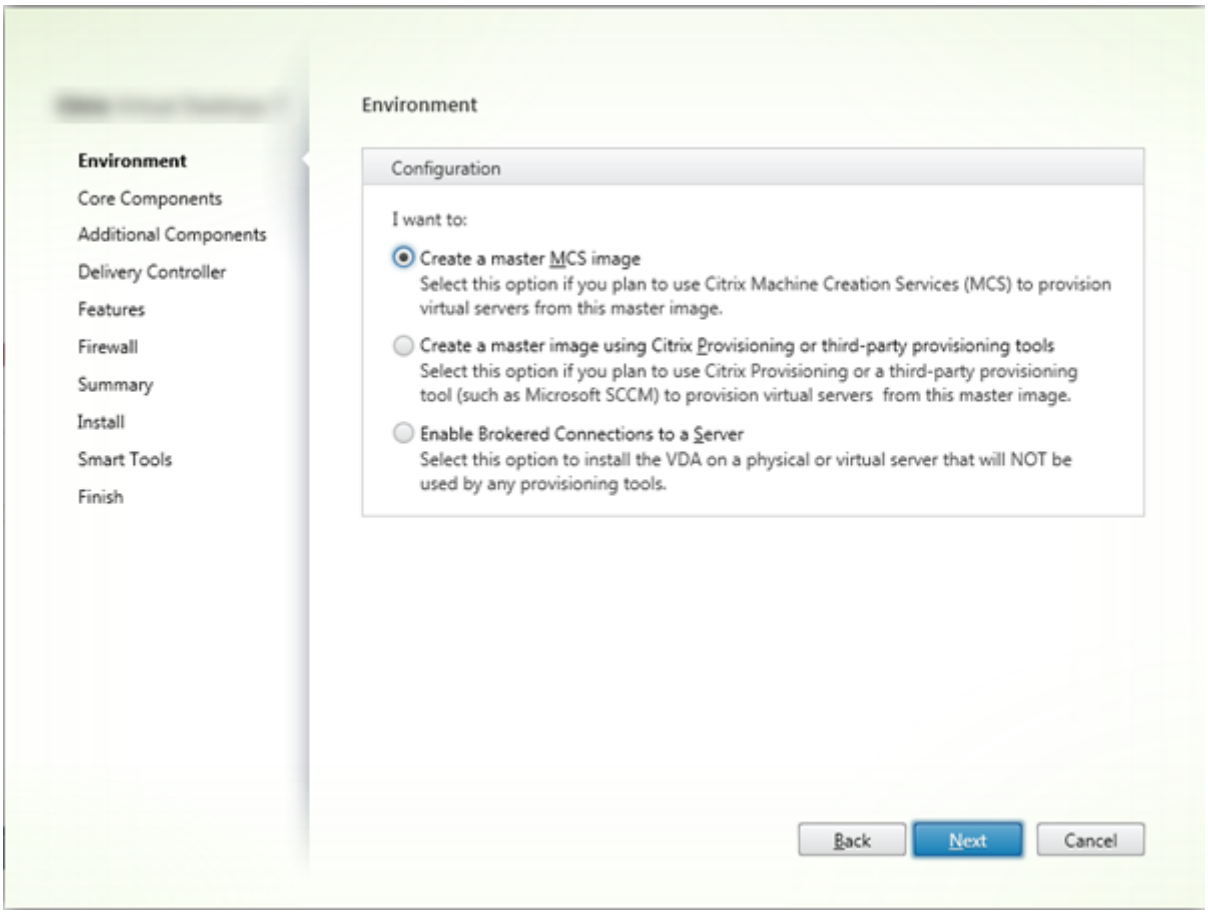


Select the **Virtual Delivery Agent** entry. The installer knows whether it's running on a singe-session or multi-session OS, so it offers only the appropriate VDA type.

For example, when you run the installer on a Windows Server 2016 machine, the VDA for multi-session OS option is available. The VDA for single-session OS option is not offered.

If you try to install (or upgrade to) a Windows VDA on an OS that is not supported for this Citrix Virtual Apps and Desktops version, a message guides you to information that describes your options.

Step 4. 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 a master image to provision additional 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.
Several MSIs (provisioning and other) are installed automatically when you install a VDA. The only way to prevent their installation is with the `/exclude` option in a command-line installation. For more information, see Install using the command line.

Choose one of the following:

- **Create a master MCS image:** Select this option to install a VDA on a VM master image, if you plan to use Machine Creation Services to provision VMs. This option installs the Machine Identity Service, which includes TargetOSOptimizer.exe. 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 master image, if you plan to use either Citrix Provisioning or third-party provisioning tools (such as Microsoft System Center Configuration Manager) to provision VMs. Command-line option: `/masterpvsimage`

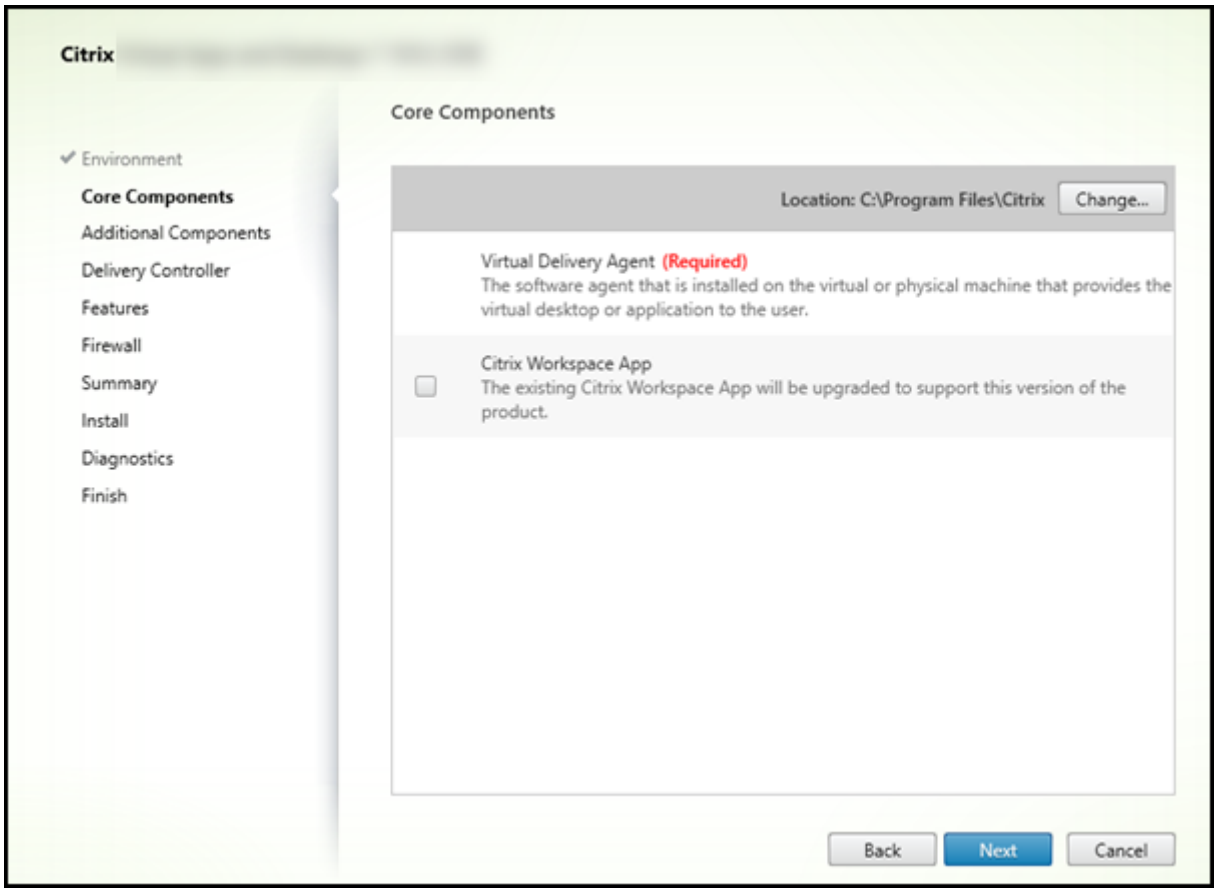
- (Appears only on multi-session OS machines) **Enable brokered connections to a server:** Select this option to install a VDA on a physical or virtual machine that will not be used as a master image to provision other machines. Command-line option: `/remotepc`
- (Appears only on single-session OS machines) **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`

Click **Next**.

This page does not appear:

- If you're upgrading a VDA
- If you are using the `VDAWorkstationCoreSetup.exe` installer

Step 5. Select the components to install and the installation location



On the **Core components** page:

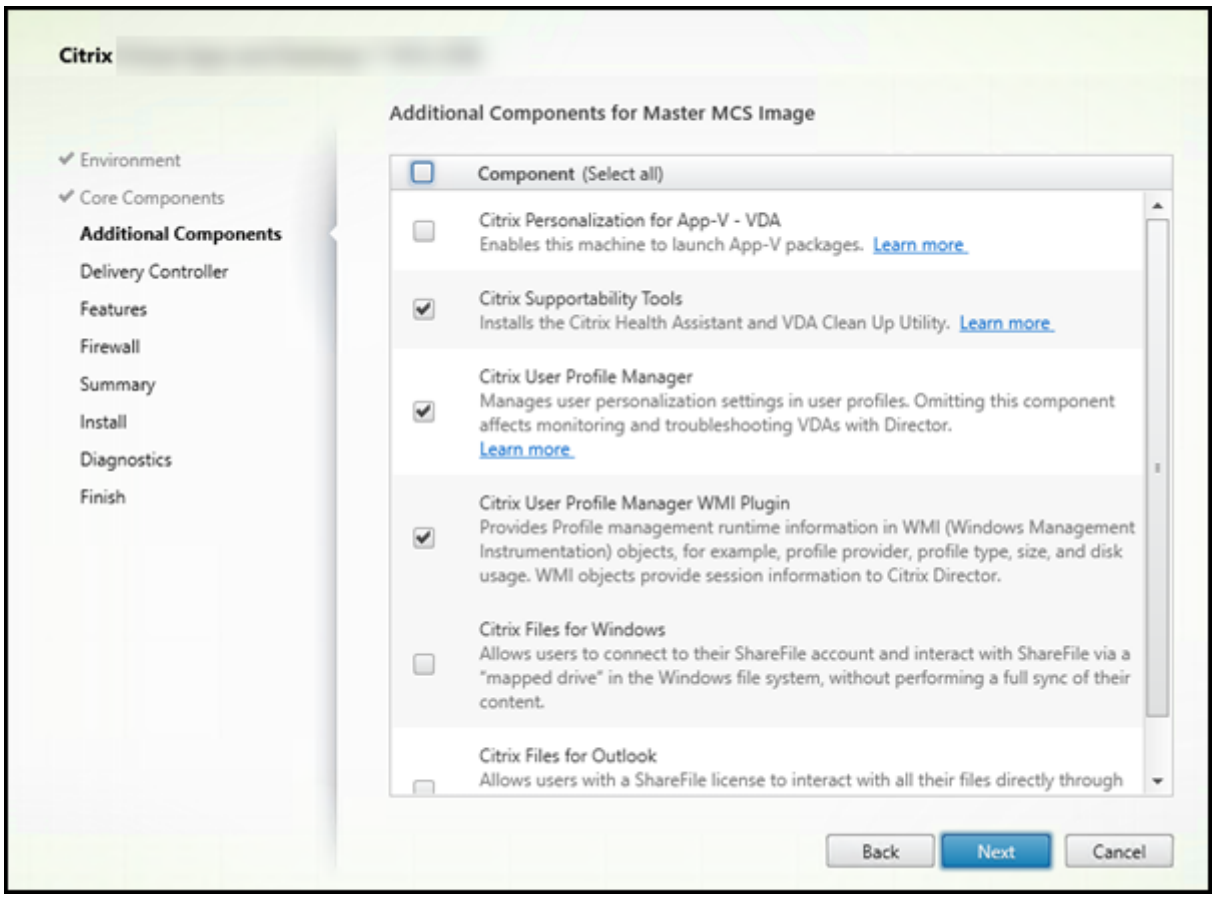
- **Location:** By default, components are installed in C:\Program Files\Citrix. This default is fine for most deployments. If you specify a different location, that location must have execute permissions for network service.

- **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.

Click **Next**.

Command-line options: `/installdir`, `/components vda plugin` to install the VDA and the Citrix Workspace app for Windows

Step 6. 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 expressly 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 User Profile Manager	Selected	Not selected
Citrix User Profile Manager WMI Plugin	Selected	Not selected
Citrix Files for Windows	Not selected	Not selected
Citrix Files for Outlook	Not selected	Not selected

This page does not appear if:

- You are using the VDAWorkstationCoreSetup.exe installer. Also, the command-line options for the additional components are not valid with that installer.
- You are upgrading a VDA and all the additional components are already installed. (If some of the additional components are already installed, the page lists only components that are not installed.)

Select or clear the following check boxes:

- **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

- **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.

  The user personalization layer technology cannot coexist with Personal vDisk (PvD) and AppDisk components.

  - For a clean installation, the Personal vDisk/AppDisk component is not available.

  - For an upgrade:
    * If PvD/AppDisk or user personalization layer is already installed, and the installation media contains a newer version of the installed component, the installed component is upgraded.
    * If PvD/AppDisk is already installed, and the installation media does not contain a newer PvD/AppDisk version, the user personalization layer can be selected for installation.
    * If neither PvD/AppDisk nor user personalization layer is already installed, the user personalization layer component is installed.

  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, such as the Citrix Health Assistant.

  Command-line option: `/includeadditional "Citrix Supportability Tools"` to enable component installation, `/exclude "Citrix Supportability Tools"` to prevent component installation

- **Citrix User Profile Manager:** 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 with Citrix Director. On the User details and End Point 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 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 User Profile Manager"` to enable component installation, `/exclude "Citrix User Profile Manager"` to prevent component installation

- **Citrix User Profile Manager WMI Plugin:** 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 User Profile Manager WMI Plugin"` to enable component installation, `/exclude "Citrix User Profile`

`Manager WMI Plugin"` to prevent component installation

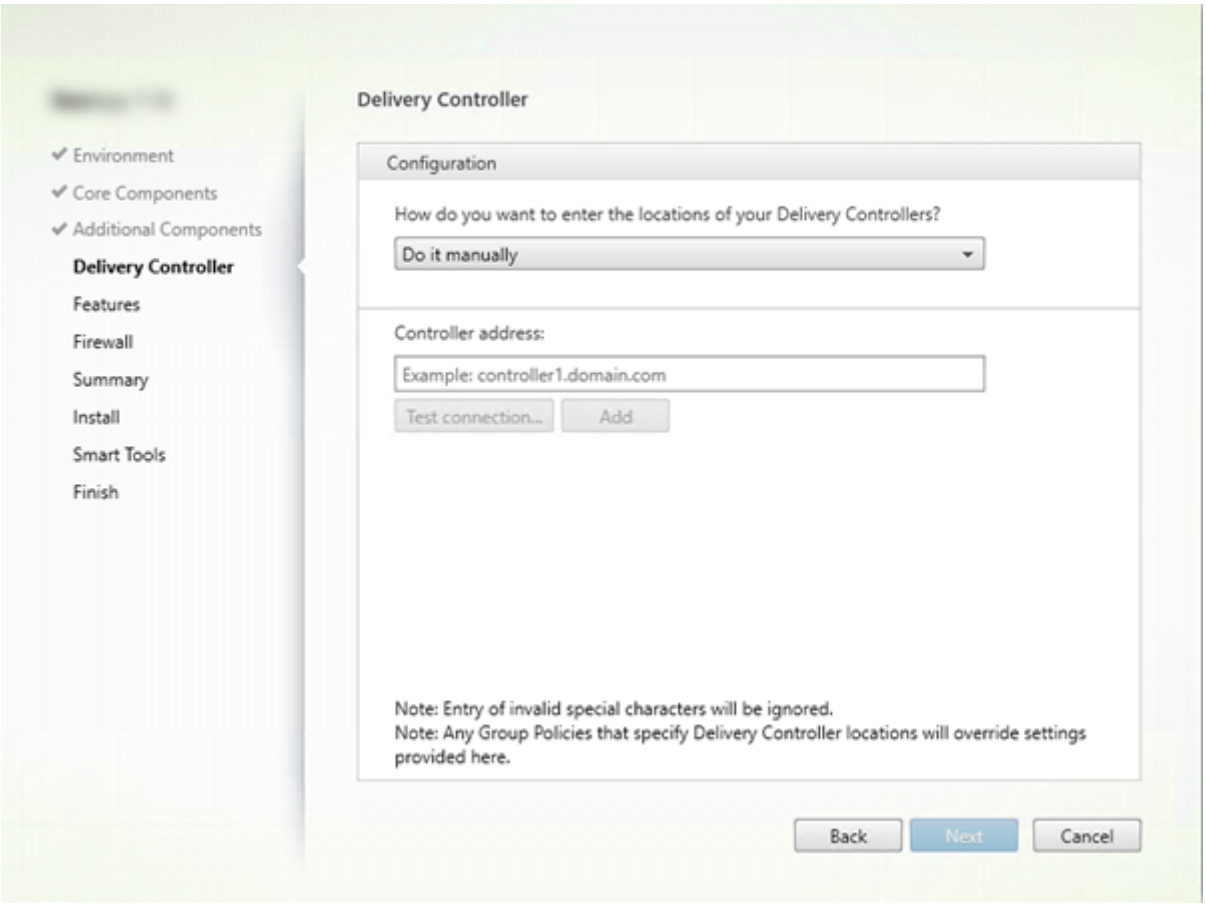
- **Citrix Files for Windows:** This component enables users to connect to their Citrix Files account. They can then interact with Citrix Files through a mapped drive in the Windows file system (without requiring a full sync of their content).

  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:** Citrix Files for Outlook 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 for co-workers, customers, and partners 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

Step 7. Delivery Controller addresses



On the **Delivery Controller** page, choose how you want to enter the addresses of installed Controllers. Citrix recommends that you specify the addresses while you're installing the VDA ("Do it manually"). The VDA cannot register with a Controller until it has this information. If a VDA cannot register, users cannot access applications and desktops on that VDA.

- **Do it manually:** (default) Enter the FQDN of an installed Controller and then click **Add**. If you've installed additional Controllers, add their addresses.
- **Do it later (Advanced):** If you choose this option, the wizard asks you to confirm that's what you want to do before continuing. To specify addresses later, you can either rerun the installer or use Citrix Group Policy. The wizard also reminds you on the **Summary** page.
- **Choose locations from Active Directory:** Valid only when the machine is joined to a domain and the user is a domain user.
- **Let Machine Creation Services do it automatically:** Valid only when using MCS to provision machines.

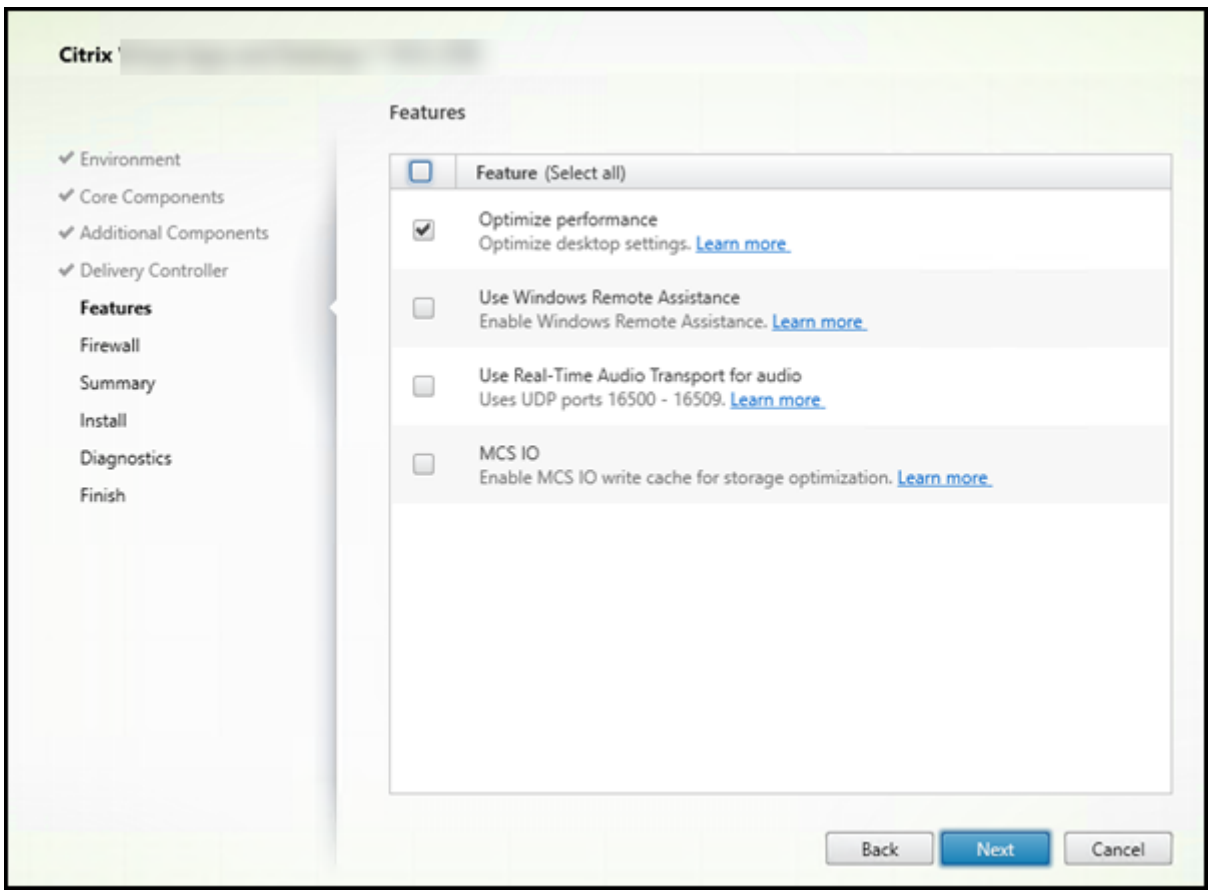
Click **Next**. If you selected "Do it later (Advanced),"you are prompted to confirm that you will specify Controller addresses later.

Other considerations:

- The address cannot contain non-alphanumeric characters.
- If you specify addresses during VDA installation and in Group Policy, the policy settings override settings provided during installation.
- Successful VDA registration requires that the firewall ports used to communicate with the Controller are open. That action is enabled by default on the **Firewall** page of the wizard.
- After you specify Controller locations (during or after VDA installation), you can use the auto-update feature to update the VDAs when Controllers are added or removed. For details about how VDAs discover and register with Controllers, see VDA registration.

Command-line option: `/controllers`

Step 8. Enable or disable features



On the **Features** page, use the check boxes to enable or disable features you want to use.

- **Optimize performance:** When you use MCS and enable this feature (default), VM optimization disables offline files, disables background defragmentation, and reduces event log size. For details, see CTX224676.

  In addition to enabling this feature, optimization requires that the Machine Identity Service be installed. That service contains the `TargetOSOptimizer.exe` file. The Machine Identity Service is installed automatically when you:

  - In the graphical interface, select **Create a master MCS image** on the **Environment** page.
  - In the command-line interface, specify `/mastermcsimage` or `/masterimage` (and do not specify `/exclude "Machine Identity Service"`).

  Command-line option: `/optimize`

  If you are using the VDAWorkstationCoreSetup.exe installer, this feature does not appear in the wizard and the command-line option is not valid. If you are using another installer in a Remote PC Access environment, disable this feature.

- **Use Windows Remote Assistance:** When this feature is enabled, Windows Remote Assistance is used with the user shadowing feature of Director. 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)

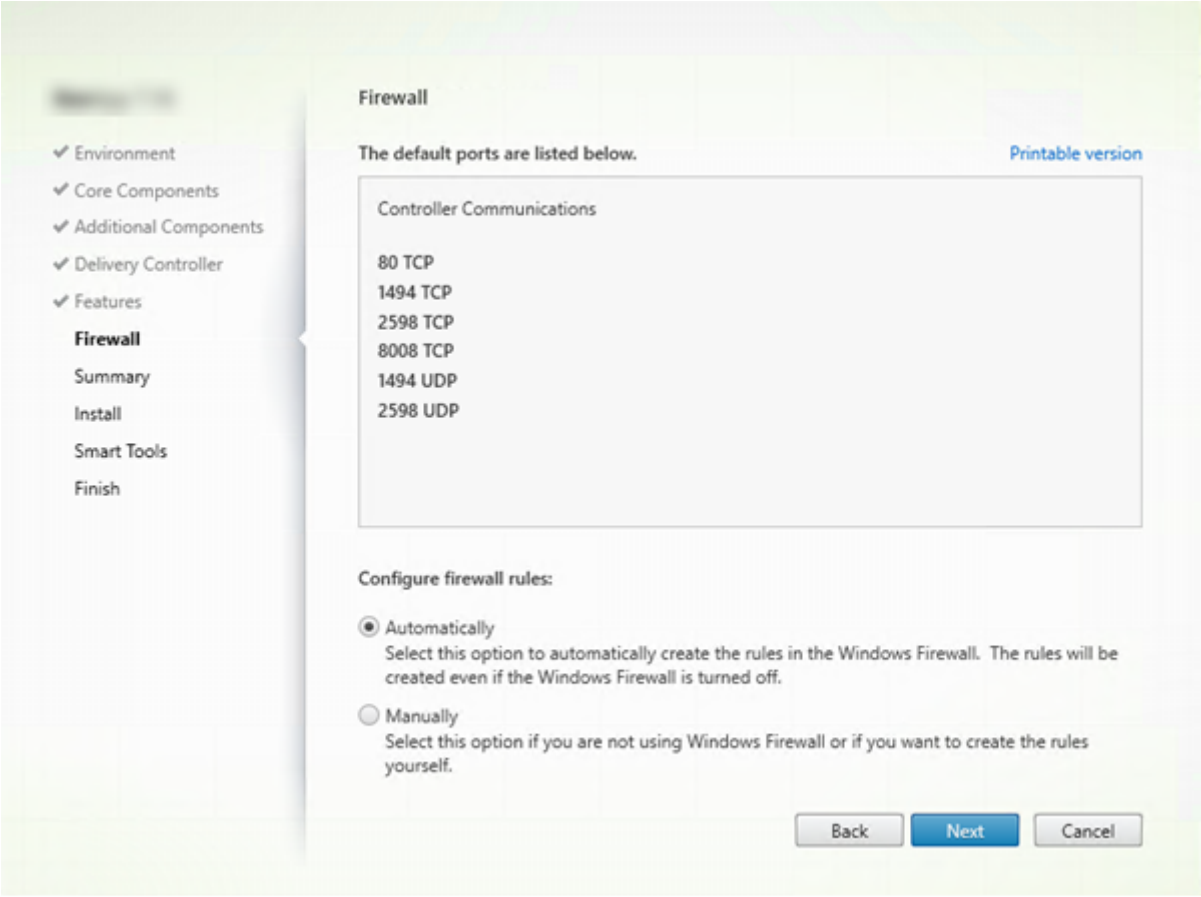
  Command-line option: `/enable_real_time_transport`

- **MCS I/O:** Valid only when using MCS to provision VMs. When selected, the MCSIO write caching driver is installed. For more information, see Storage shared by hypervisors and Configure cache for temporary data.

  Command-line option: `/install_mcsio_driver`

Click **Next**.

Step 9. Firewall ports

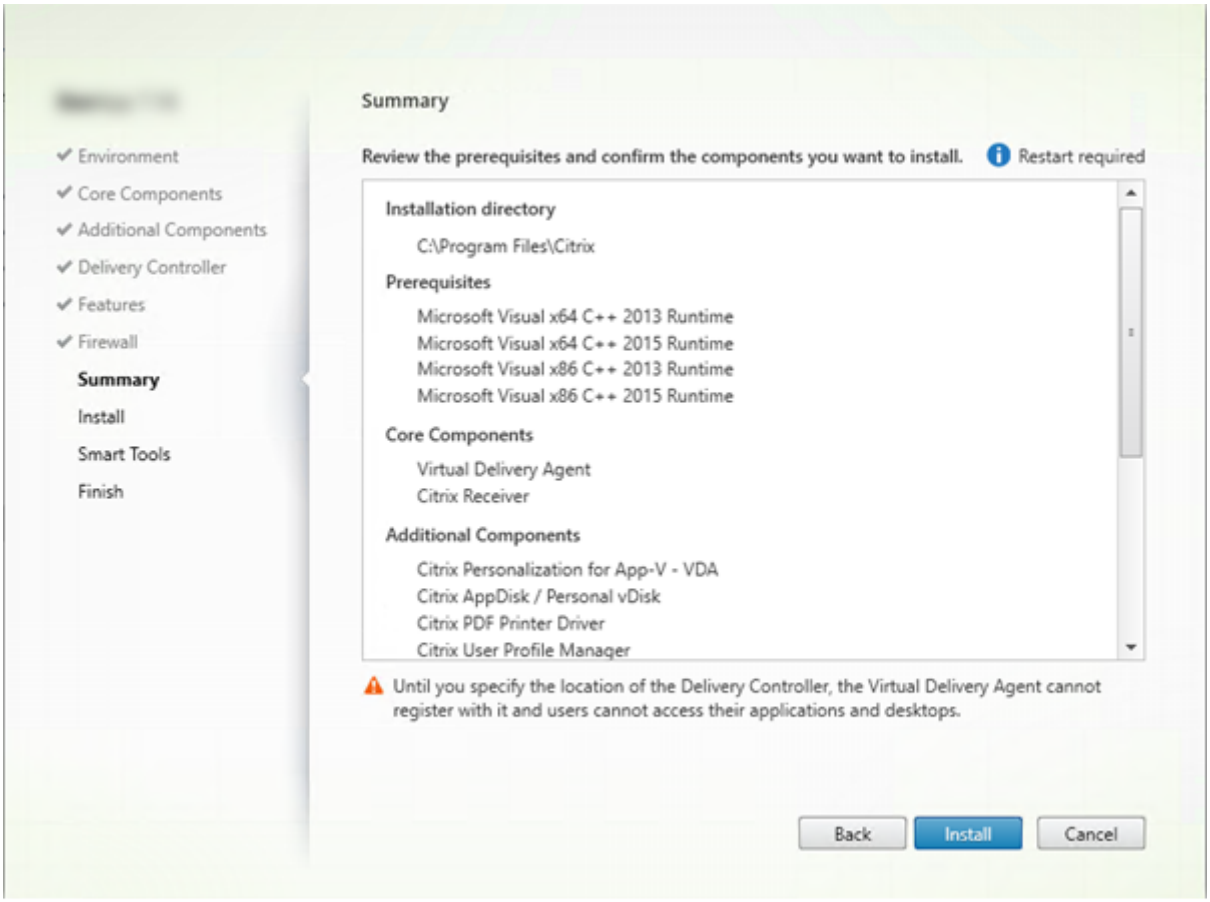


On the **Firewall** page, by default, the ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. This default setting is fine for most deployments. For port information, see Network ports.

Click **Next**.

Command-line option: `/enable_hdx_ports`

Step 10. Review prerequisites and confirm installation

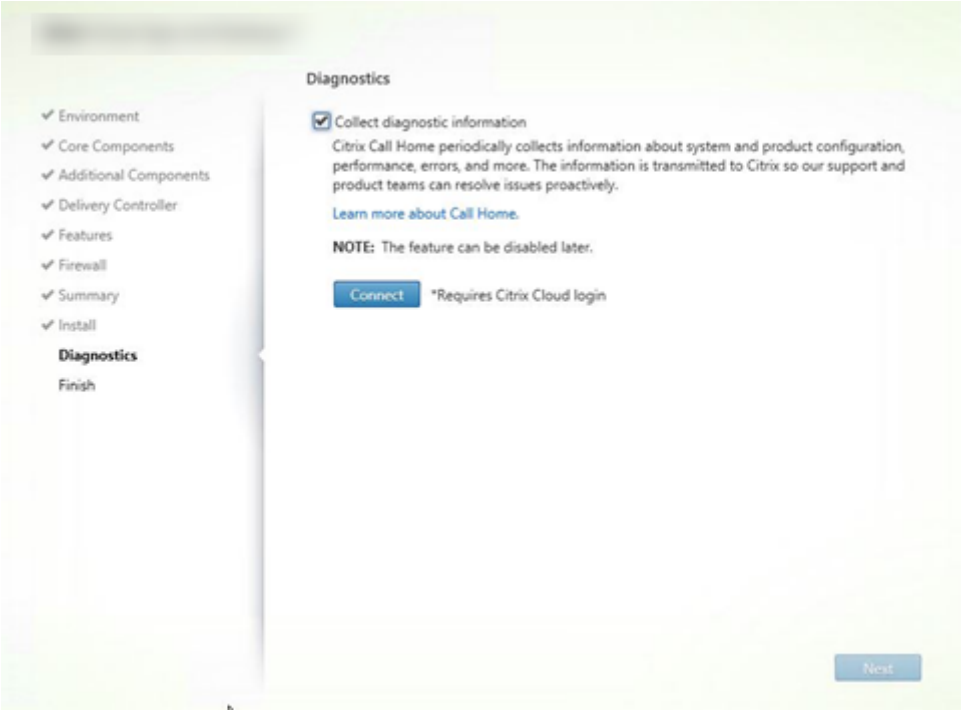


The **Summary** page lists what will be installed. Use the Back button to return to earlier wizard pages and change selections.

When you're ready, click **Install**.

If prerequisites aren't already installed/enabled, the machine may restart once or more times. See Prepare to install.

Step 11. Diagnostics

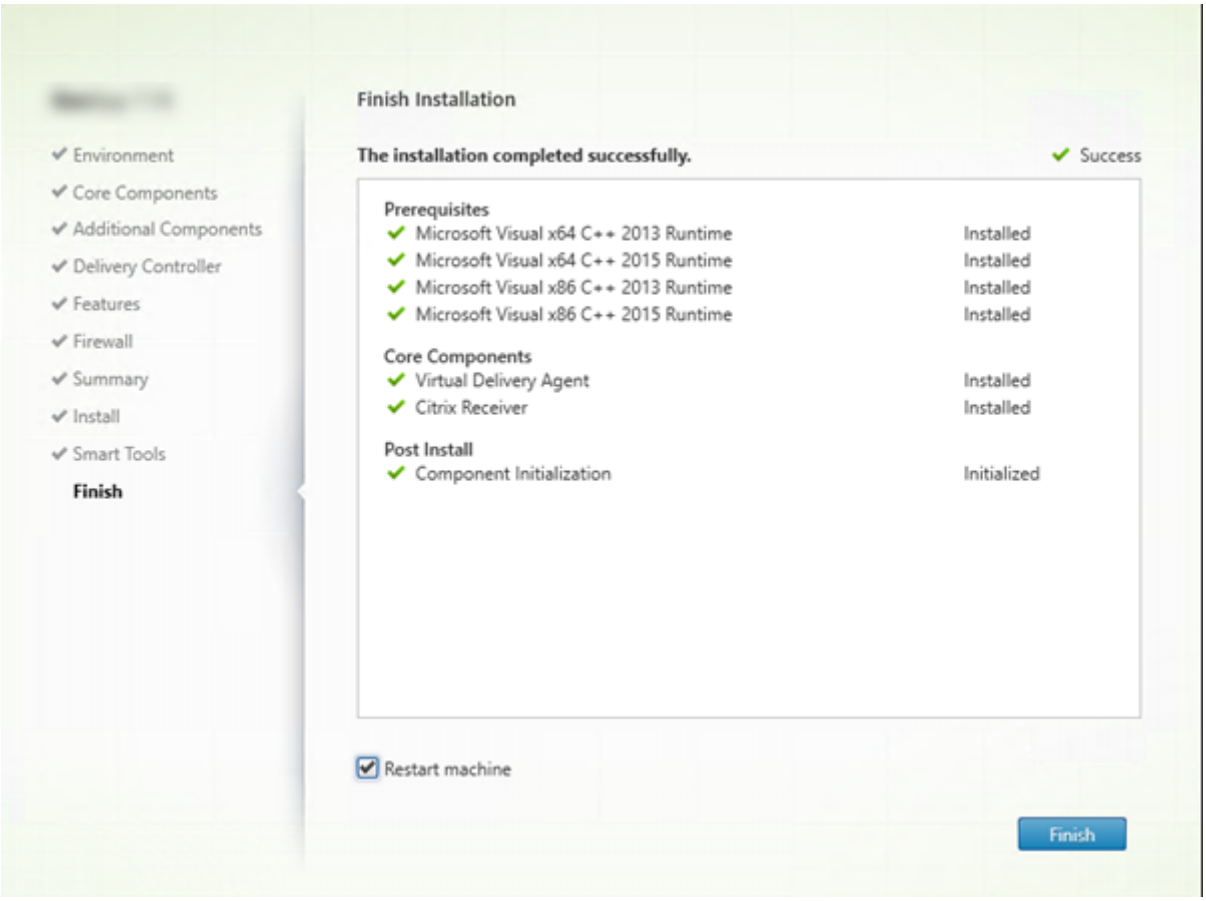


On the **Diagnostics** page, choose whether to participate in Citrix Call Home. If you choose to participate (the default), click **Connect**. When prompted, enter your Citrix account credentials.

After your credentials are validated (or if you choose not to participate), click **Next**.

For more information, see Call Home.

Step 12. Complete this installation



The **Finish** page contains green check marks for all prerequisites and components that installed and initialized successfully.

Click **Finish**. By default, the machine restarts automatically. (Although you can disable this automatic restart, the VDA cannot be used until the machine restarts.)

Next steps

Repeat the procedure above to install VDAs on other machines or images, if needed.

After you install all VDAs, launch Studio. If you haven't created a Site yet, Studio automatically guides you to that task. After that's done, Studio guides you to create a machine catalog and then a Delivery Group. See:

- Create a Site
- Create machine catalogs
- Create Delivery Groups

Customize a VDA

If you want to customize 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, you can change:
    - Controller addresses
    - TCP/IP port to register with the Controller (default = 80)
    - Whether to open Windows Firewall ports automatically

Troubleshoot

For information about how Citrix reports the result of component installations, see Citrix installation return codes.

In the Studio 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.

Install using the command line

December 23, 2022

This article applies to installing components on machines with Windows operating systems. For information about VDAs for Linux operating systems, see Linux Virtual Delivery Agents.

This article describes how to issue product installation commands. Before beginning any installation, review Prepare to install. That article includes descriptions of the available installers.

To see command execution progress and return values, you must be the original administrator or use **Run as administrator**. For more information, see the Microsoft command documentation.

As a complement to using the installation commands directly, sample scripts are provided on the product ISO that install, upgrade, or remove VDA machines in Active Directory. For details, see Install VDAs using scripts.

If you attempt to install (or upgrade to) a Windows VDA on an OS that is not supported for this product version, a message guides you to information that describes your options. This information is also available in Earlier operating systems.

For information about how Citrix reports the result of component installations, see Citrix installation return codes.

Use the full-product installer

To access the full product installer's command-line interface:

1. Download the product package from Citrix. Citrix account credentials are required to access the download site.
2. Unzip the file. Optionally, burn a DVD of the ISO file.
3. Log on to the server where you are installing the components, using a local administrator account.
4. Insert the DVD in the drive or mount the ISO file.
5. From the \x64\XenDesktop Setup directory on the media, run the appropriate command.

To install core components: Run `XenDesktopServerSetup.exe`, with the options listed in Command-line options for installing core components.

To install StoreFront: Follow the guidance in To install StoreFront at a command prompt.

To install a VDA: Run `XenDesktopVDASetup.exe` with the options listed in Command-line options for installing a VDA.

To install the Universal Print Server: Follow the guidance in Command-line options for installing a Universal Print Server.

To install the Federated Authentication Service: Citrix recommends using the graphical interface.

To install the Self-Service Password Reset Service: Follow the guidance in Self-Service Password Reset Service.

To install Session Recording: Follow the guidance in Session Recording.

Command-line options for installing core components

The following options are valid when installing core components with the `XenDesktopServerSetup.exe` command. For more detail about options, see Install core components.

- **/components** *component* [,*component*] …

  Comma-separated list of components to install or remove. Valid values are:

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio

  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server

  If this option is omitted, all components are installed (or removed, if the `/remove` option is also specified).

  (In releases before 1912 LTSR CU1, valid values included `STOREFRONT`. For version 1912 LTSR CU1 and later, use the dedicated StoreFront installation instructions noted in Use the full-product installer).

- **/configure_firewall**

  Opens all ports in the Windows firewall used by the components being installed, if the Windows Firewall Service is running, even if the firewall is not enabled. If you are using a third-party firewall or no firewall, you must manually open the ports.

- **/disableexperiencemetrics**

  Prevents automatic upload of analytics collected during installation, upgrade, or removal to Citrix.

- **/exclude** "*feature*"[,"*feature*"]

  Prevents installation of one or more comma-separated features, services, or technologies, each enclosed in straight quotation marks. Valid values are:

  - `"Local Host Cache Storage (LocalDB)"`: Prevents installation of the database used for Local Host Cache. This option has no effect on whether SQL Server Express is installed for use as the Site database.

- **/help** or **/h**

  Displays command help.

- **/ignore_hw_check_failure**

  Allows the Delivery Controller installation or upgrade to continue, even if the hardware checks fail (for example, due to insufficient RAM). For more information, see Hardware check.

- **/ignore_site_test_failure**

  Valid only during Controller upgrade. Any site test failures are ignored and the upgrade proceeds. If omitted (or set to false), any site test failure causes the installer to fail, without performing the upgrade. Default = false

- **/installdir *directory***

  Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.

- **/logpath *path***

Log file location. The specified folder must exist. The installer does not create it. Default = "%TEMP%\Citrix\XenDesktop Installer"

- **/no_pending_reboot_check**

  When installing or upgrading core components, prevents checking for a pending restart from a previous Windows installation on the machine.

- **/no_remote_assistance**

  Valid only when installing Director. Disables the user shadowing feature that uses Windows Remote Assistance.

- **/noreboot**

  Prevents a restart after installation. (For most core components, a restart is not enabled by default.)

- **/nosql**

  Prevents installation of Microsoft SQL Server Express on the server where you are installing the Controller. If this option is omitted, SQL Server Express is installed for use as the Site database. (This option has no effect on the installation of SQL Server Express LocalDB used for Local Host Cache.)

- **/quiet** or **/passive**

  No user interface appears during the installation. The only evidence of the installation process is in Windows Task Manager. If this option is omitted, the graphical interface launches.

- **/remove**

  Removes the core components specified with the /components option.

- **/removeall**

  Removes all installed core components.

- **/sendexperiencemetrics**

  Automatically sends analytics collected during the installation, upgrade, or removal to Citrix. If this option is omitted (or `/disableexperiencemetrics` is specified), the analytics are collected locally, but not sent automatically.

- **/tempdir** *directory*

  Directory that holds temporary files during installation. Default = c:\Windows\Temp.

- **/xenapp**

  Installs Citrix Virtual Apps. If this option is omitted, Citrix Virtual Apps and Desktops is installed.

Examples of installing core components

The following command installs a Citrix Virtual Apps and Desktops Controller, Studio, Citrix Licensing, and SQL Server Express on a server. Firewall ports required for component communications are opened automatically.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller
,desktopstudio,licenseserver /configure_firewall
```

The following command installs a Citrix Virtual Apps Controller, Studio, and SQL Server Express on the server. Firewall ports required for component communication are opened automatically.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

Use a standalone VDA installer

Citrix account credentials are required to access the download site. You must either have elevated administrative privileges before starting the installation or use **Run as administrator**.

1. Download the appropriate package from Citrix:

   - Multi-session OS Virtual Delivery Agent: `VDAServerSetup.exe`
   - Single-session OS Virtual Delivery Agent: `VDAWorkstationSetup.exe`
   - Single-session OS Core Services Virtual Delivery Agent: `VDAWorkstationCoreSetup.exe`

2. Either extract the files from the package to an existing directory first and then run the installation command, or simply run the package.

   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 below, 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`

   To run the downloaded package, run its name: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`. Use the valid options listed in this article.

If you are familiar with the full product installer:

- Run the standalone `VDAServerSetup.exe` or `VDAWorkstationSetup.exe` installer as if it was the `XenDesktopVdaSetup.exe` command in everything except its name.
- The `VDAWorkstationCoreSetup.exe` installer is different, because it supports a subset of the options available to the other installers.

Command-line options for installing a VDA

The following options are valid with one or more of the following commands (installers): `XenDesktopVDASetup.exe`, `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`.

For more detail about options, see Install VDAs.

- **/baseimage**

  Valid only when installing a VDA for single-session OS on a VM. Enables the use of Personal vDisks with a master image. Personal vDisk is deprecated.

  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer.

- **/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 for Windows, specify `/components vda plugins`.

  If this option is omitted, only the VDA is installed (not 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 Controllers 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 uses, 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 uses, 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 extra 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 Director. If you specify this option, Windows Remote Assistance opens the dynamic ports in the firewall.

- **/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 image that is not managed by MCS does not require the Machine Identity Service component. Valid values are:

  - `AppDisks VDA Plug-in`
  - `Personal vDisk`
  - `Machine Identity Service` (includes TargetOSOptimizer.exe)
  - `Citrix User Profile Manager`
  - `Citrix User Profile Manager WMI Plug-in`
  - `Citrix Universal Print Client`
  - `Citrix Telemetry Service`
  - `Citrix Personalization for App-V - VDA`
  - `Citrix Supportability Tools`
  - `Citrix Files for Windows`
  - `Citrix Files for Outlook`


```
- User Personalization Layer
```

Excluding Citrix Profile Management from the installation (`/exclude "Citrix User Profile Manager"`) affects monitoring and troubleshooting of VDAs with Citrix Director. 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 displays 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.

If you plan to use MCS to provision VMs, do not exclude the Machine Identity Service. Excluding that service also excludes installation of `TargetOSOptimizer.exe`.

If you specify both `/exclude` and `/includeadditional` with the same additional component name, that component is not 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 additional components that are not included by default. Valid values are:

  ```
  - Personal vDisk
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plug-in
  - Citrix Universal Print Client
  - Citrix Telemetry Service
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
  - User Personalization Layer
  ```

  If you specify both `/exclude` and `/includeadditional` with the same additional component name, that component is not installed.

If you include both `Personal vDisk` and `user personalization layer` in the same command, only `user personalization layer` is installed.

- **/installdir** *directory*

  Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.

- **/install_mcsio_driver**

  Enables MCS I/O write cache for storage optimization.

- **/logpath *path**

  Log file location. The specified folder must exist. The installer does not create it. Default = "%TEMP%\Citrix\XenDesktop Installer"

  This option is not available in the graphical interface.

- **/masterimage**

  Valid only when installing a VDA on a VM. Sets up the VDA as a master 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 a master image with Machine Creation Services. This option also installs TargetOSOptimizer.exe (unless you also specify `/exclude "Machine Identity Service"` which includes the optimizer installer). This option is equivalent to `/masterimage`.

- **/masterpvsimage**

  Specifies that this machine will be used as a master image with either Citrix Provisioning or a third-party provisioning tool (such as Microsoft System Center Configuration Manager) to provision VMs.

- **/no_mediafoundation_ack**

  Acknowledges that Microsoft Media Foundation is not installed, and several HDX multimedia features will not be installed and will 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 VDA for multi-session OS. 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 re-mount the media or want to capture information during an automated installation.

- **/optimize**

  When you use MCS and enable this feature (default), VM optimization disables offline files, disables background defragmentation, and reduces event log size. For details, see CTX224676.

  In addition to enabling this feature, optimization requires that the Machine Identity Service be installed. That service contains the TargetOSOptimizer.exe. The Machine Identity Service is installed automatically when you specify `/mastermcsimage` or `/masterimage` (and do not specify `/exclude "Machine Identity Service"`).

  Do not specify this option for Remote PC Access deployments.

- **/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.

- **/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). Excludes installation of the following components on a single-session OS:

  - Citrix Personalization for App-V
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plugin
  - Machine Identity Service (includes TargetOSOptimizer.exe)

  - Personal vDisk
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
  - User personalization layer

  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer automatically excludes installation of these components.

- **/remove**

  Removes the components specified with the /components option.

- **/removeall**

  Removes all installed VDA components.

- **/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 VDA for single-session OS on a supported Windows multi-session machine. Omit this option when installing a VDA for multi-session OS on a Windows multi-session machine. Before using this option, see Server VDI.

  This option should be used only with the full-product VDA installer. This option is not available in the graphical interface.

- **/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 Studio. 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.

Examples of installing a VDA

Install a VDA with the full-product installer:

The following command installs a VDA for single-session OS and Citrix Workspace app to the default location on a VM. This VDA will be used as a master image and use MCS to provision VMs. The VDA will register initially with the Controller on the server named `Contr-Main` in the domain `mydomain`. The VDA will use user personalization layer, optimization, and Windows Remote Assistance.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /
includeadditional "User Personalization Layer"/optimize /mastermcsimage
 /enable_remote_assistance
```

Install a single-session OS VDA with the VDAWorkstationCoreSetup standalone installer:

The following command installs a Core Services VDA on a single-session OS for use in a Remote PC Access or VDI deployment. Citrix Workspace app and other non-core services are not installed. The address of a Controller is specified, and ports in the Windows Firewall Service will be opened automatically. The administrator will handle restarts.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

Customize a VDA

After you install a VDA, you can customize several settings. From the `\x64\XenDesktop Setup` directory on the product media, run `XenDesktopVdaSetup.exe`, using one or more of the following options, which are described in Command-line options for installing a VDA.

- `/reconfigure` (required when customizing a VDA)
- `/h` or `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Command-line options for installing a Universal Print Server

The following option is valid with the `XenDesktopPrintServerSetup.exe` command.

- **/enable_upsserver_port**

Software	Folder	File name
Microsoft Visual C++ 2017 Runtime, 32- and 64-bit	Support > VcRedist_2017	`vcredist_x64.exe` and `vcredist_x86.exe`
Citrix Diagnostic Facility	x64 > Virtual Desktop Components	`cdf_x64.msi`
Universal Print Server server component	x64 > Universal Print Server	`UpsServer_x64.msi`

When this option is not specified, the installer displays the **Firewall** page from the graphical interface. Select **Automatically** to have the installer automatically add the Windows firewall rules, or **Manually** to let the administrator manually configure the firewall.

After installing the software on your print servers, configure the Universal Print Server using the guidance in Provision printers.

Install VDAs using scripts

April 20, 2023

> **Note:**
>
> Citrix is not responsible for issues caused by scripts that are adapted to match customer production environments. For any install related Citrix issues, open a technical support case with the relevant install logs using the Citrix Support portal.

This article applies to installing VDAs on machines with Windows operating systems. For information about VDAs for Linux operating systems, see the Linux Virtual Delivery Agent documentation.

The installation media contains sample scripts that install, upgrade, or remove Virtual Delivery Agents (VDAs) for machines in Active Directory. You can also use the scripts to maintain master images used by Machine Creation Services and Citrix Provisioning (formerly Provisioning Services).

Required access:

- The scripts need Everyone Read access to the network share where the VDA installation command is located. The installation command is `XenDesktopVdaSetup.exe` in the full product ISO, or `VDAWorkstationSetup.exe` or `VDAServerSetup.exe` in a standalone installer.
- Logging details are stored on each local machine. To log results centrally for review and analysis, the scripts need Everyone Read and Write access to the appropriate network share.

To check the results of running a script, examine the central log share. Captured logs include the script log, the installer log, and the MSI installation logs. Each installation or removal attempt is recorded in a time-stamped folder. The folder title indicates the operation result with the prefix PASS or FAIL. You can use standard directory search tools to find a failed installation or removal in the central log share. Those tools offer an alternative to searching locally on the target machines.

Before beginning any installation, read and complete the tasks in Prepare to install.

Install or upgrade VDAs using the script

1. Obtain the sample script **InstallVDA.bat** from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script:
    - Specify the version of the VDA to install: `SET DESIREDVERSION`. For example, version 7 can be specified as 7.0. The full value can be found on the installation media in the ProductVersion.txt file. However, a complete match is not required.
    - Specify the network share where the installer will be invoked. Point to the root of the layout (the highest point of the tree). The appropriate version of the installer (32-bit or 64-bit) is called automatically when the script runs. For example: `SET DEPLOYSHARE=\\fileserver1\share1`.
    - Optionally, specify a network share location for storing centralized logs. For example: `SET LOGSHARE=\\fileserver1\log1`).
    - Specify VDA configuration options as described in Install using the command line. The `/quiet` and `/noreboot` options are included by default in the script and are required: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`.
3. Using Group Policy Startup Scripts, assign the script to the OU containing your machines. This OU should contain only machines on which you want to install the VDA. When the machines in that OU are restarted, the script runs on all of them. A VDA is installed on each machine that has a supported operating system.

Remove VDAs using the script

1. Obtain the sample script UninstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script.
    - Specify the version of the VDA to remove: `SET CHECK\_VDA\_VERSION`. For example, version 7 can be specified as 7.0. The full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018). However, a complete match is not required.

- Optionally, specify a network share location for storing centralized logs.

3. Using Group Policy Startup Scripts, assign the script to the OU containing your machines. This OU should contain only machines from which you want to remove the VDA. When the machines in the OU are restarted, the script runs on all of them. The VDA is removed from each machine.

Troubleshoot

The script generates internal log files that describe script execution progress. The script copies a Kickoff_VDA_Startup_Script log to the central log share within seconds of starting the deployment. You can verify that the overall process is working. If this log is not copied to the central log share as expected, troubleshoot further by inspecting the local machine. The script places two debugging log files in the %temp% folder on each machine:

- Kickoff_VDA_Startup_Script_<DateTimeStamp>.log
- VDA_Install_ProcessLog_<DateTimeStamp>.log

Review these logs to ensure that the script is:

- Running as expected.
- Properly detecting the target operating system.
- Correctly configured to point to the ROOT of the DEPLOYSHARE share (contains the file named AutoSelect.exe).
- Capable of authenticating to both the DEPLOYSHARE and LOG shares.

Install VDAs using SCCM

April 20, 2023

> **Note:**
>
> Citrix is not responsible for issues that arise caused by the deployment of a Virtual Delivery Agent (VDA) using software distribution tools such as Microsoft System Center Configuration Manager (SCCM) adapted to match customer production environments. For any install related Citrix issues, open a technical support case with the relevant install logs using the Citrix Support portal.

Overview

To successfully deploy a Virtual Delivery Agent (VDA) using Microsoft System Center Configuration Manager (SCCM) or similar software distribution tools, Citrix recommends using the VDA installer in a sequence of steps.

Citrix does not recommend using the VDA Cleanup Utility as part of a VDA installation or upgrade. Use the VDA Cleanup Utility only in the limited case when the VDA installer has previously failed.

Restarts

The required number of restarts during the installation of the VDA depends on the environment. For example:

- A restart might be required for pending updates or restarts from earlier software installations.
- Files previously locked by other processes might need updates, forcing an extra restart.
- Some optional components in the VDA installer (such as Citrix Profile Management and Citrix Files) might require a restart.

The SCCM Task Sequencer manages all required restarts.

Define the task sequence

After identifying all prerequisites and restarts, use the SCCM Task Sequencer to complete the following:

- The VDA can be installed from an accessible copy of the installation media or from one of the VDA standalone installers:
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  For more information about VDA installers, see Installers.
- When upgrading a VDA, the machine on which it is installed must be in maintenance mode, with no sessions.
- When a VDA installation runs for the first time on a machine, the VDA installer being used is copied onto that machine.
  - When using a VDA installer other than `VDAWorkstationCoreSetup_XXXX.exe`, the VDA installer is copied to `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
  - When using `VDAWorkstationCoreSetup_XXXX.exe`, the VDA installer is copied to `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.

‘

- The directory location of the VDA installer is also stored in the registry "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall" "MetaInstallerInstallLocation".
- Add the command line options /NOREBOOT, /NORESUME, and /QUIET to your command line options.
  - /QUIET: Do not show the user interface during installation, so that SCCM has control of the installation process.
  - /NOREBOOT: Suppress the VDA installer from restarting automatically. SCCM triggers restarts when needed.
  - /NORESUME: Usually, when a restart is needed during the installation, the VDA installer sets a runonce registry key (\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce). When the machine restarts, Windows uses the key to launch the VDA installer. This is an issue for SCCM, because SCCM cannot monitor the installation and capture the exit code.

Example installation sequence using SCCM

The following example shows the installation sequence.

1. **SCCM TASK1:** Prepare the machine by restarting the machine.
2. **SCCM TASK2:** Start the VDA installation.
   a) Add the /quiet, /noreboot, and /noresume options to your command line options.
   b) Run the VDA installer of your choice (local image or one of the minimal installers).
   c) SCCM must capture the return code.
      - If the return code is 0 or 8, the installation is complete, and a restart is needed.
      - If a return code is 3, restart the machine and then pass control to SCCM TASK3.
3. **SCCM TASK3:** Continue VDA installation.
   a) If SCCM TASK2 does not return a 0 or 8, the installation must be continued after the restart completes.
   b) SCCM TASK3 repeats until the VDA installer returns a 0 or 8 (indicating a successful installation), or 3 (indicating SCCM TASK3 must be repeated). Treat any other return code as an error, and SCCM TASK3 should report an error and stop.
   c) Resume the VDA installation by running the appropriate VDA installer (XenDesktopVdaSetup.exe for most cases, or XenDesktopRemotePCSetup.exe if VDAWorkstationCoreSetup_XX.exe was used) from the location where it was copied (as described in Define the task sequence), with no command-line parameters. (The VDA installer uses the parameters it saved during the first run of the installer.)
   d) Watch for the return code from the VDA installer.

- 0 or 8: Success, installation complete, restart required.
- 3: Installation is not complete. Restart the machine and repeat SCCM TASK3 until a 0 or 8 is returned. Treat any other return code as an error, and SCCM TASK3 should report an error and end.

For more information about return codes see Citrix installation return codes.

VDA installation command examples

The available installation options vary, depending on which installer is used. See the following articles for command line option details.

- Install VDAs
- Install using the command line

Installation commands for Remote PC Access

- The following command uses the single-session core VDA installer (`VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

- The following command uses the single-session full VDA installer (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

Installation command for dedicated VDI

- The following command uses the single-session full VDA installer (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers "control.domain.com" /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

Create a Site

May 4, 2020

A *Site* is the name you give to a Citrix Virtual Apps and Desktops deployment. It comprises the Delivery Controllers and other core components, Virtual Delivery Agents (VDAs), connections to hosts, machine catalogs, and Delivery Groups. You create the Site after you install the core components and before creating the first machine catalog and Delivery Group.

If your Controller is installed on Server Core, use PowerShell cmdlets in the Citrix Virtual Apps and Desktops SDK to create a Site.

When you create a Site, you are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP). CEIP collects anonymous statistics and usage information, and then sends it to Citrix. The first data package is sent to Citrix approximately seven days after you create the Site. You can change your enrollment at any time after Site creation. Select **Configuration** in the Studio navigation pane, then the **Product Support** tab, and follow the guidance. For details, see http://more.citrix.com/XD-CEIP.

The user who creates a Site becomes a full administrator; for more information, see Delegated Administration.

Review this article before you create the Site, so you'll know what to expect.

Step 1. Open Studio and start the Site creation wizard

Open Studio if it is not already open. You are automatically guided to the action that starts the Site creation wizard. Select that action.

Step 2. Site type and name

On the **Introduction** page, choose a Site type:

- **Application and desktop delivery Site**. When you create an application and desktop delivery Site, you can further choose to create a full deployment Site (recommended) or an empty Site. An empty Site is only partially configured, and is usually created by advanced administrators.
- **Remote PC Access Site**. A Remote PC Access Site allows designated users to remotely access their office PCs through a secure connection.

If you create an application and desktop delivery deployment now, you can add a Remote PC Access deployment later. Conversely, if you create a Remote PC Access deployment now, you can add a full deployment later.

Type a name for the Site. After the Site is created, its name appears at the top of the Studio navigation pane: **Citrix Studio** (*site-name*).

Step 3. Databases

The **Databases** page contains selections for setting up the Site, Monitoring, and Configuration Logging databases. For details about database setup choices and requirements, see Databases.

If you choose to install SQL Server Express for use as the Site database (the default), a restart occurs after that software is installed. That restart does not occur if you choose not to install the SQL Server Express software for use as the Site database.

If you are not using the default SQL Server Express, ensure that the SQL Server software is installed on the machines before creating a Site. System requirements lists the supported versions.

If you want to add more Delivery Controllers to the Site, and have already installed the Controller software on other servers, you can add those Controllers from this page. If you also plan to generate scripts that set up the databases, add the Controllers before generating the scripts.

Step 4. Licensing

On the **Licensing** page, specify the License Server address and then indicate which license to use (install).

- Specify the License Server address in the form `name:[port]`. The *name* must be an FQDN, NetBIOS, or IP address. FQDN is recommended. If you omit the port number, the default is 27000. Click **Connect**. You cannot proceed to the next page until a successful connection is made to the License Server.
- When a connection is made, **Use an existing license** is selected by default. The display lists the compatible products that this product can be configured as, based on currently installed licenses.
  - If you want to configure this product as one of the listed products (for example, Citrix Virtual Apps Premium or Citrix Virtual Desktops Premium), using one of those licenses, select that entry.
  - If you already allocated and downloaded a license (using the Citrix Manage Licenses Tool) to use with this product, but haven't installed the license yet:
    * Click **Browse for license file**.
    * In the file explorer, locate and select the license you downloaded. The associated products now appear on the **Licensing** page of the site creation wizard. Select the entry you want to use.
  - If the product you want is not displayed, or if you have no allocated and downloaded licenses, you can allocate, download, and install a license. To do this, the License Server

must have internet access. You must have a License Access Code for the product you want. Citrix emails that code to you.

* Click **Allocate and download**.
* In the **Allocate Licenses** dialog, enter the License Access Code sent by Citrix. Click **Allocate licenses**.
* The products associated with the new license appear on the **Licensing** page of the site creation wizard. Select the entry you want to use.

Alternatively, select **Use the free 30-day trial**, and install licenses later. For details, see the Licensing documentation.

Step 5. Power management (Remote PC Access only)

See Step 8. Remote PC Access.

Step 6. Host connection, network, and storage

If you are using VMs on a hypervisor or cloud service to deliver applications and desktops, you can optionally create the first connection to that host. You can also specify storage and network resources for that connection. After creating the Site, you can modify this connection and resources, and create more connections. For details, see Connections and resources.

- For information specified on the **Connection** page, see Connections and resources.
  - If you are not using VMs on a hypervisor or cloud service (or if you use Studio to manage desktops on dedicated blade PCs), select the connection type **None**.
  - If you are configuring a Remote PC Access Site and plan to use the Wake on LAN feature, select the **Microsoft System Center Configuration Manager** type.

  In addition to the connection type, specify whether you will use Citrix tools (such as Machine Creation Services) or other tools to create VMs.
- For information specified on the **Storage** and **Network** pages, see Host storage, Storage management, and Storage selection.

Step 7. Additional Features

On the **Additional Features** page, you can select features to customize your Site. When you select the check box for an item that requires information, a configuration box appears.

- **AppDNA Integration:** (This feature is deprecated.) If you use AppDisks and have installed AppDNA. AppDNA integration allows analysis of applications in the AppDisks. You can then review compatibility issues and take remedial actions to resolve those issues.
- **App-V Publishing:** Select this feature if you use applications from Microsoft App-V packages on App-V servers. Provide the URL of the App-V management server and the URL and port number of the App-V publishing server.

  If you use applications from App-V packages on network share locations only, you do not need to select this feature.

  You can also enable/disable and configure this feature later in Studio. For more information, see App-V.

Step 8. Remote PC Access

For information about Remote PC Access deployments, see Remote PC Access.

If you use the Wake on LAN feature, complete the configuration steps on the Microsoft System Center Configuration Manager before creating the Site. For details, see Configuration Manager and Remote PC Access Wake on LAN.

When you create a Remote PC Access Site:

- If you're using the Wake on LAN feature, specify the Microsoft System Center Configuration Manager address, credentials, and connection information on the **Power Management** page.
- Specify users or user groups on the **Users** page. There is no default action that automatically adds all users. Also, specify machine accounts (domain and OU) information on the **Machine Accounts** page.

  To add user information, click **Add Users**. Select users and user groups, and then click **Add users**.

  To add machine accounts information, click **Add machine accounts**. Select the machine accounts, and then click **Add machine accounts**. Click **Add OUs**. Select the domain and Organizational Units, and indicate whether to include items in subfolders. Click **Add OUs**.

A machine catalog named "Remote PC User Machine Accounts"is created automatically. The catalog contains all the machine accounts you added in the Site creation wizard. A Delivery Group named "Remote PC User Desktops"is created automatically. The group contains all the users and user groups you added.

Step 9. Summary

The **Summary** page lists the information you specified. Use the **Back** button if you want to change anything. When you're finished, click **Create** and the Site creation begins.

Test a Site configuration

To run the tests after you create the Site, select **Citrix Studio (Site** *site-name***)** at the top of the navigation pane. Then click **Test site** in the center pane. You can view an HTML report of the Site test results.

The site test functionality might fail for a Controller installed on Windows Server 2016. The failure occurs when a local SQL Server Express is used for the Site database and the SQL Server Browser service is not started. To avoid this failure, complete the following tasks.

1. Enable the SQL Server Browser service (if necessary) and then start it.
2. Restart the SQL Server (SQLEXPRESS) service.

Site tests run automatically when you upgrade an earlier deployment. For details, see Preliminary Site tests.

Troubleshoot

After configuring the Site, you can install Studio and add it through the MMC as a snap-in on a remote machine. If you later attempt to remove that snap-in, the MMC might stop responding. As a workaround, restart the MMC.

Create machine catalogs

September 7, 2023

Collections of physical or virtual machines are managed as a single entity called a machine catalog. Machines in a catalog have the same type of operating system: multi-session OS or single-session OS. A catalog containing multi-session OS machines can contain either Windows or Linux machines, not both.

Studio guides you to create the first machine catalog after you create the site. After you create the first catalog, Studio guides you to create the first Delivery Group. Later, you can change the catalog you created, and create more catalogs.

> **Tip:**
>
> If you upgrade an existing deployment which enables the Machine Creation Services (MCS) storage optimization feature, referred to as MCS I/O, no additional configuration is required. The VDA and the Delivery Controller upgrade handle the MCS I/O upgrade.

Overview

When you create a catalog of VMs, you specify how to provision those VMs. You can use Citrix tools such as Machine Creation Services (MCS) or Citrix Provisioning (formerly Provisioning Services). Or, you can use your own tools to provide machines.

Consider:

- MCS supports a single system disk from the virtual machine image. It ignores the rest of the data disks attached to that image.
- If you use Citrix Provisioning to create machines, see the Citrix Provisioning documentation for instructions.
- If you use MCS to provision VMs, you provide a master image (or snapshot of an image) to create identical VMs in the catalog. Before you create the catalog, you first use hypervisor or cloud service tools to create and configure the master image. This process includes installing a Virtual Delivery Agent (VDA) on the image. Then you create the machine catalog in Studio. You select that image (or snapshot), 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 for those machines.
- If you are creating a catalog using the PowerShell SDK directly, you can specify a hypervisor template (VMTemplates), rather than an image or a snapshot.

When using MCS or Citrix Provisioning to create the first catalog, you use the host connection that you configured when you created the site. Later (after you create your first catalog and Delivery Group), you can change information about that connection or create more connections.

After you complete the catalog creation wizard, tests run automatically to ensure that it is configured correctly. When the tests complete, you can view a test report. Run the tests at any time from Studio.

> **Note:**
>
> MCS does not support Windows 10 IoT Core and Windows 10 IoT Enterprise. Refer to the Microsoft site for more information.

For technical details about the Citrix Provisioning tools, see Citrix Virtual Apps and Desktops Image Management.

RDS license check

Citrix Studio currently does not perform the check for valid Microsoft RDS licenses while creating a machine catalog that contains Windows multi-session OS machines. To view the status of the Microsoft RDS license for a Windows **multi-session OS machine**, go to Citrix Director. View the status of the Microsoft RDS license in the **Machine Details** panel in the **Machine Details and the User Details** page. For more information, see Microsoft RDS license health.

VDA registration

A VDA must be registered with a Delivery Controller (for on-premises deployments) or Cloud Connector (for Citrix Cloud deployments) to be considered when launching brokered sessions. Unregistered VDAs can result in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which an administrator can troubleshoot. Studio provides troubleshooting information in the catalog creation wizard, and after you add machines from 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 might not be obtained about a machine (perhaps because it had never registered), add the machine anyway.

For more information, see:

- CTX136668 for VDA registration troubleshooting guidance
- VDA versions and functional levels
- VDA registration methods

MCS catalog creation summary

Here's a brief overview of default MCS actions after you provide information in the catalog creation wizard.

- If you selected a master 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, a master 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 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 difference 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 via the delivery controller.

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 Master Base 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:

  - Personal vDisk provides end users with the ability to install applications without admin intervention on a separate disk attached to the VM.
  - AppDisk provides end users with the ability to attach the application-only disks to VMs primarily for multi-session OS Catalogs.
  - 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 above.

  Hypervisor features might also enter into the equation. For example:

  - Citrix Hypervisor IntelliCache creates a Read Disk on local storage for each Citrix Hypervisor to save on IOPS against the master image which might be held on the shared storage location.

- Hypervisor overhead

  Different hypervisors utilize specific files that create overhead for VMs. Hypervisors also use storage for management and general logging operations. Calculate 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 with a 20 GB for the virtual disk, 16 GB for the virtual machine swap file (the size of an allocated memory), and 100 MB for log files, or 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. Therefore, a catalog that employs PvD or AppDisks needs more space than a simple pooled random catalog.
  - Updating the catalog allows 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

With the Machine Creation Services (MCS) storage optimization feature, referred to as MCS I/O:

- 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`.

- Diagnostic improvements are achieved 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:

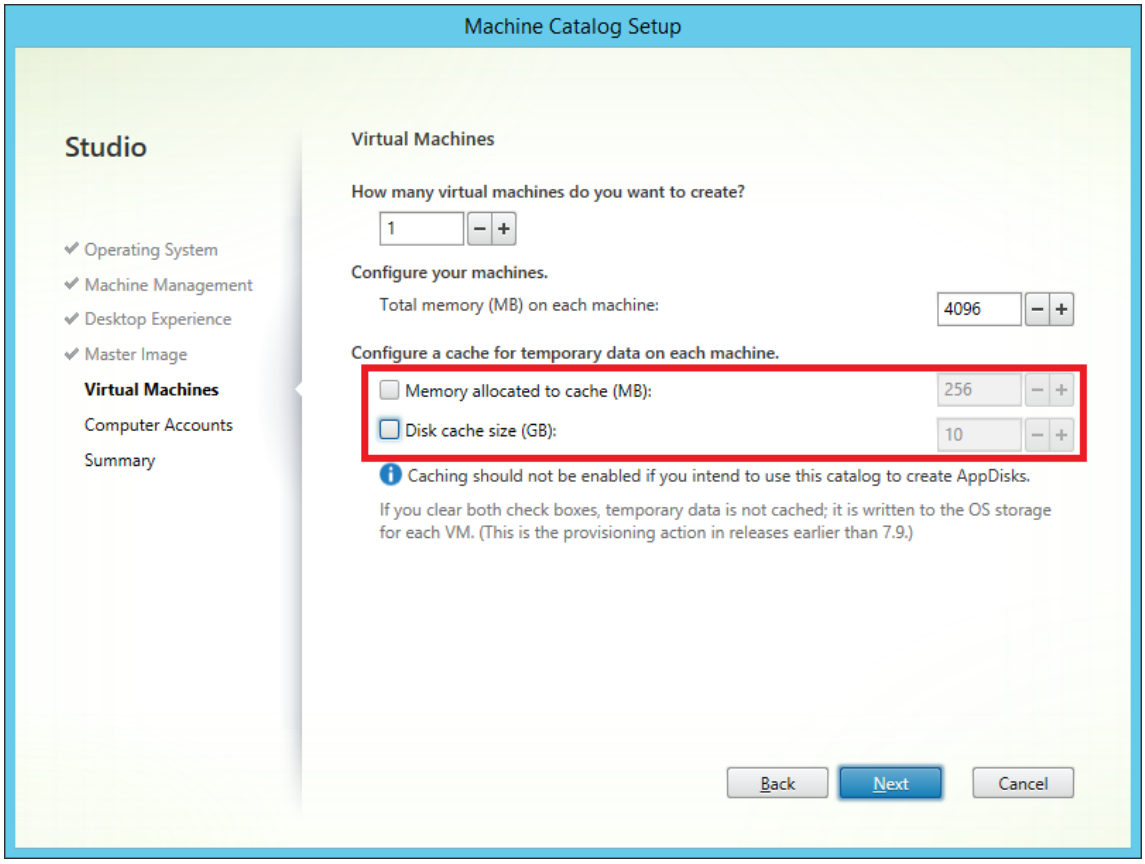
1. MCS I/O no longer supports RAM only cache. Specify a disk size in Citrix Studio during machine catalog creation.
2. The VM write cache disk is created and formatted automatically when booting a VM for the first time. Once the VM is up, the write cache file `mcsdif.vhdx` is written into the formatted volume `MCSWCDisk`.
3. Except for Microsoft Azure environments, the pagefile is redirected to this formatted volume, `MCSWCDisk`. As a result, this disk size considers the total amount of disk space, including the delta between the disk size and the generated workload plus the pagefile size, typically associated with VM RAM size. Microsoft Azure pagefile is pre-configured to use a local temporary disk and is not redirected to `MCSWCDisk` by MCS storage optimization I/O functionality.

Enabling MCS storage optimization updates To enable MCS I/O storage optimization functionality, upgrade the Delivery Controller and the VDA to the latest version of Citrix Virtual Apps and Desktops.

> **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.

When enabling the MCS storage optimization update, consider the following:

- When creating a machine catalog, the administrator can configure the RAM and disk size.



- When updating an existing machine catalog to a new VM snapshot containing a VDA with Citrix Virtual Apps and Desktops version 1903, it continues to use the existing catalog's MCS I/O setting for RAM and disk size. The existing raw disk is formatted.

> **Important:**
>
> MCS storage optimization changed with Citrix Virtual Apps and Desktops version 1912 LTSR. This release supports file-based write cache technology, providing better performance and stability. The new functionality provided by MCS I/O could require a higher write cache storage requirement compared to previous Citrix Virtual Apps and Desktops releases. Citrix recommends that you reevaluate the disk size to ensure that it has sufficient disk space for the allocated workflow and additional pagefile size. The pagefile size is typically related to the amount of system RAM. If the existing catalog disk size is insufficient, create a new machine catalog and allocate a larger write cache disk.

About Microsoft Azure environments By default, the MCS I/O write cache disk is provisioned during initial VM boot and is deleted after shutting down the VM. This is the most cost effective setting, however, the VM boot time is longer because it involves formatting the write cache disk and an extra reboot. For environments containing workloads with sensitive boot times, Citrix recommends using PowerShell to create a VM with persisted MCS I/O cache disk. The persisted cache disk is not deleted

during the power cycle event, however, the cost of Azure storage account charges should be considered.

Using PowerShell to create an Azure catalog with persistent write-back cache disk To configure an Azure catalog with persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`. This parameter supports an extra property, `PersistWBC`, used to determine how the write-back cache disk persists for Azure Resource Manager hosted 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.

> **Tip:**
>
> Because Azure presents numerous properties specific to provisioning, the `CustomProperties` field is used for many settings.

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-->
```

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**.

When the `PersistWBC` property is set to **true**, the write-back cache disk is not deleted when the Citrix Virtual Apps and Desktops administrator shuts down the machine using Citrix Studio.

When the `PersistWBC` property is set to **false**, the write-back cache disk is deleted when the Citrix Virtual Apps and Desktops administrator shuts down the machine using Citrix Studio.

> **Note:**
>
> If the `PersistWBC` property is omitted, the property defaults to **false** and the write-back cache is deleted when the machine is shutdown using Citrix Studio.

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. The `PersistWBC` value is only used for catalogs deployed to Azure Resource Manager.

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-->
```


AWS dedicated host tenancy support

You can use MCS to provision AWS dedicated hosts. An administrator can create a catalog of machines with host tenancy defined through PowerShell.

An Amazon [EC2] dedicated host is a physical server with [EC2] instance capacity that is fully dedicated, allowing you to 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.

The requirements for provisioning to AWS hosts include:

- 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.
- enable **auto-placement**.

To provision to a dedicated host in AWS using PowerShell, use the **New-ProvScheme** cmdlet with the parameter TenancyType set to *Host*.

Refer to the Citrix Developer Documentation for more information.

Prepare a master image on the hypervisor or cloud service

For information about creating connections to hypervisors and cloud providers, see Connections and resources.

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 use different terms.
- When using Citrix Provisioning, you can use a master image or a physical computer as the master target device. Citrix Provisioning uses different terminology than MCS to refer to images. See the Citrix Provisioning documentation for details.
- 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 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 Citrix Provisioning or 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, plus 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 using Studio. 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. When using Citrix Provisioning, create a VHD file for the virtual disk from your master target device before you join the master target device to a domain. See the Citrix Provisioning documentation for details.

5. 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.
6. 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, Studio creates a snapshot, but you cannot name it.

Create a machine catalog using Studio

Before starting the catalog creation wizard, review this section.

If you are using a master image, ensure that you have installed a VDA on the image before creating the catalog.

From Studio:

- If you already created a site but haven't yet created a machine catalog, Studio guides you to the correct starting place to create a catalog.
- If you already created a catalog and want to create another, select **Machine Catalogs** in the **Studio** navigation pane. Then select **Create Machine Catalog** in the **Actions** pane.

The wizard walks you through the following items. The wizard pages you see differ, depending on the selections you make.

Operating system

Each catalog contains machines of only one type. Select one.

- **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. (See the Linux VDA documentation for details about that OS.)
- **Single-session OS:** A single-session OS catalog provides VDI desktops that you can assign to various 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.

Machine management

This page does not appear when you are creating Remote PC Access catalogs.

The **Machine Management** page indicates how machines are managed and which tool you use to deploy machines.

Choose whether machines in the catalog are power managed through Studio.

- Machines are power managed through Studio or provisioned through a cloud environment, for example, VMs 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 through Studio, for example, physical machines.

If you indicated that machines are power managed through Studio or provisioned through a cloud environment, choose which tool to use to create VMs.

- **Citrix Machine Creation Services (MCS):** Uses a master image to create and manage virtual machines. Machine catalogs in cloud environments use MCS. MCS is not available for physical machines.
- **Citrix Provisioning:** (Formerly Provisioning Services.) Manages target devices as a device collection. A Citrix Provisioning virtual disk imaged from a master target device delivers desktops and applications.

  > **Note:**
  >
  > This option is no longer supported. To import a Citrix Provisioning target device into a Citrix Virtual Apps and Desktops catalog, use the **Citrix Provisioning Export Devices Wizard**.

- **Other:** 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.

Desktop types (desktop experience)

This page appears only when you are creating a catalog containing single-session OS machines.

The **Desktop Experience** page determines what occurs each time a user logs on. Select one of:

- Users connect to a new (random) desktop each time they log on.
- Users connect to the same (static) desktop each time they log on.

If you choose the second option and are using MCS to provision the machines, you can configure how user changes to the desktop are handled:

- Save user changes to the desktop on a separate Personal vDisk. (Personal vDisk is deprecated.)
- Save user changes to the desktop on the local disk.
- Discard user changes and clear the virtual desktop when the user logs off. Select this option if you are using user personalization layer.

Master image

This page appears only when you are using MCS to create VMs.

On the **Master image** page, select the connection to the host hypervisor or cloud service, and then select the snapshot or VM created earlier. If you are creating the first catalog, the only available connection is the one you configured when you created the site.

Remember:

- When you are using MCS or Citrix Provisioning, do not run Sysprep on master images.
- If you specify a master image rather than a snapshot, Studio creates a snapshot, but you cannot name it.

To enable use of the latest product features, ensure the master image has the latest VDA version installed. Do not change the default minimum VDA selection. However, if you must use an earlier VDA version, see VDA versions and functional levels.

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.

Cloud platform and service environments

When you are using a cloud service or platform to host VMs (such as Azure Resource Manager, Nutanix, or Amazon Web Services), the catalog creation wizard contains more pages specific to that host.

For details, see Where to find information about connection types.

Device Collection

This page appears only when using Citrix Provisioning to create VMs.

The **Device Collection** page displays the device collections and the devices that have not already been added to catalogs.

Select the device collections to use.

Machines

This page does not appear when you are creating Remote PC Access catalogs.

The title of this page depends on what you selected on the **Machine Management** page: **Machines**, **Virtual Machines**, or **VMs and users**.

When using MCS:

- Specify how many virtual machines to create.
- Choose the amount of memory (in MB) each VM has.
- 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 indicated on the **Desktop Experience** page that user changes to static desktops are saved on a separate Personal vDisk, specify the virtual disk size in GB and the drive letter.
- If your deployment contains more than one zone, you can select a zone for the catalog.
- If you are creating static desktop VMs, select a virtual machine copy mode. See Virtual machine copy mode.
- If you are creating random desktop VMs that do not use personal vDisks, you can configure a cache to be used for temporary data on each machine. See Configure cache for temporary data.

When using Citrix Provisioning:

The **Devices** page lists the machines in the device collection that you selected on the previous wizard page. You cannot add or remove machines on this page.

When using other tools:

Add (or import a list of) Active Directory machine account names. You can change the Active Directory account name for a VM after you add/import it. If you specified static machines on the **Desktop Experience** page, you can optionally specify the Active Directory user name for each VM you add.

After you add or import names, you can use the **Remove** button to delete names from the list, while you are still on this page.

When using Citrix Provisioning or other tools (but not MCS):

An icon and tooltip for each machine added (or imported, or from a Citrix Provisioning device collection) help identify machines that might not be eligible to add to the catalog, or be unable to register with a Delivery Controller. For details, see VDA versions and functional levels.

Virtual machine copy mode

The copy mode 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.

VDA versions and functional levels

A catalog's functional level controls which product features are available to machines in the catalog. Using features introduced in new product versions require a new VDA. Setting a functional level makes

all features introduced in that version (and later, if the functional level does not change) available to machines in the catalog. However, machines in that catalog with an earlier VDA version can not register.

A menu near the bottom of the **Machines** (or **Devices**) page allows you to select the minimum VDA level. This sets the catalog's minimum functional level. By default, the most current functional level is selected for on-premises deployments. If you follow the Citrix recommendation to always install and upgrade VDAs and core components to the latest version, you don't need to change this selection. However, if you must continue using older VDA versions, select the correct value.

A Citrix Virtual Apps and Desktops release might not include a new VDA version, or the new VDA does not impact the functional level. In such cases, the functional level might indicate a VDA version that is earlier than the installed or upgraded components. For example, although version 7.17 contains a 7.17 VDA, the default functional level ("7.9 or later") remains the most current. Therefore, after installing or upgrading components 7.9–7.16 to 7.17, you do not need to change the default functional level.

In Citrix Cloud deployments, Studio uses a default functional level that can be earlier than the most current.

The selected functional level affects the list of machines above it. In the list, a tooltip next to each entry indicates whether the machine's VDA is compatible with the catalog at that functional level.

Messages are posted on the page if the VDA on each machine does not meet or exceed the minimum functional level selected. You can continue with the wizard. Those machines will likely not be able to register with a Controller later. Alternatively, you can:

- Remove the machines containing older VDAs from the list, upgrade their VDAs and then add them back to the catalog.
- Choose a lower functional level that prevents access to the latest product features.

A message is also posted if a machine was not be added to the catalog because it is the wrong machine type. Examples include attempting to add a server to a single-session OS catalog, or adding a single-session OS machine originally created for random allocation to a catalog of static machines.

> **Important:**
>
> For release 1811, an extra functional level has been added: **1811 (or newer)**. That level is intended for use with future Citrix Virtual Apps and Desktops features. The **7.9 (or newer)** selection remains the default. That default is valid for all deployments now.
>
> If you select **1811 (or newer)**, any earlier VDA versions in that catalog are unable to register with a Controller or Cloud Connector. However, if the catalog contains only VDAs at version 1811 or later supported versions, they are all eligible to register.

Configure cache for temporary data

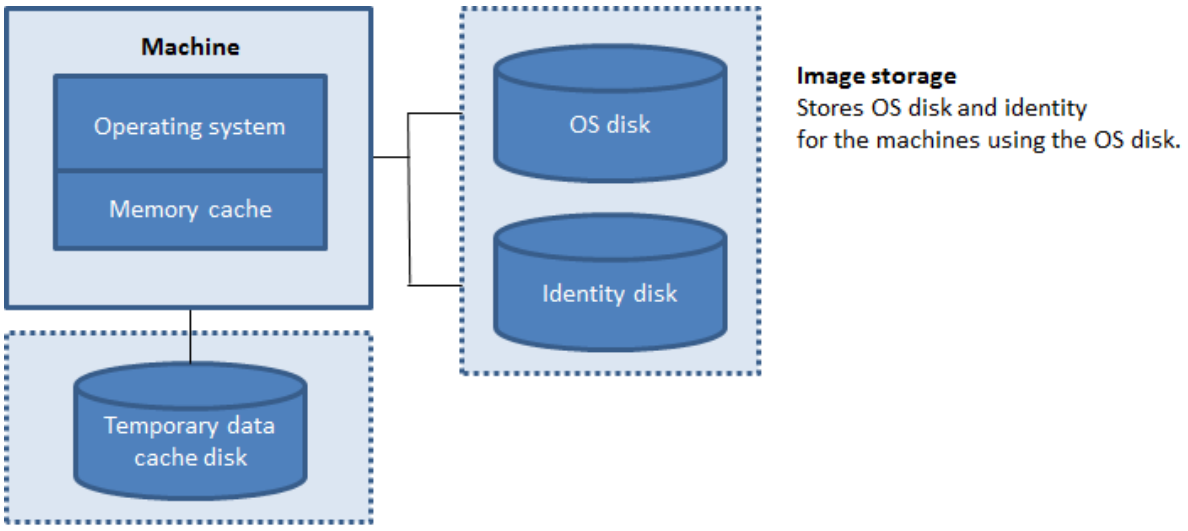
Caching temporary data locally on the VM is optional. You can enable use of the temporary data cache on the machine when you use MCS to manage pooled (not dedicated) machines in a catalog. If the catalog uses a connection that specifies storage for temporary data, you can enable and configure the temporary data cache information when you create the catalog.

> **Important:**
>
> This feature requires a current MCS I/O driver. Installing this driver is an option when you install or upgrade a VDA. By default, that driver is not installed.

You specify whether temporary data uses shared or local storage when you create the connection that the catalog uses. For more information, see Connections and resources. To configure a cache for temporary data on each machine, you can use the following two options: **Memory allocated to cache (MB)** and **Disk cache size (GB)**. By default, the two options are cleared. To enable the Memory allocated to cache (MB) option, select the Disk cache size (GB) check box. If the **Disk cache size** check box is not selected, the Memory allocated to cache option is grayed out. Depending on the connection type, the default values for these options might differ. Generally, the default values are sufficient for most cases. However, take into account 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 might install inside the session.

Windows will not allow a session to use an amount of cache disk that is larger than the amount of free space on the original master image from which machines in the machine catalog are provisioned. For example, there is no benefit specifying a 20 GB cache disk if there is only 10 GB of free space on the master image.



To configure a cache for temporary data on each machine, be aware of the following three scenarios:

- If you don't select the Disk cache size check box and the Memory allocated to cache check box, temporary data is not cached. It is directly written to the difference disk (located in the OS storage) for each VM. (This is the provisioning action in version 7.8 and earlier.)
- If you select the Disk cache size check box and don't select the Memory allocated to cache check box, temporary data is directly written to the cache disk, using a minimal amount of memory cache.
- If you select the Disk cache size check box and the Memory allocated to cache check box, temporary data is initially written to the memory cache. When the memory cache reaches its configured limit (the Memory allocated to cache value), the oldest data is moved to the temporary data cache disk.

> **Important:**
>
> - If the disk cache runs out of space, the user's session becomes unusable.
> - Do not enable caching if you intend to use this catalog to create AppDisks.
> - This feature is not available when using a Nutanix host connection.
> - You cannot change the cache values in a machine catalog after the machine is created.
>
> **Note:**
>
> - The memory cache is part of the total amount of memory on each machine. Therefore, if you enable the Memory allocated to cache option, consider increasing the total amount of memory on each machine.
> - Changing the Disk cache size from its default value can affect performance. The size must

> match user requirements and the load placed on the machine.

Network Interface Cards (NICs)

This page does not appear when you are creating Remote PC Access catalogs.

On the **Network Interface Cards** 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.

Machine accounts

This page appears only when creating Remote PC Access catalogs.

On the **Machine Accounts** page, specify the Active Directory machine accounts or Organizational Units (OUs) to add that correspond to users or user groups. Do not use a forward slash (/) in an OU name.

You can choose a previously configured power management connection or elect not to use power management. If you want to use power management but a suitable connection hasn't been configured yet, you can create that connection later and then edit the machine catalog to update the power management settings.

Computer accounts

This page appears only when using MCS to create VMs.

Each machine in the catalog must have a corresponding Active Directory computer account. On the **Computer Accounts** page, indicate whether to create accounts or use existing accounts, and the location for those accounts.

- If you create accounts, you must have permission to create computer accounts in the OU where the machines reside.

  Specify the account naming scheme for the machines that will be created, using hash marks to indicate where sequential numbers or letters appear. Do not use a forward slash (/) in an OU name. A name cannot begin with a number. 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.

- If you use existing accounts, either 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
...
<!--NeedCopy-->
```

Ensure that there are enough accounts for all the machines you're adding. Studio manages these accounts, so either allow Studio 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 machines or existing machines, select or import existing accounts and assign each machine to both an Active Directory computer account and to a user account.

For machines created with Citrix Provisioning, computer accounts for target devices are managed differently; see the Citrix Provisioning documentation.

Summary, name, and description

On the **Summary** page, review the settings you specified. Enter a name and description for the catalog. This information appears in Studio.

When you're done, click **Finish** to start the catalog creation.

Troubleshoot

> **Important:**
>
> After creating the machine catalog using Citrix Studio, you can no longer use the `Get-ProvTask` PowerShell command to retrieve the tasks associated with machine catalog creation. This restriction is a result of the fact that Studio deletes those tasks after machine catalog creation regardless of whether the catalog is created successfully.

Citrix recommends collecting logs to help the Support team provide solutions. When using Citrix Provisioning, use the following procedure to generate log files:

1. On the master image, create the following registry key with the value of 1 (as a DWORD (32-bit) value): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Shut down the master image and create a snapshot.
3. On the Delivery Controller, run the following PowerShell command: `Set-ProvServiceConfiguration -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Create a catalog based on that snapshot.
5. When the preparation VM is created on the hypervisor, log in and extract the following files from the root of C:\: Image-prep.log and PvsVmAgentLog.txt.

6. Shut down the machine, at which point it reports the failure.
7. Run the following PowerShell command to re-enable auto shutdown of the image preparation machines: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAu`
   .

Where to go next

If this is the first catalog created, Studio guides you to create a Delivery Group.

Manage machine catalogs

March 21, 2023

Introduction

You can add or remove machines from a machine catalog, rename, change the description, or manage a catalog's Active Directory computer accounts.

Maintaining catalogs can also include making sure 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 master image used in the catalog and then updating the machines. This method enables you to efficiently update large numbers of user machines.
- For machines created using Citrix Provisioning, updates to machines are propagated through the virtual disk. See the Citrix Provisioning documentation for details.
- For catalogs containing static, permanently assigned machines, and for Remote PC Access Machine catalogs, you manage updates to users' machines outside of Studio. Perform this task either individually or collectively using third-party software distribution tools.

For information about creating and managing connections to host hypervisors and cloud services, see 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 an MCS catalog created using persistent, or dedicated instances, any new machines created for the catalog use the updated image. Pre-existing instances continue to use the original instance. 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 the machine is reset.
- With persistent machine catalogs, updating the image also updates the catalog instances that use it.
- For catalogs that do not persist, if you want different images for different machines, the images must reside in separate catalogs.

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 Studio to create Active Directory computer accounts for the additional machines, you must have appropriate domain administrator permission.

To add machines to a catalog:

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a machine catalog and then select **Add machines** in the **Actions** pane.
3. Select the number of virtual machines to add.
4. 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. Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters appear. Do not use a forward slash (/) in an OU name. A name cannot begin with a number. 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.
5. If you use existing Active Directory accounts, either browse to the accounts or click **Import** and specify a .csv file containing account names. Make sure that there are enough accounts for all

the machines you're adding. Studio manages these accounts. Either allow Studio to reset the passwords for all the accounts, or specify the account password, which must be the same for all 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 Studio.

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. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **View Machines** in the **Actions** pane.
3. Select one or more machines and then select **Delete** in the **Actions** pane.

Choose whether to delete the machines being removed. If you choose to delete the machines, indicate whether the Active Directory accounts for those machines should be retained, disabled, or deleted.

When you delete an Azure Resource Manager machine catalog, the associated machines and resource groups are deleted from Azure, even if you indicate that they should be retained.

Change a catalog description or change Remote PC Access settings

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Edit Machine Catalog** in the **Actions** pane.
3. (Remote PC Access catalogs only) On the **Power Management** page, you can change the power management settings and select a power management connection. On the **Organizational Units** page, add or remove Active Directory OUs.
4. On the **Description** page, change the catalog description.

Rename a catalog

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Rename Machine Catalog** in the **Actions** pane.
3. Enter the new name.

Move a catalog to a different zone

If your deployment has more than one zone, you can move a catalog from one zone to another.

Keep in mind that moving a catalog to a different zone than the hypervisor or cloud service containing the VMs in that catalog can affect performance.

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Move** in the **Actions** pane.
3. Select the zone where you want to move the catalog.

Delete a catalog

Before deleting a catalog, ensure that:

- All users are logged off and that 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 a Delivery Group. In other words, the Delivery Group does not contain machines from the catalog.

To delete a catalog:

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Delete Machine Catalog** in the **Actions** pane.
3. Indicate whether the machines in the catalog should be deleted. If you choose to delete the machines, indicate whether the Active Directory computer accounts for those machines should be retained, disabled, or deleted.

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 OS and multi-session OS 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. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Manage AD accounts** in the **Actions** pane.

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 Active Directory should be kept, disabled, or deleted.

You can also indicate whether Active Directory accounts should be retained, disabled, or deleted when you remove machines from a catalog or delete a catalog.

Update a catalog

Citrix recommends that you save copies or snapshots of master images before you update the machines in the catalog. The database keeps a historical record of the master images used with each machine catalog. Roll back, or revert, machines in a catalog to use the previous version of the master image. Perform this task if users encounter problems with updates you deployed to their desktops, minimizing user downtime. Do not delete, move, or rename master images; otherwise, you cannot revert a catalog to use them.

For catalogs that use Citrix Provisioning (formerly Provisioning Services), you must publish a new virtual disk to apply changes to the catalog. For details, see the Citrix Provisioning documentation.

After a machine is updated, it restarts automatically.

Update or create a master image

Before you update the machine catalog, either update an existing master image or create a one on your host hypervisor.

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 revert (roll back) machines in the catalog, if needed.
2. If necessary, power on the master image, and log on.
3. Install updates or make any required changes to the master image.
4. If the master 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 the catalog is updated in Studio. Although Studio can create a snapshot, Citrix recommends that you create a snapshot using the hypervisor management console, and then select that snapshot in Studio. This enables you to provide a meaningful name and description rather than

an automatically generated name. For GPU master images, you can change the master image only through the Citrix Hypervisor console.

Update the catalog

To prepare and roll out the update to all machines in a catalog:

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Update Machines** in the **Actions** pane.
3. On the **Master Image** page, select the host and the image you want to roll out.
4. On the **Rollout Strategy** page, choose when the machines in the machine catalog are updated with the new master image: on the next shutdown or immediately.
5. Verify the information on the **Summary** page and then click **Finish**. Each machine restarts automatically after it is updated.

If you are updating a catalog using the PowerShell SDK directly, rather than Studio, you can specify a hypervisor template (VMTemplates), as an alternative to an image or a snapshot of an image.

Rollout strategy:

Updating the image on 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. Consider the following:

- New sessions cannot be launched until the update has completed on applicable machines.
- For desktop OS machines, machines are immediately updated when the machine is not in use, or when users are not logged in.
- For a server 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.

If you choose to update the image immediately, configure a distribution time and notifications.

- **Distribution time:** You can choose to update all machines at the same time, or specify the total length of time it should take to begin updating all machines in the catalog. An internal algorithm determines when each machine is updated and restarted during that interval.
- **Notification:** In the left notification dropdown, choose whether to display a notification message on the machines before an update begins. By default, no message is displayed. If you choose to display a message 15 minutes before the update begins, you can choose (in the right

dropdown) to repeat the message every five minutes after the initial message. By default, the message is not repeated. Unless you choose to update all machines at the same time, the notification message displays on each machine at the appropriate time before the update begins, calculated by an internal algorithm.

Roll back an update

After you roll out an updated/new master 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 will no longer be available. As with the rollout, rolling back a machine includes a restart.

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select the catalog and then select **Rollback machine update** in the **Actions** pane.
3. Specify when to apply the earlier master image to machines, as described above for the rollout operation.

The rollback is applied only to machines that need to be reverted. For machines that have not been updated with the new/updated master image (for example, machines with users who have not logged off), users do not receive notification messages and are not forced to log off.

Upgrade a catalog or revert an upgrade

Upgrade the machine catalog after you upgrade the VDAs on the machines to a newer version. Citrix recommends upgrading all VDAs to the latest version to enable access to all the newest features.

Before upgrading a catalog:

- If you're using Citrix Provisioning, upgrade the VDA version. The provisioning console does not retain the VDA version. Citrix Provisioning communicates directly with the Citrix Virtual Apps and Desktops Setup Wizard to set the VDA version in the created catalog.
- Start the upgraded machines so that they register with the Controller. This lets Studio determine that the machines in the catalog need upgrading.

To upgrade a catalog:

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select the catalog. The **Details** tab in the lower pane displays version information.
3. Select **Upgrade Catalog**. If Studio detects that the catalog needs upgrading, it displays a message. Follow the prompts. If one or more machines cannot be upgraded, a message explains why. Citrix recommends you resolve machine issues before upgrading the catalog to ensure that all machines function properly.

After the catalog upgrade completes, you can revert the machines to their previous VDA versions by selecting the catalog and then selecting **Undo** in the **Actions** pane.

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.

Create Delivery Groups

June 24, 2021

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 and/or desktops available to those users.

Creating a Delivery Group is the next step in configuring your deployment after creating a Site and 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.

For Remote PC Access, when you create a Site, a Delivery Group named "Remote PC Access Desktops" is automatically created.

To create a Delivery Group:

1. If you have created a Site and a machine catalog, but haven't yet created a Delivery Group, Studio guides you to the correct starting place to create a Delivery Group. If you have already created a Delivery Group and want to create another, select **Delivery Groups** in the Studio navigation pane and then select **Create Delivery Group** in the Actions pane.
2. The Create Delivery Group wizard launches with an **Introduction** page, which you can remove from future launches of this wizard.
3. The wizard then guides you through the pages described below. When you are done with each page, click **Next** until you reach the final page.

Step 1. Machines

On the **Machines** page, select a 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 (Server OS, Desktop 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.
- Citrix recommends that you install or upgrade all machines with the most recent VDA version, and then upgrade 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. (This is called the group's *functional level*.) For example, if one of the machines you select has VDA version 7.1 installed and other machines have the current 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 later VDA versions might not be available in that Delivery Group. For example, to use the AppDisks feature, the VDAs (and therefore the group's functional level) must be a minimum version 7.8.
- Each machine in a Remote PC Access catalog is automatically associated with a Delivery Group; when you create a Remote PC Access Site, a catalog named "Remote PC Access Machines"and a Delivery Group named "Remote PC Access Desktops"are created automatically.
- 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. Delivery type

This page appears only if you chose a catalog containing static (assigned) desktop OS machines.

On the **Delivery Type** page, choose either **Applications** or **Desktops**. You cannot enable both.

If you selected machines from a server OS or desktop OS random (pooled) catalog, the delivery type is assumed to be applications and desktops: you can deliver applications, desktops, or both.

Step 3. AppDisks

AppDisks are deprecated.

To add an AppDisk, click **Add**. The Select AppDisks dialog box lists available AppDisks in the left column. The right column lists the applications on the AppDisk. Selecting the **Applications** tab above the right column lists applications in a format similar to a Start menu; selecting the **Installed packages** tab lists applications in a format similar to the Programs and Features list.

Select one or more checkboxes.

Step 4. Users

Specify the users and user groups who can use the applications and desktops in the Delivery Group.

Where user lists are specified

Active Directory user lists are specified when you create or edit the following:

- A Site's user access list, which is not configured through Studio. By default, the application entitlement policy rule includes everyone. See the PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlets for details.
- Application Groups (if configured).
- Delivery Groups.
- Applications.

The list of users who can access an application through StoreFront is formed by the intersection of the above user lists. For example, to configure the use of application A to a particular department, without unduly restricing access to other groups:

- Use the default application entitlement policy rule that includes everyone.
- Configure the Delivery Group user list to allow all headquarters users to use any of the applications specified in the Delivery Group.
- (If Application Groups are configured) Configure the Application Group user list to allow members of the Administration and Finance business unit to access applications A through L.
- Configure application A's properties to restrict its visibility to only Accounts Receivable staff in Administration and Finance.

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 desktop OS machines, you can import user data (a list of users) later by editing the Delivery Group.
- **Unauthenticated (anonymous):** For Delivery Groups containing server 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 VDA for Windows Server OS (minimum version 7.6) 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 are named Anon*XYZ*, 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 authetnicated and unauthenticated users	Yes	Yes

Step 5. Applications

Good to know:

- You cannot add applications to Remote PC Access Delivery Groups.
- By default, new applications you add are placed in a folder named Applications. You can specify a different folder. For details, see the Manage Applications article.
- You can change the properties for an application when you add it to a Delivery Group, or later. For details, see the Manage 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 sufficient permission to view the application in all of 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 in Studio; otherwise, users will see duplicate names in Citrix Workspace app.

Click **Add** to display the application sources.

- **From Start menu:** Applications that are discovered on a machine created from the master 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 click **OK**.
- **Manually defined:** 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, click **OK**.
- **Existing:** Applications previously added to the Site, 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 click **OK**.
- **App-V:** Applications in App-V packages. When you select this source, a new page launches where you select the App-V server or the Application Library. Select the applications you want to add from the resulting display and then click **OK**. For more information, see App-V.

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 Site. Or, an application might not be compatible with the supported session types on machines in the selected catalog.

Step 6. Desktops

The title of this page depends on the catalog you chose on the **Machines** page:

- 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 User Assignments**.
- If you chose a catalog containing assigned machines and specified "Applications"on the **Delivery Type** page, this page is titled **Application Machine User Assignments**.

Click **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 dropdown. For more information, see Tags.
- Using the radio buttons, indicate who can launch a desktop (for groups with pooled machines) or who will be assigned a machine when they launch the desktop (for groups with assigned machines). The users can be either everyone who can access this Delivery Group, or specific users and user groups.
- 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, click **OK**.

Maximum instances of a desktop in a Site (PowerShell only)

To configure the maximum instances of a desktop in the Site (PowerShell only):

- In PowerShell, use the appropriate BrokerEntitlementPolicyRule cmdlet with the MaxPerEntitlementInstances parameter. For example, the following cmdlet modifies the "tsvda-desktop" rule to set the maximum concurrent instances of a desktop allowed in the Site to two. When there are two desktop instances running, an error occurs if a third subscriber attempts to start a desktop.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
   2
  ```

- For guidance, use the Get-Help cmdlet. For example, `Get-Help Set-BrokerEntitlementPolicyRu -Parameter MaxPerEntitlementInstances`.

Step 7. Summary

Enter a name for the Delivery Group. You can also (optionally) enter a description, which will appear in the Citrix Workspace app and in Studio.

Review the summary information and then click **Finish**. If you did not select any applications or specify any desktops to deliver, you are asked if you want to continue.

Manage Delivery Groups

November 8, 2022

Introduction

This article describes procedures for managing Delivery Groups from the management console. In addition to changing 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. 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

- Change the delivery type
- Change StoreFront addresses
- Upgrade a Delivery Group
- Manage Remote PC Access Delivery Groups

Change the delivery type of a Delivery Group

The delivery type indicates what the group can deliver: applications, desktops, or both.

Before changing an **application only** or **desktops and applications** type to the **desktops only** type, delete all applications from the group.

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Delivery Type** page, select the delivery type you want.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Change StoreFront addresses

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **StoreFront** page, select or add StoreFront URLs that are used by the Citrix Workspace app, which is installed on each machine in the Delivery Group.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

You can also specify StoreFront server addresses by selecting **Configuration > StoreFront** in the navigation pane.

Upgrade a Delivery Group or revert an upgrade

Upgrade a 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 the Delivery Group upgrade:

- 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 a Delivery Controller. This process tells the console about what needs upgrading in the Delivery Group.
- If you must continue to use earlier VDA versions, newer product features may not be available. For more information, see the upgrade documentation.

To upgrade a Delivery Group:

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Upgrade Delivery Group** in the Actions pane. The **Upgrade Delivery Group** action appears only if upgraded VDAs are detected.

The display indicates you which, if any, machines cannot be upgraded and why. You can then cancel the upgrade, resolve the machine issues, and then start the upgrade again.

After the upgrade completes, you can revert the machines to their previous states by selecting the Delivery Group and then clicking **Undo** in the Actions pane.

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 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. Select **Delivery Groups** in the navigation pane.
2. Select a Remote PC Access group.
3. In the **Details** section, click the **Machine Catalogs** tab and then select a Remote PC Access catalog.
4. To add or restore an association, click **Add Desktops**. To remove an association, click **Remove Association**.

Users

- Change user settings
- Add or remove users

Change user settings in a Delivery Group

The name of this page appears as either **User Settings** or **Basic Settings**.

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **User Settings** (or **Basic Settings**) page, change any of the settings in the following table.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **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.
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 additional encryption methods such as TLS encryption when traversing public networks. Also, SecureICA does not check data integrity.

Add or remove users in a Delivery Group

For detailed information about users, see Users.

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Users** page:
   - To add users, click **Add**, and then specify the users you want to add.
   - To remove users, select one or more users and then click **Remove**.
   - Select or clear the check box to allow access by unauthenticated users.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Import or export user lists For Delivery Groups containing physical single-session OS machines, you can import user information from a .csv file after you create the Delivery Group. You can also export user information to a .csv file. The .csv file can contain data from a previous product version.

The first line in the .csv file must contain comma-separated column headings (in any order), which can include: `ADComputerAccount`, `AssignedUser`, `VirtualMachine`, and `HostId`. Subsequent lines in the file contain comma-separated data. The `ADComputerAccount` entries can be common names, IP addresses, distinguished names, or domain and computer name pairs.

To import or export user information:

1. Select **Delivery Groups** in the navigation pane.

2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Machine Allocation** page, select **Import** list or **Export** list, and then browse to the file location.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Machines

- Change assignments of machines to users
- Change the maximum number of machines per user
- Update a machine
- Add, change, or remove a tag restriction for a desktop
- Remove a machine
- Restrict access to machines
- Prevent users from connecting to a machine (maintenance mode)
- Shut down and restart machines
- Create and manage restart schedules for machines
- Load manage machines
- Power manage 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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Desktops** or **Desktop Assignment Rules** page (the page title depends on the type of machine catalog the Delivery Group uses), specify the new users.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Change the maximum number of machines per user in a Delivery Group

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Desktop Assignment Rules** page, set the maximum desktops per user value.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Update a machine in a Delivery Group

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **View Machines** in the Actions pane.
3. Select a machine and then click **Update Machines** in the Actions pane.

To choose a different master image, select **Master 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 master 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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Desktops** page, select the desktop and click **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. Click **Apply** to apply any changes you made and keep the window open. Or, click **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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **View Machines** in the Actions pane.
3. Ensure that the machine is shut down.
4. Select the machine and then click **Remove from Delivery Group** in the Actions pane.

You can also remove a machine from a Delivery Group through the connection the machine uses.

Restrict access to machines in a Delivery Group

Any changes you make to restrict access to machines 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 SmartAccess policy expressions:** Use policy expressions to filter user connections made through Citrix Gateway.

  1. Select **Delivery Groups** in the navigation pane.
  2. Select a group and then click **Edit Delivery Group** in the Actions pane.
  3. On the **Access Policy** page, select **Connections through NetScaler Gateway**.
  4. To choose a subset of those connections, select **Connections meeting any of the following filters**. Then define the Citrix Gateway site, and add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios. For details, see the Citrix Gateway documentation.
  5. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

- **Restrict access for users through exclusion filters:** Use exclusion filters on access policies that you set in the SDK. Access policies are applied to Delivery Groups to refine connections. For example, you can restrict machine access to a subset of users, and you can specify allowed user devices. Exclusion filters further refine access policies. For example, for security, you can deny access to a subset of users or devices. By default, exclusion filters are disabled.

  For example, for a teaching lab on a corporate network subnet, to prevent access from that lab to a particular Delivery Group, regardless of who is using the machines in the lab, use the command: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

You can use the asterisk (*) wildcard to match all tags that start with the same policy expression. For example, if you add the tag `VPDesktops_Direct` to one machine and `VPDesktops_Test` to another, setting the tag in the `Set-BrokerAccessPolicy` script to `VPDesktops_*` applies the filter to both machines.

If you are connected using a web browser or with the Citrix Workspace app user experience feature enabled in the store, you cannot use a client name exclusion filter.

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. Select **Delivery Groups** in the navigation pane.
2. Select a group.
3. To turn on maintenance mode for all machines in the Delivery Group, click **Turn On Maintenance Mode** in the Actions pane.

   To turn on maintenance mode for one machine, click **View Machines** in the Actions pane. Select a machine, and then click **Turn On Maintenance Mode** in the Actions pane.
4. To turn maintenance mode off for one or all machines in a Delivery Group, follow the previous instructions, but click **Turn Off Maintenance Mode** in the Actions pane.

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 above.
- 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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **View Machines** in the Actions pane.
3. Select the machine and then click one of the following entries in the Actions pane (some options may 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.

Citrix recommends that you prevent single-session OS machine users from selecting **Shut down** within a session. See the Microsoft policy documentation for details.

You can also shut down and restart machines on a connection.

Create and manage restart schedules for machines in a Delivery Group

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 of 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 should 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 significantly 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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
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 (applled) 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. Select **Delivery Groups** in the navigation pane.
2. Select the group containing the machines to be controlled by the schedule.
3. Click **View Machines** and then select the machines you want to add a tag to.
4. Click **Manage Tags** in the Actions pane.
5. If the tag exists, enable the check box next to the tag name. If the tag does not exist, click **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. Click **Save** in the **Manage Tags** dialog.

Create a restart schedule

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Restart Schedule** page, click **Add**.
4. On the **Add Restart Schedule** page:
    - Type a schedule name and description.
    - If you're using a tag restriction, select the tag.
    - In **Restart frequency**, select how often the restart occurs: daily, weekdays, weekend days, or a specific day each week.
    - Using the 24-hour clock, specify the time of day to begin the restart.
    - For **Restart** duration, choose whether all machines should be restarted at the same time, or the total length of time to begin restarting all of the affected machines. An internal algorithm determines when each machine is restarted during that interval.
    - In **Send notification to users**, choose whether to display a notification message on the affected machines before a restart begins. By default, no message is displayed.
    - 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 is not repeated.
    - Enter the notification title and text. There is no default text.

      If you want the message to include the number of minutes before restart, include the variable **%m%**. For example: "Warning: Your computer is automatically restarted in %m%

minutes."The value decrements by five minutes in each repeated message. Unless you chose to restart all machines at the same time, the message displays on each machine at the appropriate time before the restart, calculated by the internal algorithm.

- To enable the schedule, select the check box. To disable the schedule, clear the check box.

5. Click **Apply** to apply changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Edit, remove, enable, or disable a restart schedule

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Restart Schedule** page, select the check box for a schedule.
    - To edit a schedule, click **Edit**. Update the schedule configuration, using the guidance in Create a restart schedule.
    - To enable or disable a schedule, click **Edit**. Select or clear the **Enable restart schedule** check box.
    - To remove a schedule, click **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 through 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 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 could 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, 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. You cannot set this value when configuring a restart schedule in Studio.

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), Studio (Manage) 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 heading, 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.

Power manage machines in a Delivery Group

You can power manage only virtual single-session OS machines, not physical machines (including Remote PC Access machines). Single-session OS machines with GPU capabilities cannot be suspended, so power-off operations fail. For multi-session OS machines, you can create a restart schedule.

In Delivery Groups containing pooled machines, virtual single-session OS machines can be in one of the following states:

- Randomly allocated and in use
- Unallocated and unconnected

In Delivery Groups containing static machines, virtual single-session OS machines can be:

- Permanently allocated and in use
- Permanently allocated and unconnected (but ready)
- Unallocated and unconnected

During normal use, static Delivery Groups typically contain both permanently allocated and unallocated machines. Initially, all machines are unallocated (except for those manually allocated when the Delivery Group was created). As users connect, machines become permanently allocated. You can fully power manage the unallocated machines in those Delivery Groups, but only partially manage the permanently allocated machines.

- **Pools and buffers:** For pooled Delivery Groups and static Delivery Groups with unallocated machines, a pool (in this instance) is a set of unallocated or temporarily allocated machines that are kept in a powered-on state, ready for users to connect. A user gets a machine immediately after logon. The pool size (the number of machines kept powered-on) is configurable by time of day. For static Delivery Groups, use the SDK to configure the pool.

  A buffer is an additional standby set of unallocated machines that are turned on when the number of machines in the pool falls below a threshold. The threshold is a percentage of the Delivery Group size. For large Delivery Groups, a significant number of machines might be turned on when the threshold is exceeded. So, plan Delivery Group sizes carefully or use the SDK to adjust the default buffer size.

- **Power state timers:** You can use power state timers to suspend machines after users have disconnected for a specified amount of time. For example, machines suspend automatically outside of office hours if users are disconnected for at least 10 minutes. Random machines or machines with personal vDisks automatically shut down when users log off, unless you configure the `ShutdownDesktopsAfterUse` Delivery Group property in the SDK.

  You can configure timers for weekdays and weekends, and for peak and nonpeak intervals.

- **Partial power management of permanently allocated machines:** For permanently allocated machines, you can set power state timers, but not pools or buffers. The machines are turned on at the start of each peak period, and turned off at the start of each off-peak period. You do not have the fine control that you have with unallocated machines over the number of machines that become available to compensate for machines that are consumed.

Power manage virtual single-session OS machines

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Power Management** page, select **Weekdays** in **Power manage machines**. By default, weekdays are Monday to Friday.
4. For random Delivery Groups, in **Machines to be powered on**, click **Edit** and then specify the pool size during weekdays. Then, select the number of machines to power on.
5. In **Peak hours**, set the peak and off-peak hours for each day.
6. Set the power state timers for peak and non-peak hours during weekdays: In **During peak hours > When disconnected**, specify the delay (in minutes) before suspending any disconnected machine in the Delivery Group, and then select **Suspend**. In **During off-peak hours > When disconnected**, specify the delay before turning off any logged-off machine in the Delivery Group, and then select **Shutdown**. This timer is not available for Delivery Groups with random machines.
7. Select **Weekend** in **Power manage machines**, and then configure the peak hours and power state timers for weekends.
8. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

Use the SDK to:

- Shut down, rather than suspend, machines in response to power state timers, or if you want the timers to be based on logoffs, rather than disconnections.
- Change the default weekday and weekend definitions.
- Disable power management. See CTX217289.

Power manage VDI machines transitioning to a different time period with disconnected sessions

> **Important:**
>
> This enhancement applies only to VDI machines with disconnected sessions. It does not apply to VDI machines with logged off sessions.

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 Citrix Virtual Apps and Desktops 7 1909, the machine is suspended or powered off 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 VDI 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 VDI machine with a session disconnected during peak times remained powered on when it transitioned from peak to off-peak. Starting with Citrix Virtual Apps and Desktops 7 1909, the `OffPeakDisconnectAction` and the `OffPeakDisconnectTimeout` policy actions are applied to the VDI 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 VDI (single session) 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.

Change the percentage of VDAs in a powered state for catalogs

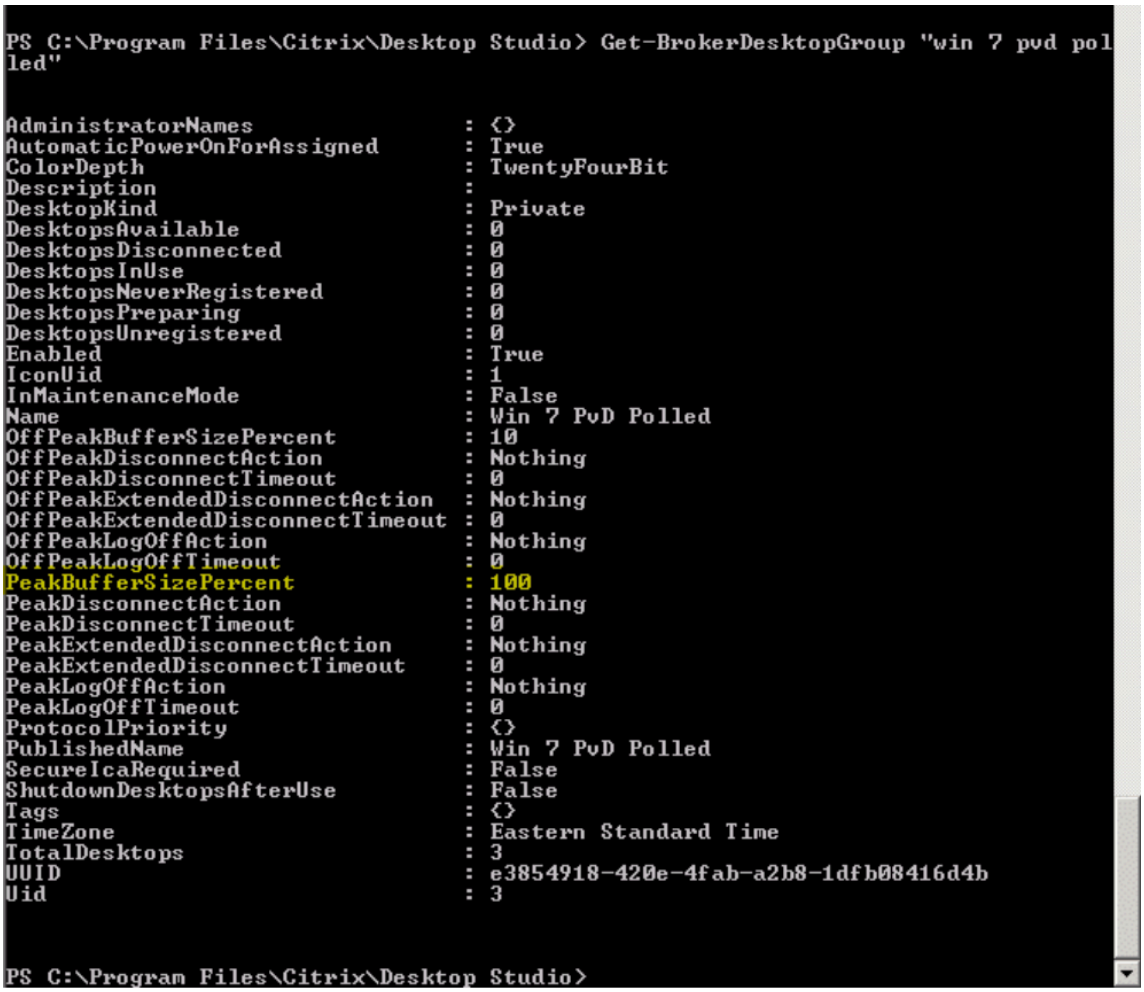
1. Adjust the peak hours for the Delivery Group from the **Power management** section for the **Delivery Group**.
2. Make a note of the Desktop Group name.
3. With administrator privileges, start PowerShell and run the following commands. Replace "Desktop Group Name"with the name of your desktop group that has a changed percentage of the VDAs running.

   ```
   asnp Citrix*

   # Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
    100
   ```

   A value of 100 means that 100% of the VDAs are in the ready state.
4. Verify the solution by running:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



It can take up to an hour for changes to take effect.

To shut down the VDAs after the user logs off, enter:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

To restart VDAs during peak hours, so that they're ready for users after they log off, enter:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

Sessions

- Log off or disconnect a session, or send a message to users
- Configure session prelaunch and session linger

Log off or disconnect a session

1. In the Studio navigation pane, select **Delivery Groups**.
2. Select a delivery group and then select **View Machines** in the **Actions** pane.
3. In the middle pane, select the machine, select **View Sessions** in the **Actions** pane, and then select a session.
    - Alternatively, in the middle pane, select the **Session** tab and then select a session.
4. To log off a user from a session, select **Log off** in the **Actions** pane. The session closes and the user is logged out. The machine becomes available to other users unless it is allocated to a specific user.
5. To disconnect a session, select **Disconnect** in the **Actions** pane. Applications continue to run in the session and the machine remains allocated to that user. The user can reconnect to the same machine.

You can configure power state timers for single-session OS machines to automatically handle unused sessions. For details, see Power manage machines.

Send a message to a Delivery Group

1. In the Studio navigation pane, select **Delivery Groups**.
2. Select a delivery group and then select **View Machines** in the **Actions** pane.
3. In the middle pane, select a machine to which you want to send a message.
4. In the **Actions** pane, select **View Sessions**.
5. In the middle pane, select all sessions and then select **Send Message** in the **Actions** pane.

6. Type your message and click **OK**. You can specify the level of severity if needed. Options include **Critical**, **Question**, **Warning**, and **Information**.

Alternatively, you can send a message by using Citrix Director. For more information, see Send messages to users.

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) and 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 additional 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-/Set-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 configured 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.

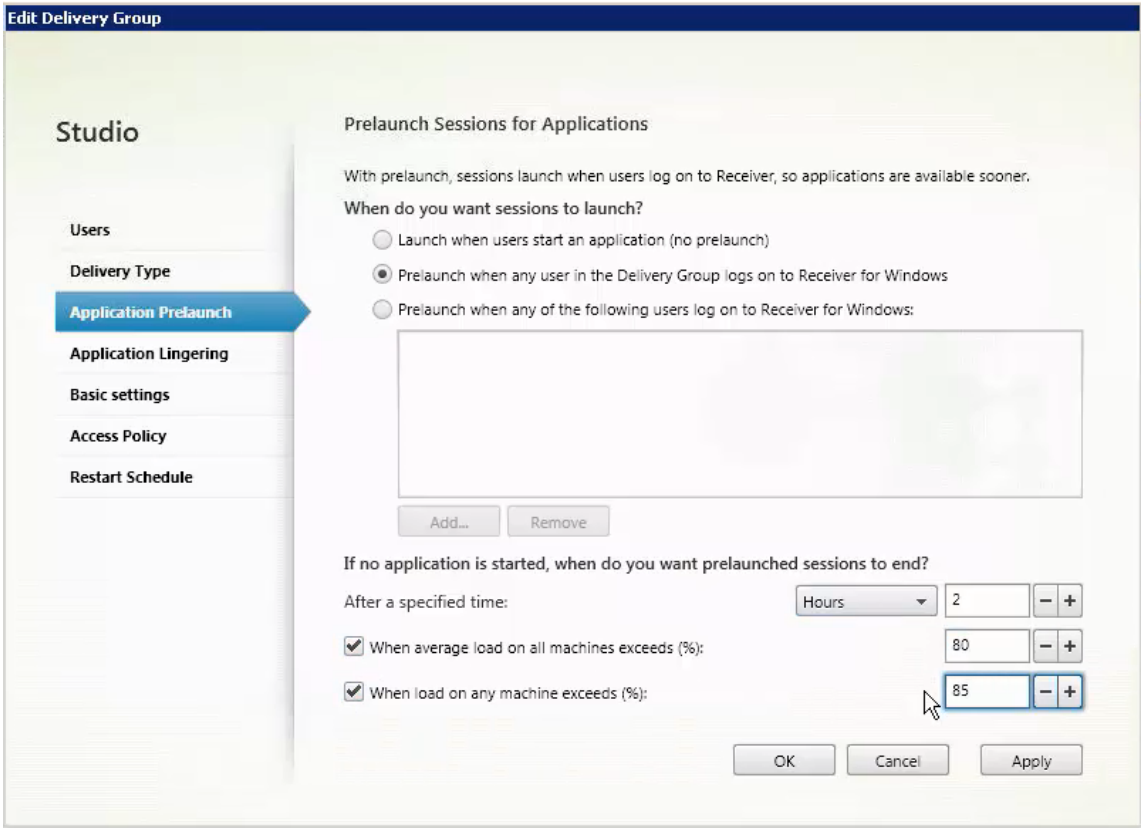
  You can configure two thresholds: the average percentage load of all servers in the Delivery Group, and the maximum percentage load of a single server in the group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended. Sessions are 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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
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.



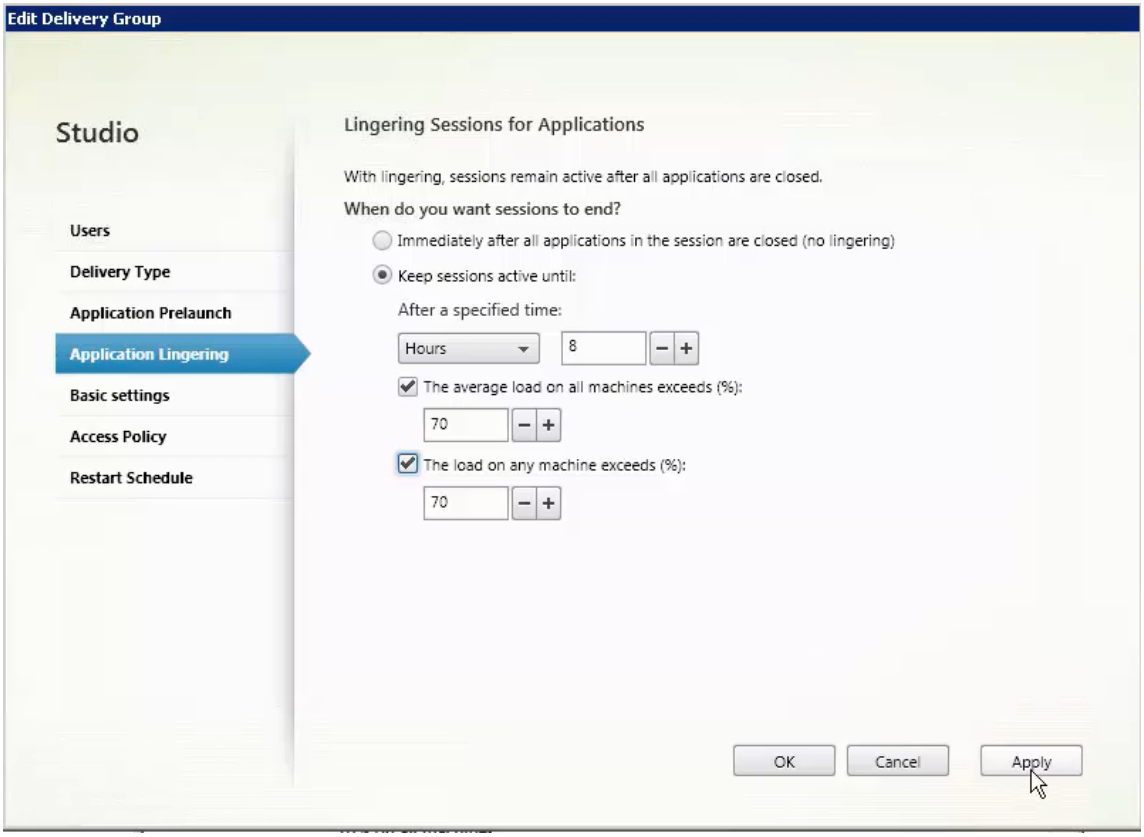
4. A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active.

    - 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. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
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.

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 should 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

February 7, 2020

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:

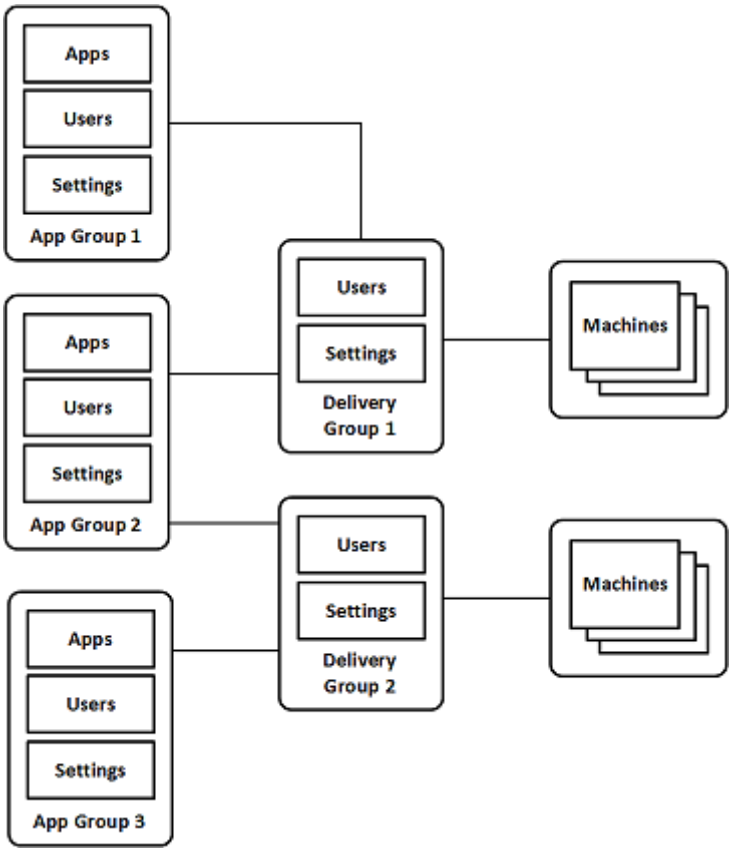
- The logical grouping of applications and their settings lets you manage those applications as a single unit. For example, you don't have to add (publish) the same application to individual Delivery Groups one at a time.
- Session sharing between Application Groups can conserve resource consumption. 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 Citrix Virtual Apps and Desktops 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.)

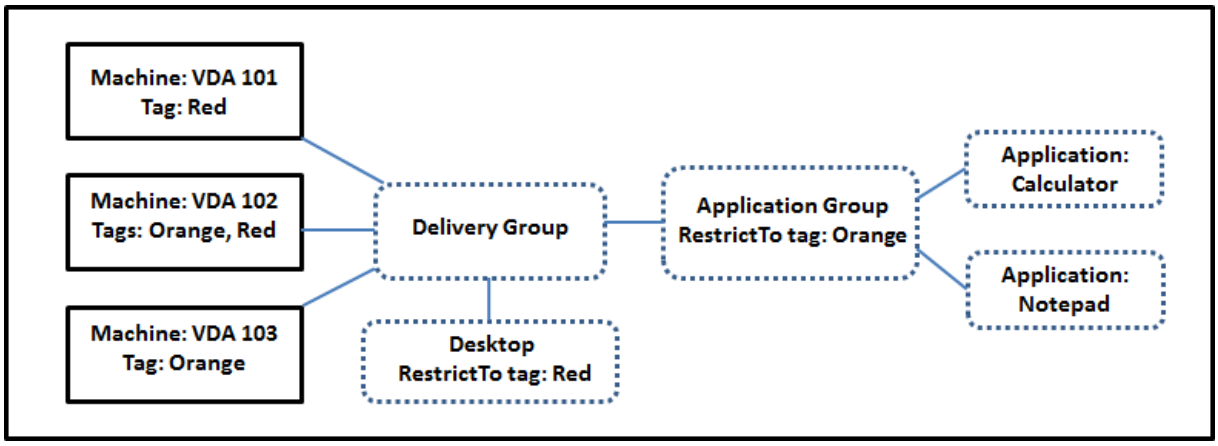
Application Group 1 is associated with Delivery Group 1. The applications in Application Group 1 can be accessed by the users specified in Application Group 1, as long as they are also in the user list for Delivery Group 1. This follows the guidance that the user list for an Application Group should 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 that your Delivery Groups be upgraded to the current version. This requires:

1. Upgrading VDAs on the machines used in the Delivery Group
2. Upgrading the machine catalogs containing those machines
3. Upgrading 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 controller finds that 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 application 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

To create an Application Group:

1. Select **Applications** in the Studio navigation pane, and then select **Create Application Group** in the Actions pane.
2. The Create Application Group wizard launches with an **Introduction** page, which you can remove from future launches of this wizard.
3. The wizard guides you through the pages described below. When you are done with each page, click **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) multi-session or single-session 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 Create Application Group 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 Studio. Otherwise, users will see duplicate names in 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.

Click 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 click **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 defined:** 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, click **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 click **OK**. This source cannot be selected If the Site has no applications.

- **App-V**: Applications in App-V packages. When you select this source, a new page launches where you select the App-V server or the Application Library. From the resulting display, select the checkboxes of applications to add, and then click **OK**. For more information, see App-V. This source cannot be selected (or might not appear) if App-V is not configured for the Site.

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 click **Finish**.

Manage Application Groups

February 6, 2020

> Note:
> When using Application Groups with the Citrix Virtual Apps and Desktops service, the "restrict by tag"feature is currently not available.

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. See Delegated Administration for details.

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. Select **Applications** in the Studio navigation pane.

2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. On the **Settings** page, select or clear the **Enable Application Group** check box.
4. Click **Apply** to apply any changes you made and keep the window open, or click **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. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. On the **Settings** page, select or clear the **Enable application session sharing between Application Groups** check box.
4. Click **Apply** to apply any changes you made and keep the window open, or click **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 may 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 either to 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 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. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Rename Application Group** in the Actions pane.
3. Specify the new unique name and then click **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. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. Select the **Delivery Groups** page.
4. To add Delivery Groups, click **Add**. Select the check boxes of available Delivery Groups. (Incompatible Delivery Groups cannot be selected.) When you finish your selections, click **OK**.
5. To remove Delivery Groups, select the check boxes of the groups you want to remove and then click **Remove**. Confirm the deletion when prompted.
6. To change the priority of Delivery Groups, select the checkbox of the Delivery Group and then click **Edit Priority**. Enter the priority (0 = highest) and then click **OK**.
7. Click **Apply** to apply any changes you made and keep the window open, or click **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. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
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 dropdown.
5. To change or remove a tag restriction, either select a different tag from the dropdown or remove the tag restriction entirely by clearing **Restrict launches to machines with this tag**.

6. Click **Apply** to apply any changes you made and keep the window open, or click **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. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
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, click **Add**, and then specify the users you want to add. To remove users, select one or more users and then click **Remove**.
4. Click **Apply** to apply any changes you made and keep the window open, or click **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. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. Select the **Scopes** page. Select or clear the check box next to a scope.
4. Click **Apply** to apply any changes you made and keep the window open, or click **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 will be 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. Select **Applications** in the Studio navigation pane.

2. Select an Application Group in the middle pane and then select **Delete Group** in the Actions pane.
3. Confirm the deletion when prompted.

Remote PC Access

February 23, 2023

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 this functionality:

- Ability to add machines by specifying OUs. This ability facilitates the addition of PCs in bulk.
- Automatic user assignment based on the user that logs into the office Windows PC. We support single user and multiple users assignments.

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 Virtual Apps and Desktops 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 the Citrix Virtual Apps and

> Desktops Service and Workspace Premium Plus.

Considerations

While all the technical requirements and considerations that apply to Citrix Virtual Apps and Desktops 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 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
  - Windows dedicated PCs
  - Windows dedicated multi-user PCs
- Single-session OS
  - Static - Dedicated Linux PCs
  - Random - Pooled Windows and Linux PCs

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.
- If it is not easy to choose OUs to add machines to the machine catalog because of the OU structure, you don't have to select any OUs. You can use PowerShell to add machines to the catalog afterward. User auto-assignments continue to work if the desktop assignment is configured correctly in the Delivery Group. A sample script to add machines to the machine catalog along with user assignments is available in GitHub.
- 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:

- 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.
- Use machine catalogs of type single-session OS for physical Linux machines.
- The integrated Wake on LAN functionality is not available for 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.
- 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 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` 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 Manager 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 `https://www.citrix.com/downloads/` 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.

Disable multiple user auto-assignments

On each Delivery Controller, add the following registry setting:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Name: AllowMultipleRemotePCAssignments
- Type: DWORD
- Data: 0

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+ALT+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

Integrated Wake on LAN is available only in on-premises Citrix Virtual Apps and Desktops and requires Microsoft System Center Configuration Manager (SCCM).

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, saving energy costs. It also enables remote access when a machine has been turned off inadvertently. For example, because of a power outage.

The Remote PC Access Wake on LAN feature is supported with
PCs that have the Wake on LAN option enabled in the BIOS/UEFI.

SCCM and Remote PC Access Wake on LAN

To configure the Remote PC Access Wake on LAN feature, complete the following before deploying the VDA.

- Configure SCCM 2012 R2, 2016, or 2019 within the organization. Then deploy the SCCM client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run (or force one manually, if necessary).
- For SCCM Wake Proxy or magic packet support:
  - Configure Wake on LAN in each PC's BIOS/UEFI settings.
  - For Wake Proxy support, enable the option in SCCM. For each subnet in the organization that contains PCs that use the Remote PC Access Wake on LAN feature, ensure that three or more machines can serve as sentinel machines.

  - For magic packet support, configure network routers and firewalls to allow magic packets to be sent, using either a subnet-directed broadcast or unicast.

After you install the VDA on office PCs, enable or disable power management when you create the connection and the machine catalog.

- If you enable power management in the catalog, specify connection details: the SCCM address, access credentials, and connection name. The access credentials must have access to collections in the scope and the **Remote Tools Operator** role.
- If you do not enable power management, you can add a power management (Configuration Manager) connection later and then edit a Remote PC Access machine catalog to enable power management.

You can edit a power management connection to configure advanced settings. You can enable:

- Wake-up proxy delivered by SCCM.
- Wake on LAN (magic) packets. If you enable Wake on LAN packets, you can select a Wake on LAN transmission method: subnet-directed broadcasts or Unicast.

The PC uses AMT power commands (if they are supported), plus any of the enabled advanced settings. If the PC does not use AMT power commands, it uses the advanced settings.

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 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.

App-V

August 18, 2020

Using App-V with Citrix Virtual Apps and Desktops

Microsoft Application Virtualization (App-V) lets you deploy, update, and support applications as services. Users access applications without installing them on their own devices. App-V and Microsoft User State Virtualization (USV) provide access to applications and data, regardless of location and connection to the internet.
The following table lists supported versions.

App-V	Citrix Virtual Apps and Desktops Delivery Controller	Citrix Virtual Apps and Desktops VDA
5.0 and 5.0 SP1	XenDesktop 7 through current, XenApp 7.5 through current	7.0 through current
5.0 SP2	XenDesktop 7 through current, XenApp 7.5 through current	7.1 through current

App-V	Citrix Virtual Apps and Desktops Delivery Controller	Citrix Virtual Apps and Desktops VDA
5.0 SP3 and 5.1	XenDesktop 7.6 through current, XenApp 7.6 through current	7.6.300 through current
App-V in Windows Server 2016	XenDesktop 7.12 through current, XenApp 7.12 through current	7.12 through current

The App-V client does not support offline access to applications. App-V integration support includes using SMB shares for applications. The HTTP protocol is not supported.
If you're not familiar with App-V, see the Microsoft documentation. Here's a recap of the App-V components mentioned in this article:

- **Management server**. Provides a centralized console to manage App-V infrastructure and delivers virtual applications to both the App-V Desktop Client and a Remote Desktop Services Client. The App-V management server authenticates, requests, and provides the security, metering, monitoring, and data gathering required by the administrator. The server uses Active Directory and supporting tools to manage users and applications.
- **Publishing server**. Provides App-V clients with applications for specific users, and hosts the virtual application package for streaming. It fetches the packages from the management server.
- **Client**. Retrieves virtual applications, publishes the applications on the client, and automatically sets up and manages virtual environments at runtime on Windows devices. You install the App-V client on the VDA, where it stores user-specific virtual application settings such as registry and file changes in each user's profile.

Applications are available seamlessly without any pre-configuration or changes to operating system settings. You can launch App-V applications from Server OS and Desktop OS Delivery Groups:

- Through Citrix Workspace app
- Through the App-V client and Citrix Workspace app
- Simultaneously by multiple users on multiple devices
- Through Citrix StoreFront

Modified App-V application properties are implemented when the application is started. For example, for applications with a modified display name or customized icon, the modification appears when users start the application. Application customizations saved in dynamic configuration files are also applied when the application is launched.

Management methods

You can use App-V packages and dynamic configuration files created with the App-V sequencer and then located on either App-V servers or network shares.

- **App-V servers:** Using applications from packages on App-V servers requires ongoing communication between Studio and the App-V servers for discovery, configuration, and downloading to the VDAs. This incurs hardware, infrastructure, and administration overhead. Studio and the App-V servers must remain synchronized, particularly for user permissions.

  This is called the *dual admin* management method because App-V package and application access requires both Studio and the App-V server consoles. This method works best in closely coupled App-V and Citrix deployments. In this method, the management server handles the dynamic configuration files. When you use the dual admin management method, the Citrix App-V components manage the registration of the appropriate publishing server required for an application launch. This ensures that the publishing server is synchronized for the user at the appropriate time. The publishing server maintains other aspects of the package life cycle (like refresh on logon and connection groups) using the settings that it is configured with.

- **Network share:** Packages and XML deployment configuration files placed on a network share remove Studio's dependence on the App-V server and database infrastructure, reducing overhead. (You must install the Microsoft App-V client on each VDA.)

  This is called the *single admin* management method because App-V package and application use only needs the Studio console. You browse to the network share and add one or more App-V packages from that location to the Site-level Application Library [1]. In this method, the Citrix App-V components process the Deployment Configuration Files when the application is launched. (User Configuration Files are not supported.) When you use the single admin management method, the Citrix App-V components manage all aspects of the Package's life cycle on the host machine. Packages are added to the machine at broker startup, or when a configuration change is detected (which can also be at session launch time). Packages are first published to individual users on demand 'just in time'when a launch request is received from the Citrix Workspace app.

  Single Admin also manages the lifecycle of connection groups required to meet the Isolation Group configuration definitions made in Studio.

  [1] *Application Library* is a Citrix term for a caching repository that stores information about App-V packages. The Application Library also stores information about other Citrix application delivery technologies.

In both management methods, if the VDA is configured to discard user data, the publishing (or synchronizing) must be redone at the next session launch.

You can use one or both management methods simultaneously. In other words, when you add applications to Delivery Groups, the applications can come from App-V packages located on App-V servers or on a network share.

> **Note:**
>
> If you are using both management methods simultaneously, and the App-V package has a dynamic configuration file in both locations, the file in the App-V server (dual management) is used.

When you select **Configuration > App-V Publishing** in the Studio navigation pane, the display shows App-V package names and sources. The source column indicates whether the packages are located on the App-V server or cached in the Application Library. When you select a package, the details pane lists the applications and shortcuts in the package.

Dynamic configuration files

Overview App-V packages can be customized using dynamic configuration files, that when applied to the package, can be used to change its characteristics. For example, you can use them to define extra application shortcuts and behaviors. Citrix App-V supports both types of dynamic configuration file. File settings are applied when the application is launched:

- Deployment Configuration Files provide machine-wide configuration for all users. These files are expected to be named <*packageFileName*>_DeploymentConfig.xml and located in the same folder as the App-V package they apply to. Supported by single and dual admin management.
- User Configuration Files provide user-specific configuration which supports per-user customizations to the package. Single Admin supports user config files named in the following format: <*packageFileName*>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml and located in the same folder as the App-V package they apply to.

When multiple user config files exist for a particular package, they are applied with the following priority:

1. User SID
2. Username
3. AD Group SID (First found wins)
4. AD Group Name (First found wins)
5. Default

For example

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml
MyAppVPackage_joeblogs_UserConfig.xml
MyAppVPackage_S-1-5-32-547_UserConfig.xml
MyAppVPackage_Power Users_UserConfig.xml
```



```
5 MyAppVPackage_UserConfig.xml
```

> **Note:**
>
> The user-specific portion of the file name can also optionally occur at the end (for example MyAppVPackage_UserConfig_**joeblogs**.xml).

Dynamic configuration file location In single admin management, the Citrix App-V components only process dynamic configuration files which are found in the same folder as their App-V package. When applications in the package are launched, any changes to the corresponding dynamic configuration files are reapplied. If your dynamic configuration files are located in a different location to their packages, use a mapping file to map packages to their deployment configuration files.

To create a mapping file

1. Open a new text file.
2. For each dynamic configuration file, add a line which specifies the path to the package using the format <PackageGuid> : path.

   For example:

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
3. Save the file as ctxAppVDynamicConfigurations.cfg in the same folder as the package. The entire directory hierarchy on the same UNC share as the App-V package is searched recursively upwards for this file every time an application in the package is launched.

> **Note**
>
> You cannot apply changes to Dynamic Deployment Configuration when there are user sessions with an application in the package open. You can apply changes to Dynamic User Configuration files if other users *but not the current user* have the an application from the package open.

Isolation groups

When you use the App-V single admin method, creating isolation groups allow you to specify interdependent groups of applications that must run in the sandbox. This feature is similar, but not identical to, App-V connection groups. Instead of the mandatory and optional package terminology used by the App-V management server, Citrix uses automatic and explicit for package deployment options.

- When a user launches an App-V application (the primary application), the isolation groups are searched for other application packages that are marked for automatic inclusion. Those packages are downloaded and included in the isolation group automatically. You do not need to add them to the Delivery Group that contains the primary application.

- An application package in the isolation group that is marked for explicit inclusion is downloaded only if you have explicitly added that application to the same Delivery Group that contains the primary application.

This allows you to create isolation groups containing a mix of automatically included applications that are available globally to all users. Plus, the group can contain a set of plug-ins and other applications (that might have specific licensing constraints), which you can limit to a certain set of users (identified through Delivery Groups) without having to create more isolation groups.

For example, application "app-a"requires JRE 1.7 to run. You can create an isolation group containing app-a (with an explicit deployment type) and JRE 1.7 (with an automatic deployment type). Then, add those App-V packages to one or more Delivery Groups. When a user launches app-a, JRE 1.7 is automatically deployed with it.

You can add an application to more than one App-V isolation group. However, when a user launches that application, the first isolation group to which that application was added is always used. You cannot order or prioritize other isolation groups containing that application.

Load balancing App-V servers

Load balancing management and publishing servers using DNS Round-Robin is supported if you are using the dual admin management method. Load balancing the management server behind Netscaler, F5 (or similar) Virtual IP is not supported because of the way Studio needs to communicate with the Management Server via remote PowerShell. For more information, see this Citrix blog article.

Setup

The following table summarizes the sequence of setup tasks for using App-V in Citrix Virtual Apps and Desktops using single- and dual admin management methods.

Single admin	Dual admin	Task
X	X	Deploy App-V
X	X	Packaging and placement
	X	Configure App-V server addresses in Studio
X	X	Install software on VDA machines
X		Add App-V packages to the Application Library

Single admin	Dual admin	Task
X		Add App-V isolation groups (optional)
X	X	Add App-V applications to Delivery Groups

Deploy Microsoft App-V

For App-V deployment instructions, see https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/.

Optionally, change App-V publishing server settings. Citrix recommends using the SDK cmdlets on the Controller. See the SDK documentation for details.

- To view publishing server settings, enter **Get-CtxAppvServerSetting -AppVPublishingServer *<pubServer>***.
- To ensure that App-V applications launch properly, enter **Set-CtxAppvServerSetting –User-RefreshonLogon 0**.

If you previously used GPO policy settings to manage publishing server settings, the GPO settings override any App-V integration settings, including cmdlet settings. This can result in App-V application launch failure. Citrix recommends that you remove all GPO policy settings and then use the SDK to configure those settings.

Packaging and placement

For either management method, create application packages using the App-V sequencer. See the Microsoft documentation for details.

- For single admin management, make the packages, and their corresponding dynamic configuration files, available on a UNC or SMB shared network location. Ensure that the Studio administrator who adds applications to Delivery Groups has at least read access to that location.
- For dual admin management, publish the packages on the App-V management server from a UNC path. (Publishing from HTTP URLs is not supported.)

Regardless of whether packages are on the App-V server or on a network share, ensure the packages have appropriate security permissions to allow the Studio administrator to access them. Network shares must be shared with "Authenticated users"to ensure that both the VDA and Studio have read access by default.

Configure App-V server addresses in Studio

> **Important:**
>
> Citrix recommends using the PowerShell cmdlets on the Controller to specify App-V server addresses if those servers use nondefault property values. See the SDK documentation for details. If you change App-V server addresses in Studio, some server connection properties you specify might be reset to default values. These properties are used on the VDAs to connect to App-V publishing servers. If this happens, reconfigure the nondefault values for any reset properties on the servers.

This procedure is valid only for the dual admin management method.

Specify App-V management and publishing server addresses for the dual admin management method either during or after Site creation. You can do this during or after creating the Site.

During Site creation:

- On the **App-V** page of the wizard, enter the URL of the Microsoft App-V management server, and the URL and port number of the App-V publishing server.
- Test the connection before continuing with the wizard. If the test fails, see the Troubleshoot section below.

After Site creation:

1. Select **Configuration > App-V Publishing** in the Studio navigation pane.
2. If you have not previously specified App-V server addresses, select **Add Microsoft Server** in the Actions pane.
3. To change App-V server addresses, select **Edit Microsoft Server** in the Actions pane.
4. Enter the URL of the Microsoft App-V management server, and the URL and port number of the App-V publishing server.
5. Test the connection to those servers before closing the dialog box. If the test fails, see the Troubleshoot section below.

Later, if you want to remove all links to the App-V management and publishing servers and stop Studio from discovering App-V packages from those servers, select **Remove Microsoft Server** in the Actions pane. This action is allowed only if no applications in packages on those servers are currently published in any Delivery Groups. If they are, you must remove those applications from the Delivery Groups before you can remove the App-V servers.

Install software on VDA machines

Machines containing VDAs must have two sets of software installed to support App-V: one from Microsoft and the other from Citrix.

Microsoft App-V client This software retrieves virtual applications, publishes the applications on the client, and automatically sets up and manages virtual environments at runtime on Windows devices. The App-V client stores user-specific virtual application settings, such as registry and file changes in each user's profile.

The App-V client is available from Microsoft. Install a client on each machine containing a VDA, or on the master image that is used in a machine catalog to create VMs. **Note**: Windows 10 (1607 or greater) and Windows Server 2016 already include the App-V client. On those OSs only, enable the App-V client by running the PowerShell **Enable-AppV** cmdlet (no parameters). The **Get-AppVStatus** cmdlet retrieves the current enablement status.

> **Tip:**
>
> After you install the App-V client, with Administrator permissions, run the PowerShell **Get-AppvClientConfiguration** cmdlet, and ensure that EnablePackageScripts is set to 1. If it is not set to 1, run **Set-AppvClientConfiguration -EnablePackageScripts $true**.

Citrix App-V components The Citrix App-V component software is excluded by default when you install a VDA.

You can control this default behavior during VDA installation. In the graphical interface, select the **Citrix Personalization for App-V - VDA** check box on the **Additional Components** page. In the command line interface, use the **/includeadditional "Citrix Personalization for App-V –VDA"** option.

If you do not include the Citrix App-V components during VDA installation, but later want to use App-V applications: In the Windows machine's Programs and Features list, right-click the **Citrix Virtual Delivery Agent** entry and then select **Change**. A wizard launches. In the wizard, enable the option that installs and enables App-V publishing components.

Add or remove App-V packages in the Application Library

These procedures are valid only for the single admin management method.

You must have at least read access to the network share containing the App-V packages.

Add an App-V package to the Application Library

1. Select **Configuration > App-V Publishing** in the Studio navigation pane.
2. Select **Add Packages** in the Actions pane.
3. Browse to the share containing the App-V packages and select one or more packages.
4. Click **Add**.

Remove an App-V package from the Application Library Removing an App-V package from the Application Library removes it from the Studio App-V Publishing node display. However, it does not remove its applications from Delivery Groups, and those applications can still be launched. The package remains in its physical network location. (This effect differs from removing an App-V application from a Delivery Group.)

1. Select **Configuration > App-V Publishing** in the Studio navigation pane.
2. Select one or more packages to be removed.
3. Select **Remove Package** in the Actions pane.

Add, edit, or remove App-V isolation groups

Add an App-V isolation group

1. Select **App-V Publishing** in the Studio navigation pane.
2. Select **Add Isolation Group** in the Actions pane.
3. In the **Add Isolation Group Settings** dialog box, type a name and description for the isolation group.
4. From the Available Packages list, select the applications you want to add to the isolation group, and then click the right arrow. The selected applications should now appear in the Packages in Isolation Group list. In the **Deployment** drop-down next to each application, select either **Explicit** or **Automatic**. You can also use the up and down arrows to change the order of applications in the list.
5. When you are done, click **OK**.

Edit an App-V isolation group

1. Select **App-V Publishing** from the Studio navigation pane.
2. Select the **Isolation Groups** tab in the middle pane and then select the isolation group you want to edit.
3. Select **Edit Isolation Group** in the Actions pane.
4. In the **Edit Isolation Group Settings** dialog box, change the isolation group name or description, add or remove applications, change their deployment type, or change the application order.
5. When you are done, click **OK**.

Remove an App-V isolation group Removing an isolation group does not remove the application packages. It removes only the grouping.

1. Select **App-V Publishing** from the Studio navigation pane.

2. Select the **Isolation Groups** tab in the middle pane and then select the isolation group you want to remove.
3. Select **Remove Isolation Group** from the Actions pane.
4. Confirm the removal.

Add App-V applications to Delivery Groups

The following procedure focuses on how to add App-V applications to Delivery Groups. For complete details about creating a Delivery Group, see Create Delivery Groups.

Step 1: Choose whether you want to create a new Delivery Group or add App-V applications to an existing Delivery Group:

To create a Delivery Group containing App-V applications:

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select **Create Delivery Group** in the Actions pane.
3. On successive pages of the wizard, specify a machine catalog and users.

To add App-V applications to existing Delivery Groups:

1. Select **Applications** in the Studio navigation pane.
2. Select **Add Applications** in the Actions pane.
3. Select one or more Delivery Groups where the App-V applications will be added.

Step 2: On the **Applications** page of the wizard, click the **Add** drop-down to display application sources. Select **App-V**.

Step 3: On the **Add App-V Applications** page, choose the App-V source: the App-V server or the Application Library. The resulting display includes the application names plus their package names and package versions. Select the check boxes next to the applications or application shortcuts you want to add. Then click **OK**.

Step 4: Complete the wizard.

Good to know:

- If you change an App-V application's properties when adding them to a Delivery Group, the changes are made when the application is started. For example, if you modify an application's display name or icon when adding it to the group, the change appears when a user starts the application.
- If you use dynamic configuration files to customize the properties of an App-V application, those properties override any changes you made when adding them to a Delivery Group.
- If you later edit a Delivery Group containing App-V applications, there is no change in App-V application performance if you change the group's delivery type from desktops and applications to applications only.

- When you remove a previously published (single admin) App-V package from a Delivery Group, Citrix App-V client components attempt to clean up, unpublish, and remove any packages that are no longer in use by the single admin management method.
- If you are using a hybrid deployment—with packages delivered by the single admin management method and an App-V publishing server, managed either by dual admin or by another mechanism (such as Group policy)—it is not possible to determine which (now potentially redundant) packages came from which source. In this case, cleanup is not attempted.
- If you publish more than 100 App-V applications in a single Delivery Group, applications may not launch. If so, use the MaxReceivedMessageSize property on the appropriate binding element to increase Max Receivable message size in the configuration of the Delivery Controller and/or the Broker Agent on the VDA.

Troubleshoot

Issues that can occur only when using the dual admin method are marked (DUAL).

(DUAL) There is a PowerShell connection error when you select **Configuration > App-V Publishing** in the Studio navigation pane.

- Is the Studio administrator also an App-V server administrator? The Studio administrator must belong to the "administrators"group on the App-V management server so that they can communicate with it.

(DUAL) The Test connection operation returns an error when you specify App-V server addresses in Studio.

- Is the App-V server powered on? Either send a Ping command or check the IIS Manager; each App-V server should be in a Started and Running state.
- Is PowerShell remoting enabled on the App-V server? If not, see https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10).
- Is the Studio administrator also an App-V server administrator? The Studio administrator must belong to the *administrators* group on the App-V management server so that they can communicate with it.
- Is file sharing enabled on the App-V server? Enter \\<App-V server FQDN> in Windows Explorer or with the Run command.
- Does the App-V server have the same file sharing permissions as the App-V administrator? On the App-V server, add an entry for \\<App-V server FQDN> in Stored User Names and Passwords, specifying the credentials of the user who has administrator privileges on the App-V server. For guidance, see http://support.microsoft.com/kb/306541.

- Is the App-V server in Active Directory?

  If the Studio machine and the App-V server are in different Active Directory domains that do not have a trust relationship, from the PowerShell console on the Studio machine, run **winrm s winrm/Config/client '@(TrustedHosts="*<App-V server FQDN>*")'**.

  If TrustedHosts is managed by GPO, the following error message displays: "*The config setting TrustedHosts cannot be changed because use is controlled by policies. The policy would need to be set to Not Configured to change the config setting*."In this case, add an entry for the App-V server name to the TrustedHosts policy in GPO (Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client).

(DUAL) Discovery fails when adding an App-V application to a Delivery Group.

- Is the Studio administrator also an App-V management server administrator? The Studio administrator must belong to the *administrators* group on the App-V management server so that they can communicate with it.
- Is the App-V management server running? Either send a Ping command or check the IIS Manager; each App-V server should be in a Started and Running state.
- Is PowerShell remoting enabled on both App-V servers? If not, see https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10).
- Do packages have the appropriate security permissions for the Studio administrator to access?

App-V applications only launch in one browser version.

- If you publish multiple sequenced versions of the same browser app, only one version of the app is able to launch at a time per user on the VDA. The same thing occurs even if Citrix components are not involved and the user starts the sequenced apps from desktop shortcuts which point to different paths.

  Whichever browser version a user launches first, determines the browser version which runs subsequently for them. When Firefox detects a second launch of itself, it prefers to create an instance of the already running process, rather than create a new process. Other browsers may behave in the same way.

  You can make the application launch in the intended Firefox browser version, by adding the command line parameter **-no-remote** to the shortcut's launch command. Other browsers offer the same or similar facility.

  > **Note:**
  >
  > You must be using XenApp 7.17 or higher to take advantage of the shortcut enumeration feature. You must also change the package in both versions of the app to get this bi-directional behavior.

App-V applications do not launch.

- (DUAL) Is the publishing server running?
- (DUAL) Do the App-V packages have appropriate security permissions so that users can access them?
- (DUAL) On the VDA, ensure that Temp is pointing to the correct location, and that there is enough space available in the Temp directory.
- (DUAL) On the App-V publishing server, run `Get-AppvPublishingServer \*` to display the list of publishing servers.
- (DUAL) On the App-V publishing server, ensure that UserRefreshonLogon is set to False.
- (DUAL) On the App-V publishing server, as an administrator, run **Set-AppvPublishingServer** and set UserRefreshonLogon to False.
- Is a supported version of the App-V client installed on the VDA? Does the VDA have the **enable package scripts** setting enabled?
- On the machine containing the App-V client and VDA, from the Registry editor (regedit), go to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Ensure that the AppVServers key has the following value format: AppVManagementServer+metadata;PublishingServer (for example: `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`).
- On the machine or master image containing the App-V client and VDA, check that the PowerShell ExecutionPolicy is set to RemoteSigned. The App-V client provided by Microsoft is not signed, and this ExecutionPolicy allows PowerShell to run unsigned local scripts and cmdlets. Use one of the following two methods to set the ExecutionPolicy: (1) As an administrator, enter the cmdlet: **Set-ExecutionPolicy RemoteSigned**, or (2) From Group Policy settings, go to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell> Turn on Script Execution.
- If the error "RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register" appears, use the MaxReceivedMessageSize property on the appropriate binding element to increase Max Receivable message size in the configuration of the Delivery Controller and/or the Broker Agent on the VDA.

If these steps do not resolve the issues, enable and examine the logs.

Logs

App-V configuration-related logs are located at C:\CtxAppvLogs. The application launch logs are located at: %LOCALAPPDATA%\Citrix\CtxAppvLogs. LOCALAPPDATA resolves to the local folder for the logged-on user. Check the local folder of the user for whom the application launch failed.

To enable Studio and VDA logs used for App-V, you must have administrator privileges. You will also need a text editor such as Notepad.

To enable Studio logs:

1. Create the folder C:\CtxAppvLogs.
2. Go to C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Open CtxAppvCommon.dll.config in a text editor and uncomment the line: <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. Restart the Broker service to start logging.

To enable VDA logs:

1. Create the folder C:\CtxAppvLogs.
2. Go to C:\Program Files\Citrix\ Virtual Desktop Agent. Open CtxAppvCommon.dll.config in a text editor and uncomment the following line: <add key =”LogFileName”value=” C:\CtxAppvLogs\log.txt”/>
3. Uncomment the line and set the value field to 1: <add key =”EnableLauncherLogs”value=”1”/>
4. Restart the machine to start logging.

AppDisks

December 12, 2022

> **Note:**
>
> AppDisks are deprecated.

Overview

Managing applications and managing the images they are installed on can be a challenge. The Citrix AppDisks feature is a solution. AppDisks separate applications and groups of applications from the operating system, enabling you to manage them independently.

You can create different AppDisks containing applications designed for individual user groups, and then assemble the AppDisks on a master image of your choice. Grouping and managing applications this way gives you finer control of applications, and reduces the number of master images you maintain. This simplifies IT administration and enables you to be more responsive to user needs. You deliver the applications in AppDisks through Delivery Groups.

If your deployment also includes Citrix AppDNA, you can integrate the AppDisks feature with it; AppDNA allows Citrix Virtual Apps and Desktops to perform automatic analysis of applications on a per-AppDisk basis. Using AppDNA helps make the most of the AppDisks feature. Without it, application compatibility is not tested or reported.

AppDisks differ from other application-provisioning technologies in two ways: isolation and change management.

- Microsoft App-V allows incompatible applications to exist together by isolating them. The AppDisks feature does not isolate applications. It separates applications (and supporting files and registry keys) from the OS. To the OS and the user, AppDisks look and behave as if they are installed directly on a master image.
- Change management (updating master images and testing the compatibility of updates with installed applications) can be a significant expense. AppDNA reports help identify issues and suggest remediation steps. For example, AppDNA can identify applications that have common dependencies such as .NET, so you can install them on a single common base image. AppDNA can also identify applications that load early in the OS startup sequence, so that you can then ensure they behave as expected.

Good to know:

- After updating an image, some applications may fail to work properly due to an ability to verify previously installed licenses. For example, after an image upgrade, launching Microsoft Office may display an error message similar to:

  "Microsoft Office Professional Plus 2010 cannot verify the license for this application. A repair attempt failed or was canceled by the user, the application will not shut down."

  To resolve this issue, uninstall Microsoft Office and install the new version on the base image.
- In some cases, downloading Metro apps from the Windows Store to a published catalog's virtual machine fails after a long time.
- Citrix recommends that you always put all Microsoft Office components in the same AppDisk. For example, one AppDisk with Microsoft Office with Project, and another AppDisk with Microsoft Office with Project and Visio.
- On some systems, SCCM crashes when updating an image. This scenario occurs when updates are made to the base image, then applied, which results in failure of the SCCM client. To resolve this issue, install the SCCM client instance in the base image first.
- In some cases, an application installed on the AppDisk may fail to appear in the Windows Start menu after it is assigned to a Delivery Group and assigned a user's virtual machine. See How applications appear in the Start Menu for more information.
- Users are unaware of the separation of applications and the OS, or any other aspect of the AppDisks feature. Applications behave as if they are installed on the image. AppDisks containing complex applications may result in a slight delay in desktop startup.
- You may only use AppDisks with Hosted Shared and Pooled desktops.
- You can use AppDisks with hosted shared desktops.
- You may be able to share AppDisks across master images and OS platforms (on a per-application basis); however, this will not work for all applications. If you have applications with an install

script for a desktop OS that prevents them from working on a server OS, Citrix recommends packaging the applications separately for the two OSs.

- In many cases, AppDisks work on different OSs. For example, you can add an AppDisk that was created on a Windows 7 VM to a Delivery Group containing Windows 2008 R2 machines, as long as both OSs have the same bitness (32 bit or 64 bit) and both support the application. However, Citrix recommends you do not add an AppDisk created on a later OS version (such as Windows 10) to a Delivery Group containing machines running an earlier OS version (such as Windows 7), because it might not work correctly.
- If you need to provide access to an AppDisk's applications to only a subset of users in a Delivery Group, Citrix recommends using Group Policy to hide an application in an AppDisk from some users. That application's executable file remains available, but will not run for those users.
- In Russian and Chinese environments running the Windows 7 OS, the reboot dialog fails to disappear automatically; in such cases, after logging on to a delivered desktop the reboot dialog appears and should disappear quickly.
- When using the `Upload-PvDDiags` script tool, log information related to the PVD user layer is missing when the user's drive designation is not set to 'P'.
- In environments set to display Basque language, a Windows 7 OS may fail to properly display the appropriate language on the reboot prompt screen. When you set the language to Basque, make sure that you have already installed French or Spanish as the parent language, then install Basque and set it as the current language.
- When shutting down a computer, the PVD update reminder pops up even if the PVD disk is set to read-only mode.
- During an in-place upgrade, a registry file (DaFsFilter) could be deleted, which causes the upgrade to fail.

> **Tip:**
>
> When creating an AppDisk, use a VM with only the OS installed (that is, do not include other apps); the OS should contain all updates prior to creating the AppDisk.

Deployment overview

The following list summarizes the steps to deploy AppDisks. Details are provided later in this article.

1. From your hypervisor management console, install a Virtual Delivery Agent (VDA) on a VM.
2. Create an AppDisk, which includes completing steps from your hypervisor management console and in Studio.
3. From your hypervisor management console, install applications on the AppDisk.

4. Seal the AppDisk (from the hypervisor management console or in Studio). Sealing allows Citrix Virtual Apps and Desktops to record the AppDisk's applications and supporting files in an Application Library (AppLibrary).
5. In Studio, create or edit a Delivery Group and select the AppDisks to include; this is called *assigning the AppDisks* (even though you use the **Manage AppDisks** action in Studio). When VMs in the Delivery Group start up, Citrix Virtual Apps and Desktops coordinate with the AppLibrary, then interact with Creation Services (MCS) or Citrix Provisioning (formerly Provisioning Services), and the Delivery Controller to stream the boot devices after AppDisks are configured on them.

Requirements

Using AppDisks has requirements in addition to those listed in System requirements.

The AppDisks feature is supported only in deployments containing (at minimum) XenApp and XenDesktop 7.8 versions of the Delivery Controller and Studio, including the prerequisites that the installer automatically deploys (such as .NET).

AppDisks can be created on the same Windows OS versions that are supported for VDAs. The machines selected for Delivery Groups that will use AppDisks must have at least VDA version 7.8 installed.

Citrix recommends that you install or upgrade all machines with the most recent VDA version (and then upgrade machine catalogs and Delivery Groups, if 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. This is called the group's *functional level*. For more information about functional level, see Create Delivery Groups.

To provision VMs that will be used to create AppDisks, you can use:

- MCS provided with the Delivery Controller.
- Citrix Provisioning version provided on the download page with your Citrix Virtual Apps and Desktops version.
- Supported hypervisors:
  - XenServer
  - VMware (minimum version 5.1)
  - Microsoft System Center Virtual Machine Manager

AppDisks cannot be used with other host hypervisors and cloud service types supported for Citrix Virtual Apps and Desktops.

Creating AppDisks is not supported with machines in MCS catalogs that use caching of temporary data.

> **Note:**
>
> You can attach AppDisks to MCS-provisioned machines using write caching, but they cannot be used to create AppDisks.

Remote PC Access catalogs do not support AppDisks.

The Windows Volume Shadow Service must be enabled on the VM where you are creating an AppDisk. This service is enabled by default.

Delivery Groups used with AppDisks can contain machines from pooled random Machine Catalogs containing server OS or desktop OS machines. You cannot use AppDisks with machines from other catalog types, such as pooled static or dedicated (assigned).

Machines on which Studio is installed must have .NET Framework 3.5 installed (in addition to any other installed .NET versions).

AppDisks can affect storage. For details, see Storage and performance considerations.

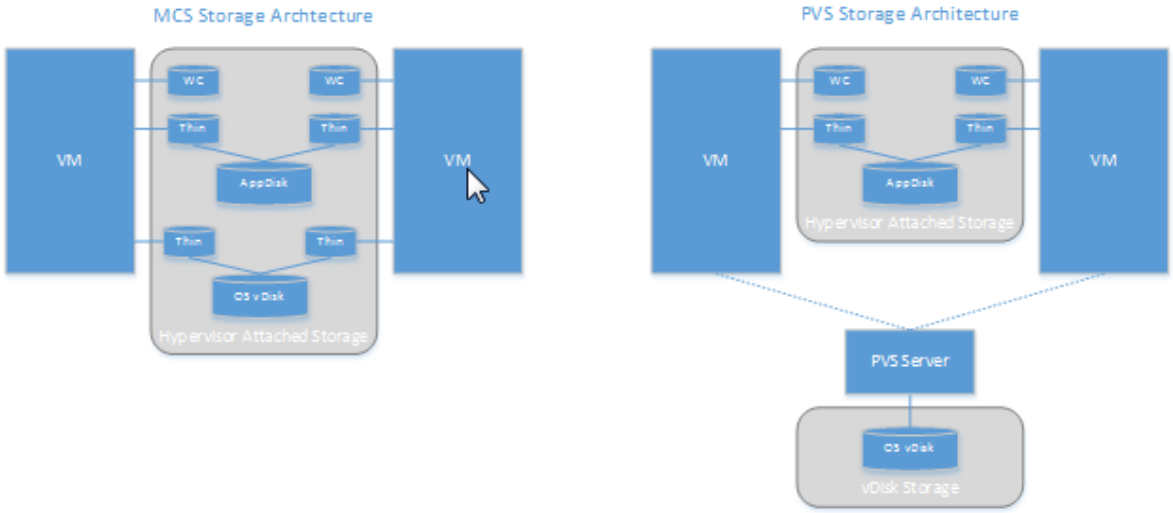
If you use AppDNA:

- Review the AppDNA documentation and the AppDisk FAQ.
- The AppDNA software must be installed on a different server from a Controller. Use the AppDNA version supplied with this Citrix Virtual Apps and Desktops release. For other AppDNA requirements, see its documentation.
- On the AppDNA server, make sure there is a firewall exception for the default port 8199.
- Do not disable an AppDNA connection while creating an AppDisk.
- When you create the Citrix Virtual Apps and Desktops Site, you can enable compatibility analysis with AppDNA on the **Additional Features** page of the Site creation wizard. You can also enable/disable it later by selecting **Configuration > AppDNA** in the Studio navigation pane.
- Clicking on the View Issue Report link in Studio displays the AppDNA report, however the OS combinations that AppDNA uses by default are Window 7 64-bit for desktop delivery groups and Windows Server 2012 R2 for server delivery groups. If your delivery groups contain different versions of Windows, the default image combinations in the reports that Studio shows will be incorrect. To work around this issue, manually edit the solution in AppDNA after Studio has created it.
- There is a dependency between Studio and AppDNA server versions.
  - From version 7.12, Studio must be the same, or a higher version than the AppDNA server.
  - For versions 7.9 and 7.11, Studio and AppDNA server versions must match.
  - The following table summarizes which versions work together (Yes = versions work together, - = versions don't work together):

Product Version	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	Yes	-	-	-	-	-
AppDNA 7.11	-	Yes	-	-	-	-
AppDNA 7.12	-	-	Yes	Yes	Yes	Yes
AppDNA 7.13	-	-	Yes	Yes	Yes	Yes
AppDNA 7.14	-	-	-	-	Yes	Yes
AppDNA 7.15	-	-	-	-	-	Yes

Storage and performance considerations

Separating applications and the OS using two disks, and storing those disks in different areas can affect your storage strategy. The following graphic illustrates the MCS and Citrix Provisioning storage architectures. "WC"indicates the write cache, and "Thin"indicates the thin disk used to store differences between a VM's AppDisk and OS virtual disks.



In MCS environments:

- You can continue to balance the size of the AppDisks and OS virtual disks (vDisks) using your organization's existing sizing guidelines. If AppDisks are shared between multiple Delivery Groups, the overall storage capacity can be reduced.

- OS vDisks and AppDisks are located in the same storage areas, so plan your storage capacity requirements carefully to avoid any negative effect on capacity when you deploy AppDisks. AppDisks incur overhead, so be sure your storage accommodates that overhead and the applications.
- There is no net effect on IOPS because the OS vDisks and AppDisks are located in the same storage area. There are no write cache considerations when using MCS.

In Citrix Provisioning environments:

- You must allow for the increased capacity and IOPS as applications move from AppDisk storage to the hypervisor-attached storage.
- With Citrix Provisioning, OS vDisks and AppDisks use different storage areas. The OS vDisk storage capacity is reduced, but the hypervisor-attached storage is increased. So, you should size your Citrix Provisioning environments to accommodate those changes.
- AppDisks in the hypervisor-attached storage require more IOPS while the OS vDisks require fewer.
- Write cache: Citrix Provisioning uses a dynamic VHDX file on an NTFS formatted drive; when blocks are written to the write cache, the VHDX file is dynamically extended. When AppDisks are attached to their associated VM, they are merged with the OS vDisks to provide a unified view of the file system. This merging typically results in additional data being written to the write caches, which increases the size of the write cache file. You should account for this in your capacity planning.

In either MCS or Citrix Provisioning environments, remember to decrease the size of the OS vDisk to take advantage of the AppDisks you create. If you don't, plan to use more storage.

When many users in a Site turn on their computers simultaneously (for example, at the beginning of the workday), the multiple startup requests apply pressure on the hypervisor, which can affect performance. For Citrix Provisioning, applications are not located on the OS vDisk, so fewer requests are made to the Citrix Provisioning server. With the resulting lighter load on each target device, the Citrix Provisioning server can stream to more targets. However, be aware that the increased target-server density might negatively affect boot storm performance.

AppDisk creation considerations

There are two ways to create an AppDisk, install applications on it, and then seal it. Both methods include steps you complete from your hypervisor management console and in Studio. The methods differ in where you complete most the steps.

Regardless of which method you use:

- Allow 30 minutes for AppDisk creation portion.
- Do not disable an AppDNA connection while creating an AppDisk.
- When you add applications to an AppDisk, be sure to install applications for all users. Re-arm any applications that use Key Management Server (KMS) activation. For details, see the application's documentation.
- Files, folders, and registry entries created in user-specific locations during AppDisk creation are not retained. Also, some applications run a first-time-use wizard to create user data during installation. Use a profile management solution to retain this data and prevent the wizard from appearing each time the AppDisk starts.
- If you are using AppDNA, analysis starts automatically after the creation process completes. During this interval, the AppDisk's status in Studio is "Analyzing."

Citrix Provisioning considerations

AppDisks on machines from Machine Catalogs created by Provisioning Services require additional configuration during AppDisk creation. From the Provisioning Services console:

1. Create a new version of the vDisk associated with the device collection that contains the VM.
2. Place the VM into maintenance mode.
3. During AppDisk creation, select the maintenance version on the boot screen every time the VM restarts.
4. After you seal the AppDisk, place the VM back into production, and delete the vDisk version you created.

Create an AppDisk primarily in Studio

This procedure includes three tasks: create the AppDisk, create applications on the AppDisk, and then seal the AppDisk.

Create an AppDisk:

1. Select **AppDisks** in the Studio navigation pane and then select **Create AppDisk** in the Actions pane.
2. Review the information on the **Introduction** page of the wizard and then click **Next**.
3. On the **Create AppDisk** page, select the **Create new AppDisk** radio button. Select either a predefined disk size (small, medium, or large) or specify a disk size in GB; the minimum size is 3 GB. The disk size should be large enough to hold the applications you will add. Click **Next**.
4. On the **Preparation Machine** page, select a random pooled catalog to be used as the master image on which the AppDisk will be built. Note: The display lists all the Machine Catalogs in the Site, separated by type; only those catalogs that contain at least one available machine can

be selected. If you choose a catalog that does not contain random pooled VMs, the AppDisk creation will fail. After you select a VM from a random pooled catalog, click **Next**.

5. On the **Summary** page, type a name and description for the AppDisk. Review the information you specified on previous wizard pages. Click **Finish**.

Remember: If you are using Citrix Provisioning, follow the guidance in Citrix Provisioning considerations.

After the wizard closes, the Studio display for the new AppDisk indicates "Creating."After the AppDisk is created, the display changes to "Ready to install applications."

Install applications on the AppDisk:

From your hypervisor management console, install applications on the AppDisk. (**Tip:** If you forget the VM name, select **AppDisks** in the Studio navigation pane and then select **Install Applications** in the Actions pane to display its name.) See the hypervisor documentation for information about installing applications. (Remember: You must install applications on the AppDisk from your hypervisor management console. Do not use the **Install Applications** task in the Studio Actions pane.)

Seal the AppDisk:

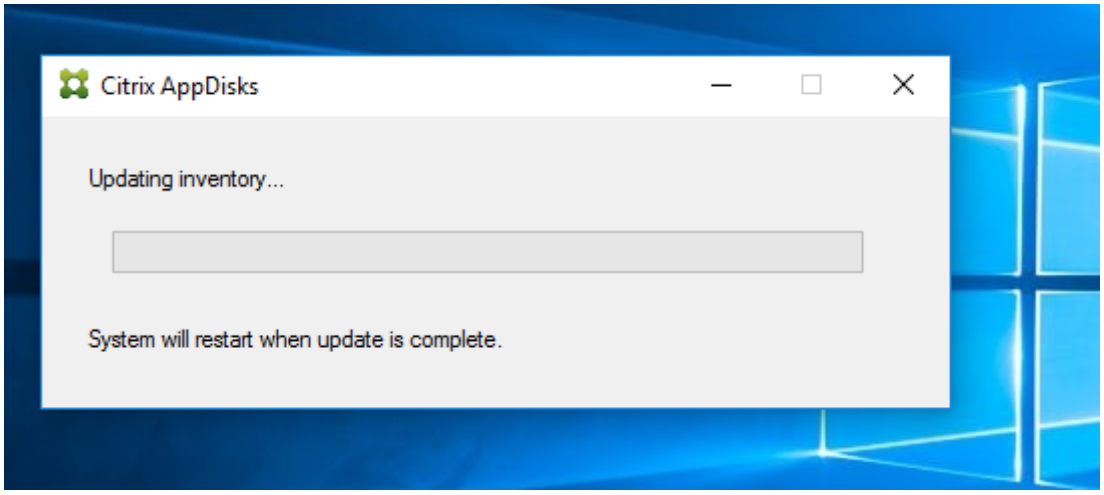
1. Select **AppDisks** in the Studio navigation pane.
2. Select the AppDisk you created, and then select **Seal AppDisk** in the Actions pane.

After you create the AppDisk, install applications on it, and then seal it, assign it to a Delivery Group.

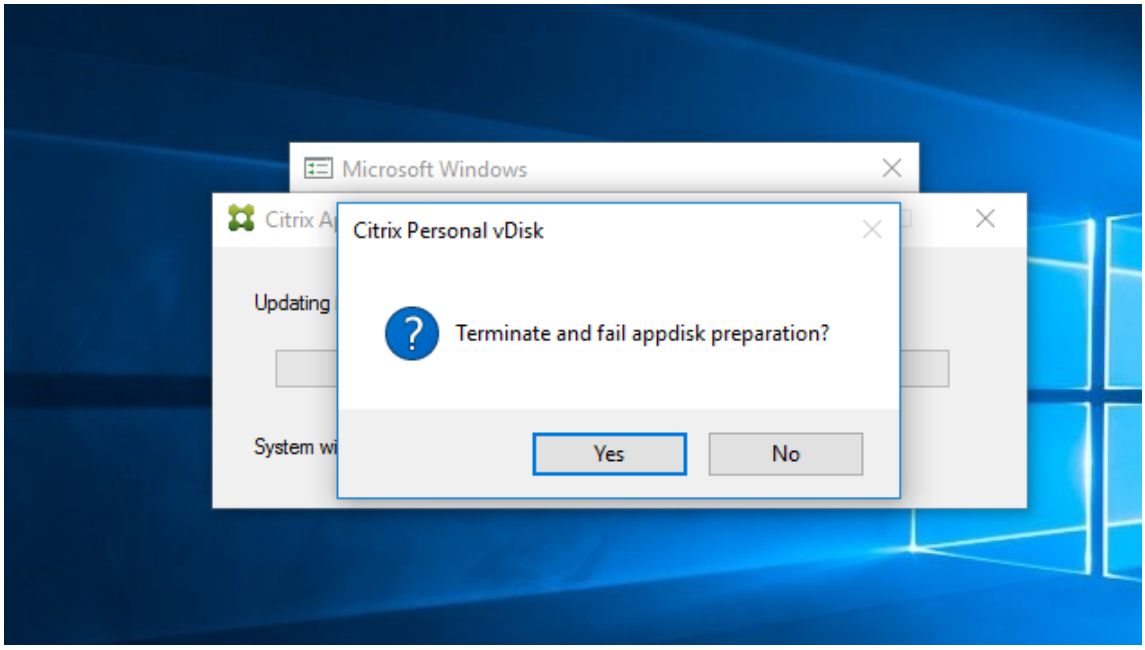
Cancel AppDisk preparation and sealing

In some cases, an administrator may need to cancel AppDisk creation or sealing:

1. Access the VM.
2. Close the dialog:



3. After closing the dialog, a popup message appears requesting verification to cancel the selected operation; click **Yes**.



> **Note**
>
> If you cancel AppDisk preparation, rebooting the machine returns it to the initial state, otherwise you need to create a clean VM.

Create an AppDisk on the hypervisor and import it to Studio

In this procedure, you complete the AppDisk creation and preparation tasks from the hypervisor management console and then import AppDisk into Studio.

Prepare, install applications, and seal an AppDisk on the hypervisor:

1. From the hypervisor management console, create a VM and install a VDA.
2. Power off the machine and take a snapshot of it.
3. Create a new machine from the snapshot and then add a new disk to it. This disk (which will become the AppDisk) must be large enough to hold all the applications you will install on it.
4. Start the machine and select **Start > Prepare AppDisk**. If this Start menu shortcut is not available on the hypervisor, open a command prompt at C:\Program Files\Citrix\personal vDisk\bin and type: **CtxPvD.Exe –s LayerCreationBegin**. The machine restarts and prepares the disk. A second restart occurs after several minutes when the preparation completes.
5. Install the applications you want to make available to users.
6. Double-click the **Package AppDisk** shortcut on the machine's desktop. The machine restarts again and the sealing process starts. When the "in process"dialog closes, power off the VM.

Use Studio to import the AppDisk you created on the hypervisor:

1. Select **AppDisks** in the Studio navigation pane and then select **Create AppDisk** in the Actions pane.
2. On the **Introduction** page, review the information and then click **Next**.
3. On the **Create AppDisk** page, select the **Import existing AppDisk** radio button. Select the resource (network and storage) where the AppDisk you created resides on the hypervisor. Click **Next**.
4. On the **Preparation Machine** page, browse to the machine, select the disk, and then click **Next**.
5. On the **Summary** page, type a name and description for the AppDisk. Review the information you specified on previous wizard pages. Click **Finish**. Studio imports the AppDisk.

After you import the AppDisk into Studio, assign it to a Delivery Group.

Assign an AppDisk to a Delivery Group

You can assign one or more AppDisks to a Delivery Group when you create the Delivery Group or later. The AppDisks information you provide is essentially the same.

If you are adding AppDisks to a Delivery Group that you are creating, use the following guidance for the **AppDisks** page in the Create Delivery Group wizard. (For information about other pages in that wizard, see Create Delivery Groups.)

To add (or remove) AppDisks in an existing Delivery Group:

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a Delivery Group and then select **Manage AppDisks** in the Actions pane. See the following guidance for the **AppDisks** page.
3. When you change the AppDisk configuration in a Delivery Group, a restart of the machines in the group is required.

AppDisks page:

The **AppDisks** page (in the Create Delivery Group wizard or in the Manage AppDisks flow) lists the AppDisks already deployed for the Delivery Group and their priority. (If you are creating the Delivery Group, the list will be empty.) For more information, see the AppDisk priority section.

1. Click **Add**. The Select AppDisks dialog box lists all AppDisks in the left column. AppDisks that are already assigned to this Delivery Group have enabled checkboxes and cannot be selected.
2. Select one or more checkboxes for available AppDisks in the left column. The right column lists the applications on the AppDisk. (Selecting the **Applications** tab above the right column lists applications in a format similar to a Start menu; selecting the **Installed packages** tab lists applications in a format similar to the Programs and Features list.)
3. After selecting one or more available AppDisks, click **OK**.

4. Click **Next** on the AppDisks page.

AppDisk priority in a Delivery Group

When a Delivery Group has more than one AppDisk assigned, the **AppDisks** page (in the Create Delivery Group, Edit Delivery Group, and Manage AppDisks displays) lists the AppDisks in descending priority. Entries at the top of the list have the higher priority. Priority indicates the order in which the AppDisks are processed.

You can use the up and down arrows adjacent to the list to change the AppDisk priority. If AppDNA is integrated with your AppDisk deployment, it automatically analyzes the applications and then sets the priority when the AppDisks are assigned to the Delivery Group. Later, if you add or remove AppDisks from the group, clicking **Auto-Order** instructs AppDNA to re-analyze the current list of AppDisks and then determine the priorities. The analysis (and priority reordering, if needed) may take several moments to complete.

Manage AppDisks

After you create and assign AppDisks to Delivery Groups, you can change the AppDisk's properties through the AppDisks node in the Studio navigation pane. Changes to applications in an AppDisk must be done from the hypervisor management console.

Important Windows Update considerations:

You can use the Windows Update service to update applications (such as the Office suite) on an AppDisk. However, do not use the Windows Update Service to apply operating system updates to an AppDisk. Apply operating system updates to the master image, not the AppDisk; otherwise, the AppDisk will not initialize correctly.

- When applying patches and other updates to applications in an AppDisk, apply only those that the application requires. Do not apply updates for other applications.
- When installing Windows updates, first deselect all entries and then select the subset required by the applications on the AppDisks you're updating.

Antivirus considerations for AppDisk creation

In some cases, you may run into problems trying to create an AppDisk due to scenarios where the base VM has an antivirus (A/V) agent installed. In such cases, AppDisk creation may fail when certain processes are flagged by the A/V agent. These processes, **CtxPvD.exe** and **CtxPvDSrv.exe** must be added to the exception list for the A/V agent used by the base VM.

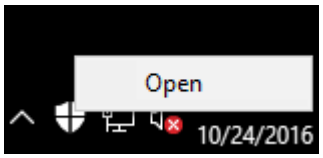
This section provides information about adding exceptions for the following antivirus applications:

- Windows Defender (for Windows 10)
- OfficeScan (version 11.0)
- Symantec (version 12.1.16)
- McAfee (version 4.8)

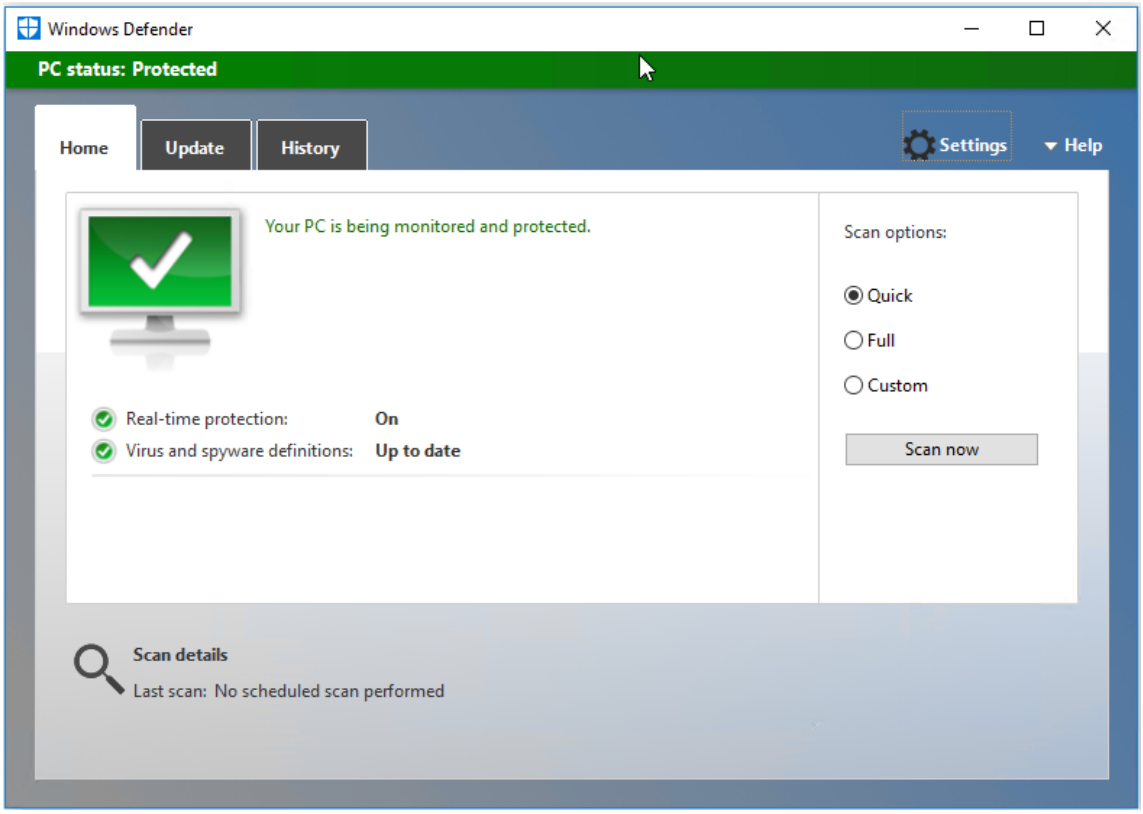
Windows Defender

If your base VM uses Windows Defender (version 10):

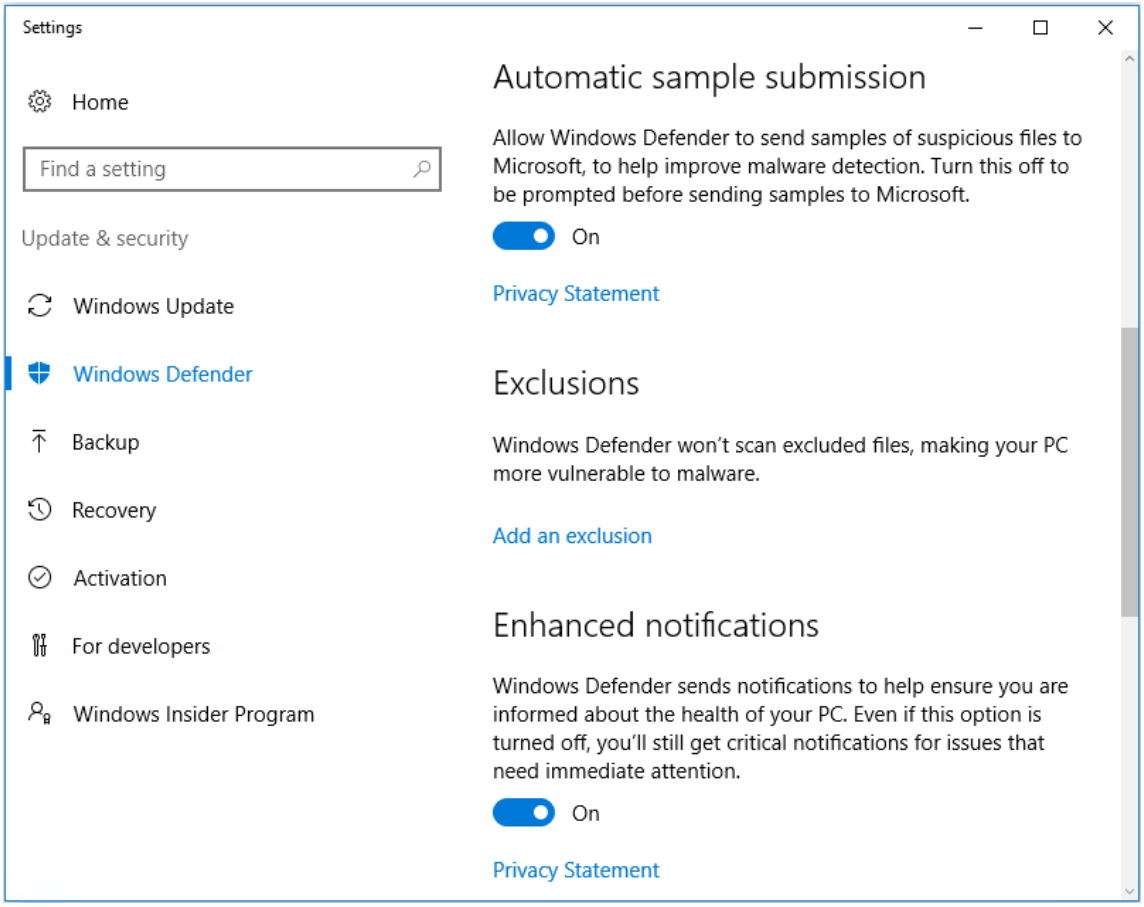
1. Log into your computer with local administrator privileges.
2. Select the Windows Defender icon and right click to display the **Open** button:



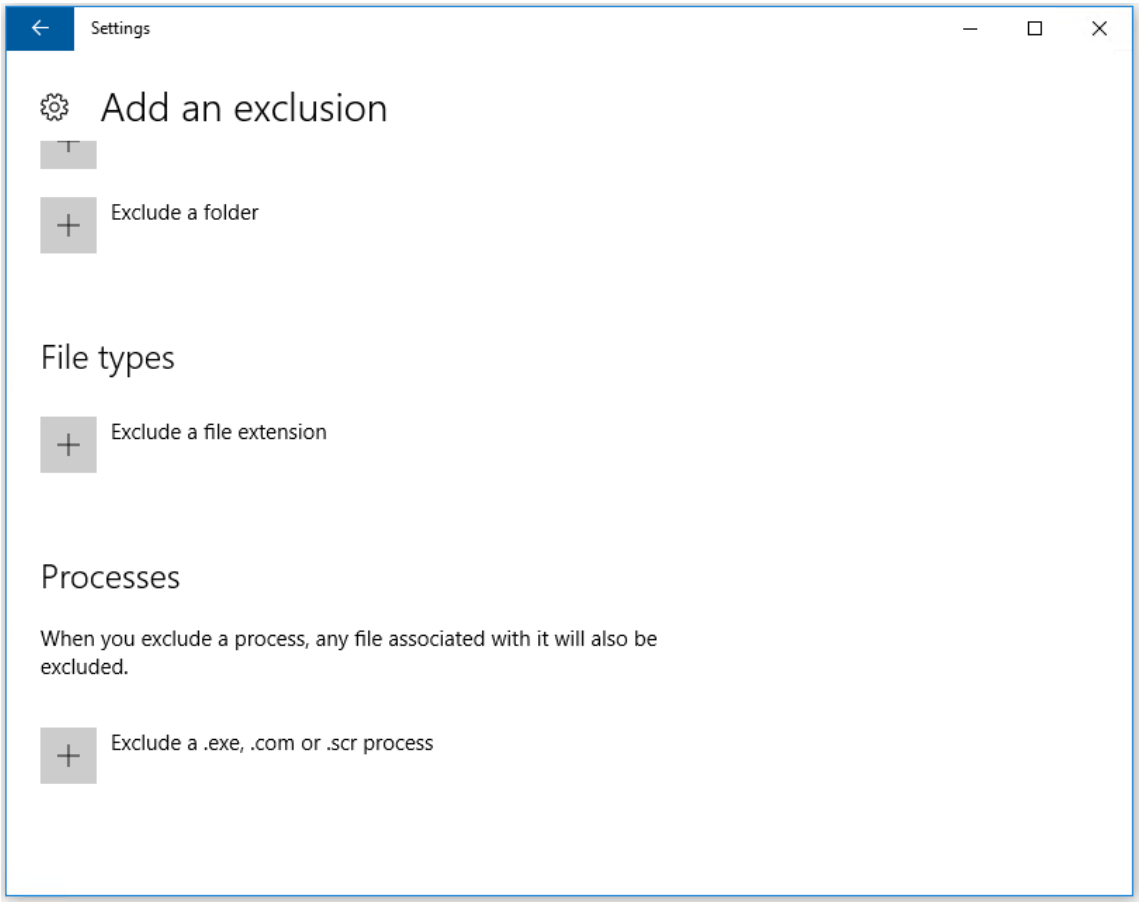
3. In the Windows Defender console, select **Settings** in the upper right portion of the interface:



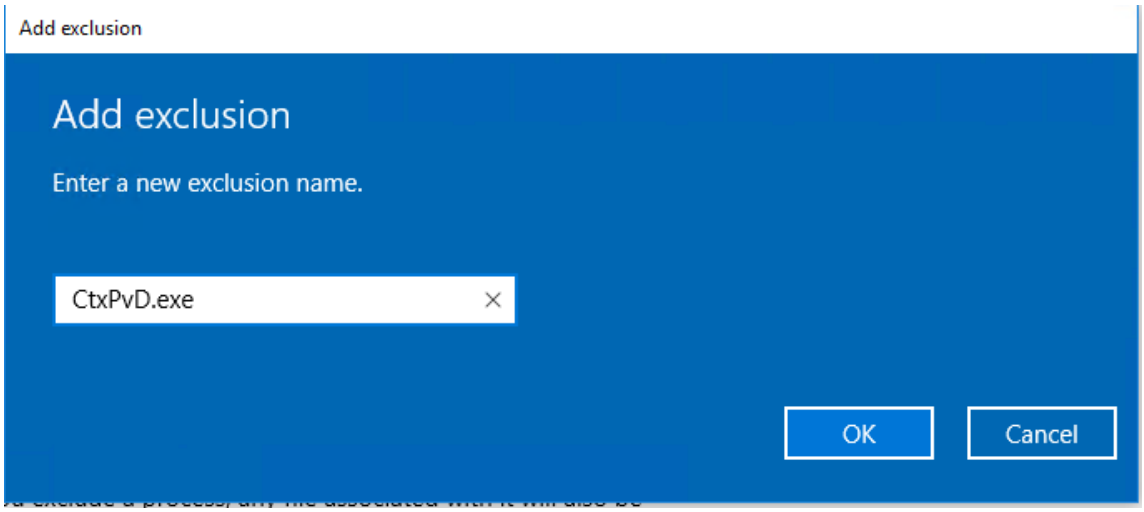
4. In the **Exclusions** portion of the Settings screen, click **Add an exclusion**:



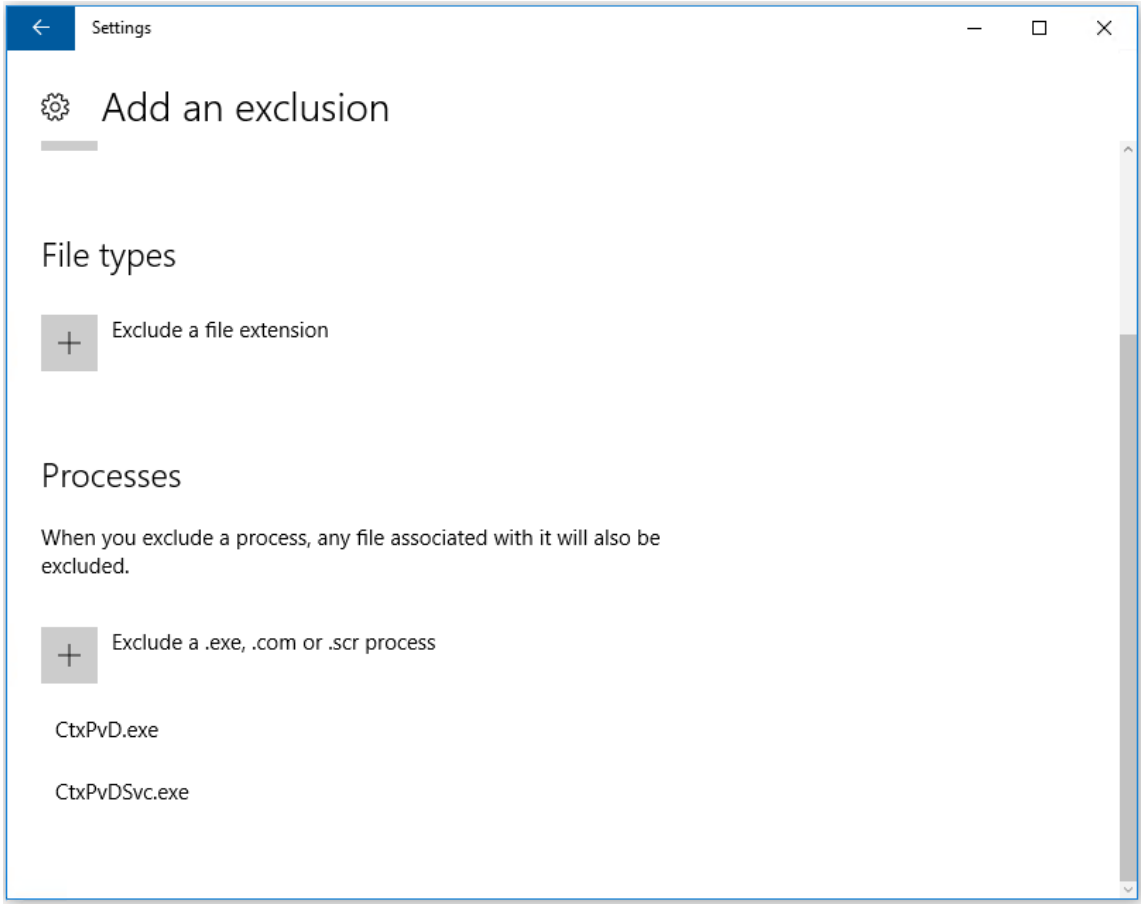
5. In the **Add an exclusion** screen, select **Exclude a .exe, .com, or .scr process**:



6. In the **Add exclusion** screen, enter the name of the exclusion; both **CtxPvD.exe** and **CtxPvDSvc.exe** must be added to prevent conflicts when creating an AppDisk. After entering the exclusion name, click **OK**:



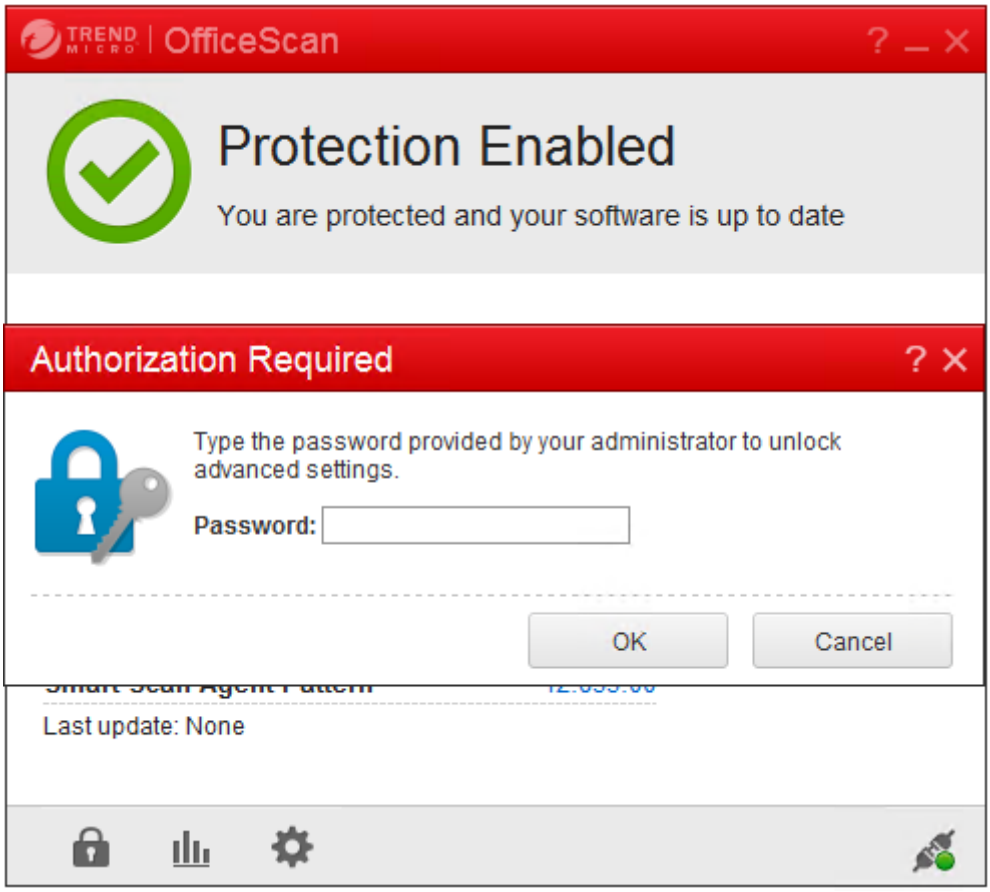
After adding the exclusions, they appear in the list of excluded processes in the **Settings** screen:



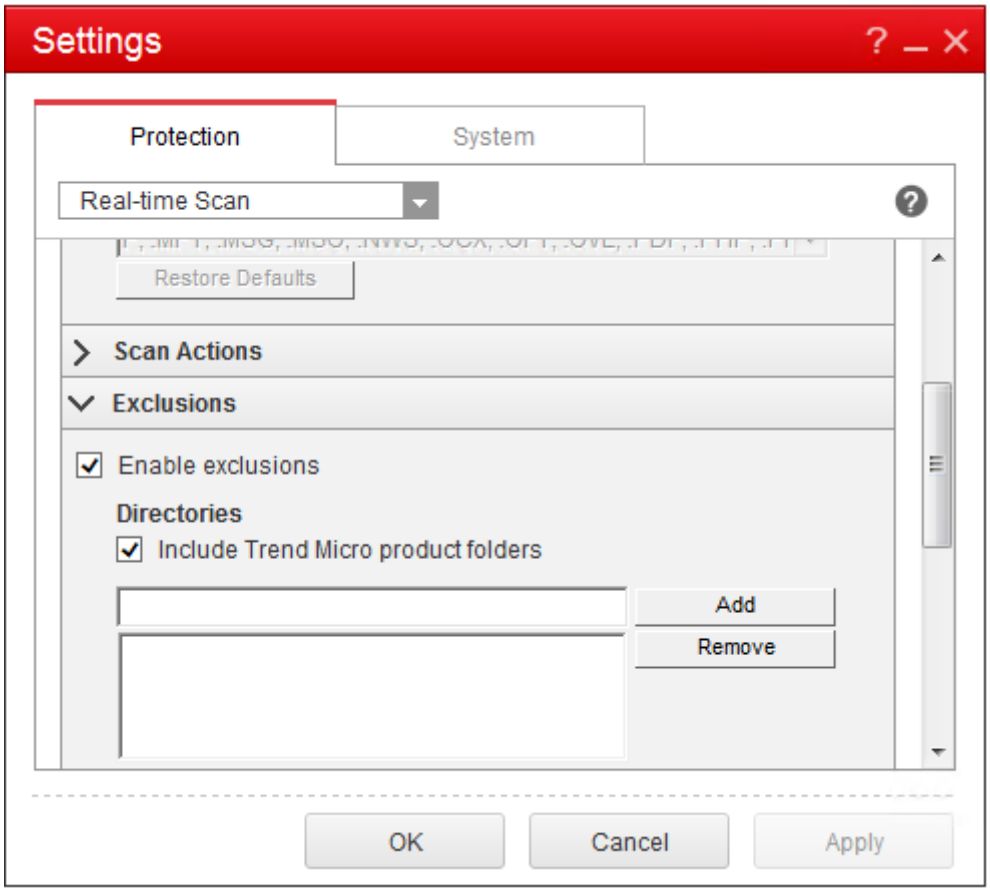
OfficeScan

If your base VM uses OfficeScan (version 11):

1. Launch the OfficeScan console.
2. Click the lock icon in the lower left portion of the interface, and enter your password:



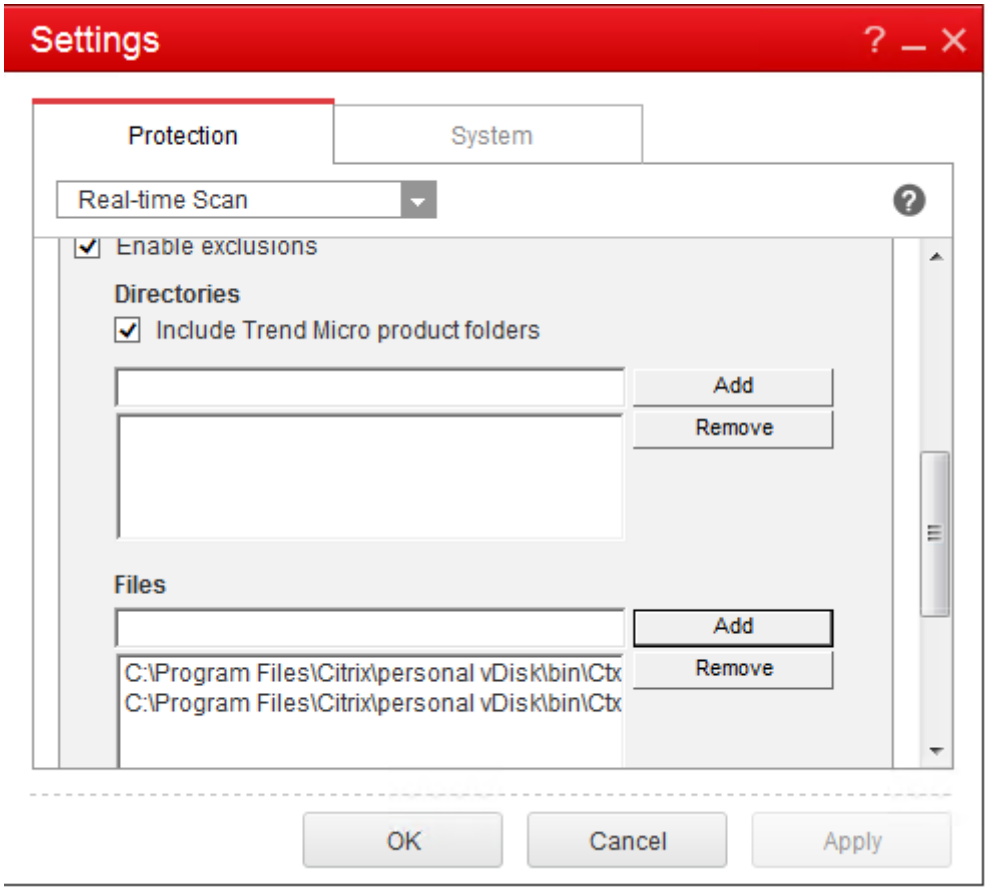
3. Click the **Settings** icon to display configuration options.
4. In the Settings screen, select the **Protection** tab.
5. In the Protection tab, scroll down until you locate the **Exclusions** section.



6. In the **Files** section, click **Add**, and enter the following AppDisk processes to the exception list:

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
   ```

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
   ```

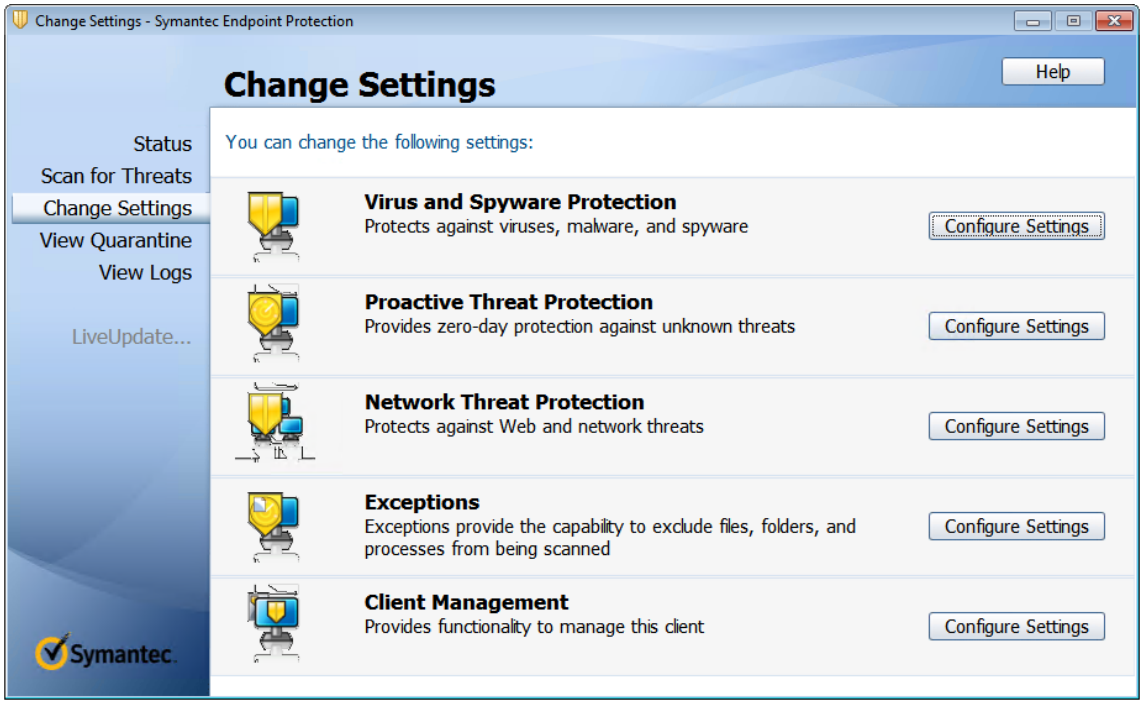



7. Click **Apply**, then **OK** to add the exclusions.

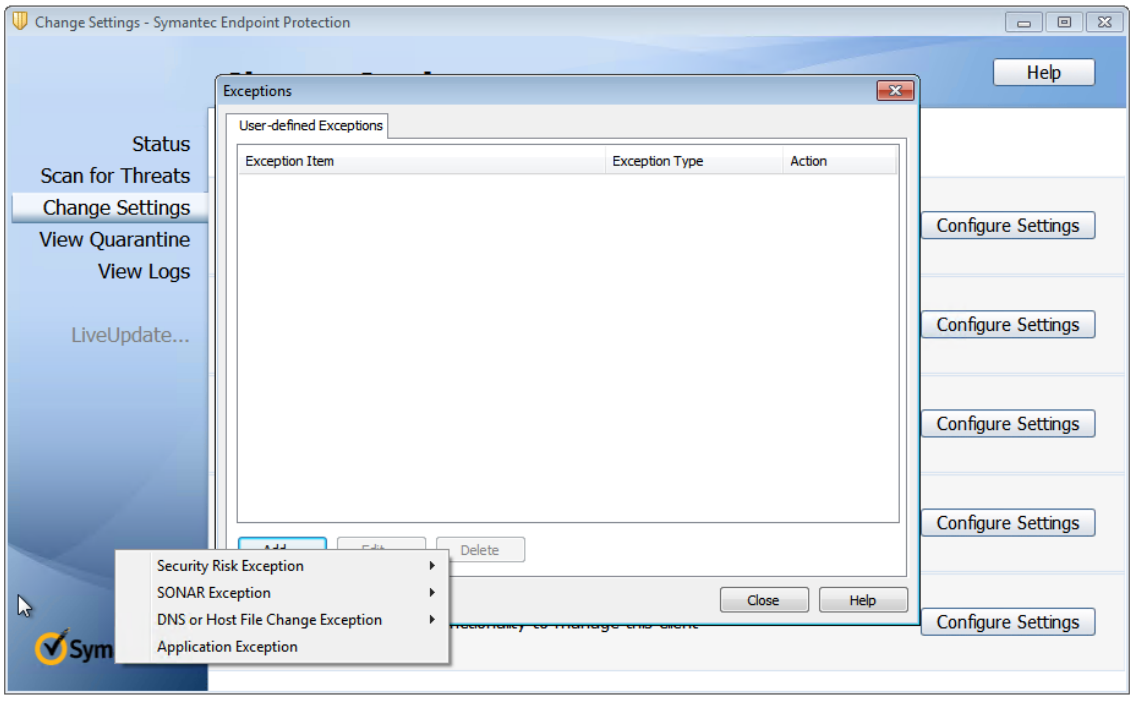
Symantec

If your base VM uses Symantec (version 12.1.16):

1. Launch the Symantec console.
2. Click **Change Settings**.
3. In the **Exceptions** section, click **Configure Settings**:



4. In the Configure Settings screen, click **Add**.
5. After clicking Add, a context menu appears to allow you to specify the application type. Select **Application Exception**:

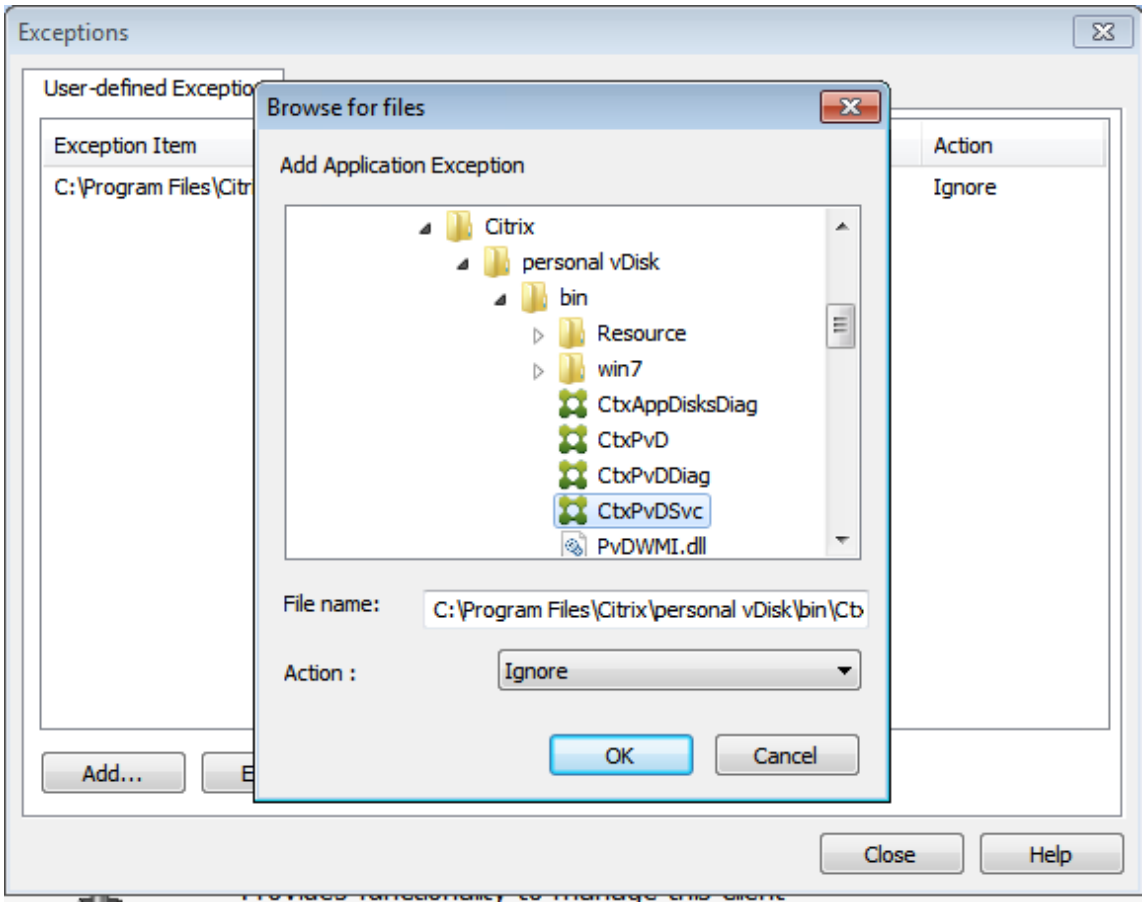


6. In the Exceptions screen, enter the following AppDisk file paths and set the action to **Ignore**:

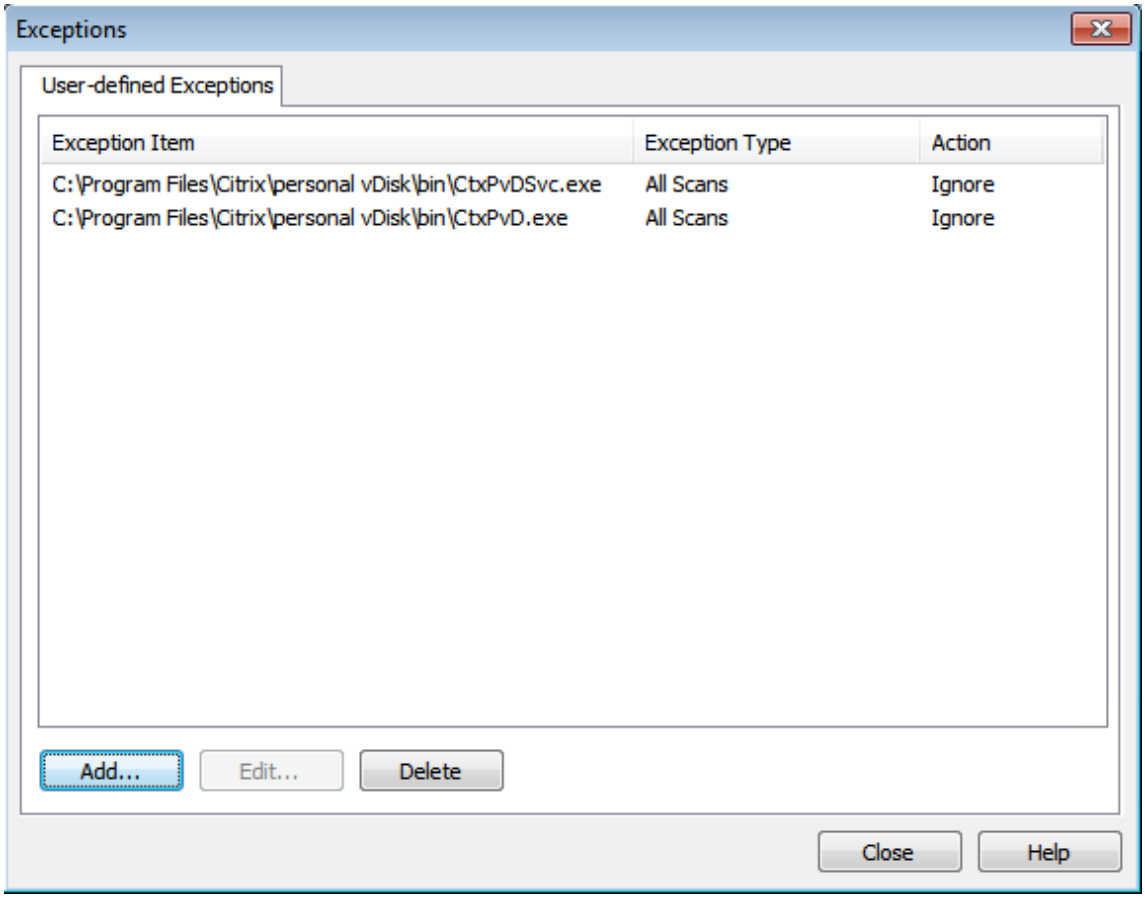
```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
```



```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```



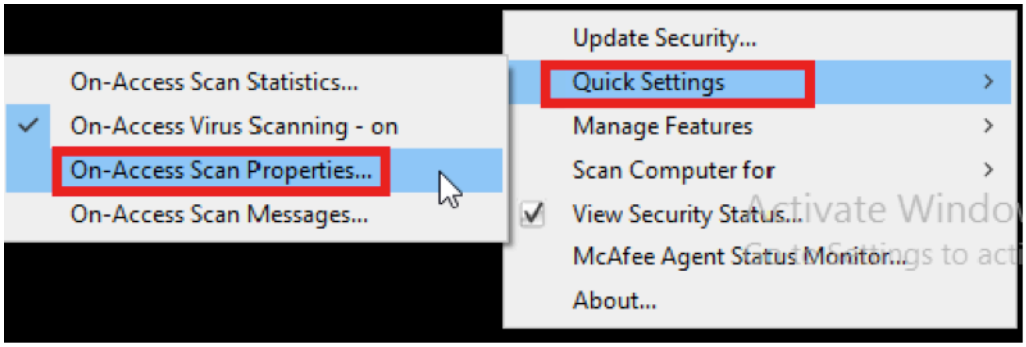
The noted exceptions are added to the list. Close the window to apply your changes.



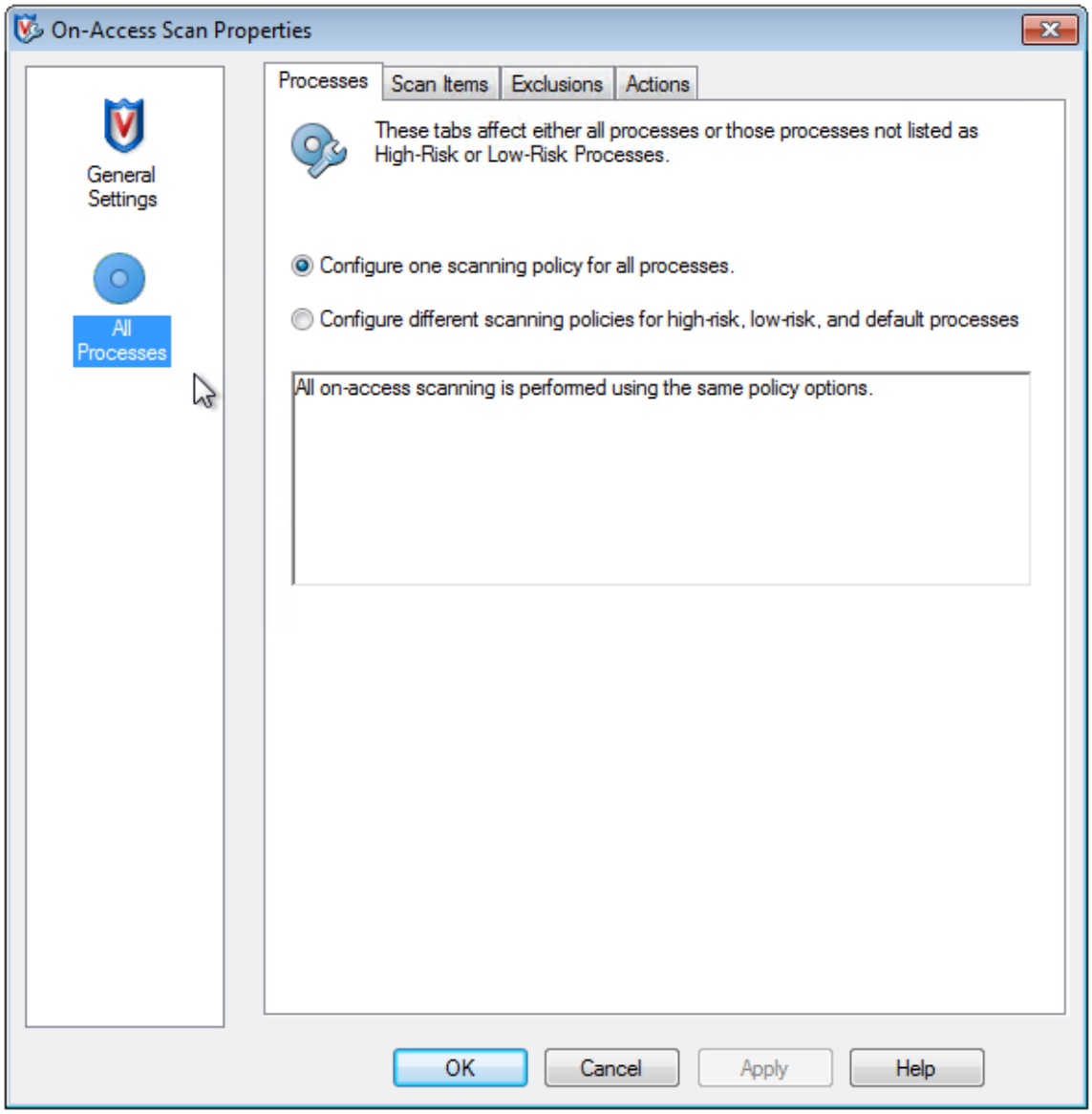
McAfee

If your base VM uses McAfee (verson 4.8):

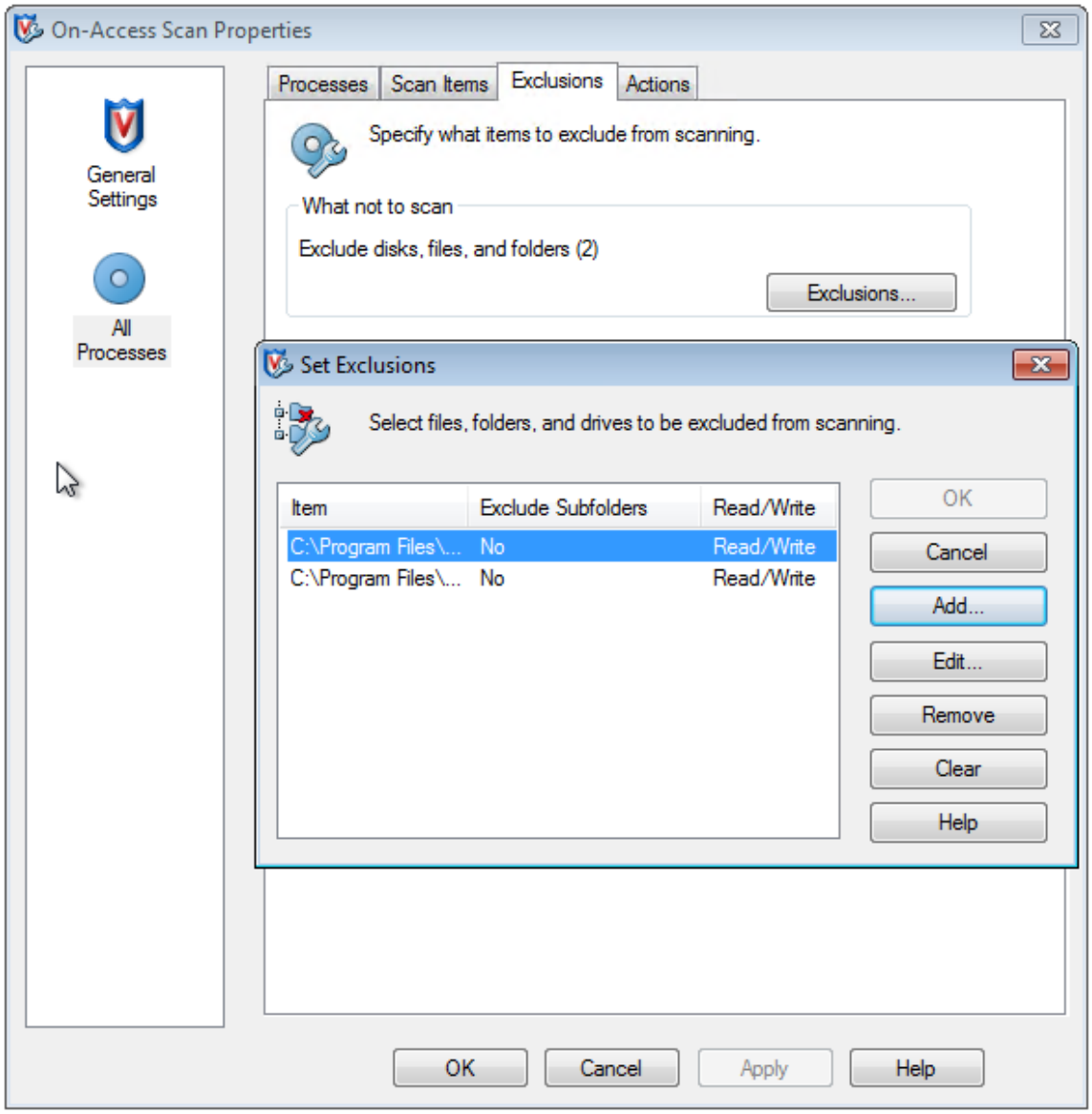
1. Right click the McAfee icon, and expand the **Quick Settings** option.
2. In the expanded menu, select **On-Access Scan Properties**:



3. In the **On-Access Scan Properties** screen, click **All Processes**:



4. Select the **Exclusions** tab.
5. Click the **Exclusions** button.
6. In the **Set Exclusions** screen, click **Add**:

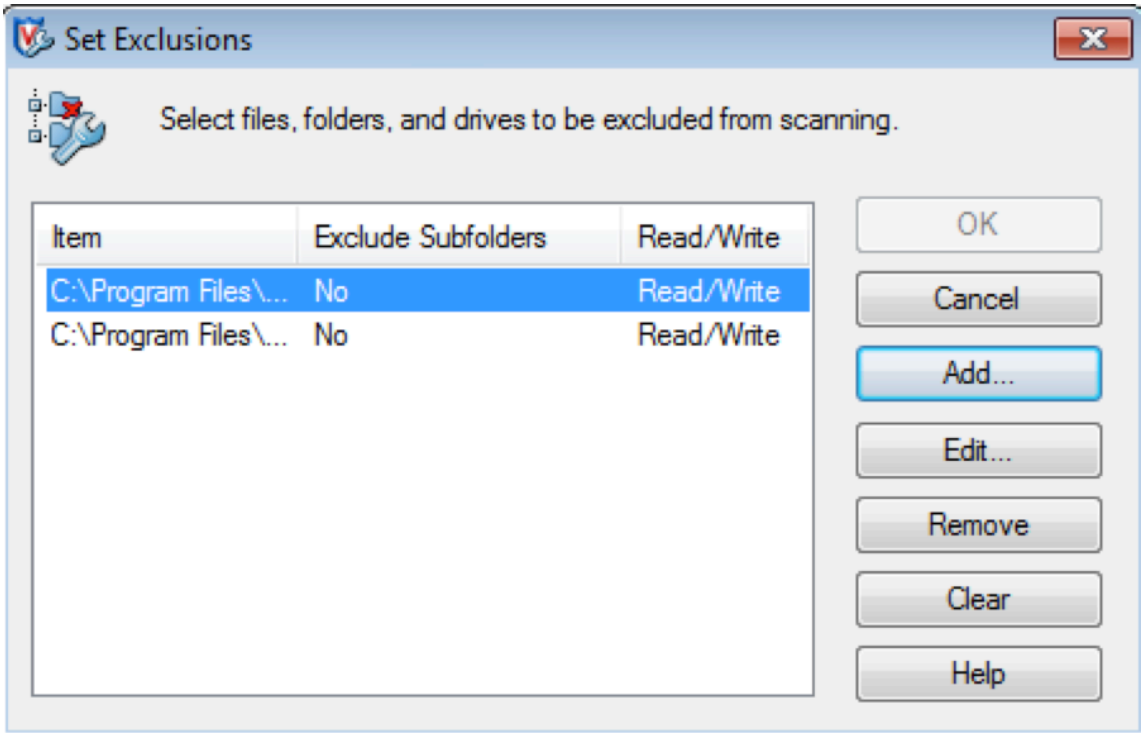


7. In the **Add Exclusion Item** screen, select **By name/location (can include wildcards * or ?)**. Click **Browse** to locate the exclusion executables:

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
   ```

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
   ```

8. Click **OK**.
9. The **Set Exclusions** screen now displays the added exclusions. Click **OK** to apply the changes:



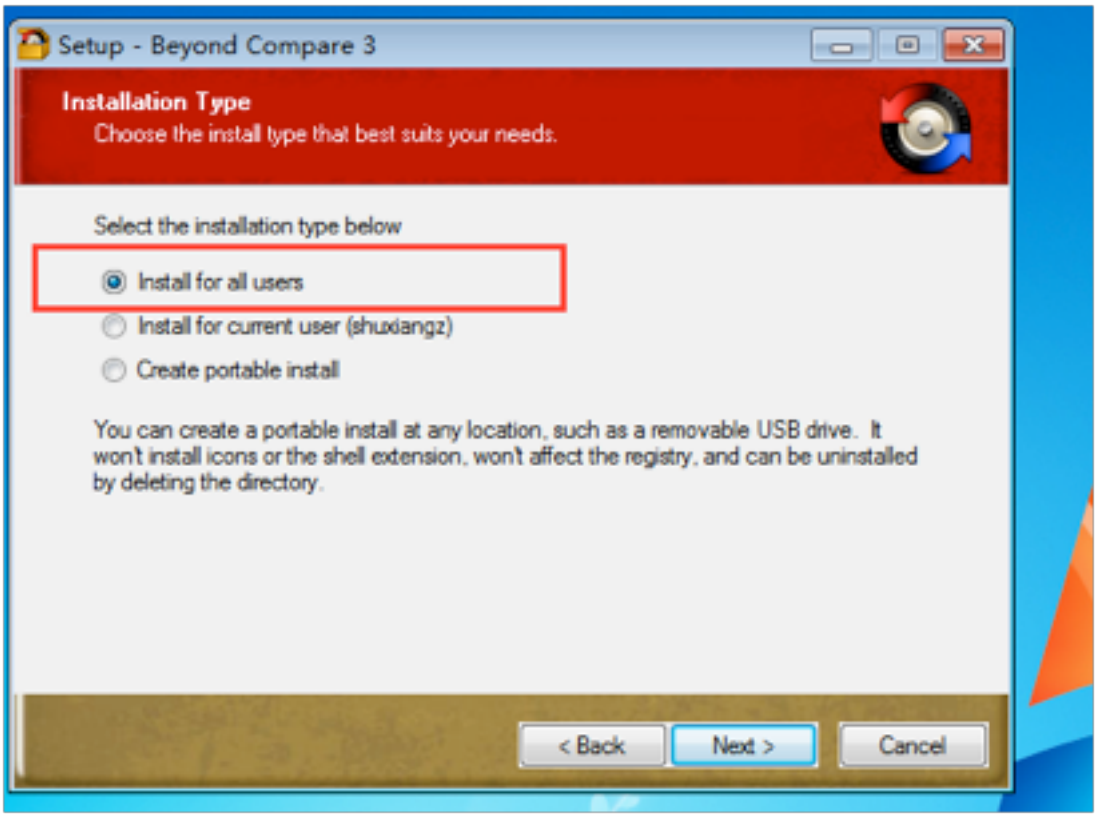
After configuring these exclusions, create the AppDisk.

How applications appear in the Start menu

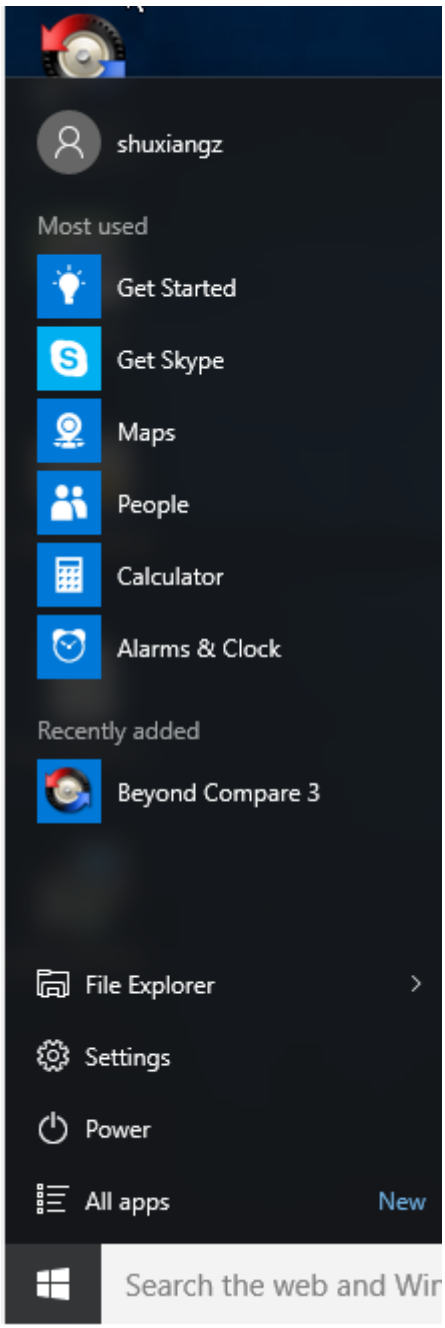
If a new AppDisk is created and an app is made available for all users the disk is attached to the desktop and a shortcut appears for the app in the Start menu. When an AppDisk is created and installed for the current user only and the disk is attached to the desktop, the shortcut for the app fails to appear in the Start menu.

For example, create a new app and make it available for all users:

1. Install an app on the AppDisk (for example, *Beyond Compare* is the selected app):

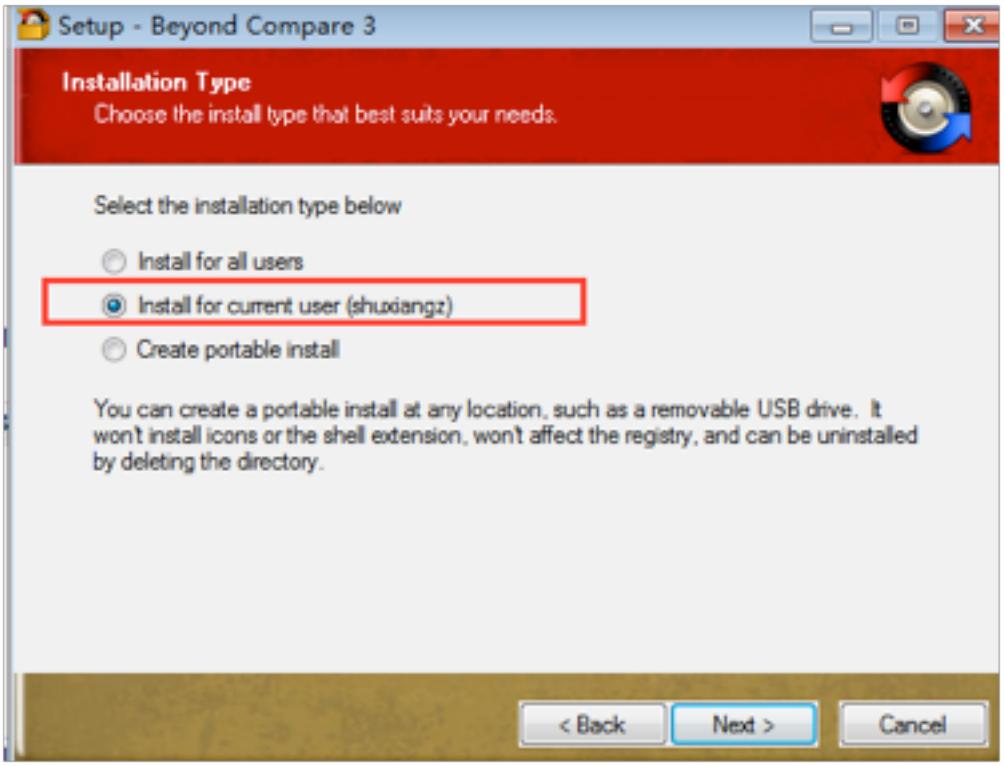


2. Attach the disk to the desktop; the shortcut for the newly installed app (*Beyond Compare*) appears in the Start menu:

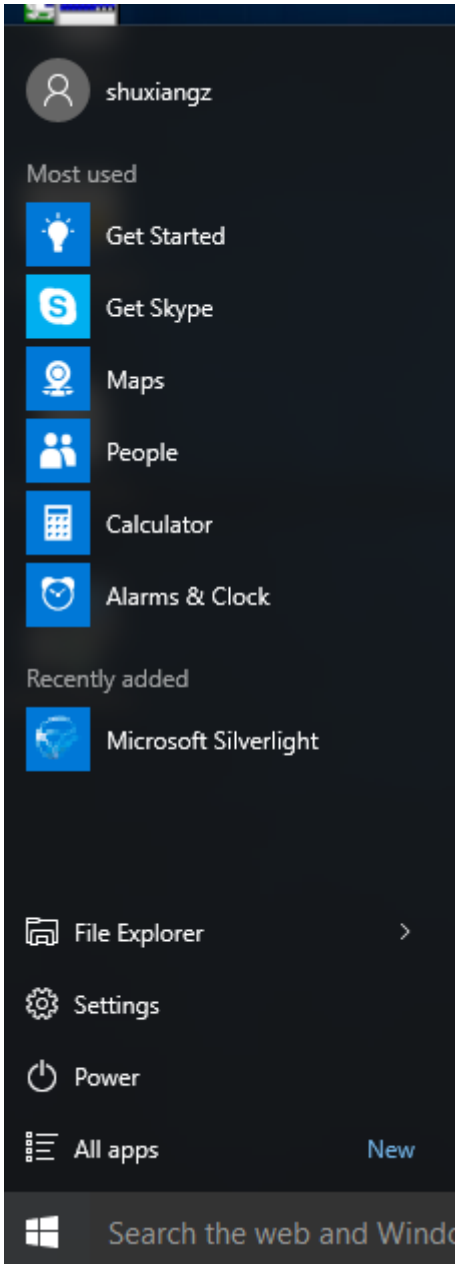


To install an app for the current user only:

1. Install an app on the AppDisk and make it available for the current user:



2. Attach the disk to the desktop; note that the shortcut does not appear in the Start menu:



AppDisk logging

AppDisk users can obtain diagnostic information and optionally upload it to the Citrix Insight Services (CIS) website.

How does it work?

This functionality uses a script-based PowerShell tool which identifies all of the log files created by AppDisk/PVD, collects output from PowerShell commands containing information about the system

(and processes), compresses everything into a single organized file, and finally provides the option to either save the compressed folder locally, or upload it to CIS (Citrix Insight Services).

> **Note:**
>
> CIS gathers anonymous diagnostic information that it uses to improve AppDisk/PvD functionality. Access the Citrix CIS website to manually upload the diagnostic bundle. You must login with your Citrix credentials to access this site.

Using PowerShell scripts to collect AppDisk/PVD log files

The AppDisk/PvD installer adds two scripts for diagnostic data collection:

- `Upload-AppDDiags.ps1`: performs AppDisk diagnostic data collection
- `Upload-PvDDiags.ps1`: performs PvD diagnostic data collection

These scripts are added in C:\Program Files\Citrix\personal vDisk\bin\scripts. You must execute these PowerShell scripts as an administrator.

Upload-AppDDiags.ps1 Use this script to initiate AppDisk diagnostic data collection and optionally manually upload the data to the CIS website.

```
Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters
>]
```

`-OutputFile`: Local path for zip file instead of uploading to CIS. When `–OutputFile` is omitted, the upload occurs. when `–OutputFile` is specified, the script creates a zip file that you can upload manually later.

Exmaples:

- `Upload-AppDDiags`: Uploads diagnostic data to Citrix CIS website using credentials entered by interactive user.
- `Upload-AppDDiags -OutputFile C:\MyDiags.zip`: Saves AppDisk diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.

Upload-PvDDiags.ps1 Use this script to initiate PvD diagnostic data collection and optionally manually upload the data to the CIS website.

```
Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

`-OutputFile`: Local path for zip file instead of uploading to CIS. When `–OutputFile` is omitted, the upload occurs. when `–OutputFile` is specified, the script creates a zip file that you can upload manually later.

Examples:

- `Upload-PvDDiags`: Uploads PvD diagnostic data to Citrix CIS website using credentials entered by interactive user.
- `Upload-PvDDiags -OutputFile C:\MyDiags.zip`: Saves PvD diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.

Publish content

February 7, 2020

You can publish an application that is simply a URL or UNC path to a resource, such as a Microsoft Word document or a web link. This feature is known as published content. The ability to publish content adds flexibility to how you deliver content to users. You benefit from the existing access control and management of applications. And, you can specify what to use to open the content: local or published applications.

The published content appears just like other applications in StoreFront and Citrix Workspace app. Users access it in the same way they access applications. On the client, the resource opens as usual.

- If a locally installed application is appropriate, it is launched to open the resource.
- If a File Type Association has been defined, a published application launches to open the resource.

You publish content using the PowerShell SDK. (You cannot use Studio to publish content. However, you can use Studio to edit application properties later, after they are published.)

Configuration overview and preparation

Publishing content uses the New-BrokerApplication cmdlet with the following key properties. (See the cmdlet help for descriptions of all cmdlet properties.)

```
1 New-BrokerApplication –ApplicationType PublishedContent -
     CommandLineExecutable location -Name app-name -DesktopGroup delivery
     -group-name
2 <!--NeedCopy-->
```

The ApplicationType property must be `PublishedContent`.

The `CommandLineExecutable` property specifies the location of the published content. The following formats are supported, with a limit of 255 characters.

- HTML website address (for example, http://www.citrix.com)

- Document file on a web server (for example, `https://www.citrix.com/press/pressrelease.doc`)
- Directory on an FTP server (for example, `ftp://ftp.citrix.com/code`)
- Document file on an FTP server (for example, `ftp://ftp.citrix.com/code/Readme.txt`>)
- UNC directory path (for example, `file://myServer/myShare or \\\\\myServer\\myShare`)
- UNC file path (for example, `file://myServer/myShare/myFile.asf` or `\\myServer\myShare\myFile.asf`)

Ensure that you have the correct SDK.

- For Citrix Virtual Apps and Desktops service deployments, download and install the Citrix Virtual Apps and Desktops Remote PowerShell SDK.
- For on-premises Citrix Virtual Apps and Desktops deployments, use the PowerShell SDK that is installed with the Delivery Controller. Adding a published content application requires a minimum version 7.11 Delivery Controller.

The following procedures use examples. In the examples:

- A machine catalog has been created.
- A Delivery Group named PublishedContentApps has been created. The group uses a Server OS machine from the catalog. The WordPad application has been added to the group.
- Assignments are made for the Delivery Group name, the CommandLineExecutable location, and the application name.

Get started

On the machine containing the PowerShell SDK, open PowerShell.

The following cmdlet adds the appropriate PowerShell SDK snap-in, and assigns the returned Delivery Group record.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

If you are using the Citrix Virtual Apps and Desktops service, authenticate by entering your Citrix Cloud credentials. If there is more than one customer, choose one.

Publish a URL

After assigning the location and application name, the following cmdlet publishes the Citrix home page as an application.


```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication –ApplicationType PublishedContent –
    CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
    Uid
<!--NeedCopy-->
```

Verify success:

- Open StoreFront and log on as a user who can access applications in the PublishedContentApps Delivery Group. The display includes the newly created application with the default icon. To learn about customizing the icon, see https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Click the Citrix Home Page application. The URL launches in a new tab in a locally running instance of your default browser.

Publish resources located at UNC paths

In this example, the administrator has already created a share named PublishedResources. After assigning the locations and application names, the following cmdlets publish an RTF and a DOCX file in that share as a resource.

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf
    "
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.
    docx"
$docxAppName = "PublishedDOCX"

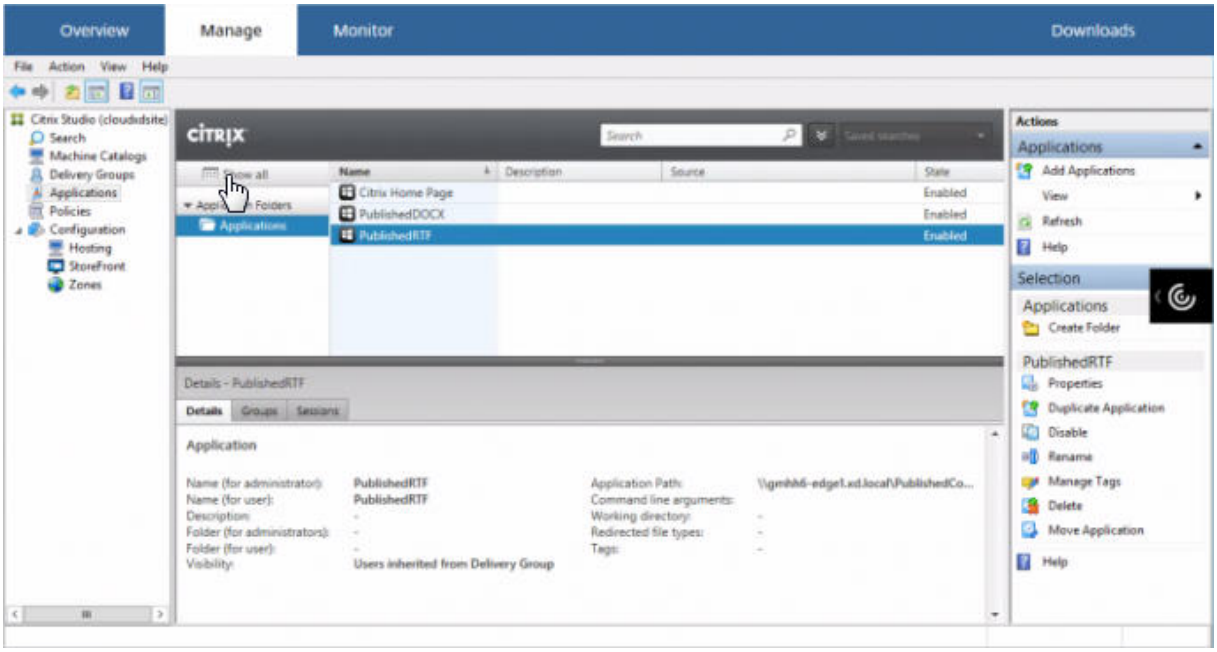
New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

Verify success:

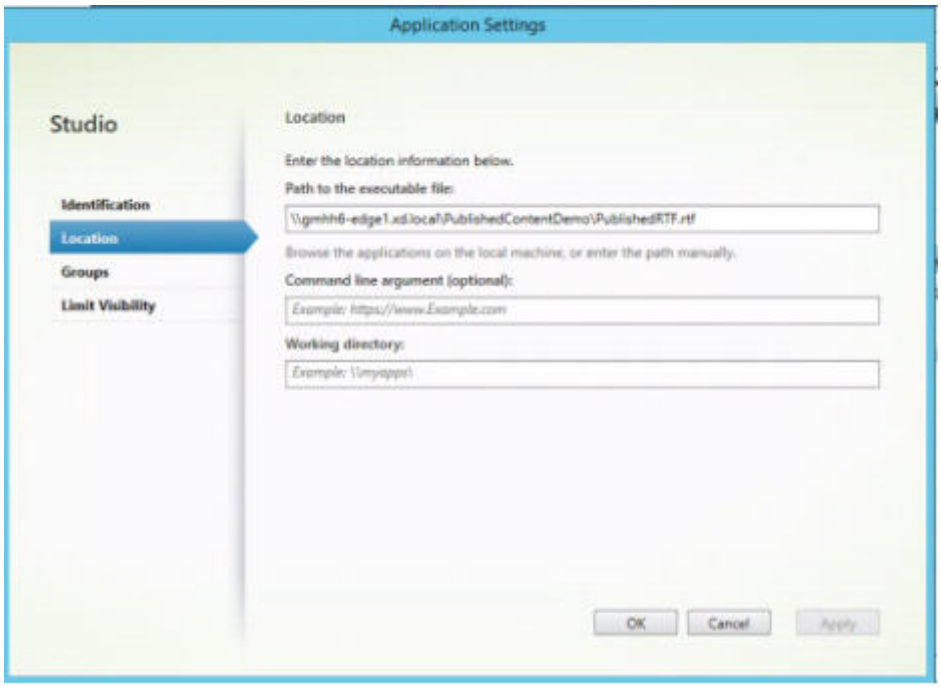
- Refresh your StoreFront window to see the newly published documents.
- Click the **PublishedRTF** and **PublishedDOCX** applications. Each document opens in a locally running WordPad.

View and edit PublishedContent applications

You manage published content using the same methods that you use for other application types. The published content items appear in the Applications list in Studio and can be edited in Studio.

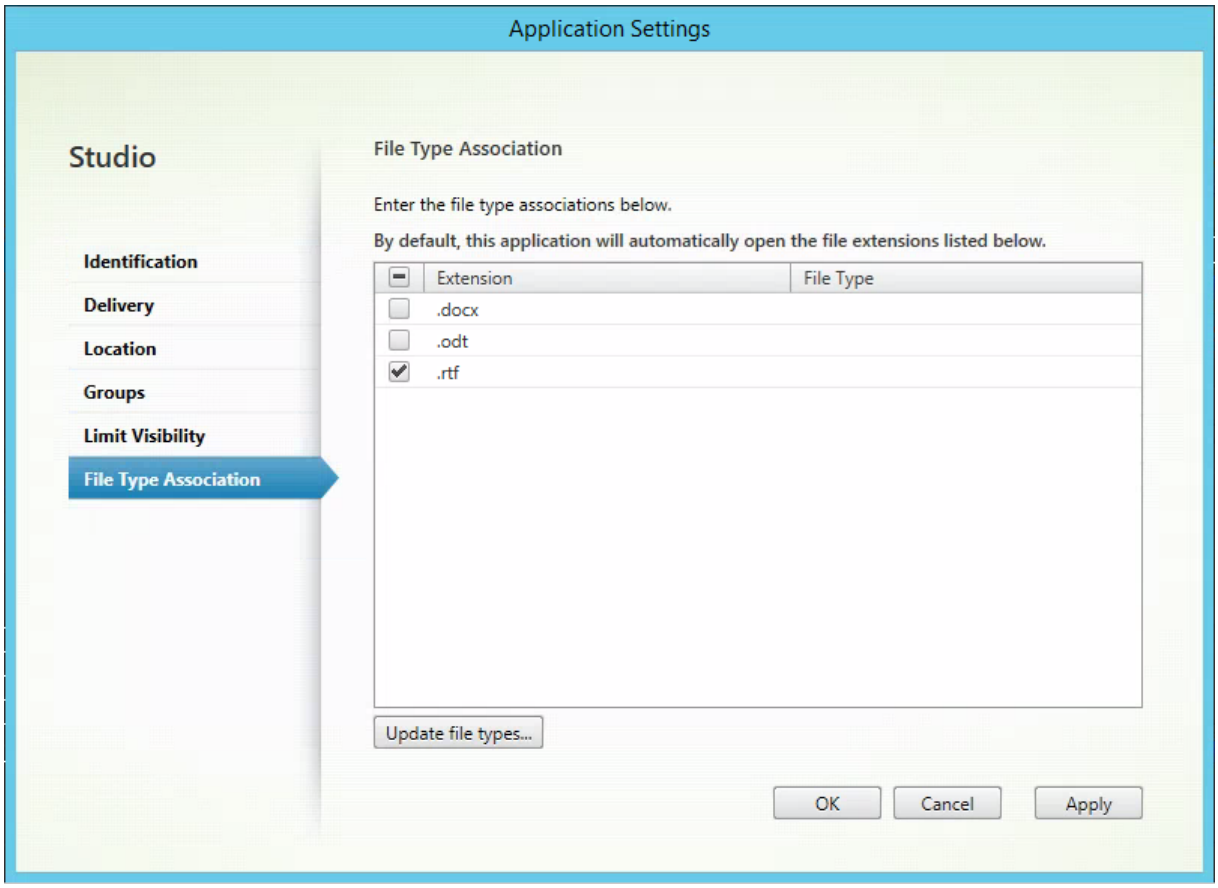


Application properties (such as user visibility, group association, and shortcut) apply to the published content. However, you cannot change the command-line argument or working directory properties on the **Location** page. To change the resource, modify the **Path to the executable file** field on that page.

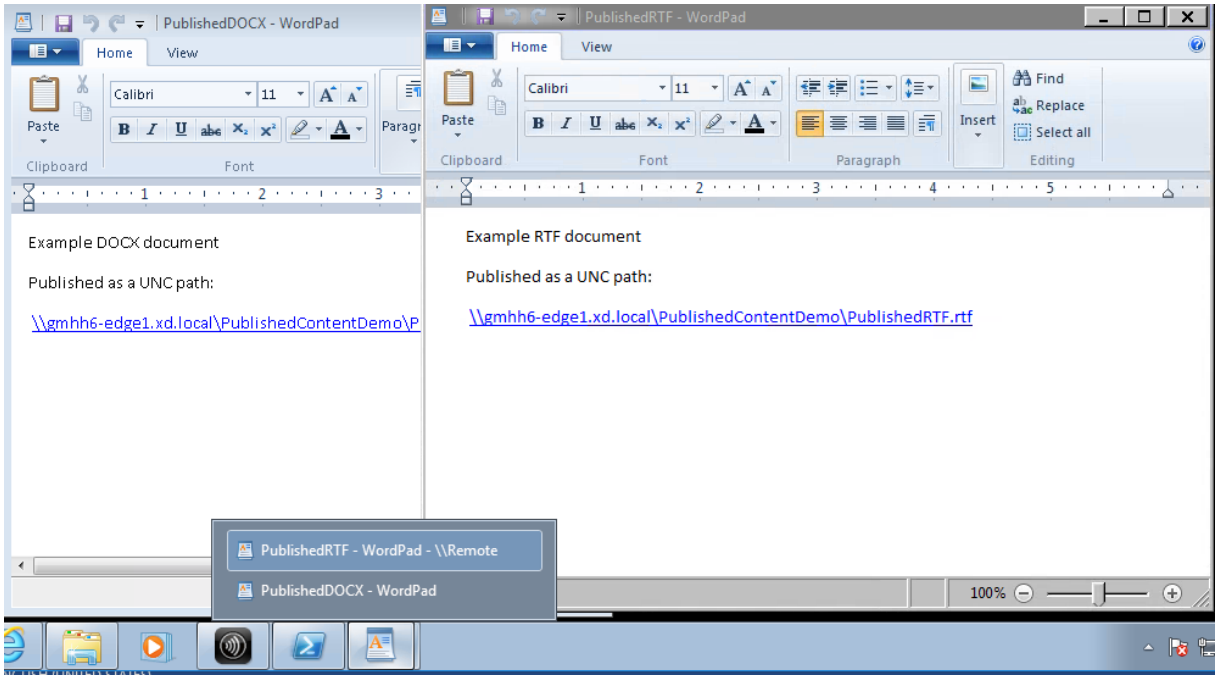


To use a published application to open a PublishedContent application (rather than a local application), edit the published application's **File Type Association** property. In this example, the published WordPad application was edited to create a File Type Association for .rtf files.

Turn on maintenance mode for the Delivery Group before editing the File Type Association. Remember to turn off maintenance mode when you're done.



Refresh StoreFront to load the File Type Association changes, and then click the PublishedRTF and PublishedDOCX applications. Notice the difference. PublishedDOCX still opens in the local WordPad. However, PublishedRTF now opens in the published WordPad due to the file type association.



For more information

- Create machine catalogs
- Create Delivery Groups
- Change application properties

Server VDI

February 6, 2020

Use the Server VDI (Virtual Desktop Infrastructure) feature to deliver a desktop from a server operating system for a single user.

- Enterprise administrators can deliver server operating systems as VDI desktops, which can be valuable for users such as engineers and designers.
- Service Providers can offer desktops from the cloud; those desktops comply with the Microsoft Services Provider License Agreement (SPLA).

You can use the Enhanced Desktop Experience Citrix policy setting to make the server operating system look like a desktop operating system.

The following features cannot be used with Server VDI:

- Personal vDisks
- Hosted applications
- Local App Access
- Direct (non-brokered) desktop connections
- Remote PC Access

Server VDI is currently supported on Windows Server 2019 and Windows Server 2016 machines.

For Server VDI to work with TWAIN devices such as scanners, the Windows Server Desktop Experience feature must be installed.

Install and configure Server VDI

1. Prepare the Windows server for installation.
    - Use Windows Server Manager to ensure that the Remote Desktop Services role services are not installed. If they were previously installed, remove them. The VDA installation fails if these role services are installed.
    - Ensure that the "Restrict each user to a single session"property is enabled. On the Windows server, edit the registry for the Terminal Server setting:
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer
        - DWORD fSingleSessionPerUser = 1
2. Use the Citrix Virtual Apps and Desktops installer's command line interface to install a VDA on a supported server or server master image, specifying the "quiet"and "servervdi"options. (By default, the installer's graphical interface blocks the Windows single-session OS VDA on a server operating system. Using the command line overrides this behavior.) Use one of the following commands:
    - Citrix Virtual Apps and Desktops deployments:
        - `XenDesktopVdaSetup.exe /quiet /servervdi`
        - `VDAWorkstationSetup.exe /quiet /servervdi`
    - Citrix Virtual Apps and Desktops service deployments:
        - `VDAWorkstationSetup.exe /quiet /servervdi`

    For other options:

    - You can specify the Delivery Controller or Cloud Connector with the "controllers"option.
    - Use the `enable_hdx_ports` option to open ports in the firewall, unless the firewall is to be configured manually.
    - Add the `mastermcsimage` (or `masterimage`) option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.

- Do not include options for features that are not supported with Server VDI, such as "baseimage"(for personal vDisks).
- For all option details, see Install using the command line.

3. Create a machine catalog for Server VDI. In the catalog creation wizard:

   - On the **Operating System** page, select **Single-session OS**.
   - On the **Summary** page, specify a machine catalog name and description for administrators that clearly identifies it as Server VDI. This is the only indicator in Studio that the catalog supports Server VDI.

   When using Search in Studio, the Server VDI catalog is displayed on the **Single-session OS Machines** tab, even though the VDA was installed on a server.

4. Create a Delivery Group and select the Server VDI catalog you created.

If you did not specify the Delivery Controllers or Cloud Connector while installing the VDA, remember to specify them afterward. For details, see VDA registration.

User personalization layer

February 7, 2020

The user personalization layer feature for Citrix Virtual Apps and Desktops extends the capabilities of non-persistent machine catalogs. User personalization layers preserve users'data and locally installed applications across sessions. Powered by Citrix App Layering, this feature replaces Personal vDisk (PvD).

Like PvD, the user personalization layer feature works with Citrix Provisioning and Machine Creation Services (MCS) in a non-persistent machine catalog. The feature components are installed alongside the Virtual Delivery Agent within the master Windows 10 image.

The applications and data that users create are stored on their own user layer virtual hard drive in a VHD file which is mounted on the image.

This document includes instructions for deploying and configuring the user personalization layer feature. It describes the requirements for successful deployment, limitations, and known issues.

To use the User personalization layer feature, you must first deploy it using the steps detailed in the article. Until then, the feature is not available for you to use.

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 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 (on their user layer), if they attempt to add or edit a local user or group required by the application, the user or group changes do *not* persist.

> **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
- Citrix Provisioning, version 1909 or later
- Windows File Share (SMB)
- Windows 10 Enterprise x64, version 1607 or later

> **Important:**
>
> - If you installed the preview version of the user personalization layer feature, uninstall the software and reboot the master image before installing this release.
> - As described in the steps below, you must define the policies within Studio, and assign those to the specific delivery group bound to a machine catalog where the User personalization layer is deployed. Leaving the master image with no User personalization layer configuration ensures that the services remain idle and cannot interfere with authoring activities. If you set the policies in the master image, User personalization layer services attempt to run and mount a user layer in the master image. Since that environment is for authoring changes to the image, this is not ideal and could cause unexpected behaviors and instability in the master image.

Recommendations

Follow the recommendations in this section for a successful user personalization layer deployment.

Profile Management solution

We recommend using a Profile Management solution, such as Citrix Profile Management, with the user personalization layer feature.

If you are using Profile Management with the user personalization layer feature, turn off the deletion of the user's information on logoff. Depending on how you are deploying the settings, you can turn off deletion either using a Group Policy Object (GPO) or the policy on the Delivery Controller (DDC).

For details about available Profile Management policies, see Profile Management policy descriptions and defaults.

Microsoft System Center Configuration Manager (SCCM)

If you are using SCCM with the user personalization layer feature, follow Microsoft best practices for preparing your image in a VDI environment. Refer to this Microsoft TechNet article for more information.

Maximum user layer size

We recommend at least 10 GB as the user layer size.

> **Note:**
>
> During installation, the value zero (0) results in the default user layer size of 10 GB.

A quota set in Windows can override the maximum user layer size You can override the maximum user layer size set in Studio, by defining a quota for the user layer file share. If a quota is defined, the user layer is configured to be a maximum of the quota size.

To set a hard quota on the user layer size, use either of Microsoft's quota tools:

- File Server Resource Manager (FSRM)
- Quota Manager

The quota must be set on the user layer directory named Users.

> **Note:**
>
> Increasing or decreasing the quota only impacts new user layers. It does not change the maximum size of existing user layers. Those remain unchanged when the quota is updated.

Deploy a User personalization layer

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.

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.

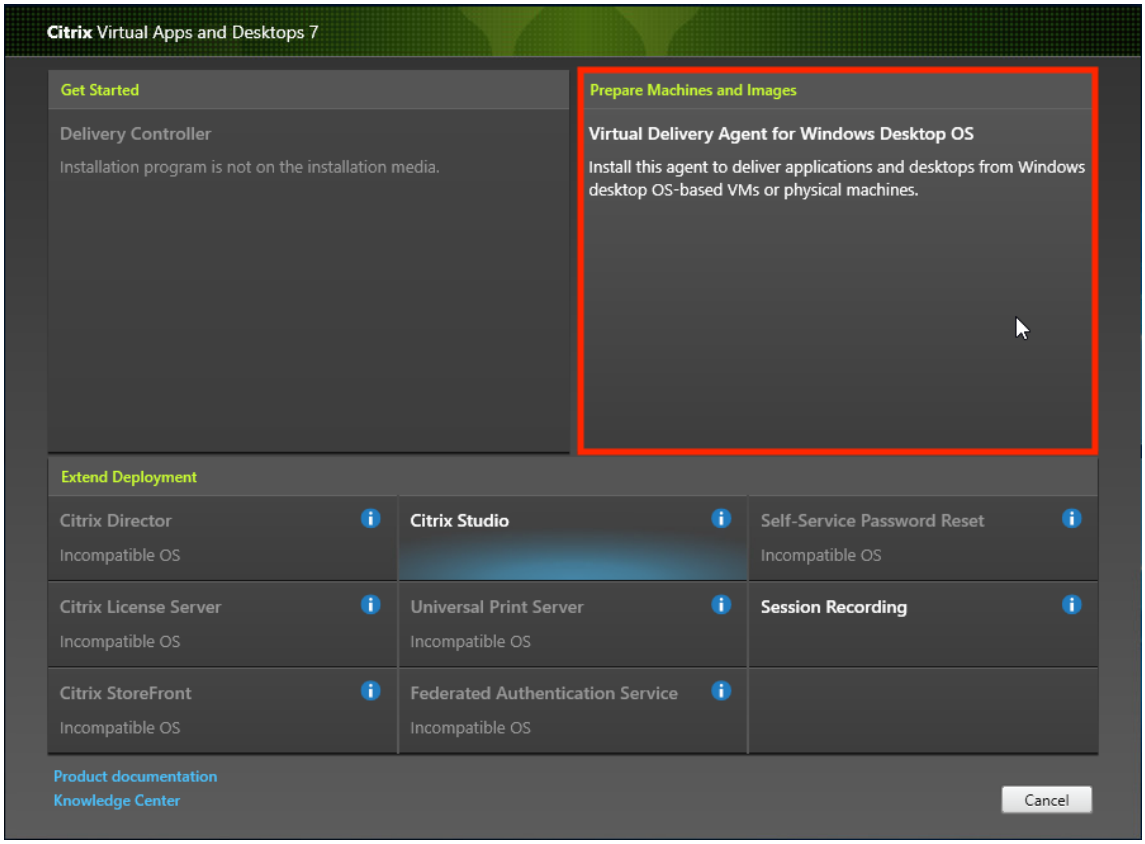
Step 2: Prepare your master image

To prepare your master image:

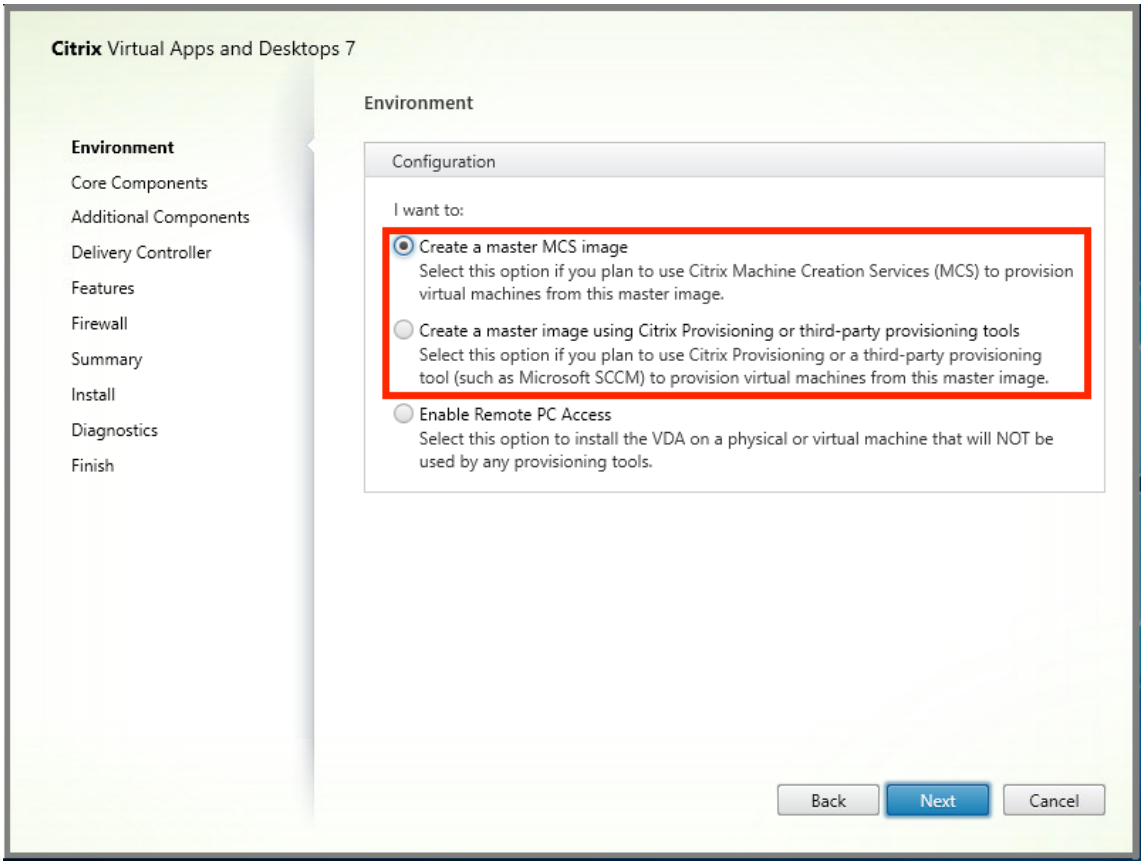
1. Locate the master image. Install your organization's enterprise applications and any other apps your users generally find useful.

2. Install the Virtual Delivery Agent (VDA) 1912. 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, Citrix User Personalization Layer, as follows:

    a) Click the tile, **Virtual Delivery Agent for Windows Desktop OS**:

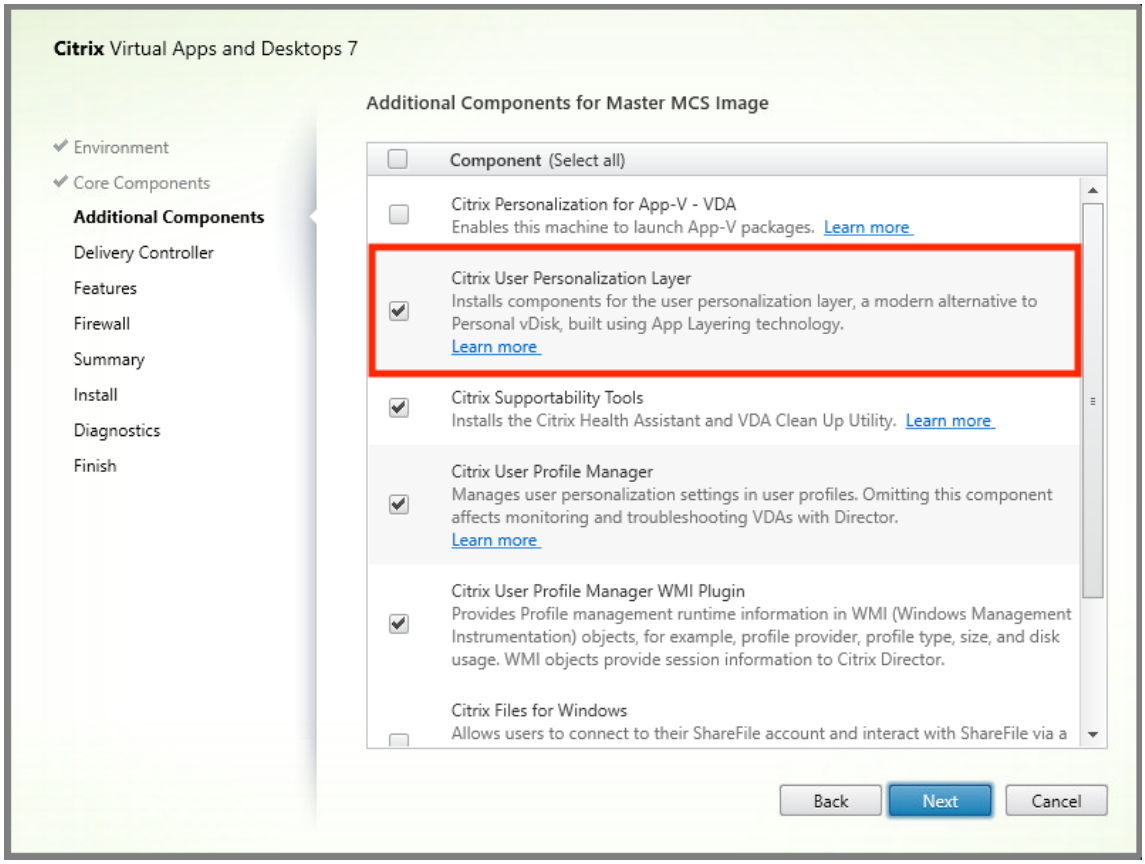


    a) **Environment:** Select either Create a master MCS image or Create a master image using Citrix Provisioning or third-party provisioning tools.



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.

3. Leave **Windows updates** disabled. The user personalization layer installer disables Windows updates on the image. Leave the updates disabled.

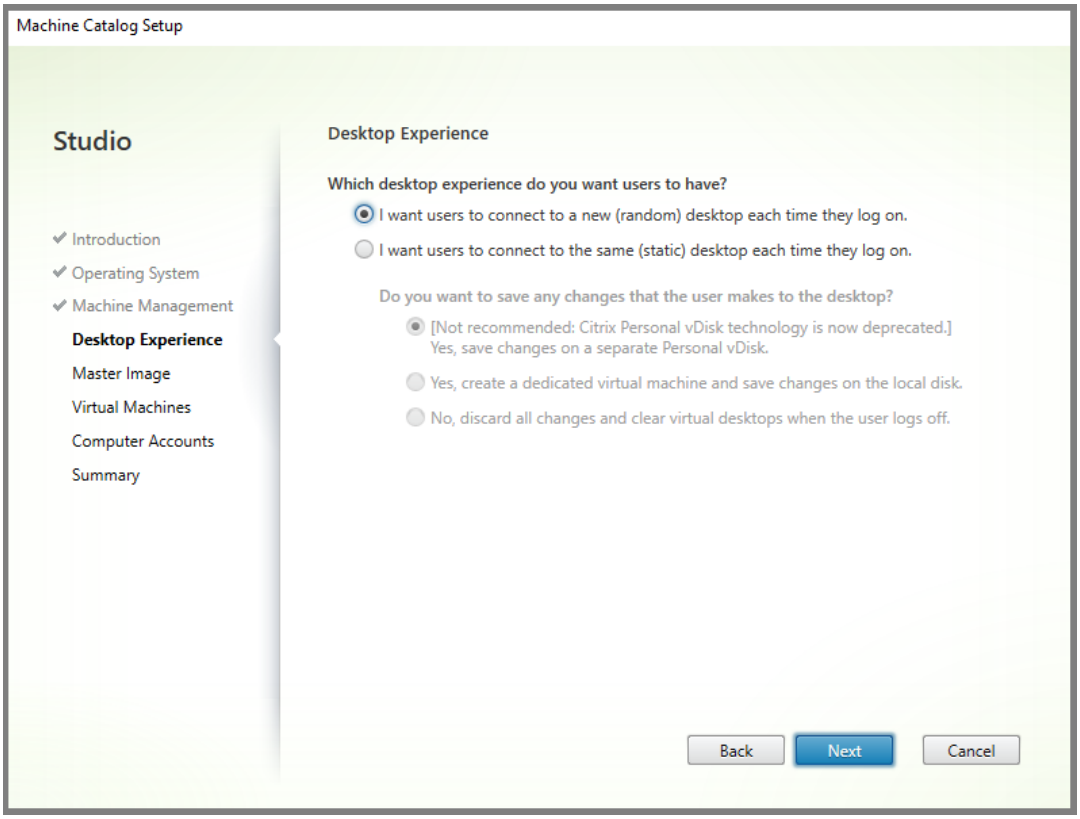
The image is ready for you to upload into Studio.

Step 3: Create a machine catalog

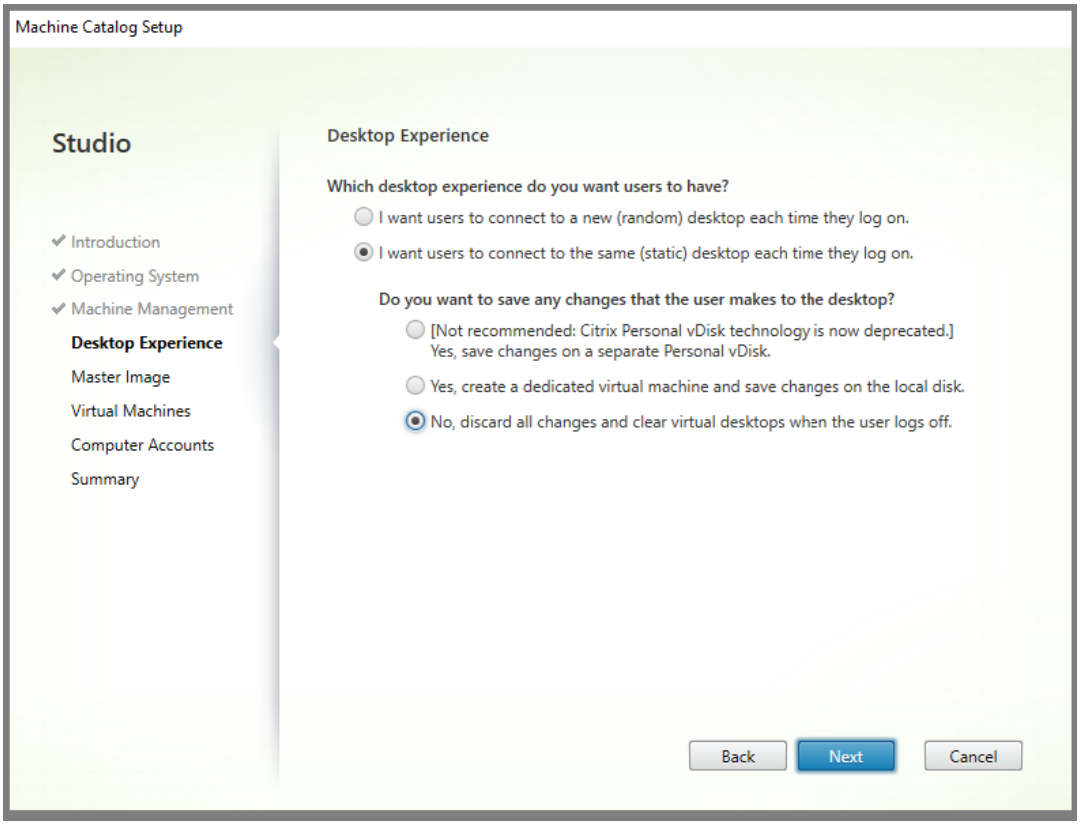
In Studio, follow the steps to create a machine catalog. Use the following options during catalog creation:

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 **Master 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

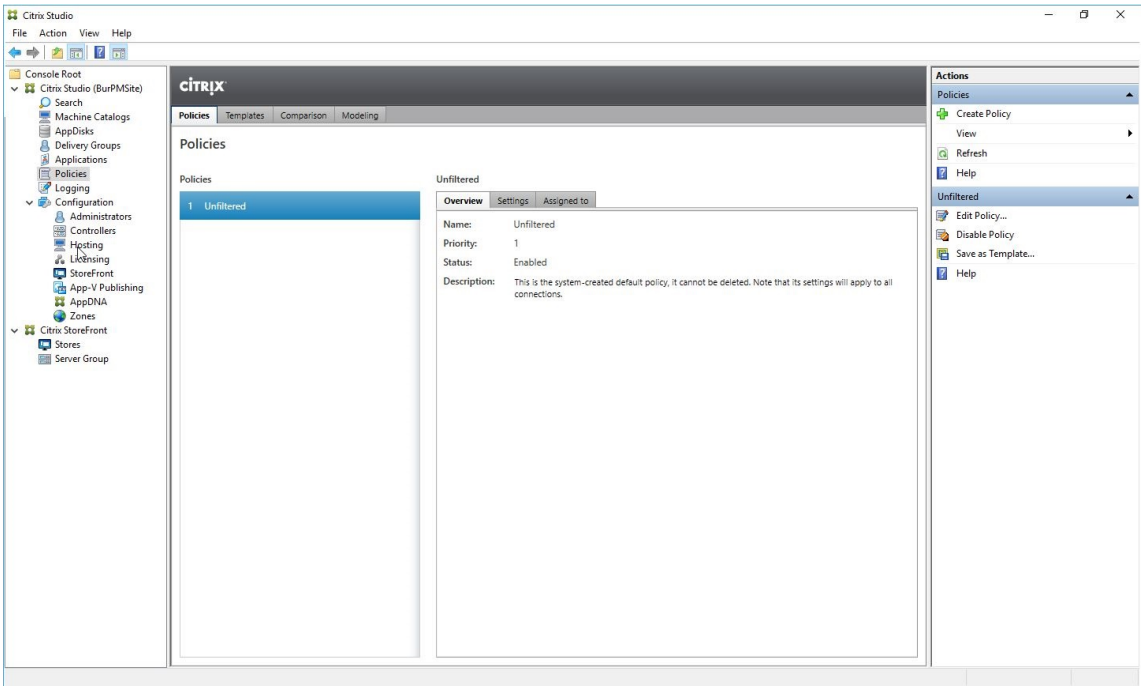
To enable mounting of user layers within the Virtual Delivery Agents, you use configuration parameters to specify:

- Where on the network to access the user layers.

- How large to permit the user layer disks to grow.

The following steps explain how to define the parameters as custom Citrix policies in Studio, and then assign them to your delivery group.

1. In Studio, select Policies in the navigation pane:

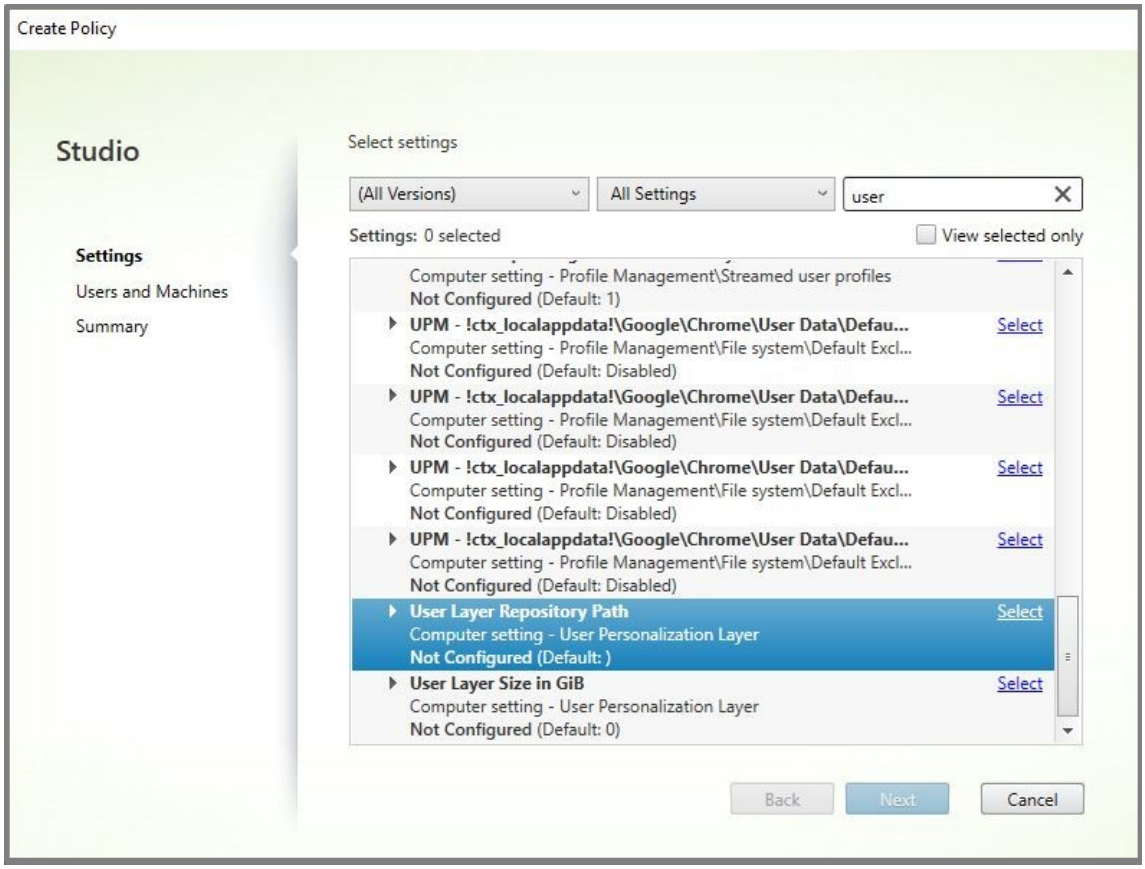


2. Select Create Policy in the Actions pane. The Create Policy window appears.
3. Type ‘user layer’into the search field. The following two policies appear in the list of available policies:

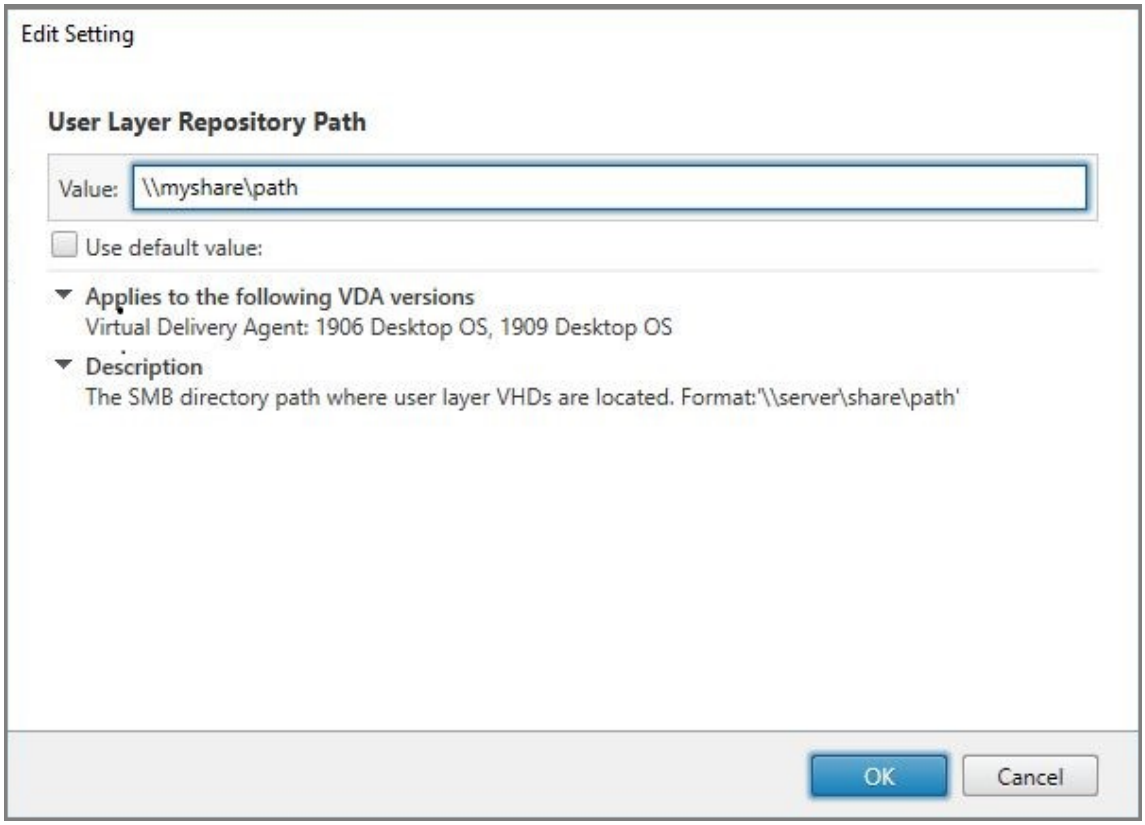
    - User Layer Repository Path
    - User Layer Size GB

    > **Note:**
    >
    > Changing the User Layer Size in the policy does not change the size of existing layers.

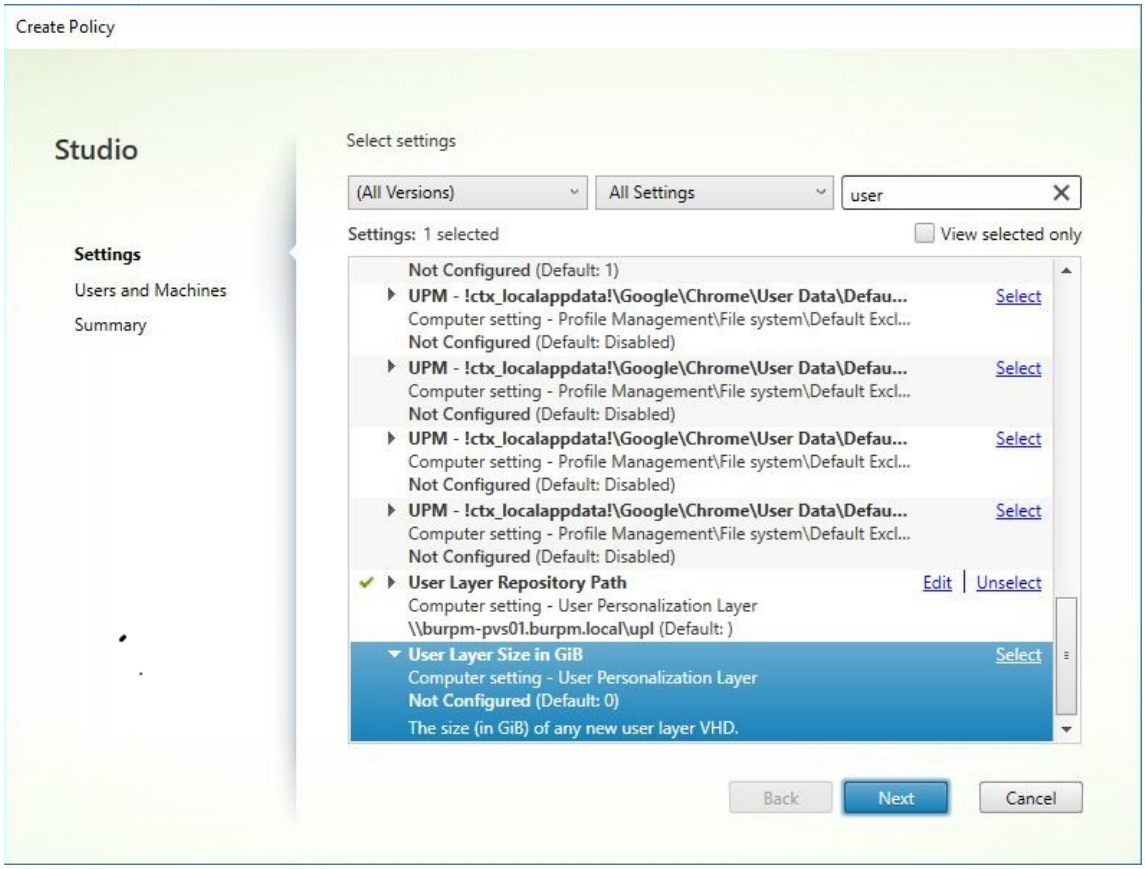
4. Click **Select** next to User Layer Repository Path. The Edit Setting window appears.



5. Enter a path in the format `\\server name or address\folder name` in the Value field, Click **OK**:



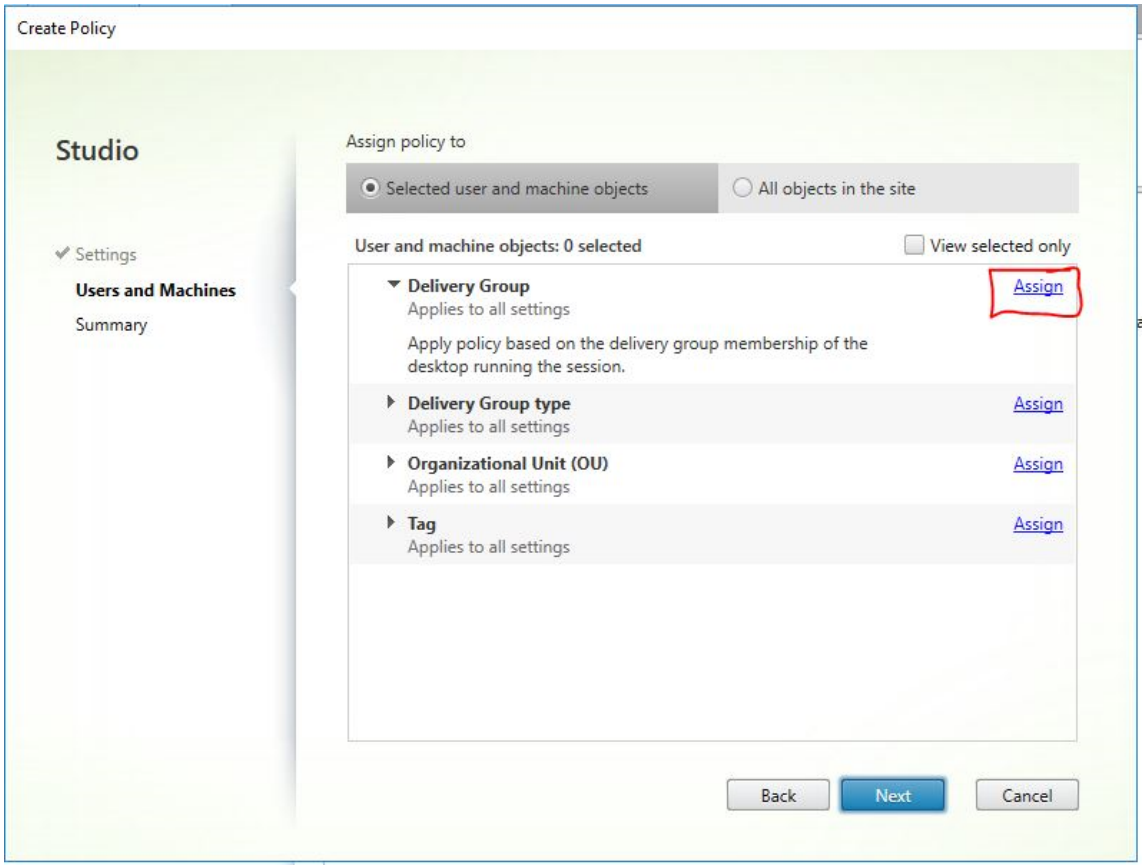
6. Optional: Click **Select** next to User Layer Size in GB:



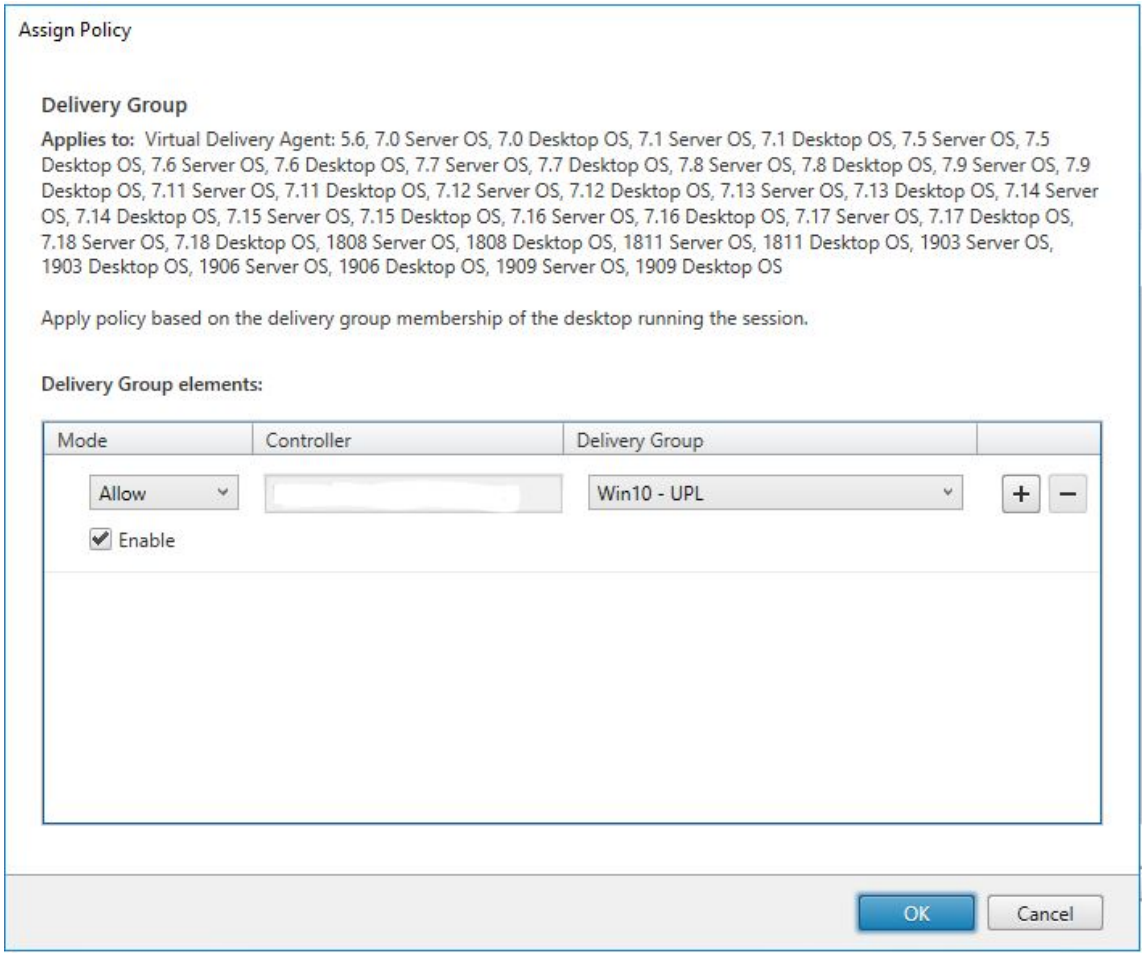
7. The Edit Settings window appears.
8. Optional: Change the default value of '0'to the maximum size (in GB) that the user layer can grow. Click OK.

   > **Note:**
   >
   > If you keep the default value, the maximum user layer size is 10 GB.

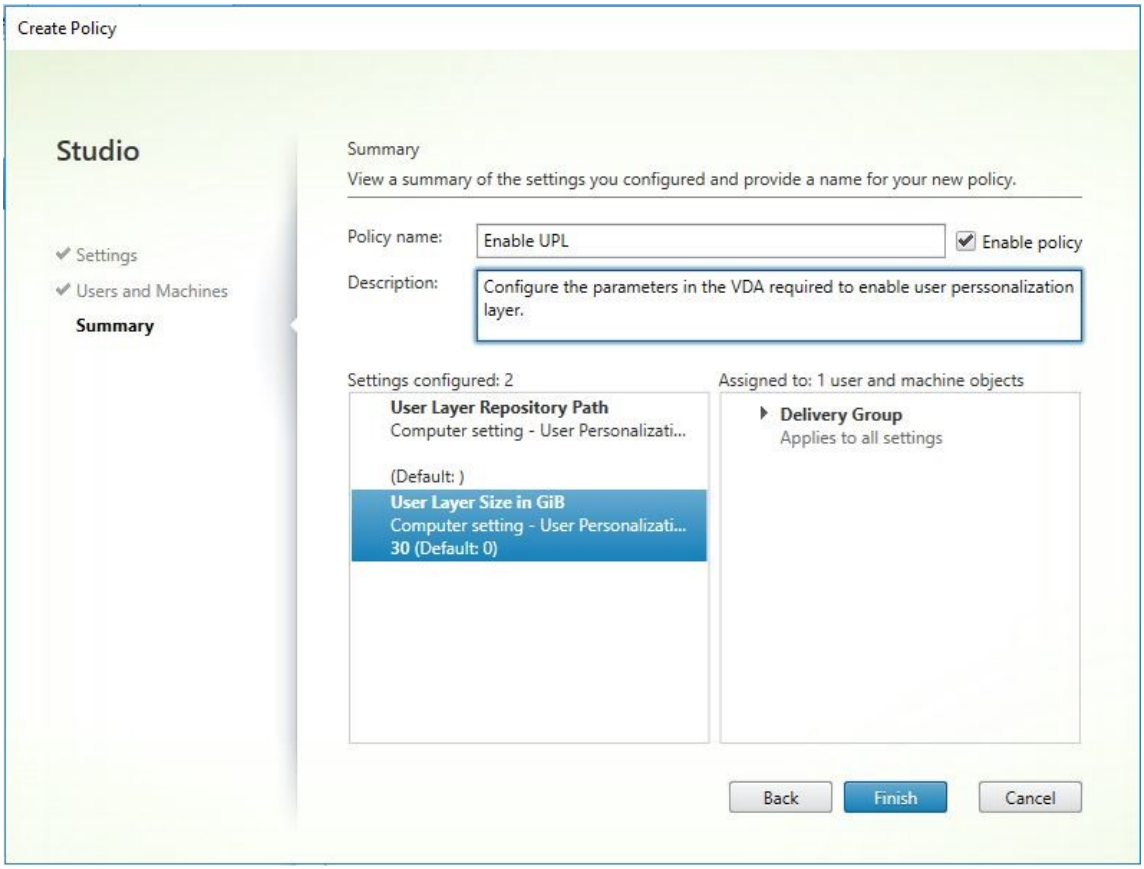
9. Click Next to configure Users and Machines. Click the Delivery Group Assign link highlighted in this image:



10. In the Delivery Group menu, select the delivery group created in the previous section. Click OK.



11. Enter a name for the policy. Click the check box to enable the policy, and click Finish.



Configure security settings on user layer folder

As a domain administrator, you can specify more than one storage location for your user layers. For each storage location (including the default) create a `\Users` subfolder and secure that 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
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.

- *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.

- *System not reset after user sign-out*

  This system was not shut down properly. Please log off immediately and contact your system administrator.

Log files to use when troubleshooting

The log file, ulayersvc.log, contains the output of the user personalization layer software where changes are logged.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
<!--NeedCopy-->
```

Limitations

Keep the following limitations in mind when installing and using the user personalization layer feature.

- 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 user personalization layer.
- Do *not* migrate existing user layers from the full App Layering product to user personalization layer.

- Do *not* change the user layer SMB path to access user layers created using a different master OS image.
- Do *not* enable Secure Boot within User presonalization layer virtual machines, as it is not currently supported.
- Microsoft SCCM Software Center can show an app installed on the user layer as unavailable, even if previously installed. The issue occurs when a user logs out of a session, and then back into a session on another machine in the pool. This behavior is a property of SCCM running in a VDI environment. Software Center only shows applications that the user has installed on the current machine, but the applications are still installed and fully functional.

  To verify that an application is installed, the user can select the application in Software Center and click **Install**. If the application is already installed in their user layer, SCCM updates the status to "Installed"and lists the app with the installed applications.
- 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.
- Group Polices (Computer Configurations): User layer settings override settings applied to the Master Image. Therefore, the changes that are made 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.

Personal vDisk

May 4, 2020

> **Note:**
>
> Personal vDisk is deprecated. The user personalization layer feature handles user persistence.

The personal vDisk feature retains the single image management of pooled and streamed desktops while allowing users to install applications and change their desktop settings. Unlike traditional Virtual Desktop Infrastructure (VDI) deployments involving pooled desktops, where users lose their customization and personal applications when the administrator changes the master image, deployments using personal vDisks retain those changes. This means administrators can easily and centrally manage their master images while providing users with a customized and personalized desktop experience.

Personal vDisks provide this separation by redirecting all changes made on the user's VM to a separate disk (the personal vDisk), which is attached to the user's VM. The content of the personal vDisk is blended at runtime with the content from the master image to provide a unified experience. In this way, users can still access applications provisioned by their administrator in the master image.

Personal vDisks have two parts, which use different drive letters and are by default equally sized:

- User profile - This contains user data, documents, and the user profile. By default this uses drive P: but you can choose a different drive letter when you create a catalog with machines using personal vDisks. The drive used also depends on the EnableUserProfileRedirection setting.
- Virtual Hard Disk (.vhd) file - This contains all other items, for example applications installed in C:\Program Files. This part is not displayed in Windows Explorer and, since Version 5.6.7, does not require a drive letter.

Personal vDisks support the provisioning of department-level applications, as well as applications downloaded and installed by users, including those that require drivers (except phase 1 drivers), databases, and machine management software. If a user's change conflicts with an administrator's change, the personal vDisk provides a simple and automatic way to reconcile the changes.

In addition, locally administered applications (such as those provisioned and managed by local IT departments) can also be provisioned into the user's environment. The user experiences no difference in usability; personal vDisks ensure all changes made and all applications installed are stored on the vDisk. Where an application on a personal vDisk exactly matches one on a master image, the copy on the personal vDisk is discarded to save space without the user losing access to the application.

Physically, you store personal vDisks on the hypervisor but they do not have to be in the same location as other disks attached to the virtual desktop. This can lower the cost of personal vDisk storage.

During Site creation, when you create a connection, you define storage locations for disks that are used by VMs. You can separate the Personal vDisks from the disks used by the operating system. Each VM must have access to a storage location for both disks. If you use local storage for both, they must be accessible from the same hypervisor. To ensure this requirement is met, Studio offers only compatible storage locations. Later, you can also add personal vDisks and storage for them to existing hosts (but not machine catalogs) from Configuration > Hosting in Studio.

Back up personal vDisks regularly using any preferred method. The vDisks are standard volumes in a hypervisor's storage tier, so you can back them up, just like any other volume.

What's new in personal vDisk 7.6.1

The following improvements are included in this release:

- This version of personal vDisk contains performance improvements that reduce the amount of time it takes to apply an image update to a personal vDisk catalog.

The following known issues are fixed in this release:

- Attempting an in-place upgrade of a base virtual machine from Microsoft Office 2010 to Microsoft Office 2013 resulted in the user seeing a reconfiguration window followed by an error message; "Error 25004. The product key you entered cannot be used on this machine."In the past, it was recommended that Office 2010 be uninstalled in the base virtual machine before installing Office 2013. Now, it is no longer necessary to uninstall Office 2010 when performing an in-place upgrade to the base virtual machine (#391225).
- During the image update process, if a higher version of Microsoft .NET exists on the user's personal vDisk, it was overwritten by a lower version from the base image. This caused issues for users running certain applications installed on personal vDisk which required the higher version, such as Visual Studio (#439009).
- A Provisioning Services imaged disk with personal vDisk installed and enabled, cannot be used to create a non-personal vdisk machine catalog. This restriction has been removed (#485189).

About Personal vDisk 7.6

New in version 7.6:

- Improved personal vDisk error handling and reporting. In Studio, when you display PvD-enabled machines in a catalog, a "PvD"tab provides monitoring status during image updates, plus estimated completion time and progress. Enhanced state displays are also provided.
- A personal vDisk Image Update Monitoring Tool for earlier releases is available from the ISO media (ISO\Support\Tools\Scripts\PvdTool). Monitoring capabilities are supported for previous releases, however the reporting capabilities will not be as robust compared to the current release.
- Provisioning Services test mode allows you to boot machines with an updated image in a test catalog. After you verify its stability, you can promote the test version of the personal vDisk to production.
- A new feature enables you to calculate the delta between two inventories during an inventory, instead of calculating it for each PvD desktop. New commands are provided to export and import a previous inventory for MCS catalogs. (Provisioning Services master vDisks already have the previous inventory.)

Known issues from 7.1.3 fixed in version 7.6:

- Interrupting a personal vDisk installation upgrade can result in corrupting an existing personal vDisk installation. [#424878]
- A virtual desktop may become unresponsive if the personal vDisk runs for an extended period of time and a non-page memory leak occurs. [#473170]

New known issues in version 7.6:

- The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the PROCESS exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. [#326735]
- Hard links between files inherited from the master image are not preserved in personal vDisk catalogs. [#368678]
- After upgrading from Office 2010 to 2013 on the Personal vDisk master image, Office might fail to launch on virtual machines because the Office KMS licensing product key was removed during the upgrade. As a workaround, uninstall Office 2010 and reinstall Office 2013 on the master image. [#391225]
- Personal vDisk catalogs do not support VMware Paravirtual SCSI (PVSCSI) controllers. To prevent this issue, use the default controller. [#394039]
- For virtual desktops that were created with Personal vDisk version 5.6.0 and are upgraded to 7, users who logged on to the master virtual machine (VM) previously might not find all their files in their pooled VM. This issue occurs because a new user profile is created when they log on to their pooled VM. There is no workaround for this issue. [#392459]
- Personal vDisks running Windows 7 cannot use the Backup and Restore feature when the Windows system protection feature is enabled. If system protection is disabled, the user profile is backed up, but the userdata.v2.vhd file is not. Citrix recommends disabling system protection and using Backup and Restore to back up the user profile. [#360582]
- When you create a VHD file on the base VM using the Disk Management tool, you might be unable to mount the VHD. As a workaround, copy the VHD to the PvD volume. [#355576]
- Office 2010 shortcuts remain on virtual desktops after this software is removed. To work around this issue, delete the shortcuts. [#402889]
- When using Microsoft Hyper-V, you cannot create a catalog of machines with personal vDisks when the machines are stored locally and the vDisks are stored on Cluster Shared Volumes (CSVs); catalog creation fails with an error. To work around this issue, use an alternative storage setup for the vDisks. [#423969]
- When you log on for the first time to a virtual desktop that is created from a Provisioning Services catalog, the desktop prompts for a restart if the personal vDisk has been reset (using the command ctxpvd.exe -s reset). To work around this issue, restart the desktop as prompted. This is a once-only reset that is not required when you log on again. [#340186]
- If you install .NET 4.5 on a personal vDisk and a later image update installs or modifies .NET 4.0, applications that are dependent on .NET 4.5 fail. To work around this issue, distribute .NET 4.5

from the base image as an image update."
- See also the Known Issues documentation for the XenApp and XenDesktop 7.6 release.

About Personal vDisk 7.1.3

Known issues from 7.1.1 fixed in version 7.1.3:

- Direct upgrades from personal vDisk 5.6.0 to personal vDisk 7.x may cause the personal vDisk to fail. [#432992]
- Users might only be able to connect intermittently to virtual desktops with personal vDisks. [#437203]
- If a personal vDisk image update operation is interrupted while personal vDisk 5.6.5 or later is upgraded to personal vDisk 7.0 or later, subsequent update operations can fail. [#436145]

About Personal vDisk 7.1.1

Known issues from 7.1 fixed in version 7.1.1:

- Upgrading to Symantec Endpoint Protection 12.1.3 through an image update causes symhelp.exe to report corrupt antivirus definitions. [#423429]
- Personal vDisk can cause pooled desktops to restart if Service Control Manager (services.exe) crashes. [#0365351]

New known issues in version 7.1.1: none

About Personal vDisk 7.1

New in version 7.1:

- You can now use Personal vDisk with desktops running Windows 8.1, and event logging has been improved.
- Copy-on-Write (CoW) is no longer supported. When upgrading from Version 7.0 to 7.1 of Personal vDisk, all changes to data managed by CoW are lost. This was a feature for evaluation in XenDesktop 7 and was disabled by default, so if you did not enable it, you are not affected.

Known issues from 7.0.1 fixed in version 7.1:

- If the value of the Personal vDisk registry key EnableProfileRedirection is set to 1 or ON, and later, while updating the image, you change it to 0 or OFF, the entire Personal vDisk space might get allocated to user-installed applications, leaving no space for user profiles, which remain on the vDisk. If this profile redirection is disabled for a catalog and you enable it during an image update, users might not be able to log on to their virtual desktop. [#381921]

- The Desktop Service does not log the correct error in the Event Viewer when a Personal vDisk inventory update fails. [#383331]
- When upgrading to Personal vDisk 7.x, modified rules are not preserved. This issue has been fixed for upgrades from Version 7.0 to Version 7.1. When upgrading from Version 5.6.5 to Version 7.1, you must first save the rule file and then apply the rules again after the upgrade. [#388664]
- Personal vDisks running Windows 8 cannot install applications from the Windows Store. An error message stating, "Your purchase couldn't be completed," appears. Enabling the Windows Update Service does not resolve this issue, which has now been fixed. However, user-installed applications must be reinstalled after the system restarts. [#361513]
- Some symbolic links are missing in Windows 7 pooled desktops with personal vDisks. As a result, applications that store icons in C:\Users\All Users do not display these icons in the Start menu. [#418710]
- A personal vDisk does not start if an Update Sequence Number (USN) journal overflow occurs due to a large number of changes made to the system after an inventory update. [#369846]
- A personal vDisk does not start with status code 0x20 and error code 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 displays the message "Proactive Threat Protection is malfunctioning" and this component's Live Update Status is not available. [#390204]

New known issues in version 7.1: See the Known Issues documentation for the XenDesktop 7.1 release.

About Personal vDisk 7.0.1

New in version 7.0.1: Personal vDisk is now more robust to environment changes. Virtual desktops with personal vDisks now register with the Delivery Controller even if image updates fail, and unsafe system shutdowns no longer put the vDisks into a permanently disabled state. In addition, using rules files you can now exclude files and folders from the vDisks during a deployment.

Known issues from 5.6.13 fixed in version 7.0.1:

- Changes to a group's membership made by users on a pooled virtual desktop might be lost after an image update. [#286227]
- Image updates might fail with a low disk space error even if the personal vDisk has enough space. [#325125]
- Some applications fail to install on virtual desktops with a personal vDisk, and a message is displayed that a restart is required. This is due to a pending rename operation. [#351520]
- Symbolic links created inside the master image do not work on virtual desktops with personal vDisks. [#352585]
- In environments that use Citrix Profile management and personal vDisk, applications that examine user profiles on a system volume might not function properly if profile redirection is enabled. [#353661]

- The inventory update process fails on master images when the inventory is bigger than 2GB. [#359768]
- Image updates fail with error code 112 and personal vDisks are corrupted even if the vDisks have enough free space for the update. [#363003]
- The resizing script fails for catalogs with more than 250 desktops. [#363365]
- Changes made by users to an environment variable are lost when an image update is performed. [#372295]
- Local users created on a virtual desktop with a personal vDisk are lost when an image update is performed. [#377964]
- A personal vDisk may fail to start if an Update Sequence Number (USN) journal overflow occurred due to a large number of changes made to the system after an inventory update. To avoid this, increase the USN journal size to a minimum of 32 MB in the master image and perform an image update. [#369846]
- An issue has been identified with Personal vDisk that prevents the correct functioning of AppSense Environment Manager registry hiving actions when AppSense is used in Replace Mode. Citrix and AppSense are working together to resolve the issue, which is related to the behavior of the RegRestoreKey API when Personal vDisk is installed.[#0353936]

Release-independent known issues

- If Windows Store and Metro Apps are updated on the master image, it may cause conflicts for PvD enabled target devices after the vDisk is upgraded to test or production. In addition, Metro Apps may fail to launch while triggering application event log errors. Citrix recommends that you disable Windows Store and Metro Apps for PvD enabled target devices.
- When an application installed on a personal vDisk (PvD) is related to another application of the same version that is installed on the master image, the application on the PvD could stop working after an image update. This occurs if you uninstall the application from the master image or upgrade it to a later version, because that action removes the files needed by the application on the PvD from the master image. To prevent this, keep the application containing the files needed by the application on the PvD on the master image.

  For example, the master image contains Office 2007, and a user installs Visio 2007 on the PvD; the Office applications and Visio work correctly. Later, the administrator replaces Office 2007 with Office 2010 on the master image, and then updates all affected machines with the updated image. Visio 2007 no longer works. To avoid this, keep Office 2007 in the master image. [#320915]
- When deploying McAfee Virus Scan Enterprise (VSE), use version 8.8 Patch 4 or later on a master image if you use personal vDisk. [#303472]

- If a shortcut created to a file in the master image stops working (because the shortcut target is renamed within PvD), recreate the shortcut. [#367602]
- Do not use absolute/hard links in a master image. [#368678]
- The Windows 7 backup and restore feature is not supported on the personal vDisk. [#360582]
- After an updated master image is applied, the local user and group console becomes inaccessible or shows inconsistent data. To resolve the issue, reset the user accounts on the VM, which requires resetting the security hive. This issue was fixed in the 7.1.2 release (and works for VMs created in later releases), but the fix does not work for VMs that were created with an earlier version and then upgraded. [#488044]
- When using a pooled VM in an ESX hypervisor environment, users see a restart prompt if the selected SCSI controller type is "VMware Paravirtual."For a workaround, use an LSI SCSI controller type. [#394039]
- After a PvD reset on a desktop created through Provisioning Services, users may receive a restart prompt after logging on to the VM. As a workaround, restart the desktop. [#340186]
- Windows 8.1 desktop users might be unable to log on to their PvD. An administrator might see message "PvD was disabled due to unsafe shutdown"and the PvDActivation log might contain the message "Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]." This occurs when a user's VM shuts down unsafely. As a workaround, reset the personal vDisk. [#474071]

Install and upgrade

March 7, 2022

Personal vDisk 7.x is supported on the current Citrix Virtual Apps and Desktops version (and earlier versions, beginning with XenDesktop 5.6). The "System requirements"documentation for each version lists the supported operating systems for Virtual Delivery Agents (VDAs), and the supported versions of hosts (virtualization resources), and Citrix Provisioning (formerly Provisioning Services). For details about Citrix Provisioning tasks, see its current documentation.

Install and enable PvD

You can install and then enable PvD components when you install or upgrade a VDA for Desktop OS on a machine. These actions are selected on the **Additional Components** and **Features** pages of the installation wizard, respectively. For more information, see Install VDAs.

If you update the PvD software after installing the VDA, use the PvD MSI provided on the Citrix Virtual Apps and Desktops installation media.

Enabling PvD:

- If you are using Machine Creation Services (MCS), PvD is enabled automatically when you create a machine catalog of desktop OS machines that will use a personal vDisk.
- If you are using Citrix Provisioning, PvD is enabled automatically when you run the inventory during the master (base) image creation process, or when auto-update runs the inventory for you.

Therefore, if you install the PvD components but do not enable them during VDA installation, you can use the same image to create both PvD desktops and non-PvD desktops, because PvD is enabled during the catalog creation process.

Add personal vDisks

You add personal vDisks to hosts when you configure a Site. You can choose to use the same storage on the host for VMs and personal vDisks, or you can use different storage for personal vDisks.

Later, you can also add personal vDisks and their storage to existing hosts (connections), but not machine catalogs.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select Add Personal vDisk storage in the Actions pane, and specify the storage location.

Upgrade PvD

The easiest way to upgrade personal vDisk from an earlier 7.x version is to simply upgrade your desktop OS VDAs to the version provided with the most recent Citrix Virtual Desktops version. Then, run the PvD inventory.

Uninstall PvD

You can use one of two ways to remove the PvD software:

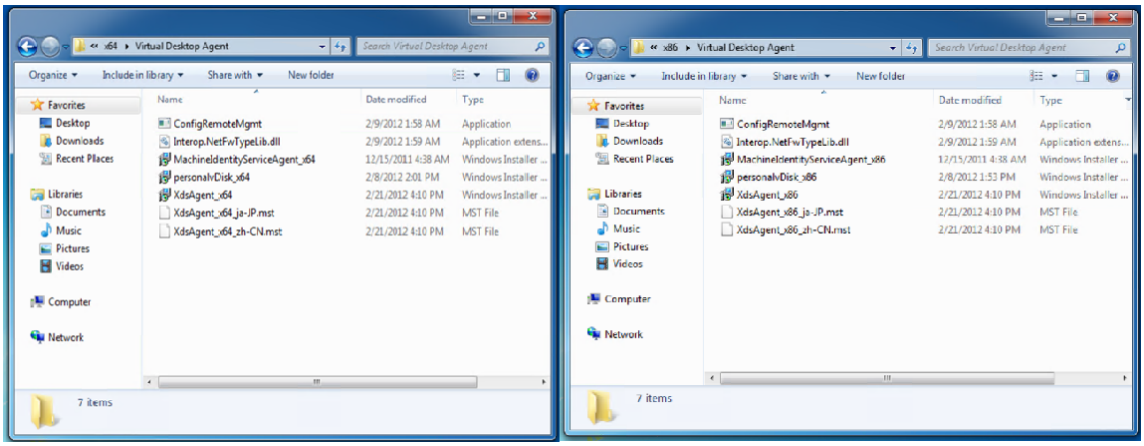
- Uninstall the VDA. This removes the PvD software as well.
- If you updated PvD using the PvD MSI, then you can uninstall it from the Programs list.

If you uninstall PvD and then want to reinstall the same or a newer version, first back up the registry key HKLM\Software\Citrix\personal vDisk\config, which contains environment configuration settings that might have changed. Then, after installing PvD, reset the registry values that might have changed, by comparing them with the backed-up version.

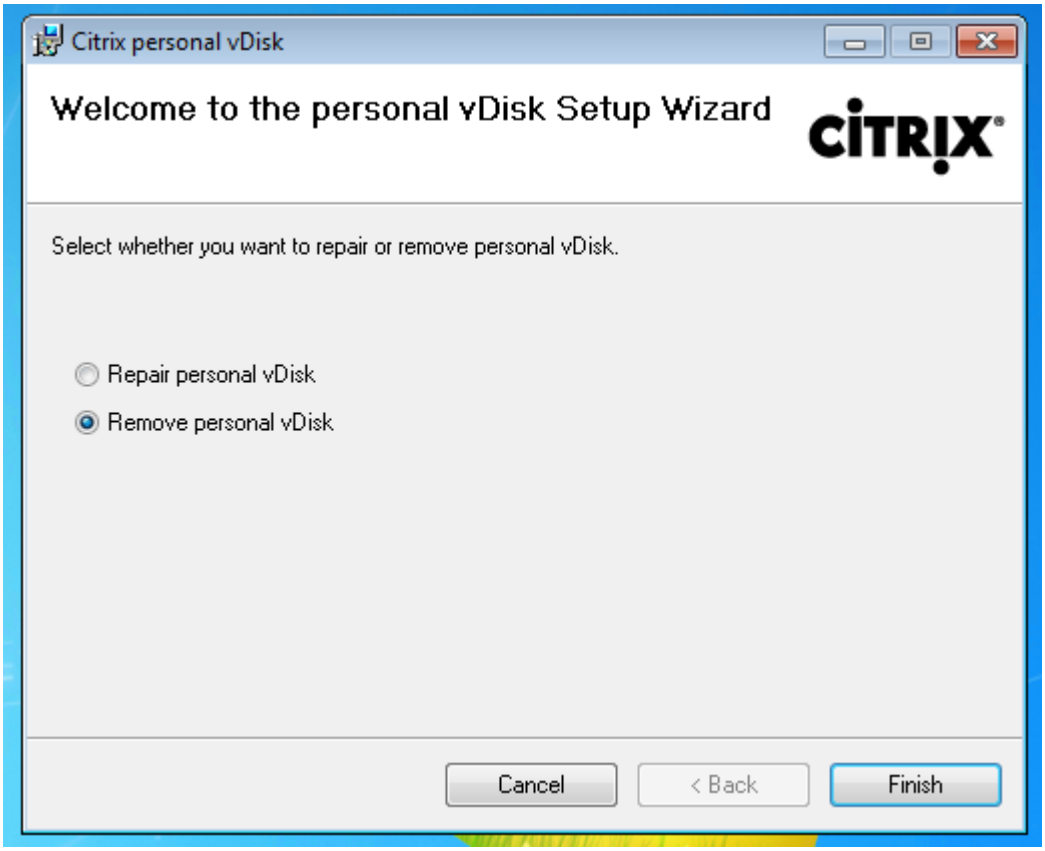
Uninstalling may fail when a personal vDisk with Windows 7 (64 bit) is installed in the base image. To resolve this issue, Citrix recommends that you remove the personal vDisk before upgrading.

1. Select the appropriate copy of the vDisk installer from the Citrix Virtual Apps and Desktops media. Locate the latest personal vDisk MSI installer in one of the following directories (depending on whether the upgraded VM is 32 or 64-bits):

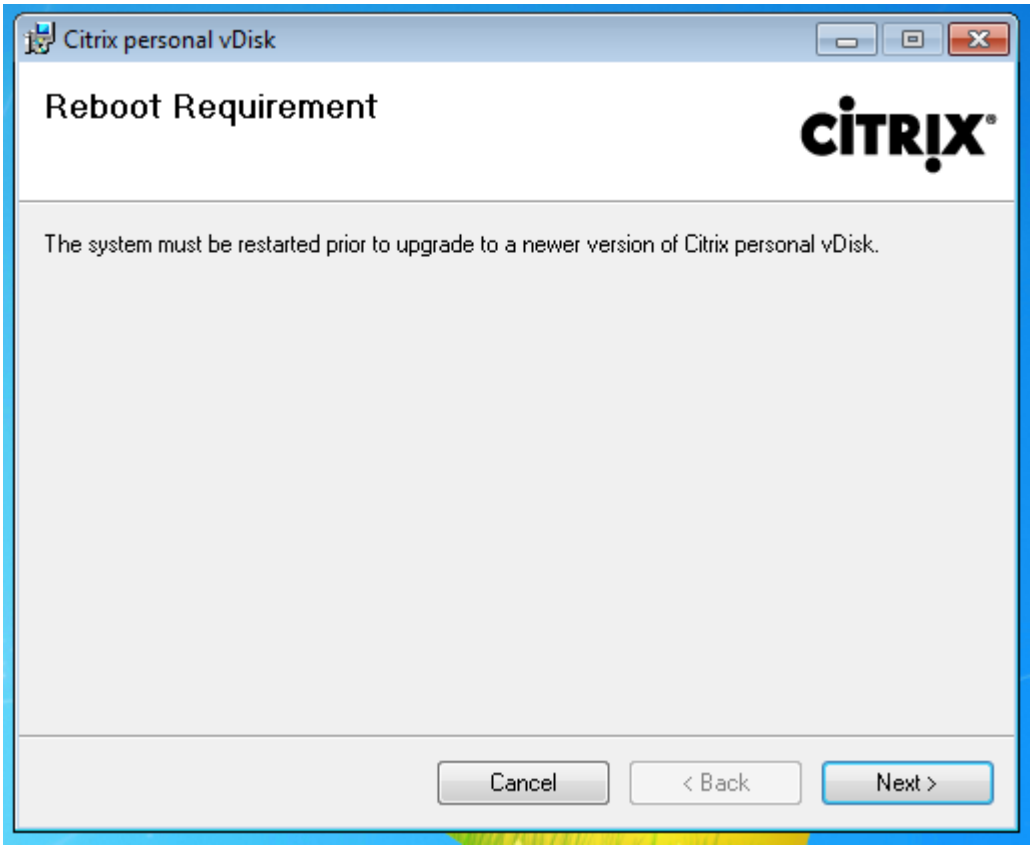
    - 32-bit: XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
    - 64-bit: XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



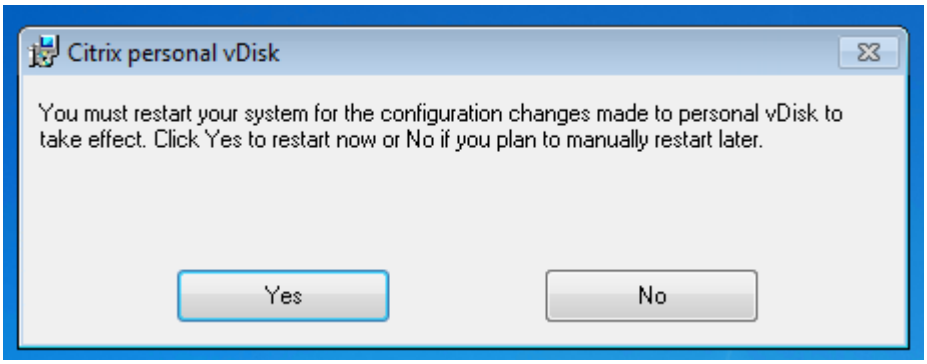
2. Remove the personal vDisk installation. Select the personal vDisk MSI installer package found in step 1. The personal vDisk setup screen appears.
3. Select **Remove personal vDisk**.
4. Click **Finish**.



5. The Reboot Requirement page appears. Click **Next**:



6. Click **Yes** to restart the system and to apply your configuration changes:



Configure and manage

November 10, 2020

This topic covers items you should consider when configuring and managing a personal vDisk (PvD) environment. It also covers best practice guidelines and task descriptions.

For procedures that include working in the Windows registry:

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.

Considerations: personal vDisk size

The following factors affect the size of the main personal vDisk volume:

- **Size of the applications that users will install on their PvDs**

  At restarts, PvD determines the free space remaining in the application area (UserData.v2.vhd). If this falls below 10%, the application area is expanded into any unused profile area space (by default, the space available on the P: drive). The space added to the application area is approximately 50% of the combined free space remaining in both the application area and the profile area.

  For example, if the application area on a 10 GB PvD (which by default is 5 GB) reaches 4.7 GB and the profile area has 3 GB free, the increased space that is added to the application area is calculated as follows:

  increased space = (5.0-4.7)/2 + 3.0/2 = 1.65 GB

  The space added to the application area is only approximate because a small allowance is made for storing logs and for overhead. The calculation and the possible resizing is performed on each restart.

- **Size of users' profiles (if a separate profile management solution is not used)**

  In addition to the space required for applications, ensure there is sufficient space available on personal vDisks to store users' profiles. Include any non-redirected special folders (such as My Documents and My Music) when calculating space requirements. Existing profile sizes are available from the Control Panel (sysdm.cpl).

  Some profile redirection solutions store stub files (sentinel files) instead of real profile data. These profile solutions might appear to store no data initially but actually consume one file directory entry in the file system per stub file; generally, approximately 4 KB per file. If you use such a solution, estimate the size based on the real profile data, not the stub files.

  Enterprise file sharing applications (such as ShareFile and Dropbox) might synchronize or download data to users' profile areas on the personal vDisks. If you use such applications, include enough space in your sizing estimates for this data.

- **Overhead consumed by the template VHD containing the PvD inventory**

  The template VHD contains the PvD inventory data (sentinel files corresponding to the master image content). The PvD application area is created from this VHD. Because each sentinel file

or folder comprises a file directory entry in the file system, the template VHD content consumes PvD application space even before any applications are installed by the end user. You can determine the template VHD size by browsing the master image after an inventory is taken. Alternatively, use the following equation for an approximately calculation:

template VHD size = (number of files on base image) x 4 KB

Determine the number of files and folders by right-clicking the C: drive on the base VM image and selecting Properties. For example, an image with 250,000 files results in a template VHD of approximately 1,024,000,000 bytes (just under 1 GB). This space will be unavailable for application installations in the PvD application area.

- **Overhead for PvD image update operations**

  During PvD image update operations, enough space must be available at the root of the PvD (by default, P:) to merge the changes from the two image versions and the changes the user has made to their PvD. Typically, PVD reserves a few hundred megabytes for this purpose, but extra data that was written to the P: drive might consume this reserved space, leaving insufficient space for the image update to complete successfully. The PvD pool statistics script (located on the Citrix Virtual Apps and Desktops installation media in the Support/Tools/Scripts folder) or the PvD Image Update Monitoring Tool (in the Support/Tools/Scripts\PvdTool folder) can help identify any PvD disks in a catalog that are undergoing an update and that are nearly full.

  The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. Excluding these executables from scanning by the antivirus software can improve inventory and image update performance by up to a factor of ten.

- **Overhead for unexpected growth (unexpected application installations, and so on)**

  Consider allowing extra (either a fixed amount or a percentage of the vDisk size) to the total size to accommodate unexpected application installations that the user performs during deployment.

How-to: Configure the personal vDisk size and allocation

You can manually adjust the automatic resizing algorithm that determines the size of the VHD relative to the P: drive, by setting the initial size of the VHD. This can be useful if, for example, you know users will install a number of applications that are too big to fit on the VHD even after it is resized by the algorithm. In this case, you can increase the initial size of the application space to accommodate the user-installed applications.

Preferably, adjust the initial size of the VHD on a master image. Alternatively, you can adjust the size of the VHD on a virtual desktop when a user does not have sufficient space to install an application.

However, you must repeat that operation on each affected virtual desktop; you cannot adjust the VHD initial size in a catalog that is already created.

Ensure the VHD is big enough to store antivirus definition files, which are typically large.

Locate and set the following registry keys in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (Do not modify other settings in this registry key.) All settings must be specified on the master image (except for MinimumVHDSizeInMB, which can be changed on an individual machine); settings specified on the master image are applied during the next image update.

- **MinimumVHDSizeMB**

  Specifies the minimum size (in megabytes) of the application part (C:) of the personal vDisk. The new size must be greater than the existing size but less than the size of the disk minus PvDReservedSpaceMB.

  Increasing this value allocates free space from the profile part on the vDisk to C:. This setting is ignored if a lower value than the current size of the C: drive is used, or if EnableDynamicResizeOfAppContainer is set to 0.

  Default = 2048

- **EnableDynamicResizeOfAppContainer**

  Enables or disables the dynamic resizing algorithm.

  - When set to 1, the application space (on C:) is resized automatically when the free space on C: falls below 10%. Allowed values are 1 and 0. A restart is required to effect the resize.
  - When set to 0, the VHD size is determined according to the method used in XenDesktop versions earlier than 7.x.

  Default = 1

- **EnableUserProfileRedirection**

  Enables or disables redirecting the user's profile to the vDisk.

  - When set to 1, PvD redirects users' profiles to the personal vDisk drive (P: by default). Profiles are generally redirected to P:\Users, corresponding to a standard Windows profile. This redirection preserves the profiles in case the PvD desktop must be reset.
  - When set to 0, all of the space on the vDisk minus PvDReservedSpaceMB is allocated to C:, the application part of the vDisk, and the vDisk drive (P:) is hidden in Windows Explorer. Citrix recommends disabling redirection by setting the value to 0, when using Citrix Profile management or another roaming profile solution.

    This setting retains the profiles in C:\Users instead of redirecting them to the vDisk, and lets the roaming profile solution handle the profiles.

This value ensures that all of the space on P: is allocated to applications.

It is assumed that if this value is set to 0, a profile management solution is in place. Disabling profile redirection without a roaming profile solution in place is not recommended because subsequent PvD reset operations result in the profiles being deleted.

Do not change this setting when the image is updated because it does not change the location of existing profiles, but it will allocate all the space on the Personal vDisk to C: and hide the PvD.

Configure this value before deploying a catalog. You cannot change it after the catalog is deployed.

Important: Beginning with XenDesktop 7.1, changes to this value are not honored when you perform an image update. Set the key's value when you first create the catalogs from which the profiles will originate. You cannot modify the redirection behavior later.

Default = 1

- **PercentOfPvDForApps**

  Sets the split between the application part (C:) and the profile part of the vDisk. This value is used when creating new VMs, and during image updates when EnableDynamicResizeOfAppContainer is set to 0.

  Changing PercentOfPvDForApps makes a difference only when EnableDynamicResizeOfAppContainer is set to 0. By default, EnableDynamicResizeOfAppContainer is set to 1 (enabled), which means is that the AppContainer (which you see as the C drive) only expands when it is close to being full (that is, dynamic) - when less than 10% free space remains.

  Increasing PercentOfPvDForApps only increases the maximum space for which the Apps portion is allowed to expand. It does not provision that space for you immediately. You must also configure the split allocation in the master image, where it will be applied during the next image update.

  If you have already generated a catalog of machines with EnableDynamicResizeOfAppContainer set to 1, then change that setting to 0 in the master image for the next update, and configure an appropriate allocation split. The requested split size will be honored as long as it is larger than the current allocated size for the C drive.

  If you want to maintain complete control over the space split, set this value to 0. This allows full control over the C drive size, and does not rely on a user consuming space below the threshold to expand the drive.

  Default = 50% (allocates equal space to both parts)

- **PvDReservedSpaceMB**

  Specifies the size of the reserved space (in megabytes) on the vDisk for storing Personal vDisk logs and other data.

If your deployment includes XenApp 6.5 (or an earlier version) and uses application streaming, increase this value by the size of the Rade Cache.

Default = 512

- **PvDResetUserGroup**

  Valid only for XenDesktop 5.6 - Allows the specified group of users to reset a Personal vDisk. Later versions use Delegated Administration for this.

Other settings:

- **Windows Update Service:** Ensure that you configure Windows to 'Never Check for Updates' and that the Windows update service is set to 'Disabled'in the master image. In addition, Citrix recommends that you disable Windows Store and Metro App updates and features.
- **Windows updates:** These include Internet Explorer updates and must be applied on the master image.
- **Updates requiring restarts:** Windows updates applied to the master image might require multiple restarts to fully install, depending on the type of patches delivered in those updates. Ensure you restart the master image properly to fully complete the installation of any Windows updates applied to it before taking the PvD inventory.
- **Application updates:** Update applications installed on the master image to conserve space on users'vDisks. This also avoids the duplicate effort of updating the applications on each user's vDisk.

Considerations: Applications on the master image

Some software might conflict with the way that PvD composites the user's environment, so you must install it on the master image (rather than on the individual machine) to avoid these conflicts. In addition, although some other software might not conflict with the operation of PvD, Citrix recommends installing it on the master image.

Applications that must be installed on the master image:

- Agents and clients (for example, System Center Configuration Manager Agent, App-V client, Citrix Workspace app)
- Applications that install or modify early-boot drivers
- Applications that install printer or scanner software or drivers
- Applications that modify the Windows network stack
- VM tools such as VMware Tools and XenServer Tools

Applications that should be installed on the master image:

- Applications that are distributed to a large number of users. In each case, turn off application updates before deployment:

  - Enterprise applications using volume licensing, such as Microsoft Office, Microsoft SQL Server
  - Common applications, such as Adobe Reader, Firefox, and Chrome
- Large applications such as SQL Server, Visual Studio, and application frameworks such as .NET

The following recommendations and restrictions apply to applications installed by users on machines with personal vDisks. Some of these cannot be enforced if users have administrative privileges:

- Users should not uninstall an application from the master image and reinstall the same application on their personal vDisk.
- Take care when updating or uninstalling applications on the master image. After you install a version of an application on the image, a user might install an add-on application (for example, a plug-in) that requires this version. If such a dependency exists, updating or uninstalling the application on the image might make the add-on malfunction. For example, with Microsoft Office 2010 installed on a master image, a user installs Visio 2010 on their personal vDisk. A later upgrade of Office on the master image might make the locally-installed Visio unusable.
- Software with hardware-dependent licenses (either through a dongle or signature-based hardware) is unsupported.

Considerations: Citrix Provisioning

When using Citrix Provisioning with PvD:

- The Soap Service account must be added to the Administrator node of Studio and must have the Machine Administrator or higher role. This ensures that the PvD desktops are put into the Preparing state when the Citrix Provisioning vDisk is promoted to production.
- The Citrix Provisioning versioning feature must be used to update the personal vDisk. When the version is promoted to production, the Soap Service puts the PvD desktops into the Preparing state.
- The personal vDisk size should always be larger than the Citrix Provisioning write cache disk (otherwise, Citrix Provisioning might erroneously select the personal vDisk for use as its write cache).
- After you create a Delivery Group, you can monitor the personal vDisk using the Resize and poolstats scripts (`personal-vdisk-poolstats.ps1`).

Size the write cache disk correctly. During normal operation, PvD captures most user writes (changes) and redirects them to the personal vDisk. This implies that you can reduce the size of the Citrix Provisioning write cache disk. However, when PvD is not active (such as during image update operations), a small Citrix Provisioning write cache disk can fill up, resulting in machine crashes.

Citrix recommends that you size Citrix Provisioning write cache disks according to Citrix Provisioning best practice and add space equal to twice the size of the template VHD on the master image (to ac-

commodate merge requirements). It is extremely unlikely that a merge operation will require all of this space, but it is possible.

When using Citrix Provisioning to deploy a catalog with PvD-enabled machines:

- Follow the guidance in the Citrix Provisioning documentation.
- You can change the power action throttling settings by editing the connection in Studio; see below.
- If you update the Citrix Provisioning vDisk, after you install/update applications and other software and restart the vDisk, run the PvD inventory and then shut down the VM. Then, promote the new version to Production. The PvD desktops in the catalog should automatically enter the Preparing state. If they do not, check that the Soap Service account has machine administrator or higher privileges on the Controller.

The Citrix Provisioning test mode feature enables you to create a test catalog containing machines using an updated master image. If tests confirm the test catalog's viability, you can promote it to production.

Considerations: Machine Creation Services

When using Machine Creation Services (MCS) to deploy a catalog with PvD-enabled machines:

- Follow the guidance in the product documentation.
- Run a PvD inventory after you create the master image and then power off the VM (PvD will not function correctly if you do not power off the VM). Then, take a snapshot of the master image.
- In the Create Machine Catalog wizard, specify the personal vDisk size and drive letter.
- After you create a Delivery Group, you can monitor the personal vDisk using the Resize and poolstats scripts (`personal-vdisk-poolstats.ps1`).
- You can change the power action throttling settings by editing the connection in Studio; see below.
- If you update the master image, run the PvD inventory after you update the applications and other software on the image, and then power off the VM. Then, take a snapshot of the master image.
- Use the PvD Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to validate that there is sufficient space on each PvD-enabled VM that will use the updated master image.
- After you update the machine catalog, the PvD desktops enter the Preparing state as they individually process the changes in the new master image. The desktops are updated according to the rollout strategy specified during the machine update.
- Use the PvD Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to monitor the PvD in the Preparing state.
- The selection of PVD and MCS IO caching are mutually exclusive. If you install PVD, you will not be able to create a catalog with MCS IO caching enabled.

How-to: Exclude files and folders from vDisks

Use the rules files to exclude files and folders from the vDisks. You can do this when the personal vDisks are in deployment. The rules files are named custom_*_rules.template.txt and are located in the \config folder. Comments in each file provide additional documentation.

How-to: Run the inventory when updating a master image

When you enable PvD and after any update to the master image after installation, it is important to refresh the disk's inventory (called "run the inventory") and create a new snapshot.

Because administrators, not users, manage master images, if you install an application that places binary files in the administrator's user profile, the application is not available to users of shared virtual desktops (including those based on pooled machine catalogs and pooled with PvD machine catalogs). Users must install such applications themselves.

It is best practice to take a snapshot of the image after each step in this procedure.

1. Update the master image by installing any applications or operating system updates, and performing any system configuration on the machine.

   For master images based on Windows XP that you plan to deploy with Personal vDisks, check that no dialog boxes are open (for example, messages confirming software installations or prompts to use unsigned drivers). Open dialog boxes on master images in this environment prevent the VDA from registering with the Delivery Controller. You can prevent prompts for unsigned drivers using the Control Panel. For example, navigate to System > Hardware > Driver Signing, and select the option to ignore warnings.

2. Shut down the machine. For Windows 7 machines, click Cancel when Citrix Personal vDisk blocks the shutdown.

3. In the Citrix Personal vDisk dialog box, click Update Inventory. This step may take several minutes to complete.

   Important: If you interrupt the following shutdown (even to make a minor update to the image), the Personal vDisk's inventory no longer matches the master image. This causes the Personal vDisk feature to stop working. If you interrupt the shutdown, you must restart the machine, shut it down, and when prompted click Update Inventory again.

4. When the inventory operation shuts down the machine, take a snapshot of the master image.

You can export an inventory to a network share and then import that inventory to a master image. For details, see Export and import a PvD inventory.

How-to: Configure connection throttling settings

The Citrix Broker Service controls the power state of the machines that provide desktops and applications. The Broker Service can control several hypervisors through a Delivery Controller. Broker power actions control the interaction between a Controller and the hypervisor. To avoid overloading the hypervisor, actions that change a machine's power state are assigned a priority and sent to the hypervisor using a throttling mechanism. The following settings affect the throttling. You specify these values by editing a connection (Advanced page) in Studio.

To configure connection throttling values:

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Edit Connection in the Actions pane.
3. You can change the following values:

    - **Simultaneous actions (all types):** The maximum number of simultaneous in-progress power actions allowed. This setting is specified as both an absolute value and as a percentage of the connection to the hypervisor. The lower of the two values is used.
      Default = 100 absolute, 20%
    - **Simultaneous Personal vDisk inventory updates:** The maximum number of simultaneous Personal vDisk power actions allowed. This setting is specified as both an absolute value and a percentage of the connection. The lower of the two values is used.
      Default = 50 absolute, 25%
      To calculate the absolute value: determine the total IOPS (TIOPS) supported by the end-user storage (this should be specified by the manufacturer or calculated). Using 350 IOPS per VM (IOPS/VM), determine the number of VMs that should be active at any given time on the storage. Calculate this value by dividing total IOPS by IOPS/VM.
      For example, if the end-user storage is 14000 IPS, the number of active VMs is 14000 IOPS / 350 IOPS/VM = 40.
    - **Maximum new actions per minute:** The maximum number of new power actions that can be sent to the hypervisor per minute. Specified as an absolute value.
      Default = 10

To help identify optimal values for these settings in your deployment:

1. Using the default values, measure the total response time for an image update of a test catalog. This is the difference between the start of an image update (T1) and when the VDA on the last machine in the catalog registers with the Controller (T2). Total response time = T2 - T1.
2. Measure the input/output operations per second (IOPS) of the hypervisor storage during the image update. This data can serve as a benchmark for optimization. (The default values may be the best setting; alternatively, the system might max out of IOPS, which will require lowering the setting values.)

3. Change the "Simultaneous Personal vDisk inventory updates"value as described below (keeping all other settings unchanged).

    a) Increase the value by 10 and measure the total response time after each change. Continue to increase the value by 10 and test the result, until deterioration or no change in the total response time occurs.
    b) If the previous step resulted in no improvement by increasing the value, decrease the value in increments of 10 and measure the total response time after each decrease. Repeat this process until the total response time remains unchanged or does not improve further. This is likely the optimal PvD power action value.

4. After obtaining the PvD power action setting value, tweak the simultaneous actions (all types) and maximum new actions per minute values, one at a time. Follow the procedure described above (increasing or decreasing in increments) to test different values.

How-to: System Center Configuration Manager 2007 with PvD

System Center Configuration Manager (Configuration Manager) 2012 requires no special configuration and can be installed in the same way as any other master image application. The following information applies only to System Center Configuration Manager 2007. Configuration Manager versions earlier than Configuration Manager 2007 are not supported.

Complete the following to use Configuration Manager 2007 agent software in a PvD environment.

1. Install the Client Agent on the master image.

    a) Install the Configuration Manager client on the master image.
    b) Stop the ccmexec service (SMS Agent) and disable it.
    c) Delete SMS or client certificates from the local computer certificate store as follows:
        - Mixed mode: Certificates (Local Computer)\SMS\Certificates
        - Native mode
            - Certificates (Local Computer)\Personal\Certificates
            - Delete the client certificate that was issued by your certificate authority (usually, an internal Public Key Infrastructure)
    d) Delete or rename C:\Windows\smscfg.ini.

2. Remove information that uniquely identifies the client.

    a) (Optional) Delete or move log files from C:\Windows\System32\CCM\Logs.
    b) Install the Virtual Delivery Agent (if not installed previously), and take the PvD inventory.
    c) Shut down the master image, take a snapshot, and create a machine catalog using this snapshot.

3. Validate personal vDisk and start services. Complete these steps once on each PvD desktop, after it has been started for the first time. This can be done using a domain GPO, for example.
    - Confirm that PvD is active by checking for the presence of the registry key HKLM\Software\Citrix\personal vDisk\config\virtual.
    - Set the ccmexec service (SMS agent) to Automatic and start the service. The Configuration Manager client contacts the Configuration Manager server, and retrieves new unique certificates and GUIDs.

Tools

November 10, 2020

You can use the following tools and utilities to tailor, expedite, and monitor PvD operations.

Custom rules files

The custom rule files provided with PvD let you modify the default behavior of PvD image updates in the following ways:

- The visibility of files on the PvD
- How changes made to the files are merged
- Whether the files are writable

For detailed instructions on the custom rules files and the CoW feature, refer to the comments in the files located in C:\ProgramData\Citrix\personal vDisk\Config on the machine where PvD is installed. The files named "custom_*"describe the rules and how to enable them.

Resize and poolstats scripts

Two scripts are provided to monitor and manage the size of PvDs; they are located in the Support\Tools\Scripts folder on the Citrix Virtual Apps and Desktops installation media.

Use resize-personalvdisk-pool.ps1 to increase the size of the PvDs in all of the desktops in a catalog. The following snap-ins or modules for your hypervisor must be installed on the machine running Studio:

- XenServer requires XenServerPSSnapin
- vCenter requires vSphere PowerCli
- System Center Virtual Machine Manager requires the VMM console

Use personal-vdisk-poolstats.ps1 to check the status of image updates and to check the space for applications and user profiles in a group of PvDs. Run this script before updating an image to check whether any desktop is running out of space, which helps prevent failures during the update. The script requires that Windows Management Instrumentation (WMI-In) firewall is enabled on the PvD desktops. You can enable it on the master image or through GPO.

If an image update fails, the entry in the Update column gives the reason.

Reset the application area

If a desktop becomes damaged or corrupted (by installing a broken application or some other cause), you can revert the application area of the PvD to a factory-default (empty) state. The reset operation leaves user profile data intact.

To reset the application area of the PvD, use one of the following methods:

- Log on to the user's desktop as Administrator. Launch a command prompt, and run the command C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset.
- Locate the user's desktop in Citrix Director. Click **Reset Personal vDisk** and then click **OK**.

Export and import a PvD inventory

The image update process is an integral part of rolling out new images to PvD desktops; it includes adjusting the existing Personal vDisk to work with the new base image. For deployments that use Machine Creations Services (MCS), you can export an inventory from an active VM to a network share, and then import it into a master image. A differential is calculated using this inventory in the master image. Although using the export/import inventory feature is not mandatory, it can improve the performance of the overall image update process.

To use the export/import inventory feature, you must be an administrator. If required, authenticate to the file share used for the export/import with "net use."The user context must be able to access any file shares used for the export/import.

- To export an inventory, run the export command as an administrator on a machine containing a VDA with PvD enabled (minimum version 7.6):

  Ctxpvdsvc.exe exportinventory "<path-to-export-location>"

  The software detects the current inventory's location and exports the inventory to a folder named "ExportedPvdInventory"to the specified location. Here's an excerpt from the command output:

```
1  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
       exportinventory
```



```
2  \\share location\ExportedInventory
3  Current inventory source location C:\CitrixPvD\Settings\Inventory
       \VER-LAS
4  ...
5  Exporting current inventory to location \\ ….
6  ...
7  Deleting any pre-existing inventory folder at \\ ….
8  .Successfully exported current inventory to location \\ …. Error
       code = OPS
9  <!--NeedCopy-->
```

- To import a previously-exported inventory, run the import command as an administrator on the master image:

To import:

Run the import command as an administrator on the master image.

`Ctxpvdsvc.exe importinventory "<path-to-exported-inventory>"`

The <path to exported inventory> should be the full path to the inventory files, which is usually <network location\ExportedPvdInventory>.

The inventory is obtained from the import location (where it was previously exported using the exportinventory option) and imports the inventory to the inventory store on the master image. Here's an excerpt of the command output:

```
1  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
       importinventory
2  \\share location\ExportedInventory\ExportedPvdInventory
3  Importing inventory \\share location\ExportedInventory\
       ExportedPvdInventory
4  …
5  Successfully added inventory \\share location\ExportedInventory\
       ExportedPvdInventory to the
6  store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
7  <!--NeedCopy-->
```

After the export, the network share should include the following filenames. After the import, the inventory store on the master image should include the same file names.

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT

- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Displays, messages, and troubleshooting

February 6, 2020

Monitor PvD through reports

You can use a diagnostic tool to monitor the changes made by users to both parts of their Personal vDisks (the user data and the application parts). These changes include applications that users have installed and files they have modified. The changes are stored in a set of reports.

1. On the machine you want to monitor, run `C:\\Program Files\\Citrix\\personal vDisk\\bin\\CtxPvdDiag.exe`.
2. Browse to a location where you want to store the reports and logs, select the reports to generate, and then click **OK**. The available reports are listed below.

Software hive report: This report generates two files: `Software.Dat.Report.txt` and `Software.Dat.delta.txt`.

The `Software.Dat.Report.txt` file records the changes made by the user to the HKEY_LOCAL_MACHINE\Soft hive. It contains the following sections:

- List of applications installed on the base: Applications that were installed in Layer 0.
- List of user installed software: Applications the user installed on the application part of the personal vDisk.
- List of software uninstalled by user: Applications the user removed that were originally in Layer 0.

See the hive delta report for information about the Software.Dat.delta.txt.

System hive report: The generated SYSTEM.CurrentControlSet.DAT.Report.txt file records changes the user made to the HKEY_LOCAL_MACHINE\System hive. It contains the following sections:

- List of user installed services: services and drivers the user installed.
- Startup of following services were changed: services and drivers whose start type the user modified.

Security hive report: The generated SECURITY.DAT.Report.txt file monitors all changes that the user makes in the HKEY_LOCAL_MACHINE\Security hive.

Security Account Manager (SAM) hive report: The generated SAM.DAT.Report.txt file monitors all changes that the user makes in the HKEY_LOCAL_MACHINE\SAM hive.

Hive delta report: The generated Software.Dat.delta.txt file records all registry keys and values added or removed, and all values the user modified in the HKEY_LOCAL_MACHINE\Software hive.

Personal vDisk logs: The log files Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log, and vDeskService-<#>.log are generated by default in P:\Users\<user account>\AppData\Local\Temp\PVDLOGS, but are moved to the selected location.

Windows operating system logs:

- EvtLog_App.xml and EvtLog_System.xml are the application and system event logs in XML format from the personal vDisk volume.
- Setupapi.app.log and setuperr.log contain log messages from when msiexec.exe was run during personal vDisk installation.
- Setupapi.dev.log contains device installation log messages.
- Msinfo.txt contains the output of msinfo32.exe. For information, see the Microsoft documentation.

File system report: The generated FileSystemReport.txt file records changes the user made to the file system in the following sections:

- Files Relocated: Files in Layer 0 that the user moved to the vDisk. Layer 0 files are inherited from the master image by the machine to which the personal vDisk is attached.
- Files Removed: Files in Layer 0 that were hidden by a user's action (for example, removing an application).
- Files Added (MOF,INF,SYS): Files with .mof, .inf, or .sys extensions that the user added to the personal vDisk (for example, when they installed an application such as Visual Studio 2010 that registers a .mof file for autorecovery).
- Files Added Other: Other files that the user added to the vDisk (for example, when installing an application).
- Base Files Modified But Not Relocated: Files in Layer 0 that the user modified but that the personal vDisk Kernel-Mode drivers did not capture in the vDisk.

Image updates

In Studio, when you choose a PvD-enabled machine in a machine catalog, the "PvD" tab provides monitoring status during image updates, plus estimated completion time and progress. The possible state displays during an image update are: Ready, Preparing, Waiting, Failed, and Requested.

An image update can fail for different reasons, including lack of space or a desktop not finding the PvD in sufficient time. When Studio indicates that an image update failed, an error code with descriptive text is provided to help troubleshooting. Use the Personal vDisk Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to monitor image update progress and obtain error codes associated with the failure.

If an image update fails, the following log files can provide further troubleshooting information:

- PvD service log - C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD activation log i- P:\PVDLOGS\PvDActivation.log.txt

The most recent content is at the end of the log file.

Error messages: 7.6 and later

The following errors are valid for PvD version 7.6 and later:

- **An internal error occurred. Review the Personal vDisk logs for further details. Error code %d (%s)**

  This is a catch-all for uncategorized errors, so it has no numeric value. All unexpected errors encountered during inventory creation or Personal vDisk update are indicated by this error code.

  - Collect logs and contact Citrix support.
  - If this error occurs during catalog update, roll back the catalog to the previous version of the master image.

- **There are syntax errors in the rule files. Review the logs for further details.**

  Error code 2. The rule file contains syntax errors. The Personal vDisk log file contains the name of the rule file and line number where the syntax error was found. Fix the syntax error in the rule file and retry the operation.

- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is corrupt or unreadable.**

  Error code 3. The last inventory is stored in "UserData.V2.vhd" in "\ProgramData\CitrixPvD\Settings\Inventory
  LAST". Restore the inventory corresponding to the last version of the master image by importing the 'VER-LAST' folder from a known working PvD machine associated with the previous version of the master image.

- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is higher version.**

  Error code 4. This is caused by personal vDisk version incompatibility between the last master image and the current master image. Retry updating the catalog after installing the latest version of personal vDisk in the master image.

- **Change journal overflow was detected.**

  Error code 5. A USN journal overflow was caused by a large number of changes made to the master image while creating the inventory. If this continues to occur after multiple attempts, use procmon to determine if third party software is creating/deleting a large number of files during inventory creation.

- **The Personal vDisk could not find a disk attached to the system for storing user data.**

  Error code 6. First, verify that the PvD disk is attached to the VM through the hypervisor console. This error typically happens due to "Data Leak Prevention"software preventing access to the PvD disk. If the PvD disk is attached to the VM, try adding an exception for "attached disk"in the "Data Leak Prevention"software configuration.

- **The system has not been rebooted post-installation. Reboot to implement the changes.**

  Error code 7. Restart the desktop and retry the operation.

- **Corrupt installation. Try re-installing Personal vDisk.**

  Error code 8. Install personal vDisk and try again.

- **Personal vDisk inventory is not up to date. Update the inventory in the master image, and then try again.**

  Error code 9. The personal vDisk inventory was not updated in the master image before shutting down the desktop. Restart the master image and shut down the desktop through the "Update personal vDisk"option, and then create a new snapshot; use that snapshot to update the catalog.

- **An internal error occurred while starting the Personal vDisk. Review the Personal vDisk logs for further details.**

  Error code 10. This could be caused by the PvD driver failing to start a virtualization session due to an internal error or personal vDisk corruption. Try restarting the desktop through the Controller. If the problem persists, collect the logs and contact Citrix Support.

- **The Personal vDisk timed out while trying to find a storage disk for users'personalization settings.**

  Error code 11. This error occurs when the PvD driver fails to find the PvD disk within 30 seconds after restart. This is usually caused by an unsupported SCSI controller type or storage latency. If this occurs with all desktops in the catalog, change the SCSI controller type associated with the "Template VM"/ "Master VM"to a type supported by personal vDisk technology. If this occurs with only some desktops in the catalog, it might be due to spikes in storage latency due to a large number of desktops starting at the same time. Try limiting the maximum active power actions setting associated with the host connection.

- **The Personal vDisk has been de-activated because an unsafe system shutdown was detected. Restart the machine.**

  Error code 12. This could be due to a desktop failing to complete the boot process with PvD enabled. Try restarting the desktop. If the problem persists, watch the desktop startup through the hypervisor console and check if the desktop is crashing. If a desktop crashes during startup, restore the PvD from backup (if you maintain one) or reset the PvD.

- **The drive letter specified for mounting the Personal vDisk is not available.**

  Error code 13. This could be caused by PvD failing to mount the PvD disk at the mount specified by the administrator. The PvD disk will fail to mount if the drive letter is already used by other hardware. Select a different letter as the mount point for the personal vDisk.

- **Personal vDisk kernel mode drivers failed to install.**

  Error code 14. Personal vDisk installs drivers during the first inventory update after installation. Some antivirus products prevent installation of the driver when attempted outside the context of an installer. Temporarily disable the antivirus real time scan or add exceptions in the antivirus for PvD drivers during the first time inventory creation.

- **Cannot create a snapshot of the system volume. Make sure that the Volume Shadow Copy service is enabled.**

  Error code 15. This could occur because the Volume Shadow Copy service is disabled. Enable the Volume Shadow Copy service and retry taking an inventory.

- **The change journal failed to activate. Try again after waiting for few minutes.**

  Error code 16. Personal vDisk uses change journal for tracking changes made to master image. During an inventory update, if PvD detects that the change journal is disabled, it attempts to enable it; this error occurs when that attempt fails. Wait for few minutes and retry.

- **There is not enough free space in the system volume.**

  Error code 17. There is not enough free space available on the C drive of the desktop for the image update operation. Expand the system volume or remove unused files to free space in the system volume. The image update should begin again after the next restart.

- **There is not enough free space in the Personal vDisk storage. Expand Personal vDisk storage to provide more space.**

  Error code 18. There is not enough free space available on the personal vDisk drive when performing an image update operation. Expand personal vDisk storage or remove unused files to free space in the personal vDisk storage. The image update should restart after next reboot.

- **Personal vDisk storage is over-committed. Expand Personal vDisk storage to provide more space.**

Error code 19. There is not enough free space available on the personal vDisk drive to fully accommodate thick provisioned "UserData.V2.vhd". Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

- **Corrupt system registry.**

  Error code 20. The system registry is corrupt, damaged, missing, or unreadable. Reset the personal vDisk or restore it from an earlier backup.

- **An internal error occurred while resetting the Personal vDisk. Check Personal vDisk logs for further details.**

  Error code 21. This is a catch-all for all the errors encountered during a personal vDisk reset. Collect the logs and contact Citrix Support.

- **Failed to reset the Personal vDisk because there is not enough free space in the personal vDisk storage.**

  Error code 22. There is not enough free space available on the Personal vDisk drive when performing a reset operation. Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

Error messages: earlier than 7.6

The following errors are valid for PvD 7.x versions earlier than 7.6:

- **Startup failed. Personal vDisk was unable to find a storage disk for user personalization settings.**

  The PvD software could not find the Personal vDisk (by default, the P: drive) or could not mount it as the mount point selected by the administrator when they created the catalog.

  - Check the PvD service log for following entry: "PvD 1 status –> 18:183".
  - If you are using a version of PvD earlier than Version 5.6.12, upgrading to the latest version resolves this issue.
  - If you are using Version 5.6.12 or later, use the disk management tool (diskmgmt.msc) to determine whether the P: drive is present as an unmounted volume. If present, run chkdsk on the volume to determine if it is corrupt, and try to recover it using chkdsk.

- **Startup failed. Citrix Personal vDisk failed to start. For further assistance …. Status code: 7, Error code: 0x70**

  Status code 7 implies that an error was encountered while trying to update the PvD. The error could be one of the following:

Error code	Description
0x20000001	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000004	Failed to acquire required privileges for updating the PvD.
0x20000006	Failed to load hive from the PvD image or from PvD inventory, most likely due to corrupt PvD image or inventory.
0x20000007	Failed to load the file system inventory, most likely due to a corrupt PvD image or inventory.
0x20000009	Failed to open the file containing file system inventory, most likely due to a corrupt PvD image or inventory.
0x2000000B	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000010	Failed to load the diff package.
0x20000011	Missing rule files.
0x20000021	Corrupt PvD inventory.
0x20000027	The catalog "MojoControl.dat"is corrupt.
0x2000002B	Corrupt or missing PvD inventory.
0x2000002F	Failed to register user installed MOF on image update, upgrade to 5.6.12 to fix the issue.
0x20000032	Check the PvDactivation.log.txt for the last log entry with a Win32 error code.
0x20	Failed to mount application container for image update, upgrade to 5.6.12 to fix the issue.
0x70	There is not enough space on the disk.

- **Startup failed. Citrix Personal vDisk failed to start [or Personal vDisk encountered an internal error]. For further assistance …Status code: 20, Error code 0x20000028**

  The personal vDisk was found but a PvD session could not be created.

  Collect the logs and check SysVol-IvmSupervisor.log for session creation failures:

  1. Check for the following log entry "IvmpNativeSessionCreate: failed to create native session, status XXXXX".

2. If the status is 0xc00002cf, fix the problem by adding a new version of the master image to the catalog. This status code implies that the USN Journal overflowed due to a large number of changes after an inventory update.
3. Restart the affected virtual desktop. If the problem persists, contact Citrix Technical Support.

- **Startup failed. Citrix Personal vDisk has been deactivated because an unsafe system shutdown was detected. To retry, select Try again. If the problem continues, contact your system administrator.**

  The pooled VM cannot complete its startup with the PvD enabled. First determine why startup cannot be completed. Possible reasons are that a blue screen appears because:

  - An incompatible antivirus product is present, for example old versions of Trend Micro, in the master image.
  - The user has installed software that is incompatible with PvD. This is unlikely, but you can check it by adding a new machine to the catalog and seeing whether it restarts successfully.
  - The PvD image is corrupt. This has been observed in Version 5.6.5.

  To check if the pooled VM is displaying a blue screen, or is restarting prematurely:

  - Log on to the machine through the hypervisor console.
  - Click Try Again and wait for the machine to shut down.
  - Start the machine through Studio.
  - Use the hypervisor console to watch the machine console as it starts.

  Other troubleshooting:

  - Collect the memory dump from the machine displaying the blue screen, and send it for further analysis to Citrix Technical Support.
  - Check for errors in the event logs associated with the PvD:
    1. Mount UserData.V2.vhd from the root of the P: drive using DiskMgmt.msc by clicking Action > Attach VHD.
    2. Launch Eventvwr.msc.
    3. Open the system event log (Windows\System32\winevt\logs\system.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.
    4. Open the application event log (Windows\System32\winevt\logs\application.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.

- **The Personal vDisk cannot start. The Personal vDisk could not start because the inventory has not been updated. Update the inventory in the master image, then try again. Status code: 15, Error code: 0x0**

The administrator selected an incorrect snapshot while creating or updating the PvD catalog (that is, the master image was not shut down using Update Personal vDisk when creating the snapshot).

Events logged by Personal vDisk

If Personal vDisk is not enabled, you can view the following events in Windows Event Viewer. Select the Applications node in the left pane; the Source of the events in the right pane is Citrix Personal vDisk. If Personal vDisk is enabled, none of these events are displayed.

An Event ID of 1 signifies an information message, an ID of 2 signifies an error. Not all events may be used in every version of Personal vDisk.

Event ID	Description
1	Personal vDisk Status: Update Inventory Started.
1	Personal vDisk Status: Update Inventory completed. GUID: %s.
1	Personal vDisk Status: Image Update Started.
1	Personal vDisk Status: Image Update completed.
1	Reset in progress.
1	OK.
2	Personal vDisk Status: Update Inventory Failed with: %s.
2	Personal vDisk Status: Image Update Failed with: %s.
2	Personal vDisk Status: Image Update Failed with Internal Error.
2	Personal vDisk Status: Update Inventory Failed with: Internal Error.
2	Personal vDisk has been disabled because of an improper shutdown.
2	Image update failed. Error code %d.
2	Personal vDisk encountered an internal error. Status code[%d] Error code[0x%X].
2	Personal vDisk reset failed.
2	Unable to find disk for storing user personalization settings.

Event ID	Description
2	There is not enough space available on the storage disk to create a Personal vDisk container.

Migrating PvD to App Layering

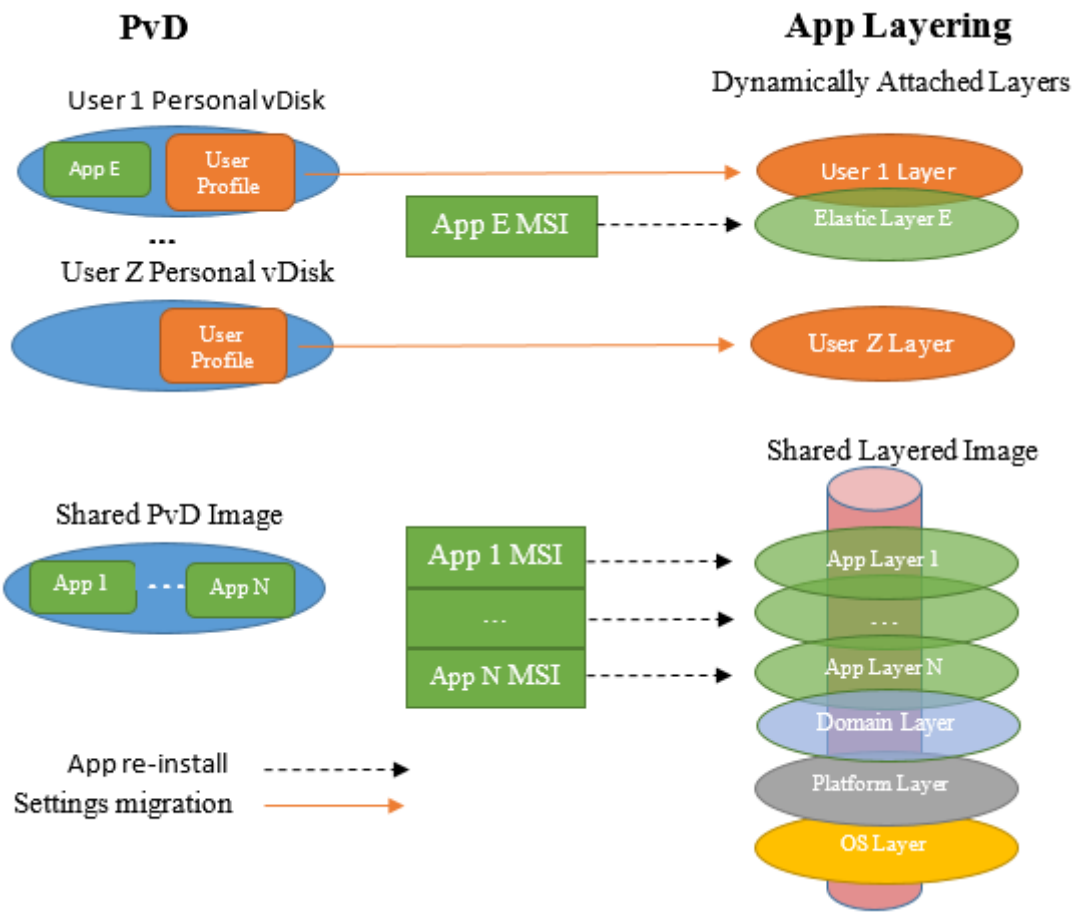
February 7, 2020

Citrix is replacing Personal vDisk (PvD) functionality with Citrix App Layering technology. Use the information in this article to create an App Layering VM that is functionally equivalent to a PvD-based VM.

For information about layers, and the process of creating and publishing image templates, see the Citrix App Layering documentation.

Typical PvD VMs consist of a shared image and a Personal vDisk. The shared image is distributed among multiple users, each of whom has their own user-specific Personal vDisk. A typical App Layering VM consists of multiple layers, including an OS, platform, and usually one or more application layers. This VM is shared by multiple users, each of whom has their own User Layer.

When migrating a set of users who share a PvD image VM, a functionally equivalent App Layering Shared Image VM is created. Each user has their personal profile and settings migrated from their Personal vDisk to their new App Layering User Layer, as illustrated in the following image:



This article takes a different approach for migrating a user's personal data versus migrating applications. For personal data, this article recommends tools for copying it from a Personal vDisk to a User Layer. For applications, it does not recommend copying them. Instead it recommends personal data be reinstalled in an App Layer. Also, this article assumes:

- That the PvD VM is running Windows 7. Migration for other OS versions should be similar if App Layering supports them. For example, App Layering does not support Windows XP.
- Citrix Hypervisor is used as the hypervisor, and that you are familiar with managing it using XenCenter.
- Machine Catalog Services (MCS) or Citrix Provisioning (formerly Provisioning Services) are used for provisioning purposes. For MCS or Citrix Provisioning, you need the Citrix Virtual Apps and Desktops ISO. For Citrix Provisioning, you need the "ProvisioningServicesxxx.iso."
- Citrix Virtual Desktops is used to manage the generated App Layering VMs.

If you are using a different hypervisor or provisioning service, the migration procedures noted in this article are similar.

The examples in this article assume that the user is a member of an Active Directory (AD) domain.

PvD versus App Layering

App Layering encourages the clean separation of applications from user-specific information. Applications are located in App Layers, often with one app per Layer, and user-specific information is located in a User Layer. As a best practice, a user would not install an application in their User Layer if they thought the application might have general utility. Instead they would install it in an Elastic App Layer, which would be dynamically attached to their (and others) VMs when they log in.

PvD does not support this clean separation because it has only two layers: the Shared Image, shared by multiple users, and a user-specific vDisk. Users would often install an application in their user vDisk if it was not available in the Shared Image.

When migrating a Shared PvD Image to App Layering you must determine all the applications it contains. For each application (or related set of applications) you create an App Layer. Consider the following:

- If the application has general utility, you attach the App Layer to an Image Template, which is then published in a Layered Image.
- If the application has utility to some smaller group of users, you assign it to that group. Then when members of that group log into the VM, it is dynamically attached as an Elastic App Layer.
- If the application has specific value to only one user, you install it in the user's User Layer.

Miscellaneous App Layering artifacts

In the process of creating an App Layering VM, some artifacts are created, including packaging VMs, connectors, agents, and VM templates. These elements are unique to App Layering and are described briefly in the following sections. For a complete description, please see the App Layering documentation.

Packaging VMs

App Layering's method for customizing the content of Platform Layers and App Layers is to create a *Packaging VM*, sometimes referred to as *Install Machines*. Creating a layer is a six step process:

1. From the Enterprise Layer Manager (ELM) you create the layer and specify its name and other information.
2. ELM generates a Packaging VM and copies it (typically) to your hypervisor.
3. From your hypervisor you boot the Packaging VM and customize it.
4. When you're finished customizing, click the **Shutdown to Finalize** icon, which is on the Packaging VM desktop. This action performs a layer integrity check, ensuring that no reboots are pending and that ngen is not running. It does not finish until all such tasks are complete.

5. From ELM, click the **Finalize** action.
6. ELM finishes generating the layer based on your customized Packaging VM and deletes the Packaging VM.

App Layering does not use a Packaging VM to create the OS Layer. Instead, you create a VM, customize it as needed, and the ELM imports it.

Connectors and agents

The ELM communicates with several other entities, such as hypervisors, file shares, and provisioning tools. It performs various tasks on those entities, such as creating VMs, and involves copying various kinds of data, such as VHDs and files, to or from those entities.

A connector is an object that ELM uses when communicating with some other entity to perform a set of tasks. It is configured with the name, or IP address, of the other entity, the credentials needed to access that entity and any other information required to perform its tasks. For example, a file path on the entity where data is read or written.

The following elements create connectors:

- Citrix Hypervisor Connector: ELM uses this connector to create or delete VMs, such as the Packaging VMs, from Citrix Hypervisor.
- Network File Share Connector: This connector is configured from the 'System'tab, 'Settings and Configurations'subtab, in the 'Network File Share'section. ELM and VMs use this process to create files in a network file share.
- Citrix MCS for Citrix Hypervisor Connector: If you are using MCS as your provisioning service, this connector is created. ELM uses it to copy Layered Images to Citrix Hypervisor after stripping out drivers not required by MCS.
- Citrix Provisioning Connector: If you are using Citrix Provisioning as your provisioning service, you create this connector. ELM uses it to copy the Layered Image VHD to the Citrix Provisioning Server. It creates a vDisk there after stripping out drivers not required by Citrix Provisioning.

VM template

If you are using Citrix Hypervisor as your hypervisor, a VM Template is created based on your OS Layer VM. This template contains information about the OS, such as network interfaces and the number of processors. It is created after your OS Layer is created. It is used when a Citrix Hypervisor connector is created.

Installing the Unidesk Agent on the Citrix Provisioning Server

If you are deploying using Citrix Provisioning, you must install the Unidesk Agent on the Citrix Provisioning Server. This lets ELM run commands on the Citrix Provisioning Server.

See "Install the App Layering Agent (required for Citrix Provisioning and Connector Scripts)"in the App Layering documentation.

Shared image migration

To migrate a Shared PvD Image to App Layering, you create a Shared Layered Image that is functionally equivalent to the Shared PvD Image. The Shared Layered Image is constructed by publishing an Image Template. The Image Template combines an OS Layer, a Platform Layer and one or more App Layers, each of which you create. These procedures are described in the following sections.

OS layer

Use the following steps to create an OS Layer.

From XenCenter:

Create a VM on Citrix Hypervisor. This is the basis for both your OS Layer and your VM Template.

The VM's OS version should match that of the Shared PvD Image that you're migrating. In these instructions we assume you are running Windows 7.

From the OS Layer VM:

Log in using the local admin account.

Install any outstanding Windows Updates.

Perform the preparation activities described in the App Layering documentation, "Prepare a Windows 7 image."

From XenCenter:

Make a copy of your OS Layer VM. Delete any local storage. Convert the VM to a Template. You use this VM Template when creating a Citrix Hypervisor connector.

From ELM:

From the **Layers** tab, click **Create OS Layer**.

If you are using Citrix Hypervisor and have not yet created a Citrix Hypervisor connector, do so now. When prompted for the 'Virtual Machine Template', specify the VM Template you created in the preceding section.

When prompted to 'Select Virtual Machine', pick your OS Layer VM.

After assigning an Icon and specifying any other detailed information, press 'Create Layer'. This copies your OS Layer VM into the ELM store and generate your OS Layer.

This completes the creation of your OS Layer, making it deployable.

Platform layer

Once the OS Layer is generated, you can proceed with creating a Platform Layer for the Shared Image.

One step in customizing the Platform Layer is to join the users' Active Directory domain. If the users are members of several different domains, you must create a separate Platform Layer for each domain. This article assumes all the users are members of a single domain.

From ELM:

1. In the **Layers** tab, click **Create Platform Layer**.
2. In the 'OS Layers' panel select the OS Layer you created in the preceding section.
3. In the 'Connector' panel select the Citrix Hypervisor Connector you created in the preceding section. ELM uses this information when writing the Platform Layer Packaging VM to Citrix Hypervisor.
4. In the 'Platform Types' panel select 'This platform will be used for publishing Layered Images'.
5. Pick the appropriate Hypervisor. In this article we assume you are using 'Citrix Hypervisor'.
6. Pick the appropriate Provisioning Service. We assume you are using either 'Citrix MCS' or 'Citrix PVS' (if using Citrix Provisioning).
7. For Connection Broker, select 'Citrix XenDesktop'.

After assigning an icon and specifying any other detailed information, click **Create Layer**. This action generates a Platform Layer Packaging VM. Once complete, the creation task's status indicates 'Action Required.'

From XenCenter:

When your Platform Layer Packaging VM is generated, it appears in XenCenter. Perform the following:

1. Boot it.
2. From your Platform Layer Packaging VM, log in using the local admin account.
3. If prompted, reboot, and log in again.
4. Join the users' Active Directory domain in the usual way. That is, **Control Panel > System > Change Settings \ > Change**. Reboot and log in again using the local admin account.

Install the Citrix Virtual Delivery Agent (VDA):

1. Mount the Citrix Virtual Apps and Desktops ISO.
2. Run AutoSelect.exe if it doesn't start automatically.
3. Click **Start** beside Citrix Virtual Desktops.
4. Click **Virtual Delivery Agent for Desktop OS**.

   In general, pick the defaults in the option panels that follow. However,

   - You can specify your Delivery Controller when prompted, or specify 'Do It Later (Advanced)'.
   - Ensure that 'Personal vDisk'is not selected.

   After the VDA is installed the Platform Layer Packaging VM reboots.

Log in again.

If you are using Citrix Provisioning as your provisioning service, you also need to install the Target Device software. To do this:

1. Mount the 'ProvisionServicesxxx.iso'.
2. Run 'AutoSelect.exe'if it doesn't start automatically.
3. Click 'Target Device Installation'.
4. Click 'Target Device Installation'again to start the Installation Wizard. The installer installs the Citrix Diagnostic Facility (CDF) and the Citrix Provisioning Service Target Device code.
5. In general you pick the defaults in the option panels that follow.
6. When the Installation Wizard finishes uncheck 'Launch Imaging Wizard'and click 'Finish'.
7. Allow the VM to restart and log in.
8. Run the Citrix Provisioning Optimizer utility.

After installing all platform-related software and making any customizations, click the 'Shutdown to Finalize'desktop icon.

From ELM:

Select your Platform Layer's icon, its status should be 'Editing', and click **Finalize**.

App layers

Once the Platform Layer is generated, you can proceed with creating App Layers from the Shared PvD Image. Determine the applications installed in the Shared PvD Image. There are several ways to do this, including:

- If you have a bootable version of the Shared PvD Image, boot it and, from the control panel select 'Programs and Features'.

- Otherwise from Citrix Virtual Desktops, use the Shared PvD Image to create a PvD VM for a dummy user. Because the dummy user's Personal vDisk is empty, all the applications shown by 'Programs and Features'have been installed on the Shared PvD Image.

Use the **Programs and Features** panel to verify all the required applications.

Alternatively you can use the PCmover program, described in the Migration Tools section. It does a good job of identifying applications on a computer. It detects programs that have been installed in some ad-hoc manner, so they don't appear in 'Programs and Features'. If used for this purpose, allow it to perform its analysis without actually performing any transfers. Once it has performed its analysis and you have noted all of the Shared Image's applications, you would simply cancel of PCmover. For details, see the section **Using PCmover to Determine Required Applications** later in this article.

> **Tip:**
>
> If you are migrating several PvD VMs, this would be a good opportunity to boot each to compile a list of user-installed applications. Any applications that you find over and above the ones you found in the Shared Image are user-installed applications.

Once you have a complete list of required applications, create one or more App Layers, installing one or more of the required applications in each App Layer. For example, related applications might all be installed in one App Layer. Applications used by several users might be installed in an Elastic App Layer. An application used by a single user might be installed in their User Layer. Although for many applications it is straight forward to create an App Layer, others require special preparation.

For many applications it is straightforward to create an App Layer, others require special preparation. Check the various configuration recipes developed by Citrix Solution Architects and by the App Layering community. You find, for example, that there are some applications that can only be installed in a User Layer and not in an App Layer.

For each App Layer, from ELM:

1. In the **Layers** tab, click **Create App Layer**.
2. In the **Layer Details** section, specify the Layer Name and Version.
3. In the OS Layer pick the OS Layer you created in the preceding section.
4. If this application depends applications in another App Layer, specify them in the Prerequisite Layers. This determines the order in which you create your App Layers.
5. In the Connector, pick the Citrix Hypervisor Connector you created in the preceding section. ELM uses this connector to write the App Layer Packaging VM to Citrix Hypervisor where, using XenCenter, you can boot and customize it.
6. When all options have been specified, click **Create Layer**. This generates an App Layer Packaging VM. When this is complete the creation task's status indicates 'Action Required.'In this example no Platform Layer is needed because we assume this App Layer is deployed on the same hypervisor as was chosen when you created the OS Layer.

From XenCenter:

When your App Layer Packaging VM is generated, it appears in XenCenter. Perform the following tasks:

1. Boot it.
2. From your App Layer Packaging VM, log in using the local admin account.
3. If it immediately requires a reboot, do that and log in again.
4. Install this App Layer's applications and make any necessary customizations. Because this Layer is shared by multiple users, user-specific customization and settings should not be made. They are performed when a user's Personal vDisk is migrated, as described later in this article.
5. After installing this layer's applications and making any customizations, click the **Shutdown to Finalize** desktop icon.

From ELM:

1. Select the App Layer's icon; its status should be *Editing*.
2. Click **Finalize**. This completes the creation of this App Layer, making it deployable.
3. Repeat this procedure for each required App Layer.

Image template

Having generated your OS Layer, Platform Layer and one or more App Layers, you can now proceed with creating an Image Template. Decide which App Layers should be bound into the Layered Image and which should be dynamically assigned to users as Elastic App Layers. Consider:

- Any App Layers that you include in the Image Template are available to all users of the Shared Layered Image.
- Any App Layers that you assign to specific users (or AD groups) are available only to those users (or AD groups). You have the flexibility of changing such assignments later, making App Layers available to different users or groups.

> **Important:**
>
> These two alternatives are mutually exclusive; you should never include an App Layer in an Image Template and also assign it to a user. Doing so is unnecessary and not supported.

As a rule of thumb, applications that were installed in the Shared PvD Image should be included in the Image Template. Applications that were installed in some user's Personal vDisk should be assigned as Elastic App Layers, and applications used by a single user and unlikely to be shared are installed in that user's User Layer.

From ELM:

1. In the **Images** tab, click **Create Template**.
2. Provide a name and version.
3. Specify the OS Layer created in the preceding section.
4. Select any App Layers that you want included in the Image Template. Do not select App Layers that you intend to assign to users and AD groups as Elastic App Layers.
5. Select a Connector Configuration. This determines where the Shared Image is deployed when it is published. Create a Connector Configuration the first time you use a new deployment target.

Assuming you are using Citrix Hypervisor, you have three types of deployment available:

- Citrix Hypervisor: Using the Citrix Hypervisor connector, ELM deploys the published Shared Image as a VM to Citrix Hypervisor where, using XenCenter, you can boot it. Typically, though, choose one of the following two choices, Citrix Provisioning or MCS.
- Citrix Provisioning: The published Shared Image is deployed as a vDisk on a Citrix Provisioning Server. When creating a Connector Configuration of this type you must specify the name of the Citrix Provisioning Server. Login credentials for a user with permission to manage Citrix Provisioning. For details see "Connector Configuration & Optional Script (Citrix Provisioning)" in the online App Layering documentation.
- Citrix MCS for Citrix Hypervisor: The published Shared Image is deployed as a VM on Citrix Hypervisor where, using Citrix Virtual Desktops, you can use it to create a Machine Catalog.

When creating this type of Connector Configuration you must specify the Citrix Hypervisor address and credentials so ELM can write there, and the target Storage Repository. Also specify the VM Template you created in the preceding section.

In addition:

- Select a Platform Layer: either the MCS or Citrix Provisioning platform layer that you created in the preceding section or, if you are deploying to Citrix Hypervisor, skip this option.
- In the **Layered Image Disk** panel: If the 'SysPrep'option appears, select 'Not Generalized'.
- For 'Elastic Layering': select 'Application and User Layers'. This setting has two effects.
  - It allows extra App Layers to be assigned to users and AD groups, layers that are dynamically attached when a user logs in.
  - It causes a new User Layer to be created on behalf of a user the first time they log in. (In App Layering version 4.1 this option is only available if explicitly enabled. To enable, from ELM in the 'System'tab in the 'Settings and Configuration'subtab, in the 'Labs'section, select the 'User Layers'checkbox.)

A User Layer captures the user's profile, settings, documents, etc. As described in the following section, this is the target where the Migration Tools transfer all user-specific information from the user's Personal vDisk.

In the **Confirm and Complete** panel, click **Create Template**. This should complete almost immediately.

Publishing the shared layered image

The final step in generating the Shared Layered Image is to select the **Image Template created above** and click **Publish Layered Image**.

When this completes the resulting Layered Image is deployed as either (1) for MCS, a VM in Citrix Hypervisor, or (2) for Citrix Provisioning, a vDisk in the Citrix Provisioning server.

Now you can use the normal MCS or Citrix Provisioning management tools to create a Citrix Virtual Desktops machine catalog and Delivery Group:

- For MCS, use Studio to create a machine catalog and import the Shared Layered Image VM.
- For Citrix Provisioning, use the Citrix Virtual Desktops Setup Wizard to create a machine catalog in Studio.

The final step in migrating a user's PvD VM to App Layering is described in the following section. As a preview of the process: you concurrently run the original PvD VM and the new App Layering VM, log in as the user to the App Layering VM, and execute a migration tool to transfer the user's profile and settings from PvD to the App Layering User Layer.

Migration tools

Citrix recommends that you use one of two tools, PCmover or USMT, to migrate personal information from a user's Personal vDisk to their App Layering User Layer.

- PCmover is a program sold by LapLink.com. You can run a user's PvD VM and the App Layering VM, and use PCmover to transfer the user's settings from the former to the latter. The two VMs can either be run concurrently with the information being transferred over a network, or they can be run consecutively with the information transferred by a file.

  PCmover has an easy-to-use GUI, with which you can precisely tailor the information being transferred. If you have several PvD VMs to migrate, you should consider using the PCmover Policy Manager to create a Policy File. Using a Policy File, you can perform migrations with minimal interactions.

  For details see the PCmover User Guide.

- USMT is a set of programs available from Microsoft as part of the Windows Automation Installation kit (AIK). A scanstate program is run on the PvD VM to write a transfer file. A loadstate program is run on the App Layering VM to read and apply the transfer file. The details of what

information is transferred are determined by several XML files. Those files can be edited if the defaults do not suit your needs.

In this article we assume you run PCmover.

Migrating user information

At this point you should have taken your original Shared PvD Image and created a functionally equivalent App Layering Shared Layered Image. You have one or more user PvD VMs, each with a Personal vDisk containing user profile and other information that you want to migrate to an App Layering User Layer.

For each such user you start the user's PvD VM, start the Shared Layered Image, and, on both VMs, log in using the user's domain credentials and run PCmover.

To migrate user information:

1. Install PCmover in a share accessible from both the PvD VM and the Shared Layered Image.
2. From Studio, start the user's PvD VM. Log in as the user. Disable firewalls.
3. From ELM, assign to the user any Elastic App Layers they require.
4. Ensure that the user has write access to the directory where their User Layer exists. Look for 'Configure Security on User Layer Folders'in the online documentation.
5. From Studio, start the Shared Layered Image VM. Log in as the user. The first time the user logs in, the VM creates a User Layer in the Network File Share. Disable firewalls, anti-virus, and anti-spyware applications.
6. Run PCmover on the PvD VM.
    a) Select 'PC to PC Transfer'and 'Next'.
    b) Select 'Old'and 'Next'.
    c) Select 'Wifi or Wired Network'and 'Next'.
    d) PCmover spends a few minutes scanning the PvD VM. After that select 'Next'.
    e) Assuming you do not want to receive an email notification when the transfer is complete, simply select 'Next'.
    f) Enter a password or not. A password ensures that the user information is sent from the PvD VM to only the Shared Layered Image VM and to no other VM. Then select 'Next'.
7. Run PCmover on the App Layering VM.
    a) Select 'PC to PC Transfer'and 'Next'.
    b) Select 'New'and 'Next'.
    c) Enter the required Serial Number Validation values.
    d) For 'Network Name'specify the name of the PvD VM and 'Next'
    e) Visit the 'Application Selections'panel. We recommend deselecting all applications. You should have created App Layers for all the required applications.

f) Visit the 'User Account Selections' panel. We recommend editing any users other than the Personal vDisk's owner and marking them as 'Do not transfer this user'.
g) Visit the 'Custom Settings' panel. We recommend selecting 'Files and Settings Only'.
h) Visit the 'Drive Selections' panel. We recommend editing any drives other than 'C:' and marking them as 'Do not transfer this drive'.
i) After visiting all the panels, click 'Next'.
j) Assuming you do not want to receive an email notification when the transfer is complete, simply select 'Next'.

At this point PCmover starts transferring files and settings from the PvD VM to the user's App Layering User Layer.

Using PCmover to determine required applications

You can use PCmover to analyze a PvD VM and determine the installed applications. This provides an alternative to using the **Control** Panel's 'Programs and Features'.

1. Run PCmover on the PvD VM.
2. Select 'PC to PC Transfer' and 'Next'.
3. Select 'Old' and 'Next'.
4. Select 'File Storage Device' and 'Next'.
5. Visit the 'Application Selections' panel and note the installed applications.
6. Cancel PCmover.

Remove components

February 6, 2020

To remove components, Citrix recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script on the installation media.

When you remove components, prerequisites are not removed, and firewall settings are not changed. For example, when you remove a Delivery Controller, the SQL Server software and the databases are not removed.

If you upgraded a Controller from an earlier deployment that included Web Interface, you must remove the Web Interface component separately. You cannot use the installer to remove Web Interface.

For information about removing features not mentioned below, see the feature's documentation.

Preparation

Before removing a Controller, remove it from the Site. For details, see Remove a Controller.

Close Studio and Director before removing them.

Remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- To remove a Controller, Studio, Director, License Server, or StoreFront, right-click **Citrix Virtual Apps *version*** or **Citrix Virtual Desktops *version*** and select **Uninstall**. The installer launches. Select the components to be removed.

  Alternatively, you can remove StoreFront by right-clicking **Citrix StoreFront** and selecting **Uninstall**.
- To remove a VDA, right-click **Citrix Virtual Delivery Agent *version*** and select **Uninstall**. The installer launches and you can select the components to be removed. The machine restarts automatically after the removal, by default.
- To remove the Universal Print Server, right-click **Citrix Universal Print Server** and select **Uninstall**.

Remove core components using the command line

From the \x64\XenDesktop Setup directory on the installation media, run the `XenDesktopServerSetup.exe` command.

- To remove one or more components, specify the `/remove` and `/components` options.
- To remove all components, specify the `/removeall` option.

For command and parameter details, see Install using the command line.

For example, the following command removes Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

Remove VDAs using the command line

From the \x64\XenDesktop Setup directory on the installation media, run the `XenDesktopVdaSetup.exe` command.

- To remove one or more components, use the /remove and /components options.

- To remove all components, use the /removeall option.

For command and parameter details, see Install using the command line.

The machine restarts automatically after the removal, by default.

For example, the following command removes the VDA and Citrix Workspace app.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

To remove VDAs using a script in Active Directory; see Install or remove VDAs using scripts.

Upgrade and migrate

September 9, 2022

About upgrading

Upgrading changes your deployment to the Citrix Virtual Apps and Desktops 7 1912 Long Term Service (LTSR) without having to set up new machines or sites. This is known as an in-place upgrade.

Upgrading gives you access to the latest features and technologies that you're eligible for. Upgrades can also contain fixes, clarifications, and enhancements from earlier versions.

Versions you can upgrade

You can upgrade to the LTSR from:

- XenApp and XenDesktop 7.6 LTSR with or without CUs, up to and including CU9 (only for platforms mentioned in System Requirements)
- XenApp and XenDesktop 7.15 LTSR with or without CUs, up to and including CU7
- XenApp and XenDesktop 7.16
- XenApp and XenDesktop 7.17
- XenApp and XenDesktop 7.18
- Citrix Virtual Apps and Desktops 7 1808
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1909

Important notice about upgrading VDAs

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 never used PvD.

Learn if you're affected

How PvD 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.

If you don't know whether your VDA has PvD installed, run the installer for the new VDA (1912 LTSR or later) on the machine or image.

- If PvD is installed, a message appears, indicating there is an incompatible component.
  - For the graphical interface, click **Cancel** on the page containing the message, and then confirm that you want to close the installer.
  - From the CLI, the command simply fails with the displayed message.
- If PvD is not installed, the upgrade proceeds.

What to do

If the VDA does not have PvD installed, follow the usual upgrade procedure.

If the VDA has PvD installed:

1. Uninstall the current VDA. For details, see Remove components.
2. Install the new VDA.

If you want to continue using PvD you can do so only on VDA 7.15 LTSR through Win 7 and Win 10 (1607 or earlier) versions.

How to upgrade

Review the documentation before beginning the upgrade.

To upgrade the core components and VDAs:

1. Run the installer on the machines where the components are installed. The software determines if an upgrade is available and installs the newer version.
2. Use the newly upgraded Studio to upgrade the database and the site.

Upgrade preparation and guidance: The Upgrade a deployment article is your primary information source for the core components and VDAs. That article describes the upgrade sequence and order, limitations, preparation steps, and other considerations. It also provides the step-by-step upgrade procedure, and instructions for upgrading the databases and the site after you upgrade the core components.

Installation specifics: After you complete any preparation work and you are ready to start the installer, the installation article shows you what you will see (if you're using the graphical interface) or what to type (if you're using the command-line interface) to upgrade the components. When the installer completes, return to the guidance in Upgrade a deployment for database and site upgrades.

- Install/upgrade core components using the graphical interface
- Install/upgrade core components using the command line
- Install/upgrade VDAs using the graphical interface
- Install/upgrade VDAs using the command line

For information about installing Controller hotfixes, see CTX201988.

Upgrade Licensing

For a comprehensive look at managing Citrix Licensing, see Activate, upgrade, and manage Citrix licenses.

For an on-premises deployment, you can use the full-product installer to upgrade the License Server. Or, you can download and upgrade the license components separately. See Upgrade.

Upgrade other components

In addition to the core components and VDAs, on-premises Citrix Virtual Apps and Desktops deployments include the following components that you can upgrade when newer versions are released.

- StoreFront
- AppDNA

- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

Frequently asked questions

This section answers some commonly asked questions about upgrading Citrix Virtual Apps and Desktops.

- **What is the correct order to upgrade my Virtual Apps and Desktops environment?**

  The VDA can be upgraded at any time, in any order. Upgrade half of the Controllers before upgrading your site. Then upgrade the remaining Controllers after the site upgrade. For more information, see Upgrade sequence and Upgrade procedure.

- **My site has several Delivery Controllers (in different zones). What happens if I upgrade only some of them? Am I required to upgrade every Controller in the site during the same maintenance window?**

  The best practice is to upgrade all Delivery Controllers during the same maintenance window, as various services on each Controller communicate with each other. Keeping different versions might cause issues. During a maintenance window, we recommend you upgrade half of the Controllers, upgrade the site, and then upgrade the remaining Controllers. (For details, see the Upgrade procedure.)

- **Can I go directly to the latest version, or do I have to do incremental upgrades?**

  You can almost always upgrade to the latest version and skip intermediate releases, unless explicitly stated in the **What's new** article for the version you're upgrading to. See the Upgrade Guide.

- **Can a customer upgrade from a Long Term Service Release (LTSR) environment to a Current Release?**

  Yes. Customers are not required to remain on a Long Term Service Release for an extended period. Customers can move an LTSR environment to a Current Release, based on business requirements and features.

- **Are mixed versions of components allowed?**

  Within each site, Citrix recommends upgrading all components to the same version. Although you can use earlier versions of some components, all of the features in the latest version might not be available. For more information, see Mixed environment considerations.

- **How often must a Current Release be upgraded?**

  Current Releases reach End of Maintenance (EOM) 6 months after the release date. Citrix recommends customers adopt the latest Current Release. Current Releases reach End of Life (EOL) 18 months after the release date. For more information, see Current Release Lifecycle.

- **What is recommended: upgrade to LTSR or CR?**

  Current Releases (CRs) deliver the latest and most innovative app, desktop, and server virtualization features and functionality. This allows you to stay on cutting edge technology and ahead of your competition.

  Long Term Service Releases (LTSRs) are ideal for large enterprise production environments that prefer to retain the same base version for an extended period.

  For details, see Servicing Options.

- **Do I need to upgrade my licenses?**

  You need to ensure that the current license date has not expired, and is valid for the release you are upgrading to. See CTX111618. For information about renewal, see Customer Success Services renewal licenses.

- **How long does an upgrade take?**

  The time required to upgrade a deployment varies, depending on the infrastructure and network. So, we can't provide an exact time.

- **What are the best practices?**

  Ensure that you understand and follow the preparation guidance.

- **Which operating systems are supported?**

  See System requirements.

  If you have an earlier operating system that is not valid for the version you're upgrading to, see What you can do.

- **Which versions of VMware vSphere (vCenter + ESXi) are supported?**

  Hosts/virtualization resources lists the supported versions for all supported hosts, including VMware.

- **When does my version go EOL?**

  Check the Product Matrix.

- **What are the known issues with the latest release?**

  - Citrix Virtual Apps and Desktops
  - StoreFront

- Citrix Provisioning
- Citrix License Server
- Citrix Workspace App

Migrate

Migrating moves data from an earlier deployment to a later version. Migrating includes installing newer components and creating a new Site, exporting data from the older farm, and then importing the data to the new Site.

- For information about architecture, component, and feature changes that were introduced with the 7.x releases, see Changes in 7.x.
- For information about migrating from XenApp 6.x, see Migrate XenApp 6.x.

More information

Long Term Service Release (LTSR) deployment updates use Cumulative Updates (CUs). A CU updates baseline components of the LTSR, and each CU includes its own metainstaller.

Each CU has dedicated documentation. For example, for the 7.15 LTSR, check the link on that LTSR's What's new page for the latest CU. Each CU page includes supported version information, instructions, and a link to the CU download package.

Changes in 7.x

February 6, 2020

Citrix Virtual Apps and Desktops architecture, terminology, and features changed, beginning with the XenApp and XenDesktop 7.x releases. If you are familiar with only earlier (pre-7.x) versions, this article can acquaint you with the changes.

After you have moved to a 7.x version, changes to later versions are listed in What's new.

Unless specifically noted, *7.x* and "later versions" refer to XenApp version 7.5 or later, and XenDesktop version 7 or later, including all Citrix Virtual Apps and Desktops releases.

This article provides an overview. For comprehensive information about moving from pre-7.x to later versions, see Upgrade to XenApp 7.

Element differences between XenApp 6 and later versions

Although they are not exact equivalents, the following table helps map functional elements from XenApp 6.5 and previous versions to later versions. Descriptions of architectural differences follow.

Instead of this in XenApp 6.x and earlier	Think of this in newer versions
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Farm	Site
Worker Group	Machine catalog, Delivery Group
Worker	Virtual Delivery Agent (VDA), multi-session OS machine, multi-session OS VDA, single-session OS machine, single-session OS VDA
Remote Desktop Services (RDS) or Terminal Services machine	Multi-session OS machine, multi-session OS VDA
Zone and Data Collector	Delivery Controller
Delivery Services Console	Citrix Studio and Citrix Director
Publishing applications	Delivering applications
Data store	Database
Load Evaluator	Load Management Policy
Administrator	Delegated Administrator, Role, Scope

Architecture differences

Beginning with 7.x versions, Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) is based on FlexCast Management Architecture (FMA). FMA is a service-oriented architecture that allows interoperability and management modularity across Citrix technologies. FMA provides a platform for application delivery, mobility, services, flexible provisioning, and cloud management.

FMA replaces the Independent Management Architecture (IMA) used in XenApp 6.5 and previous versions.

These are the key elements of FMA in terms of how they relate to elements of XenApp 6.5 and previous versions:

- **Delivery Sites:** Farms were the top-level objects in XenApp 6.5 and previous versions. In later versions, the Site is the highest level item. Sites offer applications and desktops to groups of users. FMA requires that you must be in a domain to deploy a Site. For example, to install the

servers, your account must have local administrator privileges and be a domain user in the Active Directory.

- **Machine catalogs and Delivery Groups:** Machines hosting applications in XenApp 6.5 and previous versions belonged to Worker Groups for efficient management of the applications and server software. Administrators could manage all machines in a Worker Group as a single unit for their application management and load-balancing needs. Folders were used to organize applications and machines. In later versions, you use a combination of machine catalogs, Delivery Groups, and Application Groups to manage machines, load balancing, and hosted applications or desktops. You can also use application folders.
- **VDAs:** In XenApp 6.5 and previous versions, worker machines in Worker Groups ran applications for the user and communicated with data collectors. In later versions, the VDA communicates with Delivery Controllers that manage the user connections.
- **Delivery Controllers:** In XenApp 6.5 and previous versions there was a zone master responsible for user connection requests and communication with hypervisors. In later versions, Controllers in the Site distribute and handle connection requests. In XenApp 6.5 and previous versions, zones provided a way to aggregate servers and replicate data across WAN connections. Although zones have no exact equivalent in later versions, the zones and zone preference functionality enables you to help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of a WAN.
- **Studio and Director:** Use the Studio console to configure your environments and provide users with access to applications and desktops. Studio replaces the Delivery Services Console in XenApp 6.5 and previous versions. Administrators use Director to monitor the environment, shadow user devices, and troubleshoot IT issues. To shadow users, Windows Remote Assistance must be enabled; it is enabled by default when the VDA is installed.
- **Delivering applications:** XenApp 6.5 and previous versions used the Publish Application wizard to prepare applications and deliver them to users. In later versions, you use Studio to create and add applications to make them available to users who are included in a Delivery Group and optionally, Application Groups. Using Studio, you first configure a Site, create and specify Machine Catalogs, and then create Delivery Groups that use machines from those catalogs. The Delivery Groups determine which users have access to the applications you deliver. You can optionally choose to create Application Groups as an alternative to multiple Delivery Groups.
- **Database:** Later versions do not use the IMA data store for configuration information. They use a Microsoft SQL Server database to store configuration and session information.
- **Load Management Policy:** In XenApp 6.5 and previous versions, load evaluators use predefined measurements to determine the load on a machine. User connections can be matched to the machines with a lower load. In later versions, use load management policies for balancing loads across machines.
- **Delegated Administration:** In XenApp 6.5 and previous versions, you created custom administrators and assigned them permissions based on folders and objects. In later versions, cus-

tom administrators are based on role and scope pairs. A role represents a job function and has defined permissions associated with it to allow delegation. A scope represents a collection of objects. Built-in administrator roles have specific permissions sets, such as help desk, applications, hosting, and catalog. For example, help desk administrators can work only with individual users on specified sites, while full administrators can monitor the entire deployment and resolve system-wide IT issues.

Feature comparison

The transition to FMA also means some features available in XenApp 6.5 and previous versions may be implemented differently or may require you to substitute other features, components, or tools to achieve the same goals.

Instead of this in XenApp 6.5 and earlier	Use this in later versions
Session prelaunch and session linger configured with policy settings	Session prelaunch and session linger configured by editing Delivery Group settings. As in XenApp 6.5, these features help users connect to applications quickly, by starting sessions before they are requested (session prelaunch) and keeping sessions active after a user closes all applications (session linger). In later versions, you enable these features for specified users by configuring these settings for existing Delivery groups. See Configure session prelaunch and session linger.
Support for unauthenticated (anonymous) users provided by granting rights to anonymous user when setting the properties of published applications	Support for unauthenticated (anonymous) users is provided by configuring this option when setting user properties of a Delivery Group. See Users.
Local host cache permits a worker servers to function even when a connection to the data store is not available	Local Host Cache allows connection brokering operations to continue when the connection between a Controller and the Site database fails. This implementation is more robust and requires less maintenance. See Local Host Cache.
Application streaming	Citrix App-V delivers streamed applications, which are managed using Studio. See App-V.
Web Interface	Citrix recommends you transition to StoreFront.

Instead of this in XenApp 6.5 and earlier	Use this in later versions
SmartAuditor to record on-screen activity of a user's session	Beginning with 7.6 Feature Pack 1, this functionality is provided by Session Recording. You can also use Configuration Logging to log all session activities from an administrative perspective.
Power and Capacity Management to help reduce power consumption and manage server capacity	Use the Microsoft Configuration Manager.

Feature support and changes

The following features are not currently provided, no longer supported, or have changed significantly in Citrix Virtual Apps and Desktops, beginning with XenApp and XenDesktop 7.x versions.

Secure ICA encryption below 128-bit: In releases earlier than 7.x, Secure ICA could encrypt client connections for basic, 40-bit, 56-bit, and 128-bit encryption. In 7.x releases, Secure ICA encryption is available only for 128-bit encryption.

Legacy printing: The following printing features are not supported in 7.x releases:

- Backward compatibility for DOS clients and 16-bit printers.
- Support for printers connected to Windows 95 and Windows NT operating systems, including enhanced extended printer properties and Win32FavorRetainedSetting.
- Ability to enable or disable auto-retained and auto-restored printers.
- DefaultPrnFlag, a registry setting for servers that is used to enable or disable auto-retained and auto-restored printers, which store in user profiles on the server.

Legacy client printer names are supported.

Secure Gateway: In releases earlier than 7.x, Secure Gateway was an option to provide secure connections between the server and user devices. Citrix Gateway is the replacement option for securing external connections.

Shadowing users: In releases earlier than 7.x, administrators set policies to control user-to-user shadowing. In 7.x releases, shadowing end-users is an integrated feature of the Director component, which uses Windows Remote Assistance to allow administrators to shadow and troubleshoot issues for delivered seamless applications and virtual desktops.

Flash v1 Redirection: Clients that do not support second generation Flash Redirection (including Citrix Receiver for Windows earlier than 3.0, Citrix Receiver for Linux earlier than 11.100, and Citrix Online Plug-in 12.1) will fall back to server-side rendering for legacy Flash Redirection features. VDAs included with 7.x releases support second generation Flash Redirection features.

Local Text Echo: This feature was used with earlier Windows application technologies to accelerate the display of input text on user devices on high latency connections. It is not included in 7.x releases due to improvements to the graphics subsystem and HDX SuperCodec.

Single Sign-on: This feature, which provides password security, is not supported for Windows 8, Windows Server 2012, and newer supported Windows operating systems versions. It is still supported for Windows 2008 R2 and Windows 7 environments, but is not included with 7.x releases. You can locate it on the Citrix download website: https://citrix.com/downloads.

Oracle database support: 7.x releases require a SQL Server database.

Health Monitoring and Recovery (HMR): In releases earlier than 7.x, HMR could run tests on the servers in a server farm to monitor their state and discover any health risks. In 7.x releases, Director offers a centralized view of system health by presenting monitoring and alerting for the entire infrastructure from within the Director console.

Custom ICA files: Custom ICA files were used to enable direct connection from user devices (with the ICA file) to a specific machine. In 7.x releases, this feature is disabled by default, but can be enabled for normal usage using a local group or can be used in high-availability mode if the Controller becomes unavailable.

Management Pack for System Center Operations Manager (SCOM) 2007: The management pack, which monitored the activity of XenApp farms using SCOM, does not support 7.x releases. See the current Citrix SCOM Management Pack for XenApp and XenDesktop.

CNAME function: The CNAME function was enabled by default in releases earlier than 7.x. Deployments depending on CNAME records for FQDN rerouting and the use of NETBIOS names might fail. In 7.x releases, the Delivery Controller auto-update feature dynamically updates the list of Controllers and automatically notifies VDAs when Controllers are added to and removed from the Site. The Controller auto-update feature is enabled by default in Citrix policies, but can be disabled. Alternatively, you can re-enable the CNAME function in the registry to continue with your existing deployment and allow FQDN rerouting and the use of NETBIOS names. For more information, see CTX137960.

Quick Deploy wizard: In XenDesktop releases earlier than 7.x, this Studio option allowed a fast deployment of a fully installed XenDesktop deployment. The new simplified installation and configuration workflow in later releases eliminates the need for the Quick Deploy wizard option.

Remote PC Service configuration file and PowerShell script for automatic administration: Remote PC Access is now integrated into Studio and the Controller.

Workflow Studio: In releases earlier than 7.x, Workflow Studio was the graphical interface for workflow composition for XenDesktop. The feature is not supported in later releases.

Launching of non-published programs during client connection: In releases earlier than 7.x, this Citrix policy setting specified whether to launch initial applications or published applications through

ICA or RDP on the server. In 7.x releases, this setting specifies only whether to launch initial applications or published applications through RDP on the server.

Desktop launches: In releases earlier than 7.x, this Citrix policy setting specified whether non-administrative users can connect to a desktop session. In 7.x releases, non-administrative users must be in a VDA machine's Direct Access Users group to connect to sessions on that VDA. The Desktop launches setting enables non-administrative users in a VDA's Direct Access Users group to connect to the VDA using an ICA connection. The Desktop launches setting has no effect on RDP connections; users an VDA's Direct Access Users group can connect to the VDA using an RDP connection whether or not this setting is enabled.

Color depth: In Studio releases earlier than 7.6, you specified color depth in a Delivery Group's User Settings. Beginning in version 7.6, color depth for the Delivery Group can be set using the New-BrokerDesktopGroup or Set-BrokerDesktopGroup PowerShell cmdlet.

Launch touch-optimized desktop: This setting is disabled and not available for Windows 10 and Windows Server 2016 machines. For more information, see Mobile experience policy settings.

Features not in Citrix Workspace app or that have different default values

The following changes cover Citrix Workspace app (formerly Citrix Receiver):

- **COM Port Mapping:** COM Port Mapping allowed or prevented access to COM ports on the user device. COM Port Mapping was previously enabled by default. In 7.x releases, COM Port Mapping is disabled by default. For details, see Configure COM Port and LPT Port Redirection settings using the registry.
- **LPT Port Mapping:** LPT Port Mapping controls the access of legacy applications to LPT ports. LPT Port Mapping was previously enabled by default. In 7.x releases, LPT Port Mapping is disabled by default.
- **PCM Audio Codec:** Only HTML5 clients support the PCM Audio Codec in 7.x releases.
- **Support for Microsoft ActiveSync**.
- **Proxy support for older versions:** This includes:
  - Microsoft Internet Security and Acceleration (ISA) 2006 (Windows Server 2003)
  - Oracle iPlanet Proxy Server 4.0.14 (Windows Server 2003)
  - Squid Proxy Server 3.1.14 (Ubuntu Linux Server 11.10)

For more information, see the Citrix Workspace app documentation for your version.

Upgrade a deployment

December 8, 2023

Introduction

You can upgrade certain deployments to newer versions without having to first set up new machines or sites. This is called an in-place upgrade. To learn which Citrix Virtual Apps and Desktops versions you can upgrade, see the Citrix Upgrade Guide.

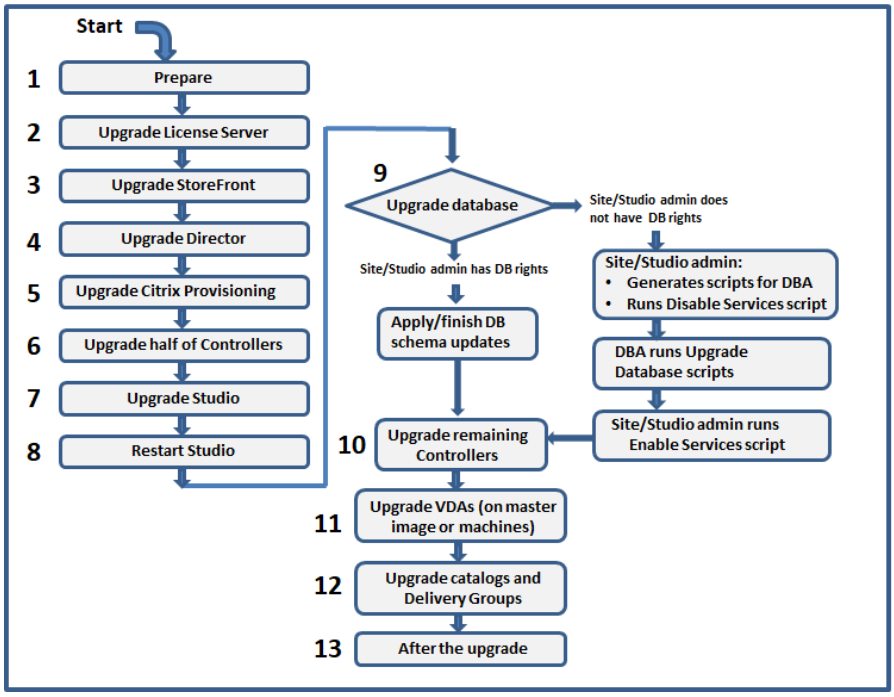
To start an upgrade, you run the installer from the new version to upgrade previously installed core components, VDAs, and certain other components. Then you upgrade the databases and the site.

You can upgrade any component that can be installed with the full-product installer (and the standalone VDA installers), if there is a newer version provided. For other components that are not installed with the full-product installer (such as Citrix Provisioning and Profile Management), see that component's documentation for guidance. For host upgrades, see the appropriate documentation.

Review all the information in this article before beginning an upgrade.

Upgrade sequence

The following diagram shows the steps the upgrade sequence. Upgrade procedure contains details of each step in the diagram.



> **Note:**
>
> To avoid failures, you must upgrade all Delivery Controllers and database before performing any of the provisioning and delivery group related tasks such as creating a new machine catalog, deleting a machine catalog, updating a machine in a delivery group, and so on.

Upgrade procedure

Most of the main product components can be upgraded by running the product installer on the machine containing the component.

If one machine contains more than one component (for example, Studio and License Server), all components on that machine are upgraded, if the product media contains newer versions of their software.

To use the installers:

- To run the full product installer's graphical interface, log on to the machine and then insert the media or mount the ISO drive for the new release. Double-click **AutoSelect**.
- To use the command-line interface, issue the appropriate command. See Install using the command line.

Step 1: Prepare

Before you begin an upgrade, make sure you're ready. Read and complete any necessary tasks:

- Upgrade VDAs to 1912 or later
- Limitations
- Mixed environment considerations
- Earlier operating systems
- Preparation
- Preliminary site tests
- SQL Server version check

Step 2: Upgrade License Server

If the installation has a new version of the Citrix License Server software, upgrade this component first before any other components.

If you have not yet determined whether your License Server is compatible with the new version, it is essential that you run the installer on the License Server before upgrading any other core components.

Step 3: Upgrade StoreFront

If the installation media contains a new version of the StoreFront software, run the installer on the machine containing the StoreFront server.

- In the graphical interface, choose **Citrix StoreFront** from the **Extend deployment** section.
- From the command line, run `CitrixStoreFront-x64.exe`, which is available in the Citrix Virtual Apps and Desktops installation media's `x64` folder.

Step 4: Upgrade Director

If the installation media contains a new version of the Director software, run the installer on the machine containing Director.

Step 5: Upgrade Citrix Provisioning

The Citrix Provisioning installation media is available separately from the Citrix Virtual Apps and Desktops installation media. To learn how to install and upgrade Citrix Provisioning server and target device software, see the Citrix Provisioning product documentation.

Step 6: Upgrade half of Delivery Controllers

For example, if your site has four Controllers, run the installer on two of them.

Leaving half of the Controllers active allows users to access the site. VDAs can register with the remaining Controllers. There might be times when the site has reduced capacity because fewer Controllers are available. The upgrade causes only a brief interruption in establishing new client connections during the final database upgrade steps. The upgraded Controllers cannot process requests until the entire site is upgraded.

If your site has only one Controller, it is inoperable during the upgrade.

Preliminary site tests run on the first Controller, before the actual upgrade starts. For details, see Preliminary site tests.

Step 7: Upgrade Studio

If you haven't already upgraded Studio (because it was on the same machine as another component), run the installer on the machine containing Studio.

Step 8: Restart Studio

Restart the upgraded Studio. The upgrade process automatically resumes.

Step 9: Upgrade database and site

> **Note:**
>
> To avoid failures, you must upgrade all Delivery Controllers and database before performing any of the provisioning and delivery group related tasks such as creating a new machine catalog, deleting a machine catalog, updating a machine in a delivery group, and so on.

Check Preparation for the permissions required to update the schema of the SQL Server databases.

- If you have sufficient permission to update the SQL Server database schema, you can initiate an automatic database upgrade. Continue with Upgrade the database and site automatically.
- If you do not have sufficient database permissions, you can initiate a manual upgrade that uses scripts, and proceed with the help of your database administrator (someone who has the required permissions). For a manual upgrade, the Studio user generates the scripts and then runs the scripts that enable and disable services. The database administrator runs other scripts that update the database schema, using either the SQLCMD utility or the SQL Server Management Studio in SQLCMD mode. Continue with Upgrade the database and site manually.
- If you have a multi-zone deployment and want to upgrade the database and site automatically, Citrix recommends that the dbschema upgrade should be performed in the same zone that hosts the SQL server databases of the site. Otherwise, upgrading the database and site automatically might fail.

Citrix strongly recommends that you back up the database before upgrading. See CTX135207. During a database upgrade, product services are disabled. During that time, Controllers cannot broker new connections for the site, so plan carefully.

Upgrade the database and site automatically

1. Start the newly upgraded Studio.
2. Indicate that you want to start the site upgrade automatically and confirm that you are ready.

The database and site upgrade proceeds.

Upgrade the database and site manually

1. Start the newly upgraded Studio.
2. Indicate that you want to upgrade the site manually. The wizard checks for License Server compatibility and requests confirmation.

3. Confirm that you have backed up the database.

   The wizard generates and displays the scripts and a checklist of upgrade steps. If a database's schema has not changed since the product version being upgraded, that script is not generated. For example, if the logging database schema does not change, the `UpgradeLoggingDatabase.sql` script is not generated.

4. Run the following scripts in the order shown.

   - `DisableServices.ps1`: The Studio user runs this PowerShell script on a Controller to disable product services.
   - `UpgradeSiteDatabase.sql`: The database administrator runs this SQL script on the server containing the Site database
   - `UpgradeMonitorDatabase.sql`: The database administrator runs this SQL script on the server containing the Monitor database.
   - `UpgradeLoggingDatabase.sql`: The database administrator runs this SQL script on the server containing the Configuration Logging database. Run this script only if this database changes (for example, after applying a hotfix).
   - `EnableServices.ps1`: The Studio user runs this PowerShell script on a Controller to enable product services.

   After the database upgrade completes and product services are enabled, Studio automatically tests the environment and configuration, and then generates an HTML report. If problems are identified, you can restore the database backup. After resolving issues, you can upgrade the database again.

5. After completing the checklist tasks, click **Finish upgrade**.

Step 10: Upgrade remaining Delivery Controllers

From the newly upgraded Studio, select **Citrix Studio** *site-name* in the navigation pane. On the **Common Tasks** tab, select **Upgrade remaining Delivery Controllers**.

After completing the upgrade and confirming completion, close and then reopen Studio. Studio might prompt for an extra site upgrade to register the Controller's services to the site, or to create a zone ID if it does not exist.

Step 11: Upgrade VDAs

> **Important:**
>
> If you're upgrading a VDA to version 1912 or later, see Upgrade VDAs to 1912 or later.

Run the product installer on machines containing VDAs.

If you used Machine Creation Services and a master image to create machines, go to your host and upgrade the VDA on the master image. You can use any of the available VDA installers.

- For graphic interface guidance, see Install VDAs.
- For command line guidance, see Install using the command line.

If you used Citrix Provisioning to create machines, see the Citrix Provisioning product documentation for guidance about upgrading.

Watch this video to learn more:

Step 12: Update machine catalogs and Delivery Groups

- Update catalogs that use machines with upgraded VDAs.
- Upgrade catalogs that use machines with upgraded VDAs.
- Upgrade Delivery Groups that use machines with upgraded VDAs.

Step 13: After the upgrade

After completing an upgrade, you can test the newly upgraded site. From Studio, select **Citrix Studio site-name** in the navigation pane. On the **Common Tasks** tab, select **Test Site**. These tests run automatically after you upgrade the database, but you can run them again at any time.

The tests might fail for a Controller on Windows Server 2016 when a local Microsoft SQL Server Express is used for the site database, if the SQL Server Browser Service is not started. To avoid this:

- Enable the SQL Server Browser Service (if necessary) and then start it.
- Restart the SQL Server (SQLEXPRESS) service.

Upgrade other components in your deployment. For guidance, see the following product documentation:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

If you need to replace the Microsoft SQL Server Express LocalDB software with a later version, see Replace SQL Server Express LocalDB.

Dbschema upgrade

When you update your deployment to a new CU, several database schemas can be upgraded. The following table lists which database schemas are upgraded in the process:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	1912 CU6	1912 CU7	1912 CU8
7.15 RTM/CU	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; logging	Site; Monitor; Config; logging
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU1		Site; Config	Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU2			Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU4					Site; Config	Site; Config	Site; Config	Site; Monitor; Config
1912 CU5						Site; Config	Site; Config	Site; Monitor; Config
1912 CU6							Config	Monitor; Config
1912 CU7								Monitor; Config

Definition of terms:

- Site: Site Datastore. Dbschema update is made to the Site Datastore.
- Monitor: Monitor Datastore. Dbschema update is made to the Monitor Datastore.
- Config: Configuration table. Desktop Studio version, Licensing information, or both are updated in the Configuration table.
- Logging: Logging Datastore. Dbschema update is made to the Logging Datastore.

Upgrade VDAs to 1912 or later

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 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.

If you don't know whether your VDA has PvD installed, run the installer for the new VDA (1912 LTSR or later) on the machine or image.

- If PvD is installed, a message appears, indicating there is an incompatible component.
  - From the graphical interface, click **Cancel** on the page containing the message, and then confirm that you want to close the installer.
  - From the CLI, the command simply fails with the displayed message.
- If PvD is not installed, the upgrade proceeds.

What to do

If the VDA does not have PvD installed, follow the usual upgrade procedure.

If the VDA has PvD installed:

1. Uninstall the current VDA. For details, see Remove components.
2. Install the new VDA.

If you want to continue using PvD on your Windows 7 or Windows 10 (1607 and earlier, without updates) machines, VDA 7.15 LTSR is the latest supported version.

Limitations

The following limitations apply to upgrades:

- **Selective component install:** If you install or upgrade any components to the new version but choose not to upgrade other components (on different machines) that require upgrade, Studio

reminds you. For example, let's say an upgrade includes new versions of the Controller and Studio. You upgrade the Controller but you do not run the installer on the machine where Studio is installed. Studio will not let you continue to manage the site until you upgrade Studio.

You do not have to upgrade VDAs, but Citrix recommends upgrading all VDAs to enable you to use all available features.

- **Early Release or Technology Preview versions:** You cannot upgrade from an Early Release, Technology Preview, or preview version.
- **Components on earlier operating systems:** You cannot install current VDAs on operating systems that are no longer supported by Microsoft or Citrix. For more information, see Earlier operating systems.
- **Mixed environments/sites:** If you must continue to run earlier version sites and current version sites, see Mixed environment considerations.
- **Product selection:** When you upgrade from an earlier version, you do not choose or specify the product (Citrix Virtual Apps or Citrix Virtual Apps and Desktops) that was set during the installation.

Mixed environment considerations

When you upgrade, Citrix recommends that you upgrade all components and VDAs so that you can access all the new and enhanced features in your edition and version.

For example, although you can use current VDAs in deployments containing earlier Controller versions, new features in the current release might not be available. VDA registration issues can also occur when using non-current versions.

In some environments, you might not be able to upgrade all VDAs to the most current version. In that case, when you create a machine catalog, you can specify the VDA version installed on the machines. (This is called the functional level.) By default, this setting specifies the minimum recommended VDA version. The default value is sufficient for most deployments. Consider changing the setting to an earlier version only if the catalog contains VDAs earlier than the default. Mixing VDA versions in a machine catalog is not recommended.

If a catalog is created with the default minimum VDA version setting, and one or more machines has a VDA earlier than the default version, those machines cannot register with the Controller, and will not work.

For more information, see VDA versions and functional levels.

Multiple sites with different versions

When your environment contains sites with different product versions (for example, a XenDesktop 7.18 site and a Citrix Virtual Apps and Desktops 1909 site), Citrix recommends using StoreFront to aggregate applications and desktops from different product versions. For details, see the StoreFront documentation.

In a mixed environment, continue using the Studio and Director versions for each release, but ensure that different versions are installed on separate machines.

Earlier operating systems

Let's say you installed an earlier version of a component on a machine that was running a supported operating system (OS) version. Now, you want to use a newer component version, but that OS is no longer supported for the current version of the component.

For example, assume that you installed a server VDA on a Windows Server 2008 R2 machine. Now you want to upgrade that VDA to the current release, but Windows Server 2008 R2 is not supported in the current release you're upgrading to.

If you try to install or upgrade a component on an operating system that is no longer allowed, an error message displays, such as "Cannot be installed on this operating system".

These considerations apply to upgrading Current Release and Long Term Service Release versions. (It does not affect applying CUs to an LTSR version.)

Follow the links to learn which OSs are supported:

- For LTSRs, select your LTSR version from the main Citrix Virtual Apps and Desktops product documentation page.
  - System requirements.
  - Components lists in articles in the What's new category.
- For CRs (Current Releases):
  - Delivery Controller, Studio, Director, VDAs, Universal Print Server
  - Federated Authentication Service
  - For StoreFront, Self-Service Password Reset, and Session Recording, see the system requirements article for the current release.

Invalid operating systems

The following table lists the earlier operating systems that are not valid for installing/upgrading components in the current release. It indicates the latest valid component version supported for each

listed OS, and the component version when installation and upgrade became invalid.

The operating systems in the table include service packs and updates.

Operating system	Component/feature	Latest valid version	Install/upgrade not possible as of version
Windows 7 and Windows 8	VDA	7.15 LTSR	7.16
Windows 7 and Windows 8	Other installer components	7.17	7.18
Windows 10 versions earlier than 1607	VDA	7.15 LTSR	7.16
Windows 10 x86 version	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Other installer components	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	Other installer components	7.17	7.18
Windows Server 2012 R2	Other installer components *	1912 LTSR	2003
Windows Server 2012 R2	Server VDI	7.15 LTSR	7.16

Windows XP and Windows Vista are not valid for any 7.x components or technologies.

* Applies to Delivery Controller, Studio, Director, and VDAs.

What you can do

You have choices. You can:

- Continue with the current OS
- Reimage or upgrade the machine
- Add new machines and then remove old machines

Continue with the current OS These methods are feasible for VDAs. If you want to continue using machines with the earlier OS, you can choose one of the following:

- Continue using the installed component version.
- Download the latest valid component version and then upgrade the component to that version. (This assumes that the latest valid component version isn't already installed.)

For example, you have a 7.14 VDA on a Windows 7 SP1 machine. The latest valid VDA version on Windows 7 OS machines is XenApp and XenDesktop 7.15 LTSR. You can either continue using 7.14, or download a 7.15 LTSR VDA and then upgrade your VDA to that version. Those earlier VDA versions work in deployments containing Delivery Controllers with newer versions. For example, a 7.15 LTSR VDA can connect to a Citrix Virtual Apps and Desktops 7 1808 Controller.

Reimage or upgrade the machine These methods are feasible for VDAs and other machines that do not have core components (such as Delivery Controllers) installed. Choose one of the following:

- After taking the machine out of service (turning on maintenance mode and allowing all sessions to close), you can reimage it to a supported Windows OS version, and then install the latest version of the component.
- To upgrade the OS without reimaging, uninstall the Citrix software before upgrading the OS. Otherwise, the Citrix software will be in an unsupported state. Then, install the new component.

Add new machines and then remove old machines This method is feasible if you must upgrade the OS on machines containing a Delivery Controller or other core component.

Citrix recommends that all Controllers in a site have the same OS. The following upgrade sequence minimizes the interval when different Controllers have different OSs.

1. Take a snapshot of all Delivery Controllers in the site and then back up the site database.
2. Install new Delivery Controllers on clean servers with supported operating systems. For example, install a Controller on two Windows Server 2016 machines.
3. Add the new Controllers to the site.
4. Remove the Controllers that are running on operating systems that are not valid for the current release. For example, remove two Controllers on two Windows Server 2008 R2 machines. Follow the recommendations for removing Controllers in Delivery Controllers.

Preparation

Before beginning an upgrade, review the following information and complete necessary tasks.

Choose an installer and interface

Use the full-product installer from the product ISO to upgrade components. You can upgrade VDAs using the full-product installer or one of the standalone VDA installers. All installers offer graphical

and command line interfaces.

For more information, see Installers.

Installation specifics: After you complete any preparation work and are ready to start the installer, the installation article shows you what you will see (if you're using the graphical interface) or what to type (if you're using the command-line interface).

- Install/upgrade core components using the graphical interface
- Install/upgrade core components using the command line
- Install/upgrade VDAs using the graphical interface
- Install/upgrade VDAs using the command line

If you originally installed a single-session VDA with the `VDAWorkstationCoreSetup.exe` installer, Citrix recommends using that installer to upgrade it. If you use the full-product VDA installer or the `VDAWorkstationSetup.exe` installer to upgrade the VDA, the components that were originally excluded might be installed, unless you expressly omit/exclude them from the upgrade.

When upgrading a VDA to this release, a machine restart occurs during the upgrade process. (This requirement started with the 7.17 release.) This cannot be avoided. The upgrade resumes automatically after the restart (unless you specify `/noresume` on the command line).

Database actions

Back up the site, monitoring, and configuration logging databases. Follow the instructions in CTX135207. If any issues are discovered after the upgrade, you can restore the backup.

For information about upgrading SQL Server versions that are no longer supported, see SQL Server version check. (This refers to the SQL Server that is used for the site, monitor, and configuration logging databases.)

Microsoft SQL Server Express LocalDB is installed automatically, for use with Local Host Cache. If you need to replace an earlier version, the new version must be at least SQL Server Express 2017 LocalDB CU16. For details about replacing SQL Server Express LocalDB with a new version after you upgrade the components and the site, see Replace SQL Server Express LocalDB.

Ensure that your Citrix licensing is up-to-date

For a comprehensive look at managing Citrix Licensing, see Activate, upgrade, and manage Citrix licenses.

You can use the full-product installer to upgrade the License Server. Or, you can download and upgrade the license components separately. See Upgrade.

Before upgrading, be sure your Customer Success Services / Software Maintenance / Subscription Advantage date is valid for the new product version. If you are upgrading from an earlier 7.x product version, the date must be at least 2019.1115.

Ensure that your Citrix License Server is compatible

Ensure that your Citrix License Server is compatible with the new version. There are two ways to do this:

- Before upgrading any other Citrix components, run the `XenDesktopServerSetup.exe` installer from the ISO layout on the machine containing a Delivery Controller. If there are any incompatibility issues, the installer reports it with recommended steps to resolve the issues.
- From the `XenDesktop Setup` directory on the installation media, run the command: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`.The display indicates whether the License Server is compatible. If the License Server is incompatible, upgrade the license server.

Back up any StoreFront modifications

Before starting an upgrade, if you have made modifications to files in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, such as *default.ica* and *usernamepassword.tfrm*, back them up for each store. After the upgrade you can restore them to reinstate your modifications.

Close applications and consoles

Before starting an upgrade, close all programs that might potentially cause file locks, including administration consoles and PowerShell sessions.

Restarting the machine ensures that any file locks are cleared, and that there are no Windows updates pending.

Before starting an upgrade, stop and disable any third-party monitoring agent services.

Ensure that you have proper permissions

In addition to being a domain user, you must be a local administrator on the machines where you are upgrading product components.

The site database and the site can be upgraded automatically or manually. For an automatic database upgrade, the Studio user's permissions must include the ability to update the SQL Server database

schema (for example, the `db_securityadmin` or `db_owner` database role). For details, see Databases.

If the Studio user does not have those permissions, initiating a manual database upgrade generates scripts. The Studio user runs some of the scripts from Studio. The database administrator runs other scripts, using a tool such as SQL Server Management Studio.

Other preparation tasks

- Back up templates and upgrade hypervisors, if needed
- Complete any other preparation tasks dictated by your business continuity plan.

Preliminary site tests

When you upgrade Delivery Controllers and a site, preliminary site tests run before the actual upgrade begins. These tests verify:

- The site database can be reached and has been backed up
- Connections to essential Citrix services are working correctly
- The Citrix License Server address is available
- The configuration logging database can be reached

After the tests run, you can view a report of the results. You can then fix any issues that were detected, and run the tests again. Failure to run the preliminary site tests and then resolve any issues can impact how your site works.

The report containing the test results is an HTML file (`PreliminarySiteTestResult.html`) in the same directory as the installation logs. That file is created if it does not exist. If the file exists, its content is overwritten.

Run the tests

- When you're using the installer's graphical interface to upgrade, the wizard includes a page where you can start the tests and then display the report. After the tests run and you have viewed the report and resolved any issues that were found, you can rerun the tests. When the tests complete successfully, click Next to continue with the wizard.
- When you're using the command-line interface to upgrade, the tests run automatically. By default, if a test fails, the upgrade is not performed. After you view the report and resolve issues, rerun the command.

Citrix recommends always running the preliminary site tests and then resolving any issues before you continue the Controller and site upgrade. The potential benefit is well worth the few moments to run the tests. However, you can override this recommended action.

- When upgrading with the graphical interface, you can choose to skip the tests and continue with the upgrade.
- When upgrading from the command line, you cannot skip the tests. By default, a failed site test causes the installer to fail, without performing the upgrade. In most cases, if you include the `/ignore_site_test_failure` option, any test failures are ignored and the upgrade proceeds. (See SQL Server version check for exceptions.)

When upgrading multiple Controllers

When you start an upgrade on one Controller, and then start an upgrade of another Controller in the same site (before the first upgrade completes):

- If the preliminary site tests have completed on the first Controller, the preliminary site tests page does not appear in the wizard on the other Controller.
- If the tests on the first Controller are ongoing when you start the upgrade on the other Controller, the site tests page appears in the wizard on the other Controller. However, if the tests on the first Controller finish, only the test results from the first Controller are retained.

Test failures not related to the site's health

- If the preliminary site tests fail due to insufficient memory, make more memory available and then rerun the tests.
- If you have permission to upgrade, but not run site tests, the preliminary site tests fail. To resolve this, rerun the installer with a user account that has permission to run the tests.

SQL Server version check

A successful Citrix Virtual Apps and Desktops deployment requires a supported version of Microsoft SQL Server for the site, monitor, and configuration logging databases. Upgrading a Citrix deployment with a SQL Server version that's no longer supported can result in functionality issues, and the site will be unsupported.

To learn which SQL Server versions are supported for the Citrix release you're upgrading to, see the System requirements article for that release.

When upgrading a Controller, the Citrix installer checks the currently installed SQL Server version used for the site, monitor, and configuration logging databases.

- If the check determines that the currently installed SQL Server version is not a supported version in the Citrix release you're upgrading to:
  - Graphical interface: The upgrade halts with a message. Click **I understand** and then click **Cancel** to close the Citrix installer. (You cannot continue with the upgrade.)
  - Command-line interface: the command fails (even if you included the /`ignore_db_check_failur` option with the command).

  Upgrade the SQL Server version, and then start the Citrix upgrade again.
- If the check cannot determine which SQL Server version is currently installed, see if your currently installed version is supported in the version you're upgrading to (System requirements).
  - Graphical interface: The upgrade halts with a message.
    - If the currently installed SQL Server version is supported, click **I understand** to close the message, and then click **Next** to continue with the Citrix upgrade.
    - If the currently installed SQL Server version is not supported, click **I understand** to close the message, and then click **Cancel** to end the Citrix upgrade. Upgrade your SQL Server to a supported version and then start the Citrix upgrade again.
  - Command-line interface: The command fails with a message. After closing the message:
    - If the currently installed SQL Server version is supported, run the command again with the /`ignore_db_check_failure` option.
    - If the currently installed SQL Server version is not supported, upgrade your SQL Server to a supported version. Run the command again to start the Citrix upgrade.

Upgrading SQL Server

If you bring up new SQL Server servers and migrate the site database, then connection strings must be updated.

If the site currently uses SQL Server Express (that Citrix installed automatically during site creation):

1. Install the latest SQL Server Express version.
2. Detach the database.
3. Attach the database to the new SQL Server Express.
4. Migrate connection strings.

For more information, see Configuring connection strings and the Microsoft SQL Server product documentation.

Replace SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB is a feature of SQL Server Express that Local Host Cache uses on a standalone basis. Local Host Cache does not require any components of SQL Server Express other than SQL Server Express LocalDB.

If you installed a Delivery Controller version earlier than 1912 and then upgrade your deployment to version 1912 or later, Citrix does not automatically upgrade the SQL Server Express LocalDB version. Why not? Because you might have non-Citrix components that rely on SQL Server Express LocalDB. If you have non-Citrix components that are using SQL Server Express LocalDB, ensure that upgrading SQL Server Express LocalDB does not disrupt those components. To upgrade (replace) the SQL Server Express LocalDB version, follow the guidance in this section.

- **When upgrading Delivery Controllers to Citrix Virtual Apps and Desktops version 1912, 1912 LTSR, or 2003:** Upgrading SQL Server Express LocalDB is optional. Local Host Cache works properly, with no loss of functionality, regardless of whether you upgrade SQL Server Express LocalDB. We added the option to move to a newer version of SQL Server Express LocalDB in case there are concerns about end of support from Microsoft for SQL Server Express LocalDB 2014.
- **When upgrading Delivery Controllers to Citrix Virtual Apps and Desktops versions newer than 2003:** The minimum supported version is SQL Server Express 2017 LocalDB Cumulative Update (CU) 16. If you originally installed a Delivery Controller earlier than version 1912, and have not replaced SQL Server Express LocalDB with a newer version since then, you must replace that database software now. Otherwise, Local Host Cache will not work.

What you need:

- The Citrix Virtual Apps and Desktops installation media (for the version you've upgraded to). The media contains a copy of Microsoft SQL Server Express LocalDB 2017 CU 16.
- A Windows Sysinternals tool that you download from Microsoft.

Procedure:

1. Complete the upgrade of your Citrix Virtual Apps and Desktops components, databases, and site. (Those database upgrades affect the site, monitoring, and configuration logging databases. They do not affect the Local Host Cache database that uses SQL Server Express LocalDB.)
2. On the Delivery Controller, download `PsExec` from Microsoft. See the Microsoft document PsExec v2.2.
3. Stop the Citrix High Availability Service.
4. From the command prompt, run `PsExec` and switch to the Network Service account.

   ```
   psexec -i -u "NT AUTHORITY\NETWORK SERVICE"cmd
   ```


Optionally, you can use `whoami` to confirm that the command prompt is running as the Network Service account.

```
whoami

nt authority\network service
```

5. Move to the folder containing SqlLocalDB.

```
cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

6. Stop and delete `CitrixHA` (LocalDB).

```
SqlLocalDB stop CitrixHA

SqlLocalDB delete CitrixHA
```

7. Remove the related files in `C:\Windows\ServiceProfiles\NetworkService`.

```
1 HADatabaseName.*
2 HADatabaseName_log.*
3 HAImportDatabaseName.*
4 HAImportDatabaseName_log.*
5 <!--NeedCopy-->
```

Tip: Your deployment might not have `HAImportDatabaseName.*` and `HAImportDatabaseName_log.*`

8. Uninstall SQL Server Express LocalDB 2014 from the server, using the Windows feature for removing programs.
9. Install SQL Server Express LocalDB 2017. In the `Support > SQLLocalDB` folder on the Citrix Virtual Apps and Desktops installation media, double-click `sqllocaldb.msi`. A restart might be requested to complete the installation. (The new SQLLocalDB resides in `C:\Program Files\Microsoft SQL Server\140\Tools\Binn`.)
10. Start the Citrix High Availability Service.
11. Ensure that the Local Host Cache database was created on each Delivery Controller. This confirms that the High Availability Service (secondary broker) can take over, if needed.
    - On the Controller server, browse to `C:\Windows\ServiceProfiles\NetworkService`.
    - Verify that `HaDatabaseName.mdf` and `HaDatabaseName_log.ldf` are created.

Upgrade a XenApp 6.5 worker to a new VDA

August 29, 2022

After you migrate a XenApp 6.5 farm, you can use your XenApp 6.5 servers that were configured in session-host only mode (also called session-only or worker servers) by removing the earlier software, upgrading the OS, and then installing a new VDA for Server OS.

Although you can upgrade a XenApp 6.5 worker server, installing the current VDA software on a clean machine provides better security.

To upgrade a XenApp 6.5 worker to a new VDA:

1. Remove Hotfix Rollup Pack 7 for XenApp 6.5, using the instructions in the hotfix readme. See CTX202095.
2. Uninstall XenApp 6.5. This process requires several restarts. If an error occurs during the uninstallation, check the uninstall error log referenced in the error message. That log file resides in the folder "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\."
3. Upgrade the server's operating system to a supported version. See the VDA for Server OS section in System requirements. for a list of supported platforms.
4. Install a VDA for Server OS, using an installer provided with this release. See Install VDAs or Install using the command line.

After you install the new VDA, from Studio in the new XenApp Site, create machine catalogs (or edit existing catalogs) for the upgraded workers.

Troubleshoot

Removal of the XenApp 6.5 software fails. The uninstall log contains the message: "Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct."

Cause: The issue occurs on systems where (1) during the initial XenApp 6.5 installation, you indicated that the Citrix XML Service (CtxHttp.exe) should not share a port with IIS, and (2) .NET Framework 3.5.1 is installed.

Resolution:

1. Remove the Web Server (IIS) role using the Windows Remove Server Roles wizard. (You can reinstall the Web Server (IIS) role later.)
2. Restart the server.
3. Using Add/Remove Programs, uninstall Citrix XenApp 6.5 and Microsoft Visual C++ 2005 Redistributable (x64), version 8.0.56336.
4. Restart the server.
5. Install the VDA for Server OS.

Migrate XenApp 6.x

March 24, 2021

> **Important:**
>
> Migrating moves data from an earlier deployment to a newer version. The process includes installing newer components and creating a new Site, exporting data from the older farm, and then importing the data to the new Site.
>
> Open source migration scripts are available at https://github.com/citrix/xa65migrationtool. However, Citrix does not support these scripts.
>
> The remainder of this article contains information that can be used as a reference with the open source migration scripts.

Introduction

You can use the Migration Tool described in this article to migrate from XenApp 6.x to XenApp 7.6. Then, you can upgrade from XenApp 7.6 to a supported LTSR or the current Citrix Virtual Apps and Desktops release; see Upgrade a deployment.

For information about architecture, component, and feature changes that were introduced with the 7.x releases, see Changes in 7.x.

XenApp 6.x Migration Tool

The XenApp 6.x Migration Tool is a collection of PowerShell scripts containing cmdlets that migrate XenApp 6.x (6.0 or 6.5) policy and farm data. On the XenApp 6.x controller server, you run export cmdlets that gather that data into XML files. Then, from the XenApp 7.6 Controller, you run import cmdlets that create objects using the data gathered during the export.

The following sequence summarizes the migration process; details are provided later.

1. On a XenApp 6.0 or 6.5 controller:
    a) Import the PowerShell export modules.
    b) Run the export cmdlets to export policy and/or farm data to XML files.
2. Copy the XML files (and icons folder if you chose not to embed them in the XML files during the export) to the XenApp 7.6 Controller.
3. On the XenApp 7.6 Controller:
    a) Import the PowerShell import modules.

b) Run the import cmdlets to import policy and/or farm data (applications), using the XML files as input.

4. Complete post-migration steps.

Before you run an actual migration, you can export your XenApp 6.x settings and then perform a preview import on the XenApp 7.6 site. The preview identifies possible failure points so you can resolve issues before running the actual import. For example, a preview might detect that an application with the same name already exists in the new XenApp 7.6 site. You can also use the log files generated from the preview as a migration guide.

Unless otherwise noted, the term 6.x refers to XenApp 6.0 or 6.5.

Migration Tool package

The migration tool contains two separate, independent packages:

- **ReadIMA:** Contains the files used to export data from your XenApp 6.x farm, plus shared modules.

Module or file	Description
ExportPolicy.psm1	PowerShell script module for exporting XenApp 6.x policies to an XML file.
ExportXAFarm.psm1	PowerShell script module for exporting XenApp 6.x farm settings to an XML file.
ExportPolicy.psd1	PowerShell manifest file for script module ExportPolicy.psm1.
ExportXAFarm.psd1	PowerShell manifest file for script module ExportXAFarm.psm1.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.
XmlUtilities.psm1	Shared PowerShell script module that contains XML functions.

- **ImportFMA:** Contains the files used to import data to your XenApp 7.6 farm, plus shared modules.

Module or file	Description
ImportPolicy.psm1	PowerShell script module for importing policies to XenApp 7.6.
ImportXAFarm.psm1	PowerShell script module for importing applications to XenApp 7.6
ImportPolicy.psd1	PowerShell manifest file for script module ImportPolicy.psm1.
ImportXAFarm.psd1	PowerShell manifest file for script module ImportXAFarm.psm1.
PolicyData.xsd	XML schema for policy data.
XAFarmData.xsd	XML schema for XenApp farm data.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.
XmlUtilities.psm1	Shared PowerShell script module that contains XML functions.

Limitations

- Not all policies settings are imported; see Policy settings not imported. Settings that are not supported are ignored and noted in the log file.
- While all application details are collected in the output XML file during the export operation, only server-installed applications are imported into the XenApp 7.6 site. Published desktops, content, and most streamed applications are not supported (see the Import-XAFarm cmdlet parameters in Step-by-step: import data for exceptions).
- Application servers are not imported.
- Many application properties are not imported because of differences between the XenApp 6.x Independent Management Architecture (IMA) and the XenApp 7.6 FlexCast Management Architecture (FMA) technologies; see Application property mapping.
- A Delivery Group is created during the import. See Advanced use for details about using parameters to filter what is imported.
- Only Citrix policy settings created with the AppCenter management console are imported; Citrix policy settings created with Windows Group Policy Objects (GPOs) are not imported.
- The migration scripts are intended for migrations from XenApp 6.x to XenApp 7.6 only.
- Nested folders greater than five levels deep are not supported by Studio and will not be imported. If your application folder structure includes folders more than five levels deep, consider

reducing the number of nested folder levels before importing.

Security considerations

The XML files created by the export scripts can contain sensitive information about your environment and organization, such as user names, server names, and other XenApp farm, application, and policy configuration data. Store and handle these files in secure environments.

Carefully review the XML files before using them as input when importing policies and applications, to ensure they contain no unauthorized modifications.

Policy object assignments (previously known as policy filters) control how policies are applied. After importing the policies, carefully review the object assignments for each policy to ensure that there are no security vulnerabilities resulting from the import. Different sets of users, IP addresses, or client names may be applied to the policy after the import. The allow/deny settings may have different meanings after the import.

Logging and error handling

The scripts provide extensive logging that tracks all cmdlet executions, informative messages, cmdlet execution results, warnings, and errors.

- Most Citrix PowerShell cmdlet use is logged. All PowerShell cmdlets in the import scripts that create new site objects are logged.
- Script execution progress is logged, including the objects being processed.
- Major actions that affect the state of the flow are logged, including flows directed from the command line.
- All messages printed to the console are logged, including warnings and errors.
- Each line is time-stamped to the millisecond.

Citrix recommends specifying a log file when you run each of the export and import cmdlets.

If you do not specify a log file name, the log file is stored in the current user's home folder (specified in the PowerShell $HOME variable) if that folder exists; otherwise, it is placed in the script's current execution folder. The default log name is "XFarmYYYYMMDDHHmmSS-xxxxxx"where the last six digits constitute a random number.

By default, all progress information is displayed. To suppress the display, specify the NoDetails parameter in the export and import cmdlet.

Generally, a script stops execution when an error is encountered, and you can run the cmdlet again after clearing the error conditions.

Conditions that are not considered errors are logged; many are reported as warnings, and script execution continues. For example, unsupported application types are reported as warnings and are not imported. Applications that already exist in the XenApp 7.6 site are not imported. Policy settings that are deprecated in XenApp 7.6 are not imported.

The migration scripts use many PowerShell cmdlets, and all possible errors might not be logged. For additional logging coverage, use the PowerShell logging features. For example, PowerShell transcripts log everything that is printed to the screen. For more information, see the help for the Start-Transcript and Stop-Transcript cmdlets.

Requirements, preparation, and best practices

To migrate, you must use the Citrix XenApp 6.5 SDK. Download that SDK from https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.html.

Review this entire article before beginning a migration.

You should understand basic PowerShell concepts about execution policy, modules, cmdlets, and scripts. Although extensive scripting expertise is not required, you should understand the cmdlets you execute. Use the Get-Help cmdlet to review each migration cmdlet's help before executing it. For example: `Get-Help -full Import-XAFarm`.

Specify a log file on the command line and always review the log file after running a cmdlet. If a script fails, check and fix the error identified in the log file and then run the cmdlet again.

Good to know

- To facilitate application delivery while two deployments are running (the XenApp 6.x farm and the new XenApp 7.6 site), you can aggregate both deployments in StoreFront or Web Interface. See the eDocs documentation for your StoreFront or Web Interface release.
- Application icon data is handled in one of two ways:
  - If you specify the EmbedIconData parameter in the Export-XAFarm cmdlet, exported application icon data is embedded in the output XML file.
  - If you do not specify the EmbedIconData parameter in the Export-XAFarm cmdlet, exported application icon data is stored under a folder named by appending the string "-icons"to the base name of the output XML file. For example, if the XmlOutputFile parameter is "FarmData.xml"then the folder "FarmData-icons"is created to store the application icons.

    The icon data files in this folder are .txt files that are named using the browser name of the published application (although the files are .txt files, the stored data is encoded binary

icon data, which can be read by the import script to re-create the application icon). During the import operation, if the icon folder is not found in the same location as the import XML file, generic icons are used for each imported application.

- The names of the script modules, manifest files, shared module, and cmdlets are similar. Use tab completion with care to avoid errors. For example, Export-XAFarm is a cmdlet. ExportXAFarm.psd1 and ExportXAFarm.psm1 are files that cannot be executed.
- In the step-by-step sections below, most <string> parameter values show surrounding quotation marks. These are optional for single-word strings.

For exporting from the XenApp 6.x server

- The export must be run on a XenApp 6.x server configured with the controller and session-host (commonly known as controller) server mode.
- To run the export cmdlets, you must be a XenApp administrator with permission to read objects. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- Ensure the XenApp 6.x farm is in a healthy state before beginning an export. Back up the farm database. Verify the farm's integrity using the Citrix IMA Helper utility (CTX133983). From the IMA Datastore tab, run a Master Check (and then use the DSCheck option to resolve invalid entries). Repairing issues before the migration helps prevent export failures. For example, if a server was removed improperly from the farm, its data might remain in the database; that could cause cmdlets in the export script to fail (for example, Get-XAServer -ZoneName). If the cmdlets fail, the script fails.
- You can run the export cmdlets on a live farm that has active user connections; the export scripts read only the static farm configuration and policy data.

For importing to the XenApp 7.6 server

- You can import data to XenApp 7.6 deployments (and later supported versions). You must install a XenApp 7.6 Controller and Studio, and create a site before importing the data you exported from the XenApp 6.x farm. Although VDAs are not required to import settings, they allow application file types to be made available.
- To run the import cmdlets, you must be a XenApp administrator with permission to read and create objects. A Full Administrator has these permissions. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- No other user connections should be active during an import. The import scripts create many new objects, and disruptions may occur if other users are changing the configuration at the same time.

Remember that you can export data and then use the -Preview parameter with the import cmdlets to see what would happen during an actual import, but without actually importing anything. The logs will indicate exactly what would happen during an actual import; if errors occur, you can resolve them before starting an actual import.

Step-by-step: export data

Complete the following steps to export data from a XenApp 6.x controller to XML files.

1. Download the XAMigration.zip migration tool package from the Citrix download site. For convenience, place it on a network file share that can be accessed by both the XenApp 6.x farm and the XenApp 7.6 site. Unzip XAMigration.zip on the network file share. There should be two zip files: ReadIMA.zip and ImportFMA.zip.
2. Log on to the XenApp 6.x controller as a XenApp administrator with at least read-only permission and Windows permission to run PowerShell scripts.
3. Copy ReadIMA.zip from the network file share to the XenApp 6.x controller. Unzip and extract ReadIMA.zip on the controller to a folder (for example: C:\XAMigration).
4. Open a PowerShell console and set the current directory to the script location. For example: `cd C:\XAMigration`.
5. Check the script execution policy by running `Get-ExecutionPolicy`.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example: `Set-ExecutionPolicy RemoteSigned`.
7. Import the module definition files ExportPolicy.psd1 and ExportXAFarm.psd1: `Import-Module .\\ExportPolicy.psd1` and `Import-Module .\\ExportXAFarm.psd1`.

   Good to know

   - If you intend to export only policy data, you can import only the ExportPolicy.psd1 module definition file. Similarly, if you intend to export only farm data, import only ExportXAFarm.psd1.
   - Importing the module definition files also adds the required PowerShell snap-ins.
   - Do not import the .psm1 script files.

8. To export policy data and farm data, run the following cmdlets.

Policy data: Run `Export-Policy`.

Parameter	Description
-XmlOutputFile “*string*.xml”	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist. Default: None; this parameter is required.
-LogFile *string*	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file’s content is overwritten. Default: See Logging and error handling.
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#”to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console

Example: The following cmdlet exports policy information to the XML file named MyPolicies.xml. The operation is logged to the file named MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies
.Log"
```

Farm data: Run `Export-XAFarm`.

Parameter	Description
XmlOutputFile "*string*.xml"	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist. Default: None; this parameter is required.
-LogFile "*string*"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#"to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-IgnoreAdmins	Do not export administrator information. See Advanced use. Default: False; administrator information is exported
-IgnoreApps	Do not export application information. See Advanced use. Default: False; application information is exported
-IgnoreServers	Do not export server information. Default: False: server information is exported

Parameter	Description
-IgnoreZones	Do not export zone information. Default: False; zone information is exported.
-IgnoreOthers	Do not export information such as configuration logging, load evaluators, load balancing policies, printer drivers, and worker groups. Default: False; other information is exported. The purpose of this switch is to allow you to proceed with an export when an error exists that would not affect the actual data being used for the exporting or importing process.
-AppLimit *integer*	Number of applications to be exported. See Requirements, preparation, and best practices. Default: All applications are exported
-EmbedIconData	Embed application icon data in the same XML file as the other objects. Default: Icons are stored separately. See Requirements, preparation, and best practices
-SkipApps *integer*	Number of applications to skip. See Advanced use. Default: No applications are skipped

Example: The following cmdlet exports farm information to the XML file named MyFarm.xml. The operation is logged to the file MyFarm.log. A folder named "MyFarm-icons"is created to store the application icon data files; this folder is at the same location as MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

After the export scripts complete, the XML files specified on the command lines contain the policy and XenApp farm data. The application icon files contain icon data files, and the log file indicate what occurred during the export.

Step-by-step: import data

Remember that you can run a preview import (by issuing the `Import-Policy` or `Import-XAFarm` cmdlet with the Preview parameter) and review the log files before performing an actual import.

Complete the following steps to import data to a XenApp 7.6 site, using the XML files generating from the export.

1. Log on to the XenApp 7.6 controller as an administrator with read-write permission and Windows permission to run PowerShell scripts.
2. If you have not unzipped the migration tool package XAMigration on the network file share, do so now. Copy ImportFMA.zip from the network file share to the XenApp 7.6 Controller. Unzip and extract ImportFMA.zip on the Controller to a folder (for example: C:\XAMigration).
3. Copy the XML files (the output files generated during the export) from the XenApp 6.x controller to the same location on the XenApp 7.6 Controller where you extracted the ImportFMA.zip files.

   If you chose not to embed the application icon data in the XML output file when you ran the Export-XAFarm cmdlet, be sure to copy the icon data folder and files to the same location on the XenApp 7.6 controller as the output XML file containing the application data and the extracted ImportFMA.zip files.
4. Open a PowerShell console and set the current directory to the script location: `cd C:\XAMigration`.
5. Check the script execution policy by running `Get-ExecutionPolicy`.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example: `Set-ExecutionPolicy RemoteSigned`.
7. Import the PowerShell module definition files ImportPolicy.psd1 and ImportXAFarm.psd1: `Import-Module .\\ImportPolicy.psd1` and `Import-Module .\\ImportXAFarm.psd1`.

   Good to know:

   - If you intend to import only policy data, you can import only the ImportPolicy.psd1 module definition file. Similarly, if you intend to import only farm data, import only ImportXAFarm.psd1.
   - Importing the module definition files also adds the required PowerShell snap-ins.
   - Do not import the .psm1 script files.
8. To import policy data and application data, run the following cmdlets.

Policy data: Run `Import-Policy`, specifying the XML file containing the exported policy data.

Parameter	Description
-XmlInputFile "*string*.xml"	XML input file name; this file contains data collected from running the Export-Policy cmdlet. Must have an .xml extension. Default: None; this parameter is required.

Parameter	Description
-XsdFile "*string*"	XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use. Default: PolicyData.XSD
-LogFile "*string*"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet. Default: See Logging and error handling.
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#"to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import. Default: False; a real import occurs

Example: The folowing cmdlet imports policy data from the XML file named MyPolcies.xml. The operation is logged to the file named MyPolicies.log.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies.
Log"
```


Applications: Run `Import-XAFarm`, specifying a log file and the XML file containing the exported farm data.

Parameter	Description
-XmlInputFile "*string*.xml"	XML input file name; this file contains data collected from running the Export-XAFarm cmdlet. Must have an .xml extension. Default: None; this parameter is required.
-XsdFile "*string*"	XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use. Default: XAFarmData.XSD
-LogFile "*string*"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#"to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console

Parameter	Description
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import. Default: False; a real import occurs
-DeliveryGroupName "*string*"	Delivery Group name for all imported applications. See Advanced use. Default: "*xenapp-farm-name* - Delivery Group"
-MatchFolder "*string*"	Import only those applications in folders with names that match the string. See Advanced use. Default: No matching occurs
-NotMatchFolder "*string*"	Import only those applications in folders with names that do not match the string. See Advanced use. Default: No matching occurs
-MatchServer "*string*"	Import only those applications from servers whose names match the string. See Advanced use.
-NotMatchServer "*string*"	Import only those applications from servers whose names do not match the string. See Advanced use. Default: No matching occurs
-MatchWorkerGroup "*string*"	Import only those applications published to worker groups with names that match the string. See Advanced use. Default: No matching occurs
-NotMatchWorkerGroup "*string*"	Import only those applications published to worker groups with names that do not match the string. See Advanced use. Default: No matching occurs
-MatchAccount "*string*"	Import only those applications published to user accounts with names that match the string. See Advanced use. Default: No matching occurs
-NotMatchAccount "*string*"	Import only those applications published to user accounts with names that do not match the string. See Advanced use. Default: No matching occurs

Parameter	Description
-IncludeStreamedApps	Import applications of type "StreamedToClientOrServerInstalled". (No other streamed applications are imported.) Default: Streamed applications are not imported
-IncludeDisabledApps	Import applications that have been marked as disabled. Default: Disabled applications are not imported

Example: The following cmdlet imports applications from the XML file named MyFarm.xml. The operation is logged to the file named MyFarm.log.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

After the import completes successfully, complete the post-migration tasks.

Post-migration tasks

After successfully importing XenApp 6.x policies and farm settings into a XenApp 7.6 site, use the following guidance to ensure that the data has been imported correctly.

Policies and policy settings

Importing policies is essentially a copy operation, with the exception of deprecated settings and policies, which are not imported. The post-migration check essentially involves comparing the two sides.

1. The log file lists all the policies and settings imported and ignored. First, review the log file and identify which settings and policies were not imported.
2. Compare the XenApp 6.x policies with the policies imported to XenApp 7.6. The values of the settings should remain the same (except for deprecated policy settings, as noted in the next step).
    - If you have a small number of policies, you can perform a side-by-side visual comparison of the policies displayed in the XenApp 6.x AppCenter and the policies displayed in the XenApp 7.6 Studio.
    - If you have a large number of policies, a visual comparison might not be feasible. In such cases, use the policy export cmdlet (Export-Policy) to export the XenApp 7.6 policies to a different XML file, and then use a text diff tool (such as windiff) to compare that file's data to the data in the XML file used during the policy export from XenApp 6.x.

3. Use the information in the Policy settings not imported section to determine what might have changed during the import. If a XenApp 6.x policy contains only deprecated settings, as a whole policy, it is not imported. For example, if a XenApp 6.x policy contains only HMR test settings, that policy is completely ignored because there is no equivalent setting supported in XenApp 7.6.

   Some XenApp 6.x policy settings are no longer supported, but the equivalent functionality is implemented in XenApp 7.6. For example, in XenApp 7.6, you can configure a restart schedule for Server OS machines by editing a Delivery Group; this functionality was previously implemented through policy settings.

4. Review and confirm how filters will apply to your XenApp 7.6 site versus their use in XenApp 6.x; significant differences between the XenApp 6.x farm and the XenApp 7.6 site could change the effect of filters.

Filters

Carefully examine the filters for each policy. Changes may be required to ensure they still work in XenApp 7.6 as originally intended in XenApp 6.x.

Filter	Considerations
Access Control	Access Control Should contain the same values as the original XenApp 6.x filters and should work without requiring changes.
Citrix CloudBridge	A simple Boolean; should work without requiring changes. (This product is now known as NetScaler SD-WAN.)
Client IP Address	Lists client IP address ranges; each range is either allowed or denied. The import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Client Name	Similar to the Client IP Address filter, the import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.

Filter	Considerations
Organizational Unit	Values might be preserved, depending on whether or not the OUs can be resolved at the time they are imported. Review this filter closely, particularly if the XenApp 6.x and XenApp 7.6 machines reside in different domains. If you do not configure the filter values correctly, the policy may be applied to an incorrect set of OUs. The OUs are represented by names only, so there is a small chance that an OU name will be resolved to an OU containing different members from the OUs in the XenApp 6.x domain. Even if some of the values of the OU filter are preserved, you should carefully review the values.
User or Group	Values might be preserved, depending on whether or not the accounts can be resolved at the time they are imported. Similar to OUs, the accounts are resolved using names only, so if the XenApp 7.6 site has a domain with the same domain and user names, but are actually two different domains and users, the resolved accounts could be different from the XenApp 6.x domain users. If you do not properly review and modify the filter values, incorrect policy applications can occur.
Worker Group	Worker groups are not supported in XenApp 7.6. Consider using the Delivery Group, Delivery Group Type, and Tag filters, which are supported in XenApp 7.6 (not in XenApp 6.x). **Delivery Group:** Allows policies to be applied based on Delivery Groups. Each filter entry specifies a Delivery Group and can be allowed or denied. **Delivery Group Type:** Allows policies to be applied based on the Delivery Group types. Each filter specifies a Delivery Group type that can be allowed or denied. **Tag:** Specifies policy application based on tags created for the VDA machines. Each tag can be allowed or denied.

To recap, filters that involve domain user changes require the most attention if the XenApp 6.x farm and the XenApp 7.6 site are in different domains. Because the import script uses only strings of domain and user names to resolve users in the new domain, some of the accounts might be resolved and others might not. While there is only a small chance that different domains and users have the same name, you should carefully review these filters to ensure they contain correct values.

Applications

The application importing scripts do not just import applications; they also create objects such as Delivery Groups. If the application import involves multiple iterations, the original application folder hierarchies can change significantly.

1. First, read the migration log files that contain details about which applications were imported, which applications were ignored, and the cmdlets that were used to create the applications.
2. For each application:
    - Visually check to ensure the basic properties were preserved during the import. Use the information in Application property mapping to determine which properties were imported without change, not imported, or initialized using the XenApp 6.x application data.
    - Check the user list. The import script automatically imports the explicit list of users into the application's limit visibility list in XenApp 7.6. Check to ensure that the list remains the same.
3. Application servers are not imported. This means that none of the imported applications can be accessed yet. The Delivery Groups that contain these applications must be assigned machine catalogs that contain the machines that have the published applications' executable images. For each application:
    - Ensure that the executable name and the working directory point to an executable that exists in the machines assigned to the Delivery Group (through the machine catalogs).
    - Check a command line parameter (which may be anything, such as file name, environment variable, or executable name). Verify that the parameter is valid for all the machines in the machine catalogs assigned to the Delivery Group.

Log files

The log files are the most important reference resources for an import and export. This is why existing log files are not overwritten by default, and default log file names are unique.

As noted in Logging and error handling, if you chose to use additional logging coverage with the PowerShell `Start-Transcript` and `Stop-Transcript` cmdlets (which record everything typed and

printed to the console), that output, together with the log file, provides a complete reference of import and export activity.

Using the time stamps in the log files, you can diagnose certain problems. For example, if an export or import ran for a very long time, you could determine if a faulty database connection or resolving user accounts took most of the time.

The commands recorded in the log files also tell you how some objects are read or created. For example, to create a Delivery Group, several commands are executed to not only create the Delivery Group object itself, but also other objects such as access policy rules that allow application objects to be assigned to the Delivery Group.

The log file can also be used to diagnose a failed export or import. Typically, the last lines of the log file indicate what caused the failure; the failure error message is also saved in the log file. Together with the XML file, the log file can be used to determine which object was involved in the failure.

After reviewing and testing the migration, you can:

1. Upgrade your XenApp 6.5 worker servers to current Virtual Delivery Agents (VDAs) by running the 7.6 installer on the server, which removes the XenApp 6.5 software and then automatically installs a current VDA. See Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS for instructions.

   For XenApp 6.0 worker servers, you must manually uninstall the XenApp 6.0 software from the server. You can then use the 7.6 installer to install the current VDA. You cannot use the 7.6 installer to automatically remove the XenApp 6.0 software.

2. From Studio in the new XenApp site, create machine catalogs (or edit existing catalogs) for the upgraded workers.
3. Add the upgraded machines from the machine catalog to the Delivery Groups that contain the applications installed on those VDAs for Windows Server OS.

Advanced use

By default, the `Export-Policy` cmdlet exports all policy data to an XML file. Similarly, `Export-XAFarm` exports all farm data to an XML file. You can use command line parameters to more finely control what is exported and imported.

Export applications partially

If you have a large number of applications and want to control how many are exported to the XML file, use the following parameters:

- AppLimit: Specifies the number of applications to export.

- SkipApps: Specifies the number of applications to skip before exporting subsequent applications.

You can use both of these parameters to export large quantities of applications in manageable chunks. For example, the first time you run `Export-XAFarm`, you want to export only the first 200 applications, so you specify that value in the AppLimit parameter.

```
Export-XAFarm -XmlOutputFile "Apps1-200.xml"
```

The next time you run `Export-XAFarm`, you want to export the next 100 applications, so you use the SkipApps parameter to disregard the applications you've already exported (the first 200), and the AppLimit parameter to export the next 100 applications.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"-AppLimit "100"-SkipApps
 "200"
```

Do not export certain objects

Some objects can be ignored and thus do not need to be exported, particularly those objects that are not imported; see Policy settings not imported and Application property mapping. Use the following parameters to prevent exporting unneeded objects:

- IgnoreAdmins: Do not export administrator objects
- IgnoreServers: Do not export server objects
- IgnoreZones: Do not export zone objects
- IgnoreOthers: Do not export configuration logging, load evaluator, load balancing policy, printer driver, and worker group objects
- IgnoreApps: Do not export applications; this allows you to export other data to an XML output file and then run the export again to export applications to a different XML output file.

You can also use these parameters to work around issues that could cause the export to fail. For example, if you have a bad server in a zone, the zone export might fail; if you include the IgnoreZones parameter, the export continues with other objects.

Delivery Group names

If you do not want to put all of your applications into one Delivery Group (for example, because they are accessed by different sets of users and published to different sets of servers), you can run `Import-XAFarm` multiple times, specifying different applications and a different Delivery Group each time. Although you can use PowerShell cmdlets to move applications from one Delivery Group to another after the migration, importing selectively to unique Delivery Groups can reduce or eliminate the effort of moving the applications later.

- Use the DeliveryGroupName parameter with the `Import-XAFarm` cmdlet. The script creates the specified Delivery Group if it doesn't exist.
- Use the following parameters with regular expressions to filter the applications to be imported into the Delivery Group, based on folder, worker group, user account, and/or server names. Enclosing the regular expression in single or double quotation marks is recommended. For information about regular expressions, see https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expressions?redirectedfrom=MSDN.

  - **MatchWorkerGroup** and **NotMatchWorkerGroup:** For example, for applications published to worker groups, the following cmdlet imports applications in the worker group named "Productivity Apps"to a XenApp 7.6 Delivery Group of the same name.

    ```
    Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.
    log –MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName '
    Productivity Apps'
    ```

  - **MatchFolder** and **NotMatchFolder:** For example, for applications organized in application folders, the following cmdlet imports applications in the folder named "Productivity Apps"to a XenApp 7.6 Delivery Group of the same name.

    ```
    Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport
    .log –MatchFolder 'Productivity Apps' –DeliveryGroupName '
    Productivity Apps'
    ```

    For example, the following cmdlet imports applications in any folder whose name contains "MS Office Apps"to the default Delivery Group.

    ```
    Import-XAFarm -XmlInputFile .\TheFarmApps.XML -MatchFolder "
    .*/MS Office Apps/.*"
    ```

  - **MatchAccount** and **NotMatchAccount:** For example, for applications published to Active Directory users or user groups, the following cmdlet imports applications published to the user group named "Finance Group"to a XenApp 7.6 Delivery Group named "Finance".

    ```
    Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.
    log –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName '
    Finance'
    ```

  - **MatchServer** and **NotMatchServer:** For example, for applications organized on servers, the following cmdlet imports applications associated with the server not named "Current" to a XenApp Delivery Group named "Legacy".

    ```
    Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.
    log -NotMatchServer 'Current'-DeliveryGroupName 'Legacy'
    ```


Customization PowerShell programmers can create their own tools. For example, you can use the export script as an inventory tool to keep track of changes in a XenApp 6.x farm. You can also modify the XSD files or (create your own XSD files) to store additional data or data in different formats in the XML files. You can specify a nondefault XSD file with each of the import cmdlets.

Although you can modify script files to meet specific or advanced migration requirements, support is limited to the scripts in their unmodified state. Citrix Technical Support will recommend reverting to the unmodified scripts to determine expected behavior and provide support, if necessary.

Troubleshooting

- If you are using PowerShell version 2.0 and you added the Citrix Group Policy PowerShell Provider snap-in or the Citrix Common Commands snap-in using the `Add-PSSnapIn` cmdlet, you might see the error message "Object reference not set to an instance of an object"when you run the export or import cmdlets. This error does not affect script execution and can be safely ignored.
- Avoid adding or removing the Citrix Group Policy PowerShell Provider snap-in in the same console session where the export and import script modules are used, because those script modules automatically add the snap-in. If you add or remove the snap-in separately, you might see one of the following errors:
  - "A drive with the name 'LocalGpo'already exists."This error appears when the snap-in is added twice; the snap-in attempts to mount the drive LocalGpo when it's loaded, and then reports the error.
  - "A parameter cannot be found that matches parameter name 'Controller'."This error appears when the snap-in has not been added but the script attempts to mount the drive. The script is not aware that the snap-in was removed. Close the console and launch a new session. In the new session, import the script modules; do not add or remove the snap-in separately.
- When importing the modules, if you right-click a .psd1 file and select **Open** or **Open with PowerShell**, the PowerShell console window will rapidly open and close until you stop the process. To avoid this error, enter the complete PowerShell script module name directly in the PowerShell console window (for example, `Import-Module .\\ExportPolicy.psd1`).
- If you receive a permission error when running an export or import, ensure you are a XenApp administrator with permission to read objects (for export) or read and create objects (for import). You must also have sufficient Windows permission to run PowerShell scripts.
- If an export fails, check that the XenApp 6.x farm is in a healthy state by running the DSMAINT and DSCHECK utilities on the XenApp 6.x controller server.
- If you run a preview import and then later run the import cmdlets again for an actual migration, but discover that nothing was imported, verify that you removed the Preview parameter from

the import cmdlets.

Policy settings not imported

The following computer and user policy settings are not imported because they are no longer supported. Please note, unfiltered policies are never imported. The features and components that support these settings have either been replaced by new technologies/components or the settings do not apply because of architectural and platform changes.

Computer policy settings not imported

- Connection access control
- CPU management server level
- DNS address resolution
- Farm name
- Full icon caching
- Health monitoring, Health monitoring tests
- License server host name, License server port
- Limit user sessions, Limits on administrator sessions
- Load evaluator name
- Logging of logon limit events
- Maximum percent of servers with logon control
- Memory optimization, Memory optimization application exclusion list, Memory optimization interval, Memory optimization schedule: day of month, Memory optimization schedule: day of week, Memory optimization schedule: time
- Offline app client trust, Offline app event logging, Offline app license period, Offline app users
- Prompt for password
- Reboot custom warning, Reboot custom warning text, Reboot logon disable time, Reboot schedule frequency, Reboot schedule randomization interval, Reboot schedule start date, Reboot schedule time, Reboot warning interval, Reboot warning start time, Reboot warning to users, Scheduled reboots
- Shadowing *
- Trust XML requests (configured in StoreFront)
- Virtual IP adapter address filtering, Virtual IP compatibility programs list, Virtual IP enhanced compatibility, Virtual IP filter adapter addresses programs list
- Workload name
- XenApp product edition, XenApp product model
- XML service port

* Replaced with Windows Remote Assistance

User policy settings not imported

- Auto connect client COM ports, Auto connect client LPT ports
- Client COM port redirection, Client LPT port redirection
- Client printer names
- Concurrent logon limit
- Input from shadow connections *
- Linger disconnect timer interval, Linger terminate timer interval
- Log shadow attempts *
- Notify user of pending shadow connections *
- Pre-launch disconnect timer interval, Pre-launch terminate timer interval
- Session importance
- Single Sign-On, Single Sign-On central store
- Users who can shadow other users, Users who cannot shadow other users *

* Replaced with Windows Remote Assistance

Application types not imported

The following application types are not imported.

- Server desktops
- Content
- Streamed applications (App-V is the new method used for streaming applications)

Application property mapping

The farm data import script imports only applications. The following application properties are imported without change.

IMA Property	FMA Property
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Description	Description

IMA Property	FMA Property
DisplayName	PublishedName
Enabled	Enabled
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

IMA and FMA have different restrictions on folder name length. In IMA, the folder name limit is 256 characters; the FMA limit is 64 characters. When importing, applications with a folder path containing a folder name of more than 64 characters are skipped. The limit applies only to the folder name in the folder path; the entire folder path can be longer than the limits noted. To avoid applications from being skipped during the import, Citrix recommends checking the application folder name length and shortening it, if needed, before exporting.

The following application properties are initialized or uninitialized by default, or set to values provided in the XenApp 6.x data:

FMA Property	Value
Name	Initialized to the full path name, which contains the IMA properties FolderPath and DisplayName, but stripped of the leading string "Applications\"
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialized using the XenApp 6.x command line arguments
IconFromClient	Uninitialized; defaults to false
IconUid	Initialized to an icon object created using XenApp 6.x icon data
SecureCmdLineArgumentsEnabled	Uninitialized; defaults to true
UserFilterEnabled	Uninitialized; defaults to false
UUID	Read-only, assigned by the Controller
Visible	Uninitialized; defaults to true

The following application properties are partially migrated:

IMA Property	Comments
FileTypes	Only the file types that exist on the new XenApp site are migrated. File types that do not exist on the new site are ignored. File types are imported only after the file types on the new site are updated.
IconData	New icon objects are created if the icon data has been provided for the exported applications.
Accounts	The user accounts of an application are split between the user list for the Delivery Group and the application. Explicit users are used to initialize the user list for the application. In addition, the "Domain Users"account for the domain of the user accounts is added to the user list for the Delivery Group.

The following XenApp 6.x properties are not imported:

IMA Property	Comments
ApplicationType	Ignored.
HideWhenDisabled	Ignored.
AccessSessionConditions	Replaced by Delivery Group access policies.
AccessSessionConditionsEnabled	Replaced by Delivery Group access policies.
ConnectionsThroughAccessGatewayAllowed	Replaced by Delivery Group access policies.
OtherConnectionsAllowed	Replaced by Delivery Group access policies.
AlternateProfiles	FMA does not support streamed applications.
OfflineAccessAllowed	FMA does not support streamed applications.
ProfileLocation	FMA does not support streamed applications.
ProfileProgramArguments	FMA does not support streamed applications.
ProfileProgramName	FMA does not support streamed applications.
RunAsLeastPrivilegedUser	FMA does not support streamed applications.
AnonymousConnectionsAllowed	FMA uses a different technology to support unauthenticated (anonymous) connections.

IMA Property	Comments
ApplicationId, SequenceNumber	IMA-unique data.
AudioType	FMA does not support advanced client connection options.
EncryptionLevel	SecureICA is enabled/disabled in Delivery Groups.
EncryptionRequired	SecureICA is enabled/disabled in Delivery Groups.
SslConnectionEnabled	FMA uses a different TLS implementation.
ContentAddress	FMA does not support published content.
ColorDepth	FMA does not support advanced window appearances.
MaximizedOnStartup	FMA does not support advanced window appearances.
TitleBarHidden	FMA does not support advanced window appearances.
WindowsType	FMA does not support advanced window appearances.
InstanceLimit	FMA does not support application limits.
MultipleInstancesPerUserAllowed	FMA does not support application limits.
LoadBalancingApplicationCheckEnabled	FMA uses a different technology to support load balancing.
PreLaunch	FMA uses a different technology to support session prelaunch.
CachingOption	FMA uses a different technology to support session prelaunch.
ServerNames	FMA uses a different technology.
WorkerGroupNames	FMA does not support worker groups.

Secure

February 6, 2020

Citrix Virtual Apps and Desktops offers a secure-by-design solution that allows you to tailor your environment to your security needs.

One security concern IT faces with mobile workers is lost or stolen data. By hosting applications and desktops, Citrix Virtual Apps and Desktops securely separates sensitive data and intellectual property from end-point devices by keeping all data in a data center. When policies are enabled to allow data transfer, all data is encrypted.

The Citrix Virtual Apps and Desktops data centers also make incident response easier with a centralized monitoring and management service. Director allows IT to monitor and analyze data that is being accessed around the network, and Studio allows IT to patch and remedy most vulnerabilities in the data center instead of fixing the problems locally on each end-user device.

Citrix Virtual Apps and Desktops also simplify audits and regulatory compliance because investigators can use a centralized audit trail to determine who accessed what applications and data. Director gathers historical data regarding updates to the system and user data usage by accessing Configuration Logging and OData API.

Delegated Administration allows you to set up administrator roles to control access to Citrix Virtual Apps and Desktops at a granular level. This allows flexibility in your organization to give certain administrators full access to tasks, operations, and scopes while other administrators have limited access.

Citrix Virtual Apps and Desktops give administrators granular control over users by applying policies at different levels of the network - from the local level to the Organizational Unit level. This control of policies determines if a user, device, or groups of users and devices can connect, print, copy/paste, or map local drives, which can minimize security concerns with third-party contingency workers. Administrators can also use the Desktop Lock feature so end users can only use the virtual desktop while preventing any access to the local operating system of the end-user device.

Administrators can increase security on Citrix Virtual Apps or Citrix Virtual Desktops by configuring the Site to use the Transport Layer Security (TLS) protocol of the Controller or between end users and Virtual Delivery Agents (VDA). The protocol can also be enabled on a Site to provide server authentication, data stream encryption, and message integrity checks for a TCP/IP connection.

Citrix Virtual Apps and Desktops also support multifactor authentication for Windows or a specific application. Multifactor authentication can also be used to manage all resources delivered by Citrix Virtual Apps and Desktops. These methods include:

- Tokens
- Smart cards
- RADIUS
- Kerberos
- Biometrics

Citrix Virtual Desktops can be integrated with many third-party security solutions, ranging from iden-

tity management to antivirus software. A list of supported products can be found at http://www.citrix.com/ready.

Select releases of Citrix Virtual Apps and Desktops are certified for Common Criteria standard. For a list of those standards, go to https://www.commoncriteriaportal.org/cc/.

Security considerations and best practices

January 6, 2023

> **Note:**
>
> Your organization may need to meet specific security standards to satisfy regulatory requirements. This document does not cover this subject, because such security standards change over time. For up-to-date information on security standards and Citrix products, consult http://www.citrix.com/security/.

Security best practices

Keep all machines in your environment up to date with security patches. One advantage is that you can use thin clients as terminals, which simplifies this task.

Protect all machines in your environment with antivirus software.

Consider using platform-specific anti-malware software.

When installing software, install to provided default paths.

- If you install software to a file location other than the provided default path, consider adding additional security measures, such as restricted permissions, to your file location.

All network communications should be appropriately secured and encrypted to match your security policy. You can secure all communication between Microsoft Windows computers using IPSec; refer to your operating system documentation for details about how to do this. In addition, communication between user devices and desktops is secured through Citrix SecureICA, which is configured by default to 128-bit encryption. You can configure SecureICA when you are creating or updating a Delivery Group.

> **Note:**
>
> Citrix SecureICA forms part of the ICA/HDX protocol but it is not a standards-compliant network security protocol like Transport Layer Security (TLS). You can also secure network communications between user devices and desktops using TLS. To configure TLS, see Transport Layer Secu-

> rity (TLS).

Apply Windows best practice for account management. Do not create an account on a template or image before it is duplicated by Machine Creation Services or Provisioning Services. Do not schedule tasks using stored privileged domain accounts. Do not manually create shared Active Directory machine accounts. These practices will help prevent a machine attack from obtaining local persistent account passwords and then using them to log on to MCS/PVS shared images belonging to others.

Firewalls

Protect all machines in your environment with perimeter firewalls, including at enclave boundaries as appropriate.

All machines in your environment should be protected by a personal firewall. When you install core components and VDAs, you can choose to have the ports required for component and feature communication opened automatically if the Windows Firewall Service is detected (even if the firewall is not enabled). You can also choose to manually configure those firewall ports. If you use a different firewall, you must manually configure it.

If you are migrating a conventional environment to this release, you may need to reposition an existing perimeter firewall or add new perimeter firewalls. For example, suppose there is a perimeter firewall between a conventional client and database server in the data center. When this release is used, that perimeter firewall must be placed so that the virtual desktop and user device are on one side, and the database servers and Delivery Controllers in the data center are on the other side. Therefore, consider creating an enclave within your data center to contain the database servers and Controllers. Also consider having protection between the user device and the virtual desktop.

> **Note:**
>
> TCP ports 1494 and 2598 are used for ICA and CGP and are therefore likely to be open at firewalls so that users outside the data center can access them. Citrix recommends that you do not use these ports for anything else, to avoid the possibility of inadvertently leaving administrative interfaces open to attack. Ports 1494 and 2598 are officially registered with the Internet Assigned Number Authority (http://www.iana.org/).

Application security

To prevent non-admin users from performing malicious actions, we recommend that you configure Windows AppLocker rules for installers, applications, executables and scripts on the VDA host and on the local Windows client.

Manage user privileges

Grant users only the capabilities they require. Microsoft Windows privileges continue to be applied to desktops in the usual way: configure privileges through User Rights Assignment and group memberships through Group Policy. One advantage of this release is that it is possible to grant a user administrative rights to a desktop without also granting physical control over the computer on which the desktop is stored.

Note the following when planning for desktop privileges:

- By default, when non-privileged users connect to a desktop, they see the time zone of the system running the desktop instead of the time zone of their own user device. For information on how to allow users to see their local time when using desktops, see the Manage Delivery Groups article.
- A user who is an administrator on a desktop has full control over that desktop. If a desktop is a pooled desktop rather than a dedicated desktop, the user must be trusted in respect of all other users of that desktop, including future users. All users of the desktop need to be aware of the potential permanent risk to their data security posed by this situation. This consideration does not apply to dedicated desktops, which have only a single user; that user should not be an administrator on any other desktop.
- A user who is an administrator on a desktop can generally install software on that desktop, including potentially malicious software. The user can also potentially monitor or control traffic on any network connected to the desktop.

Manage logon rights

Logon rights are required for both user accounts and computer accounts. As with Microsoft Windows privileges, logon rights continue to be applied to desktops in the usual way: configure logon rights through User Rights Assignment and group memberships through Group Policy.

The Windows logon rights are: log on locally, log on through Remote Desktop Services, log on over the network (access this computer from the network), log on as a batch job, and log on as a service.

For computer accounts, grant computers only the logon rights they require. The logon right "Access this computer from the network"is required:

- At VDAs, for the computer accounts of Delivery Controllers
- At Delivery Controllers, for the computer accounts of VDAs. See Active Directory OU-based Controller discovery.
- At StoreFront servers, for the computer accounts of other servers in the same StoreFront server group

For user accounts, grant users only the logon rights they require.

According to Microsoft, by default the group Remote Desktop Users is granted the logon right "Allow log on through Remote Desktop Services"(except on domain controllers).

Your organization's security policy may state explicitly that this group should be removed from that logon right. Consider the following approach:

- The Virtual Delivery Agent (VDA) for Multi-session OS uses Microsoft Remote Desktop Services. You can configure the Remote Desktop Users group as a restricted group, and control membership of the group via Active Directory group policies. Refer to Microsoft documentation for more information.
- For other components of Citrix Virtual Apps and Desktops, including the VDA for Single-session OS, the group Remote Desktop Users is not required. So, for those components, the group Remote Desktop Users does not require the logon right "Allow log on through Remote Desktop Services"; you can remove it. Additionally:
  - If you administer those computers via Remote Desktop Services, ensure that all such administrators are already members of the Administrators group.
  - If you do not administer those computers via Remote Desktop Services, consider disabling Remote Desktop Services itself on those computers.

Although it is possible to add users and groups to the login right "Deny logon through Remote Desktop Services", the use of deny logon rights is not generally recommended. Refer to Microsoft documentation for more information.

Configure user rights

Delivery Controller installation creates the following Windows services:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Manages Microsoft Active Directory computer accounts for VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Collects site configuration usage information for use by Citrix, if this collection been approved by the site administrator. It then submits this information to Citrix, to help improve the product.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Supports management and provisioning of AppDisks, AppDNA integration, and management of App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Selects the virtual desktops or applications that are available to users.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Records all configuration changes and other state changes made by administrators to the site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Site-wide repository for shared configuration.

- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Manages the permissions granted to administrators.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Manages self-tests of the other Delivery Controller services.
- Citrix Host Service (NT SERVICE\CitrixHostService): Stores information about the hypervisor infrastructures used in a Citrix Virtual Apps or Citrix Virtual Desktops deployment, and also offers functionality used by the console to enumerate resources in a hypervisor pool.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): Orchestrates the creation of desktop VMs.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Collects metrics for Citrix Virtual Apps or Citrix Virtual Desktops, stores historical information, and provides a query interface for troubleshooting and reporting tools.
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): Supports management of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Supports privileged management operations of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): Propagates configuration data from the main site database to the Local Host Cache.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): Selects the virtual desktops or applications that are available to users, when the main site database is unavailable.

Delivery Controller installation also creates the following Windows services. These are also created when installed with other Citrix components:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Supports the collection of diagnostic information for use by Citrix Support.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Collects diagnostic information for analysis by Citrix, such that the analysis results and recommendations can be viewed by administrators to help diagnose issues with the site.

Delivery Controller installation also creates the following Windows service. This is not currently used. If it has been enabled, disable it.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

Delivery Controller installation also creates these following Windows services. These are not currently used, but must be enabled. Do not disable them.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Except for the Citrix Storefront Privileged Administration Service, these services are granted the logon

right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. You do not need to change these user rights. These privileges are not used by the Delivery Controller and are automatically disabled.

Configure service settings

Except for the Citrix Storefront Privileged Administration service and the Citrix Telemetry Service, the Delivery Controller Windows services listed above in the Configure user rights section are configured to log on as the NETWORK SERVICE identity. Do not alter these service settings.

The Citrix Storefront Privileged Administration service is configured to log on Local System (NT AUTHORITY\SYSTEM). This is required for Delivery Controller StoreFront operations that are not normally available to services (including creating Microsoft IIS sites). Do not alter its service settings.

The Citrix Telemetry Service is configured to log on as its own service-specific identity.

You can disable the Citrix Telemetry Service. Apart from this service, and services that are already disabled, do not disable any other of these Delivery Controller Windows services.

Configure registry settings

It is no longer necessary to enable creation of 8.3 file names and folders on the VDA file system. The registry key **NtfsDisable8dot3NameCreation** can be configured to disable creation of 8.3 file names and folders. You can also configure this using the **fsutil.exe behavior set disable8dot3** command.

Deployment scenario security implications

Your user environment can contain either user devices that are unmanaged by your organization and completely under the control of the user, or user devices that are managed and administered by your organization. The security considerations for these two environments are generally different.

Managed user devices

Managed user devices are under administrative control; they are either under your own control, or the control of another organization that you trust. You may configure and supply user devices directly to users; alternatively, you may provide terminals on which a single desktop runs in full-screen-only mode. Follow the general security best practices described above for all managed user devices. This release has the advantage that minimal software is required on a user device.

A managed user device can be configured to be used in full-screen-only mode or in window mode:

- Full-screen-only mode: Users log on to it with the usual Log On To Windows screen. The same user credentials are then used to log on automatically to this release.
- Users see their desktop in a window: Users first log on to the user device, then log on to this release through a web site supplied with the release.

Unmanaged user devices

User devices that are not managed and administered by a trusted organization cannot be assumed to be under administrative control. For example, you might permit users to obtain and configure their own devices, but users might not follow the general security best practices described above. This release has the advantage that it is possible to deliver desktops securely to unmanaged user devices. These devices should still have basic antivirus protection that will defeat keylogger and similar input attacks.

Data storage considerations

When using this release, you can prevent users from storing data on user devices that are under their physical control. However, you must still consider the implications of users storing data on desktops. It is not good practice for users to store data on desktops; data should be held on file servers, database servers, or other repositories where it can be appropriately protected.

Your desktop environment may consist of various types of desktops, such as pooled and dedicated desktops. Users should never store data on desktops that are shared amongst users, such as pooled desktops. If users store data on dedicated desktops, that data should be removed if the desktop is later made available to other users.

Mixed-version environments

Mixed-version environments are inevitable during some upgrades. Follow best-practice and minimize the time that Citrix components of different versions co-exist. In mixed-version environments, security policy, for example, may not be uniformly enforced.

> **Note:**
>
> This is typical of other software products; the use of an earlier version of Active Directory only partially enforces Group Policy with later versions of Windows.

The following scenario describes a security issue that can occur in a specific mixed-version Citrix environment. When Citrix Receiver 1.7 is used to connect to a virtual desktop running the VDA in XenApp and XenDesktop 7.6 Feature Pack 2, the policy setting **Allow file transfer between desktop and client** is enabled in the Site but cannot be disabled by a Delivery Controller running XenApp and

XenDesktop 7.1. It does not recognize the policy setting, which was released in the later version of the product. This policy setting allows users to upload and download files to their virtual desktop, which is the security issue. To work around this, upgrade the Delivery Controller (or a standalone instance of Studio) to version 7.6 Feature Pack 2 and then use Group Policy to disable the policy setting. Alternatively, use local policy on all affected virtual desktops.

Remote PC Access security considerations

Remote PC Access implements the following security features:

- Smart card use is supported.
- When a remote session connects, the office PC's monitor appears as blank.
- Remote PC Access redirects all keyboard and mouse input to the remote session, except CTRL+ALT+DEL and USB-enabled smart cards and biometric devices.
- SmoothRoaming is supported for a single user only.
- When a user has a remote session connected to an office PC, only that user can resume local access of the office PC. To resume local access, the user presses Ctrl-Alt-Del on the local PC and then logs on with the same credentials used by the remote session. The user can also resume local access by inserting a smart card or leveraging biometrics, if your system has appropriate third-party Credential Provider integration. This default behavior can be overridden by enabling Fast User Switching via Group Policy Objects (GPOs) or by editing the registry.

> **Note:**
>
> Citrix recommends that you do not assign VDA administrator privileges to general session users.

Automatic assignments

By default, Remote PC Access supports automatic assignment of multiple users to a VDA. In XenDesktop 5.6 Feature Pack 1, administrators could override this behavior using the RemotePCAccess.ps1 PowerShell script. This release uses a registry entry to allow or prohibit multiple automatic remote PC assignments; this setting applies to the entire Site.

> **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.

To restrict automatic assignments to a single user:

On each Controller in the Site, set the following registry entry:


```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
Name: AllowMultipleRemotePCAssignments
Type: REG_DWORD
Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
   multiple user assignment.
```

If there are any existing user assignments, remove them using SDK commands for the VDA to subsequently be eligible for a single automatic assignment.

- Remove all assigned users from the VDA: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- Remove the VDA from the Delivery Group: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Restart the physical office PC.

XML trust

The XML trust setting 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 firewalls, IPsec, or other security recommendations).

This setting is disabled by default.

Use the Citrix Virtual Apps and Desktops PowerShell SDK to check, enable, or disable the XML trust setting.

- To check the XML trust setting's 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`.

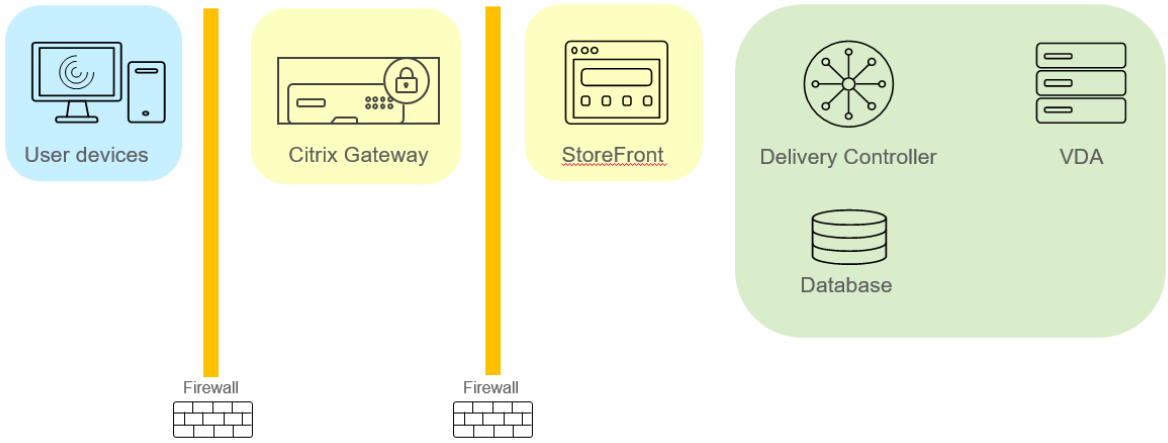
Integrate Citrix Virtual Apps and Desktops with Citrix Gateway

February 7, 2020

StoreFront servers are deployed and configured to manage access to published resources and data. For remote access, adding Citrix Gateway in front of StoreFront is recommended.

> **Note:**
>
> For detailed configuration steps on how to integrate Citrix Virtual Apps and Desktops with Citrix Gateway, see the StoreFront documentation.

The following diagram illustrates an example of a simplified Citrix deployment that includes Citrix Gateway. Citrix Gateway communicates with StoreFront to protect apps and data delivered by Citrix Virtual Apps and Desktops. The user devices run Citrix Workspace app to create a secure connection and access their apps, desktops, and files.



Users log on and authenticate using Citrix Gateway. Citrix Gateway is deployed and secured in the DMZ. Two-factor authentication is configured. Based on the user credentials, users are provided with the relevant resources and applications. Applications and data are on appropriate servers (not shown on the diagram). Separate servers used for security sensitive applications and data.

Delegated Administration

February 6, 2020

The Delegated Administration model offers the flexibility to match how your organization wants to delegate administration activities, using role and object-based control. Delegated Administration accommodates deployments of all sizes, and allows you to configure more permission granularity as

your deployment grows in complexity. Delegated Administration uses three concepts: administrators, roles, and scopes.

- **Administrators:** An administrator represents an individual person or a group of people identified by their Active Directory account. Each administrator is associated with one or more role and scope pairs.
- **Roles:** A role represents a job function, and has defined permissions associated with it. For example, the Delivery Group Administrator role has permissions such as 'Create Delivery Group' and 'Remove Desktop from Delivery Group.'An administrator can have multiple roles for a Site, so a person can be a Delivery Group Administrator and a Machine Catalog Administrator. Roles can be built-in or custom.

  The built-in roles are:

Role	Permissions
Full Administrator	Can perform all tasks and operations. A Full Administrator is always combined with the All scope.
Read Only Administrator	Can see all objects in specified scopes in addition to global information, but cannot change anything. For example, a Read Only Administrator with Scope=London can see all global objects (such as Configuration Logging) and any London-scoped objects (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).
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.

Role	Permissions
Machine Catalog Administrator	Can create and manage Machine Catalogs and provision the machines into them. Can build Machine Catalogs from the virtualization infrastructure, Provisioning Services, and physical machines. This role can manage base images and install software, but cannot assign applications or desktops to users.
Delivery Group Administrator	Can deliver applications, desktops, and machines; can also manage the associated sessions. Can also manage application and desktop configurations such as policies and power management settings.
Host Administrator	Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

In certain product editions, you can create custom roles to match the requirements of your organization, and delegate permissions with more detail. You can use custom roles to allocate permissions at the granularity of an action or task in a console.

- **Scopes:** A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your organization (for example, the set of Delivery Groups used by the Sales team). Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: 'All,' which contains all objects. The Full Administrator role is always paired with the All scope.

Example

Company XYZ decided to manage applications and desktops based on their department (Accounts, Sales, and Warehouse) and their desktop operating system (Windows 7 or Windows 8). The administrator created five scopes, then labeled each Delivery Group with two scopes: one for the department where they are used and one for the operating system they use.

The following administrators were created:

Administrator	Roles	Scopes
domain/fred	Full Administrator	All (the Full Administrator role always has the All scope)
domain/rob	Read Only Administrator	All
domain/heidi	Read Only Administrator, Help Desk Administrator	All Sales
domain/warehouseadmin	Help Desk Administrator	Warehouse
domain/peter	Delivery Group Administrator, Machine Catalog Administrator	Win7

- Fred is a Full Administrator and can view, edit, and delete all objects in the system.
- Rob can view all objects in the Site but cannot edit or delete them.
- Heidi can view all objects and can perform help desk tasks on Delivery Groups in the Sales scope. This allows her to manage the sessions and machines associated with those groups; she cannot make changes to the Delivery Group, such as adding or removing machines.
- Anyone who is a member of the warehouseadmin Active Directory security group can view and perform help desk tasks on machines in the Warehouse scope.
- Peter is a Windows 7 specialist and can manage all Windows 7 Machine Catalogs and can deliver Windows 7 applications, desktops, and machines, regardless of which department scope they are in. The administrator considered making Peter a Full Administrator for the Win7 scope. However, she decided against this, because a Full Administrator also has full rights over all objects that are not scoped, such as 'Site'and 'Administrator.'

How to use Delegated Administration

Generally, the number of administrators and the granularity of their permissions depends 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 delegation. In this case, create each administrator with the built-in Full Administrator role, which 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 are Full Administrators, and others are Help Desk Administrators. Also, an administrator might manage only certain groups of objects (scopes), such as machine catalogs. In this case, create new scopes, plus administrators with one of the built-in roles and the appropriate scopes.

- Even larger deployments might require more (or more specific) scopes, plus different administrators with unconventional roles. In this case, edit or create more scopes, create custom roles, and create each administrator with a built-in or custom role, plus existing and new scopes.

For flexibility and ease of configuration, you can create scopes when you create an administrator. You can also specify scopes when creating or editing Machine Catalogs or connections.

Create and manage administrators

When you create a Site as a local administrator, your user account automatically becomes a Full Administrator with full permissions over all objects. After a Site is created, local administrators have no special privileges.

The Full Administrator role always has the All scope; you cannot change this.

By default, an administrator is enabled. Disabling an administrator might be necessary if you are creating the administrator now, but that person won't start administration duties until later. For existing enabled administrators, you might want to disable several of them while you are reorganizing your object/scopes, then re-enable them when you are ready to go live with the updated configuration. You cannot disable a Full Administrator if it would result in there being no enabled Full Administrator. The enable/disable check box is available when you create, copy, or edit an administrator.

When you delete a role/scope pair while copying, editing, or deleting an administrator, it deletes only the relationship between the role and the scope for that administrator. It does not delete either the role or the scope. It also does not affect any other administrator who is configured with that role/scope pair.

To manage administrators, click **Configuration > Administrators** in the Studio navigation pane, and then click the **Administrators** tab in the upper middle pane.

- **Create an administrator:** Click **Create new Administrator** in the Actions pane. Type or browse to the user account name, select or create a scope, and select a role. The new administrator is enabled by default; you can change this.
- **Copy an administrator:** Select the administrator in the middle pane and then click **Copy Administrator** in the Actions pane. Type or browse to the user account name. You can select and then edit or delete any of the role/scope pairs, and add new ones. The new administrator is enabled by default; you can change this.
- **Edit an administrator:** Select the administrator in the middle pane and then click **Edit Administrator** in the Actions pane. You can edit or delete any of the role/scope pairs, and add new ones.
- **Delete an administrator:** Select the administrator in the middle pane and then click **Delete Administrator** in the Actions pane. You cannot delete a Full Administrator if it would result in there being no enabled Full Administrator.

The upper pane displays the administrators that you created. Select an administrator to view its details in the lower pane. The **Warnings** column indicates whether the role and scope pairs associated with the administrator contain unusable roles or scopes. The following warning message appears if an associated role and scope pair contains unusable roles or scopes:

- Associated role or scope not usable
  - Remove the role and scope pair from the administrator.

> **Important:**
>
> A warning message appears only when an associated role and scope pair contains unusable roles or scopes or both.

To remove the role and scope pair from the administrator, complete one of the following steps:

- Delete the role and scope pair.
  1. In the **Actions** pane, click **Edit Administrator**.
  2. In the **Edit Administrator** window, select the role and scope pair and then click **Delete**.
  3. Click **OK** to exit.
- Delete the administrator.
  1. In the **Actions** pane, click **Delete Administrator**.
  2. In the **Studio** window, Click **Delete**.

Create and manage roles

When administrators create or edit a role, they can enable only the permissions that they themselves have. This 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).

Role names can contain up to 64 Unicode characters; they cannot contain: 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, or apostrophe. Descriptions can contain up to 256 Unicode characters.

You cannot edit or delete a built-in role. You cannot delete a custom role if any administrator is using it.

> **Note:**
>
> Only certain product editions support custom roles. Only editions that support custom roles have related entries in the Actions pane.

To manage roles, click **Configuration > Administrators** in the Studio navigation pane, and then click the **Roles** tab in the upper middle pane.

- **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. Click the Administrators tab in the lower pane to display a list of administrators who currently have this role.
- **Create a custom role:** Click **Create new Role** in the Actions pane. Enter a name and description. Select the object types and permissions.
- **Copy a role:** Select the role in the middle pane and then click **Copy Role** in the Actions pane. Change the name, description, object types, and permissions, as needed.
- **Edit a custom role:** Select the role in the middle pane and then click **Edit Role** in the Actions pane. Change the name, description, object types, and permissions, as needed.
- **Delete a custom role:** Select the role in the middle pane and then click **Delete Role** in the Actions pane. When prompted, confirm the deletion.

Create and manage scopes

When you create a Site, the only available scope is the 'All' scope, which cannot be deleted.

You can create scopes using the following procedure. You can also create scopes when you create an administrator; each administrator must be associated with at least one role and scope pair. When you are creating or editing desktops, machine catalogs, applications, or hosts, you can add them to an existing scope. If you do not add them to a scope, they remain part of the 'All' scope.

Site creation cannot be scoped, nor can Delegated Administration objects (scopes and roles). However, objects you cannot scope are included in the 'All' scope. (Full Administrators always have the All scope.) Machines, power actions, desktops, and sessions are not directly scoped. Administrators can be allocated permissions over these objects through the associated machine catalogs or Delivery Groups.

Scope names can contain up to 64 Unicode characters. Scope names cannot include: 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, or apostrophe. 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 the administrator. If the edited scope is paired with one or more roles, ensure that the scope updates do not make any role/scope pair unusable.

To manage scopes, click **Configuration > Administrators** in the Studio navigation pane, and then click the **Scopes** tab in the upper middle pane.

- **Create a scope:** Click **Create new Scope** in the Actions pane. Enter a name and description. To include all objects of a particular type (for example, Delivery Groups), select the object type.

To include specific objects, expand the type and then select individual objects (for example, Delivery Groups used by the Sales team).

- **Copy a scope:** Select the scope in the middle pane and then click **Copy Scope** in the Actions pane. Enter a name and description. Change the object types and objects, as needed.
- **Edit a scope:** Select the scope in the middle pane and then click **Edit Scope** in the Actions pane. Change the name, description, object types, and objects, as needed.
- **Delete a scope:** Select the scope in the middle pane and then click **Delete Scope** in the Actions pane. When prompted, confirm the deletion.

Create reports

You can create two types of Delegated Administration reports:

- An HTML report that lists the role/scope pairs associated with an administrator, plus the individual permissions for each type of object (for example, Delivery Groups and Machine Catalogs). You generate this report from Studio.

  To create this report, click **Configuration > Administrators** in the Studio navigation pane. Select an administrator in the middle pane and then click **Create Report** in the Actions pane.

  You can also request this report when creating, copying, or editing an administrator.

- An HTML or CSV report that maps all built-in and custom roles to permissions. You generate this report by running a PowerShell script named OutputPermissionMapping.ps1.

  To run this script, you must be a Full Administrator, a Read Only Administrator, or a custom administrator with permission to read roles. The script is located in: Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

  Syntax:

  ```
  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-
  AdminAddress string] [-Show] [CommonParameters]
  ```

Parameter	Description
`-Help`	Displays script help.
`-Csv`	Specifies CSV output. Default = HTML
`-Path string`	Where to write the output. Default = stdout
`-AdminAddress string`	IP address or host name of the Delivery Controller to connect to. Default = localhost

Parameter	Description
-Show	(Valid only when the -Path parameter is also specified) When you write the output to a file, -Show causes the output to be opened in an appropriate program, such as a web browser.
CommonParameters	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For details, see the Microsoft documentation.

The following example writes an HTML table to a file named Roles.html and opens the table in a web browser.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html –Show
<!--NeedCopy-->
```

The following example writes a CSV table to a file named Roles.csv. The table is not displayed.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 –CSV -Path Roles.csv
<!--NeedCopy-->
```

From a Windows command prompt, the preceding example command is:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
<!--NeedCopy-->
```

Smart cards

May 18, 2021

Smart cards and equivalent technologies are supported within the guidelines described in this article. To use smart cards with Citrix Virtual Apps or Citrix Virtual Desktops:

- Understand your organization's security policy concerning the use of smart cards. These policies might, for example, state how smart cards are issued and how users should safeguard them.

Some aspects of these policies might need to be reassessed in a Citrix Virtual Apps or Citrix Virtual Desktops environment.
- Determine which user device types, operating systems, and published applications are to be used with smart cards.
- Familiarize yourself with smart card technology and your selected smart card vendor hardware and software.
- Know how to deploy digital certificates in a distributed environment.

> **Note:**
>
> Smart card enrollment is not supported with fast smart card. Smart card enrollment may work when fast smart card is disabled, but is dependent on the type of smart card and middleware. Contact your smart card and middleware vendor for information on their integration with Citrix Virtual Apps and Desktops and support for smart card enrollment over virtual sessions.

Types of smart cards

Enterprise and consumer smart cards have the same dimensions, electrical connectors, and fit the same smart card readers.

Smart cards for enterprise use contain digital certificates. These smart cards support Windows Logon, and can also be used with applications for digital signing and encryption of documents and email. Citrix Virtual Apps and Desktops support these uses.

Smart cards for consumer use do not contain digital certificates; they contain a shared secret. These smart cards can support payments (such as a chip-and-signature or chip-and-PIN credit card). They do not support Windows Logon or typical Windows applications. Specialized Windows applications and a suitable software infrastructure (including, for example, a connection to a payment card network) are needed for use with these smart cards. Contact your Citrix representative for information on supporting these specialized applications on Citrix Virtual Apps or Citrix Virtual Desktops.

For enterprise smart cards, there are compatible equivalents that can be used in a similar way.

- A smart card-equivalent USB token connects directly to a USB port. These USB tokens are usually the size of a USB flash drive, but can be as small as a SIM card used in a mobile phone. They appear as the combination of a smart card plus a USB smart card reader.
- A virtual smart card using a Windows Trusted Platform Module (TPM) appears as a smart card. These virtual smart cards are supported for Windows 8 and Windows 10, using Citrix Workspace app (minimum version Citrix Receiver 4.3).
  - Versions of Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) earlier than XenApp and XenDesktop 7.6 FP3 do not support virtual smart cards.
  - For more information on virtual smart cards, see Virtual Smart Card Overview.

> **Note:** The term "virtual smart card"is also used to describe a digital certificate stored on the user computer. These digital certificates are not strictly equivalent to smart cards.

Citrix Virtual Apps and Desktops smart card support is based on the Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. A minimum requirement is that smart cards and smart card devices must be supported by the underlying Windows operating system and must be approved by the Microsoft Windows Hardware Quality Labs (WHQL) to be used on computers running qualifying Windows operating systems. See the Microsoft documentation for additional information about hardware PC/SC compliance. Other types of user devices may comply with the PS/SC standard. For more information, refer to the Citrix Ready program.

Usually, a separate device driver is needed for each vendor's smart card or equivalent. However, if smart cards conform to a standard such as the NIST Personal Identity Verification (PIV) standard, it may be possible to use a single device driver for a range of smart cards. The device driver must be installed on both the user device and the Virtual Delivery Agent (VDA). The device driver is often supplied as part of a smart card middleware package available from a Citrix partner; the smart card middleware package will offer advanced features. The device driver may also be described as a Cryptographic Service Provider (CSP), Key Storage Provider (KSP), or minidriver.

The following smart card and middleware combinations for Windows systems have been tested by Citrix as representative examples of their type. However, other smart cards and middleware can also be used. For more information about Citrix-compatible smart cards and middleware, see http://www.citrix.com/ready.

Middleware	Matching cards
Gemalto Mini Driver for .NET card	Gemalto .NET v2+

For information about smart card usage with other types of devices, see the Citrix Workspace app documentation for that device.

Remote PC Access

Smart cards are supported only for remote access to physical office PCs running Windows 10, Windows 8 or Windows 7.

The following smart cards were tested with Remote PC Access:

Middleware	Matching cards
Gemalto .NET minidriver	Gemalto .NET v2+

Fast smart card

Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN situations.

Fast smart card is enabled by default on host machines with currently supported Windows VDAs. To disable Fast Smart Card on the host-side—for example for diagnostic purposes—set the 'Disable Cryptographic Redirection' registry setting to any non-zero value:

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
<!--NeedCopy-->
```

On the client side, to enable fast smart card, include the SmartCardCryptographicRedirection ICA parameter in the *default.ica* file of the associated StoreFront site:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

Limitations:

- Only Citrix Receiver for Windows supports fast smart card. If you configure fast smart cards in the default.ica file, Citrix Receivers that are not for Windows still work with existing PC/SC Redirection.
- The only double-hop scenarios that fast smart card supports are ICA > ICA with fast smart card enabled on both hops. Because fast smart card doesn't support ICA > RDP double-hop scenarios, those scenarios don't work.
- Fast smart card doesn't support Cryptography Next Generation. Thus, fast smart card doesn't support Elliptic Curve Cryptography (ECC) smart cards.
- Fast smart card supports only read-only key container operations.
- Fast smart card doesn't support changing the smart card PIN.

Types of smart card readers

A smart card reader may be built in to the user device, or be separately attached to the user device (usually via USB or Bluetooth). Contact card readers that comply with the USB Chip/Smart Card Interface Devices (CCID) specification are supported. They contain a slot or swipe into which the user inserts the smart card. The Deutsche Kreditwirtschaft (DK) standard defines four classes of contact card readers.

- Class 1 smart card readers are the most common, and usually just contain a slot. Class 1 smart card readers are supported, usually with a standard CCID device driver supplied with the operating system.

- Class 2 smart card readers also contain a secure keypad that cannot be accessed by the user device. Class 2 smart card readers may be built into a keyboard with an integrated secure keypad. For class 2 smart card readers, contact your Citrix representative; a reader-specific device driver may be required to enable the secure keypad capability.
- Class 3 smart card readers also contain a secure display. Class 3 smart card readers are not supported.
- Class 4 smart card readers also contain a secure transaction module. Class 4 smart card readers are not supported.

> **Note:**
>
> The smart card reader class is unrelated to the USB device class.

Smart card readers must be installed with a corresponding device driver on the user device.

For information about supported smart card readers, see the documentation for the Citrix Workspace app you are using. In the Citrix Workspace app documentation, supported versions are usually listed in a smart card article or in the system requirements article.

User experience

Smart card support is integrated into Citrix Virtual Apps and Desktops, using a specific ICA/HDX smart card virtual channel that is enabled by default.

Important: Do not use generic USB redirection for smart card readers. This is disabled by default for smart card readers, and is not supported if enabled.

Multiple smart cards and multiple readers can be used on the same user device, but if pass-through authentication is in use, only one smart card must be inserted when the user starts a virtual desktop or application. When a smart card is used within an application (for example, for digital signing or encryption functions), there might be additional prompts to insert a smart card or enter a PIN. This can occur if more than one smart card has been inserted at the same time.

- If users are prompted to insert a smart card when the smart card is already in the reader, they should select Cancel.
- If users are prompted for the PIN, they should enter the PIN again.

You can reset PINs using a card management system or vendor utility.

> **Important:**
>
> Within a Citrix Virtual Apps or Citrix Virtual Desktops session, using a smart card with the Microsoft Remote Desktop Connection application is not supported. This is sometimes described as a "double hop" use.

Before deploying smart cards

- Obtain a device driver for the smart card reader and install it on the user device. Many smart card readers can use the CCID device driver supplied by Microsoft.
- Obtain a device driver and cryptographic service provider (CSP) software from your smart card vendor, and install them on both user devices and virtual desktops. The driver and CSP software must be compatible with Citrix Virtual Apps and Desktops; check the vendor documentation for compatibility. For virtual desktops using smart cards that support and use the minidriver model, smart card minidrivers should download automatically, but you can obtain them from http://catalog.update.microsoft.com or from your vendor. Also, if PKCS#11 middleware is required, obtain it from the card vendor.
- Important: Citrix recommends that you install and test the drivers and CSP software on a physical computer before installing Citrix software.
- Add the Citrix Receiver for Web URL to the Trusted Sites list for users who work with smart cards in Internet Explorer with Windows 10. In Windows 10, Internet Explorer does not run in protected mode by default for trusted sites.
- Ensure that your public key infrastructure (PKI) is configured appropriately. This includes ensuring that certificate-to-account mapping is correctly configured for Active Directory environment and that user certificate validation can be performed successfully.
- Ensure your deployment meets the system requirements of the other Citrix components used with smart cards, including Citrix Workspace app and StoreFront.
- Ensure access to the following servers in your Site:
  - The Active Directory domain controller for the user account that is associated with a logon certificate on the smart card
  - Delivery Controller
  - Citrix StoreFront
  - Citrix Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optional for Remote PC Access): Microsoft Exchange Server

Enable smart card use

Step 1. Issue smart cards to users according to your card issuance policy.

Step 2. (Optional) Set up the smart cards to enable users for Remote PC Access.

Step 3. Install and configure the Delivery Controller and StoreFront (if not already installed) for smart card remoting.

Step 4. Enable StoreFront for smart card use. For details, see Configure smart card authentication in the StoreFront documentation.

Step 5. Enable Citrix Gateway/Access Gateway for smart card use. For details, see Configuring Authentication and Authorization and Configuring Smart Card Access with the Web Interface in the NetScaler documentation.

Step 6. Enable VDAs for smart card use.

- Ensure the VDA has the required applications and updates.
- Install the middleware.
- Set up smart card remoting, enabling the communication of smart card data between Citrix Workspace app on a user device and a virtual desktop session.

Step 7. Enable user devices (including domain-joined or non-domain-joined machines) for smart card use. See Configure smart card authentication in the StoreFront documentation for details.

- Import the certificate authority root certificate and the issuing certificate authority certificate into the device's keystore.
- Install your vendor's smart card middleware.
- Install and configure Citrix Workspace app for Windows, being sure to import icaclient.adm using the Group Policy Management Console and enable smart card authentication.

Step 8. Test the deployment. Ensure that the deployment is configured correctly by launching a virtual desktop with a test user's smart card. Test all possible access mechanisms (for example, accessing the desktop through Internet Explorer and Citrix Workspace app).

Smart card deployments

February 7, 2020

The following types of smart card deployments are supported by this product version and by mixed environments containing this version. Other configurations might work but are not supported.

Type	StoreFront connectivity
Local domain-joined computers	Directly connected
Remote access from domain-joined computers	Connected through Citrix Gateway
Non-domain-joined computers	Directly connected
Remote access from non-domain-joined computers	Connected through Citrix Gateway
Non-domain-joined computers and thin clients accessing the Desktop Appliance site	Connected through Desktop Appliance sites

Type	StoreFront connectivity
Domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL	Connected through XenApp Services URLs

The deployment types are defined by the characteristics of the user device to which the smart card reader is connected:

- Whether the device is domain-joined or non-domain-joined.
- How the device is connected to StoreFront.
- What software is used to view virtual desktops and applications.

In addition, smart card-enabled applications such as Microsoft Word, and Microsoft Excel can be used in these deployments. Those applications allow users to digitally sign or encrypt documents.

Bimodal authentication

Where possible in each of these deployments, Receiver supports bimodal authentication by offering the user a choice between using a smart card and entering their user name and password. This is useful if the smart card cannot be used (for example, the user has left it at home or the logon certificate has expired).

Because users of non-domain-joined devices log on to Receiver for Windows directly, you can enable users to fall back to explicit authentication. If you configure bimodal authentication, users are initially prompted to log on using their smart cards and PINs but have the option to select explicit authentication if they experience any issues with their smart cards.

If you deploy Citrix Gateway, users log on to their devices and are prompted by Receiver for Windows to authenticate to Citrix Gateway. This applies to both domain-joined and non-domain-joined devices. Users can log on to Citrix Gateway using either their smart cards and PINs, or with explicit credentials. This enables you to provide users with bimodal authentication for Citrix Gateway logons. Configure pass-through authentication from Citrix Gateway to StoreFront and delegate credential validation to Citrix Gateway for smart card users so that users are silently authenticated to StoreFront.

Multiple Active Directory forest considerations

In a Citrix environment, smart cards are supported within a single forest. Smart card logons across forests require a direct two-way forest trust to all user accounts. More complex multi-forest deployments involving smart cards (that is, where trusts are only one-way or of different types) are not supported.

You can use smart cards in a Citrix environment that includes remote desktops. This feature can be installed locally (on the user device that the smart card is connected to) or remotely (on the remote desktop that the user device connects to).

Smart card removal policy

The smart card removal policy set on the product determines what happens if you remove the smart card from the reader during a session. The smart card removal policy is configured through and handled by the Windows operating system.

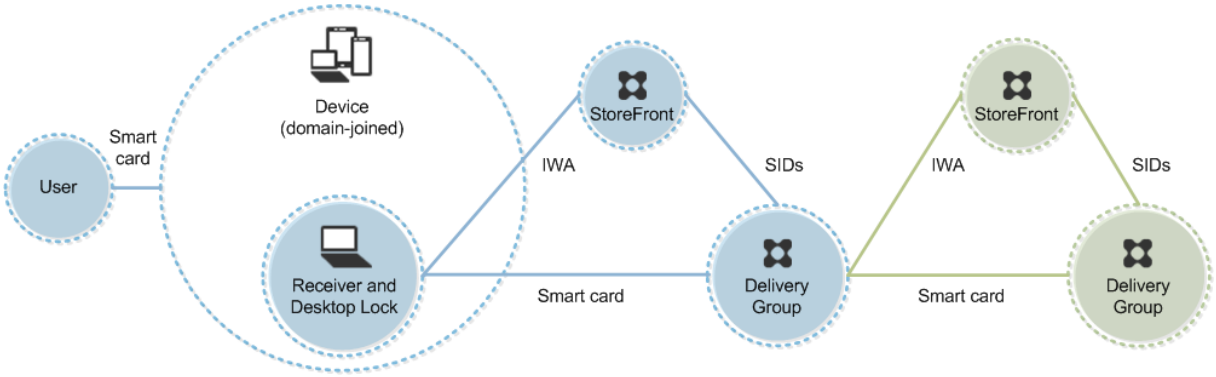
Policy setting	Desktop behavior
No action	No action.
Lock workstation	The desktop session is disconnected and the virtual desktop is locked.
Force logoff	The user is forced to log off. If the network connection is lost and this setting is enabled, the session may be logged off and the user may lose data.
Disconnect if a remote Terminal Services session	The session is disconnected and the virtual desktop is locked.

Certificate revocation checking

If certificate revocation checking is enabled and a user inserts a smart card with an invalid certificate into a card reader, the user cannot authenticate or access the desktop or application related to the certificate. For example, if the invalid certificate is used for email decryption, the email remains encrypted. If other certificates on the card, such as ones used for authentication, are still valid, those functions remain active.

Deployment example: domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.

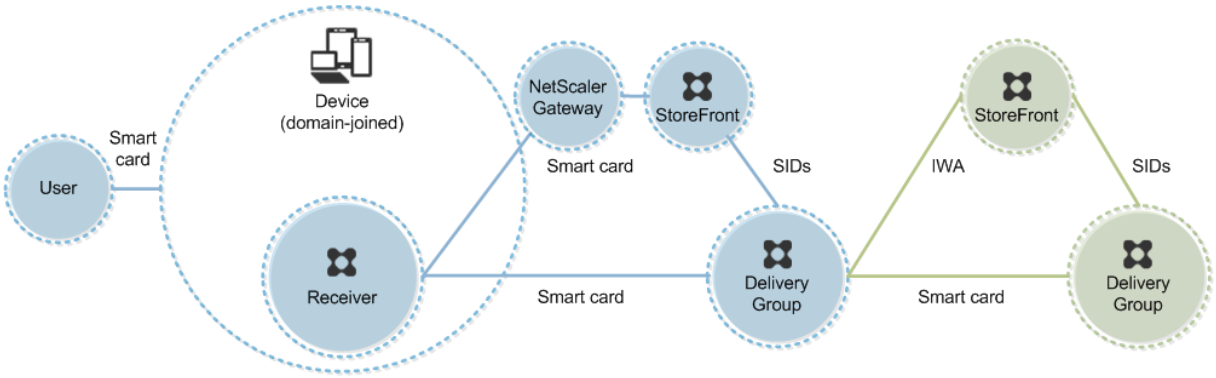


A user logs on to a device using a smart card and PIN. Receiver authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: remote access from domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect to StoreFront through Citrix Gateway/Access Gateway.



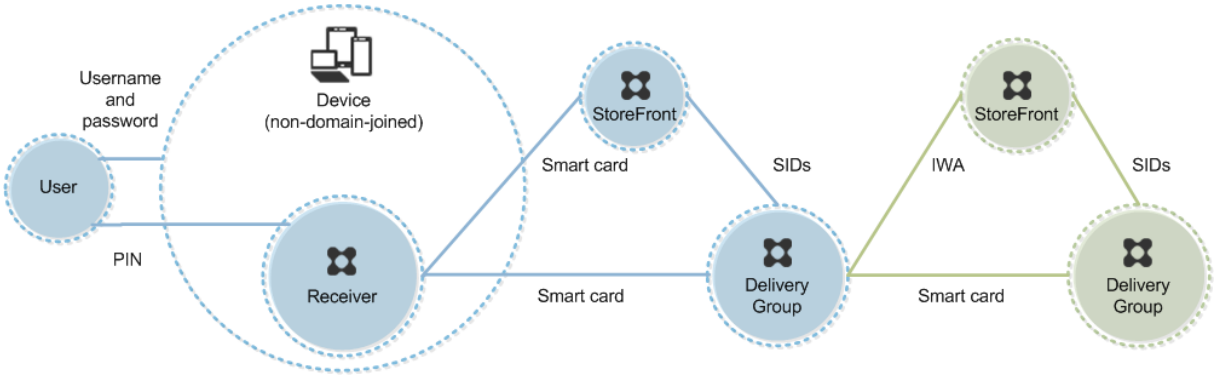
A user logs on to a device using a smart card and PIN, and then logs on again to Citrix Gateway/Access Gateway. This second logon can be with either the smart card and PIN or a user name and password because Receiver allows bimodal authentication in this deployment.

The user is automatically logged on to StoreFront, which passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is not prompted again for a PIN because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second Store-Front server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



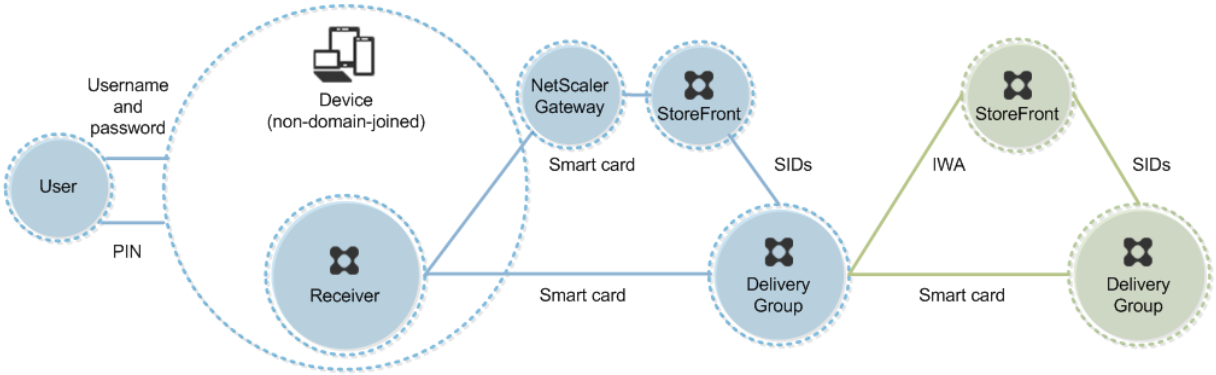
A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second Store-Front server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: remote access from non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

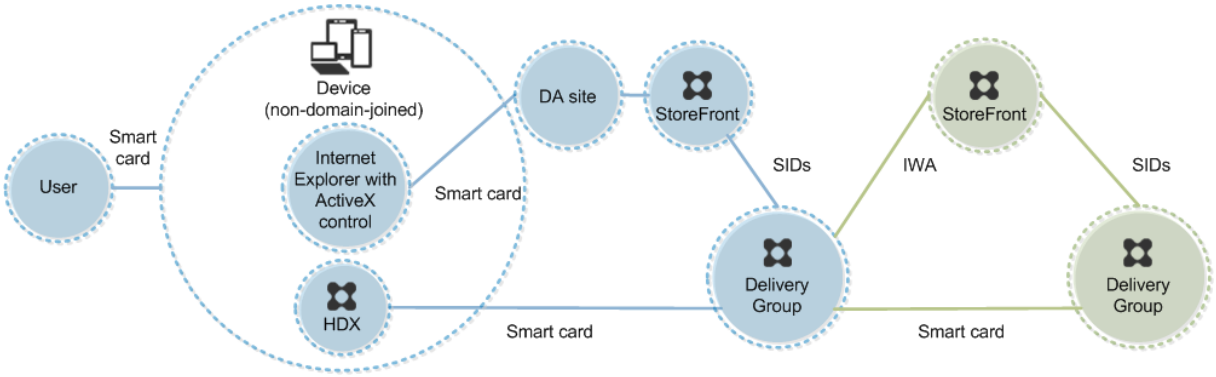
StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: non-domain-joined computers and thin clients accessing the Desktop Appliance site

This deployment involves non-domain-joined user devices that may run the Desktop Lock and connect to StoreFront through Desktop Appliance sites.

The Desktop Lock is a separate component that is released with Citrix Virtual Apps, Citrix Virtual Desktops, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.



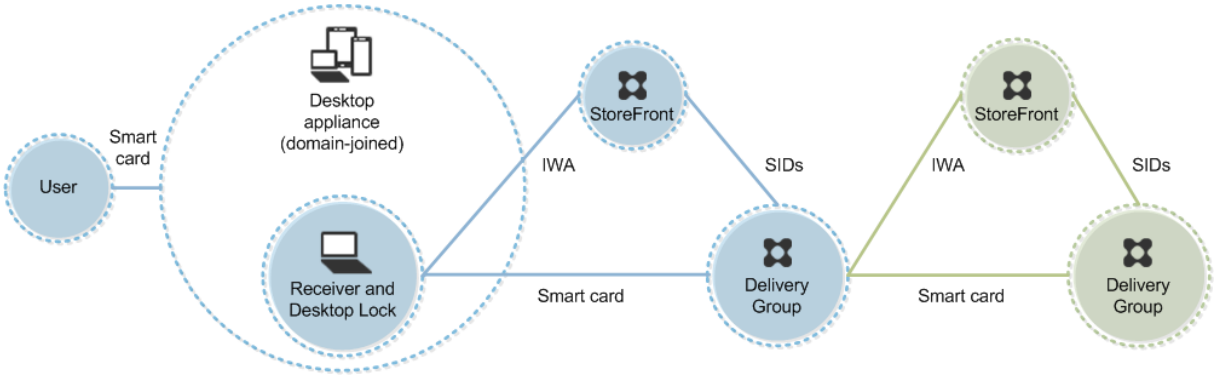
A user logs on to a device with a smart card. If Desktop Lock is running on the device, the device is configured to launch a Desktop Appliance site through Internet Explorer running in Kiosk Mode. An ActiveX control on the site prompts the user for a PIN, and sends it to StoreFront. StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. The first available desktop in the alphabetical list in an assigned Desktop Group starts.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL

This deployment involves domain-joined user devices that run the Desktop Lock and connect to StoreFront through XenApp Services URLs.

The Desktop Lock is a separate component that is released with Citrix Virtual Apps, Citrix Virtual Desktops, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.



A user logs on to a device using a smart card and PIN. If Desktop Lock is running on the device, it authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Pass-through authentication and single sign-on with smart cards

February 6, 2020

Pass-through authentication

Pass-through authentication with smart cards to virtual desktops is supported on user devices running Windows 10, Windows 8, and Windows 7 SP1 Enterprise and Professional Editions.

Pass-through authentication with smart cards to hosted applications is supported on servers running Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 SP1.

To use pass-through authentication with smart cards hosted applications, ensure you enable the use of Kerberos when you configure Pass-through with smartcard as the authentication method for the site.

Note: The availability of pass-through authentication with smart cards depends on many factors including, but not limited to:

- Your organization's security policies regarding pass-through authentication.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Pass-through authentication with smart cards is configured on Citrix StoreFront. See the StoreFront documentation for details.

Single sign-on

Single sign-on is a Citrix feature that implements pass-through authentication with virtual desktop and application launches. You can use this feature in domain-joined, direct-to-StoreFront and domain-joined, NetScaler-to-StoreFront smart card deployments to reduce the number of times that users enter their PIN. To use single sign-on in these deployment types, edit the following parameters in the default.ica file, which is located on the StoreFront server:

- Domain-joined, direct-to-StoreFront smart card deployments —Set DisableCtrlAltDel to Off
- Domain-joined, NetScaler-to-StoreFront smart card deployments —Set UseLocalUserAndPassword to On

For more instructions on setting these parameters, see the StoreFront or Citrix Gateway documentation.

The availability of single sign-on functionality depends on many factors including, but not limited to:

- Your organization's security policies regarding single sign-on.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

> **Note:**
>
> When a user logs on to the Virtual Delivery Agent (VDA) on a machine with an attached smart card reader, a Windows tile may appear representing the previous successful mode of authentication, such as smart card or password. As a result, when single sign-on is enabled, the single sign-on tile may appear. To log on, the user must select **Switch Users** to select another tile because the single sign-on tile will not work.

Transport Layer Security (TLS)

June 8, 2022

Citrix Virtual Apps and Desktops support the Transport Layer Security (TLS) protocol for TCP-based connections between components. Citrix Virtual Apps and Desktops also support the Datagram Transport Layer Security (DTLS) protocol for UDP-based ICA/HDX connections, using adaptive transport.

TLS and DTLS are similar, and support the same digital certificates. Configuring a Citrix Virtual Apps or Citrix Virtual Desktops Site to use TLS also configures it to use DTLS. Use the following procedures; the steps are common to both TLS and DTLS except where noted:

- Obtain, install, and register a server certificate on all Delivery Controllers, and configure a port with the TLS certificate. For details, see Install TLS server certificates on Controllers.

  Optionally, you can change the ports the Controller uses to listen for HTTP and HTTPS traffic.

- Enable TLS connections between Citrix Workspace app and Virtual Delivery Agents (VDAs) by completing the following tasks:

  - Configure TLS on the machines where the VDAs are installed. (For convenience, further references to machines where VDAs are installed are simply called "VDAs.") For general information, see TLS settings on VDAs. It is highly recommended that you use the Citrix supplied PowerShell script to configure TLS/DTLS. For details, see Configure TLS on a VDA using the PowerShell script. However, if you want to configure TLS/DTLS manually, see Manually configure TLS on a VDA.

  - Configure TLS in the Delivery Groups containing the VDAs by running a set of PowerShell cmdlets in Studio. For details, see Configure TLS on Delivery Groups.

    Requirements and considerations:

    * Enabling TLS connections between users and VDAs is valid only for XenApp 7.6 and XenDesktop 7.6 Sites, plus later supported releases.
    * Configure TLS in the Delivery Groups and on the VDAs after you install components, create a Site, create machine catalogs, and create Delivery Groups.
    * To configure TLS in the Delivery Groups, you must have permission to change Controller access rules. A Full Administrator has this permission.
    * To configure TLS on the VDAs, you must be a Windows administrator on the machine where the VDA is installed.
    * On pooled VDAs that are provisioned by Machine Creation Services or Provisioning Services, the VDA machine image is reset on restart, causing previous TLS settings to be lost. Run the PowerShell script each time the VDA is restarted to reconfigure the TLS settings.

> **Warning:**
>
> For tasks that include working in the Windows registry—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.

For information about enabling TLS to the Site database, see CTX137556.

Install TLS server certificates on Controllers

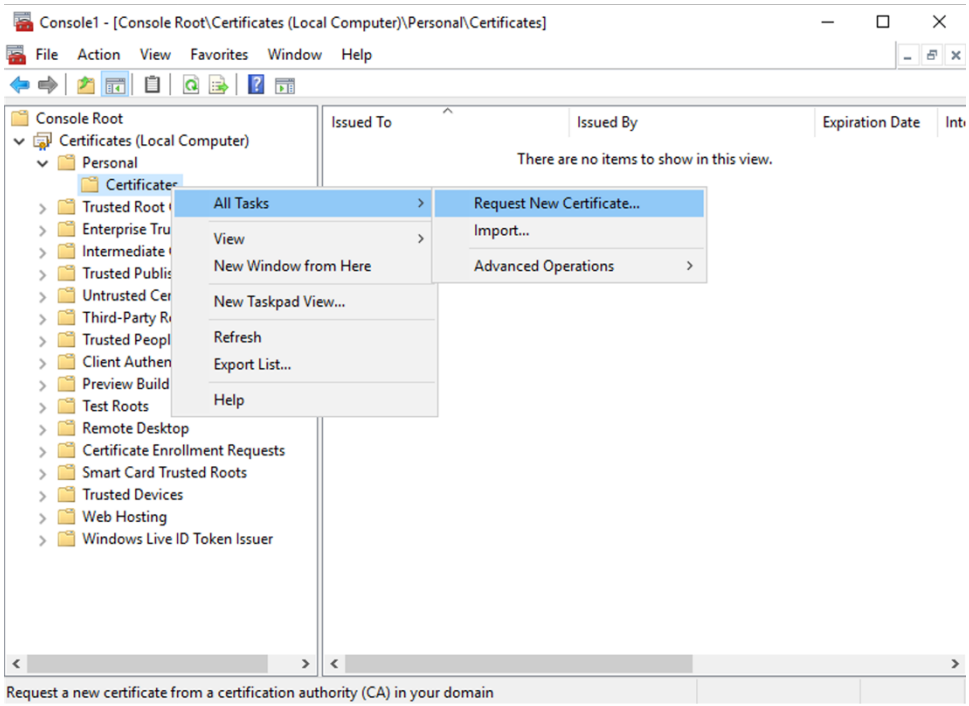
For HTTPS, the XML Service supports TLS features by using server certificates, not client certificates. This section describes acquiring and installing TLS certificates in Delivery Controllers. The same steps can be applied to Cloud Connectors to encrypt STA and XML traffic.

Although there are various different types of certificate authorities and methods of requesting certificate from them, this article describes the Microsoft Certificate Authority. The Microsoft Certificate Authority needs to have a certificate template published with a purpose of Server Authentication.

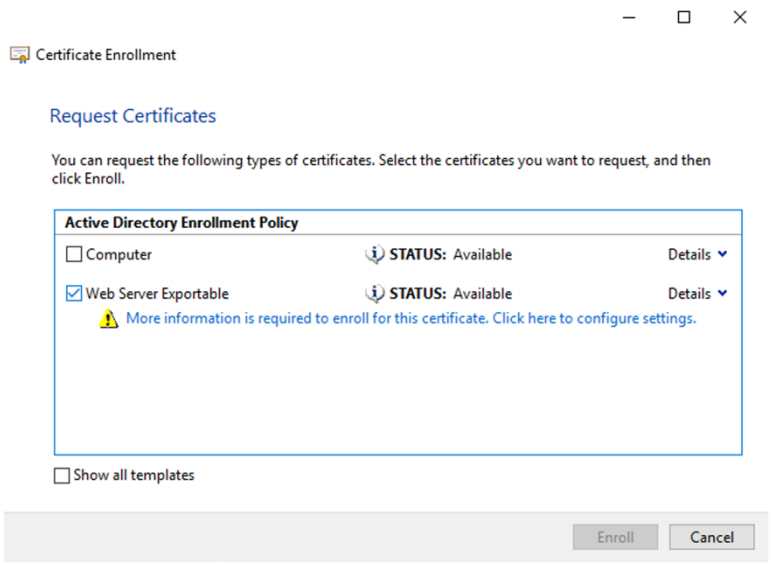
If the Microsoft Certificate Authority is integrated into an Active Directory domain or into the trusted forest the Delivery Controllers are joined to, you can acquire a certificate from the Certificates MMC snap-in Certificate Enrollment wizard.

Requesting and installing a certificate

1. On the Delivery Controller, open the MMC console and add the Certificates snap-in. When prompted select Computer account.
2. Expand **Personal > Certificates**, then use the **All Tasks > Request New Certificate** context menu command.



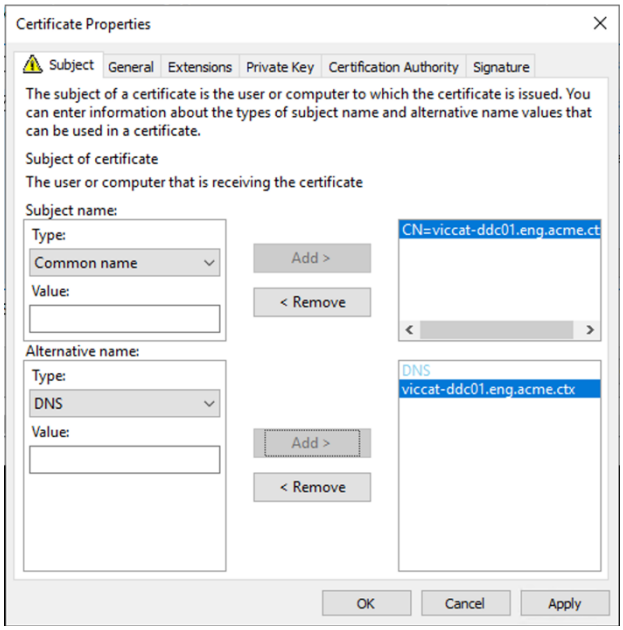
3. Click **Next** to begin, and **Next** to confirm that you are acquiring the certificate from Active Directory enrollment.
4. Select the template for Server Authentication certificate. If the template has been set up to automatically provide the values for Subject you can click **Enroll** without providing more details.



5. To provide more details for the certificate template, click the **Details** arrow button and configure the following:

   Subject name: select Common Name and add the FQDN of the Delivery Controller.

   Alternative name: select DNS and add the FQDN of the Delivery Controller.



Configuring SSL/TLS listener port

1. Open a PowerShell command window as an administrator of the machine.
2. Run the following commands to get Broker Service Application GUID:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $_; $_.GetValueNames() | ForEach-Object {
  $key.GetValue($_)  }
  | Where-Object {
  $_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
<!--NeedCopy-->
```

3. Run the following commands on the same PowerShell window to get the Thumbprint of the

certificate you installed previously:

```
$HostName = ([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $($Thumbprint)" -Foreground Yellow
<!--NeedCopy-->
```

4. Run the following commands on the same PowerShell window to configure the Broker Service SSL/TLS port and user the certificate for encryption:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1 | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint appid={
 $Formatted_Guid }
 "

$SSLxml | netsh

. netsh http show sslcert
<!--NeedCopy-->
```

When correctly configured, the output from the last command `.netsh http show sslcert` shows that the listener is using the correct `IP:port`, and that `Application ID` matches the Broker Service Application GUID.

Providing the servers trust the certificate installed on the Delivery Controllers, you can now configure StoreFront Delivery Controllers and Citrix Gateway STA bindings to use HTTPS instead of HTTP.

> **Note:**
>
> If the Controller is installed on Windows Server 2016 or Windows Server 2019, and StoreFront is installed on Windows Server 2012 R2, a configuration change is needed at the Controller or StoreFront, to change the order of TLS cipher suites. This configuration change is not needed for Controller and StoreFront with other combinations of Windows Server versions.

The cipher suite order list must include the `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, or `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` cipher suites (or both), or similar TLS_ECDHE cipher suites; and these TLS_ECDHE cipher suites must precede any TLS_DHE cipher suites.

1. Using the Microsoft Group Policy Editor, browse to Computer Configuration > Administrative Templates > Network > SSL Configuration Settings.
2. Edit the policy "SSL Cipher Suite Order". By default, this policy is set to "Not Configured". Set this policy to Enabled.
3. Arrange suites in the correct order; remove any cipher suites suites you do not want to use.

Ensure that either `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` or `TLS_ECDHE_RSA_WITH_AES_128_` , or similar TLS_ECDHE cipher suite, precedes any TLS_DHE cipher suites.

On Microsoft MSDN, see also Prioritizing Schannel Cipher Suites.

Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use non-default ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.

To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio:

BrokerService.exe -WIPORT <*http-port*> -WISSLPORT <*https-port*>

where <*http-port*> is the port number for HTTP traffic and <*https-port*> is the port number for HTTPS traffic.

> **Note:**
>
> After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
    XML_HTTPS |
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
<!--NeedCopy-->
```

Enforce HTTPS traffic only

If you want the XML Service to ignore HTTP traffic, create the following registry setting in HKLM\Software\Citrix\DesktopServer\ on the Controller and then restart the Broker Service.

To ignore HTTP traffic, create DWORD XmlServicesEnableNonSsl and set it to 0.

There is a corresponding registry DWORD value you can create to ignore HTTPS traffic: DWORD XmlServicesEnableSsl. Ensure that it is not set to 0.

TLS settings on VDAs

A Delivery Group cannot have a mixture of some VDAs with TLS configured and some VDAs without TLS configured. Before you configure TLS for a Delivery Group, ensure that you have already configured TLS for all the VDAs in that Delivery Group

When you configure TLS on VDAs, permissions on the installed TLS certificate are changed, giving the ICA Service read access to the certificate's private key, and informing the ICA Service of the following:

- **Which certificate in the certificate store to use for TLS**.
- **Which TCP port number to use for TLS connections**.

  The Windows Firewall (if enabled) must be configured to allow incoming connection on this TCP port. This configuration is done for you when you use the PowerShell script.
- **Which versions of the TLS protocol to allow.**

  > **Important:**
  >
  > Citrix recommends that you review your use of SSLv3, and reconfigure those deployments to remove support for SSLv3 where appropriate. See CTX200238.

  The supported TLS protocol versions follow a hierarchy (lowest to highest): SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. Specify the minimum allowed version; all protocol connections using that version or a higher version are allowed.

  For example, if you specify TLS 1.1 as the minimum version, then TLS 1.1 and TLS 1.2 protocol connections are allowed. If you specify SSL 3.0 as the minimum version, then connections for all the supported versions are allowed. If you specify TLS 1.2 as the minimum version, only TLS 1.2 connections are allowed.

  DTLS 1.0 corresponds to TLS 1.1, and DTLS 1.2 corresponds to TLS 1.2.
- **Which TLS cipher suites to allow.**

  A cipher suite selects the encryption that is used for a connection. Clients and VDAs can support different sets of cipher suites. When a client (Citrix Workspace app or StoreFront) connects and sends a list of supported TLS cipher suites, the VDA matches one of the client's cipher suites with one of the cipher suites in its own list of configured cipher suites, and accepts the connection. If there is no matching cipher suite, the VDA rejects the connection.

The VDA supports three sets of cipher suites (also known as compliance modes): GOV(ernment), COM(mercial), and ALL. The acceptable cipher suites also depend on the Windows FIPS mode; see http://support.microsoft.com/kb/811833 for information about Windows FIPS mode. The following table lists the cipher suites in each set:

TLS/DTLS cipher suite	ALL	COM	GOV	ALL	COM	GOV
FIPS Mode	Off	Off	Off	On	On	On
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 *	X	X	X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X	X	X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

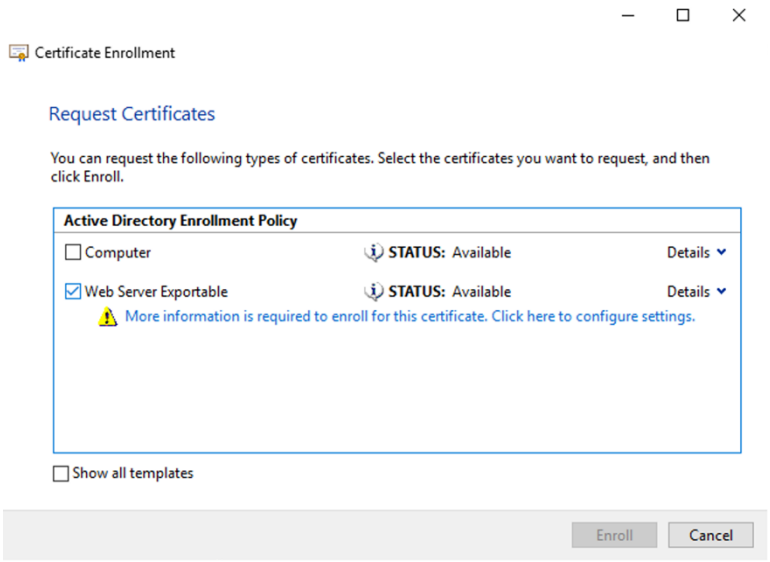
* Not supported in Windows Server 2012 R2.

> **Note:**
>
> The VDA does not support DHE ciphersuites (for example, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_DHE_RSA_WITH_AES_128_CBC_SHA.) If selected by Windows, they may not be used by Receiver.
>
> If you are using a Citrix Gateway, refer to the Citrix ADC documentation for information on cipher suite support for back-end communication. For information on TLS cipher suite support, see Ciphers available on the Citrix ADC appliances. For information on DTLS cipher suite support, see DTLS cipher support.

Requesting and installing a certificate

1. On the VDA, open the MMC console and add the Certificates snap-in. When prompted select Computer account.
2. Expand **Personal > Certificates**, then use the context menu command **All Tasks > Request New Certificate**.
3. Click **Next** to begin, and **Next** to confirm that you are acquiring the certificate from Active Directory enrollment.

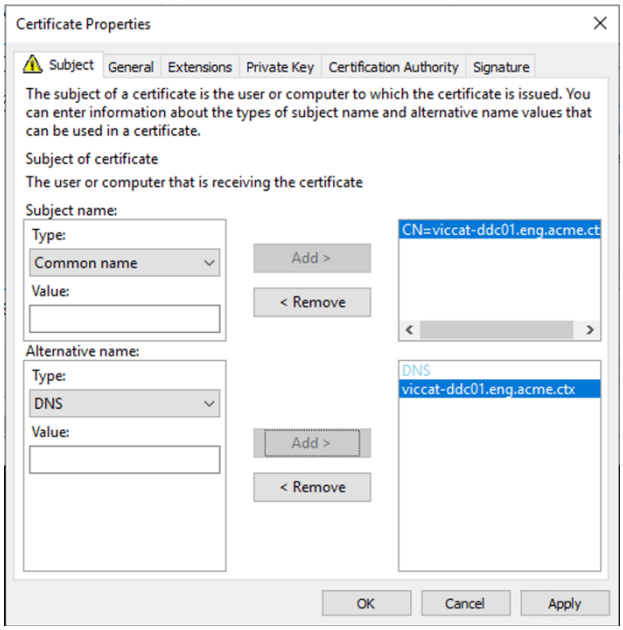
4. Select the template for Server Authentication certificate. Both the default Windows **Computer** or **Web Server Exportable** are acceptable. If the template has been set up to automatically provide the values for Subject, you can click **Enroll** without providing more details.



5. To provide more details for the certificate template, click **Details** and configure the following:

   Subject name —select type **Common name** and add the FQDN of the VDA

   Alternative name —select type **DNS** and add the FQDN of the VDA



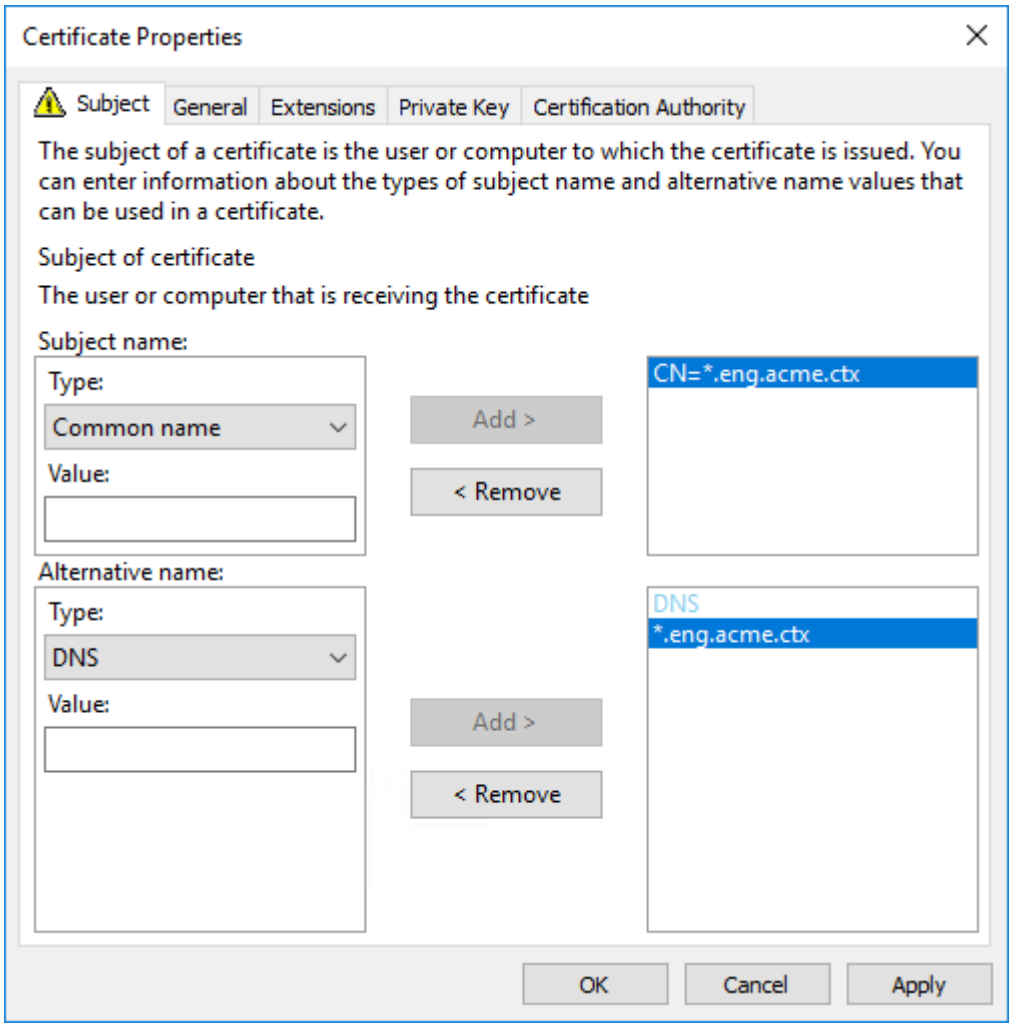
> **Note:**
>
> Use Active Directory Certificate Services Certificate Auto-Enrollment to automate issuing and deploying certificates to the VDAs. This is described in https://support.citrix.com/art

> icle/CTX205473.

You can use wildcard certificates to allow a single certificate to secure multiple VDAs:

Subject name —select type **Common name** and enter the *.primary.domain of the VDAs

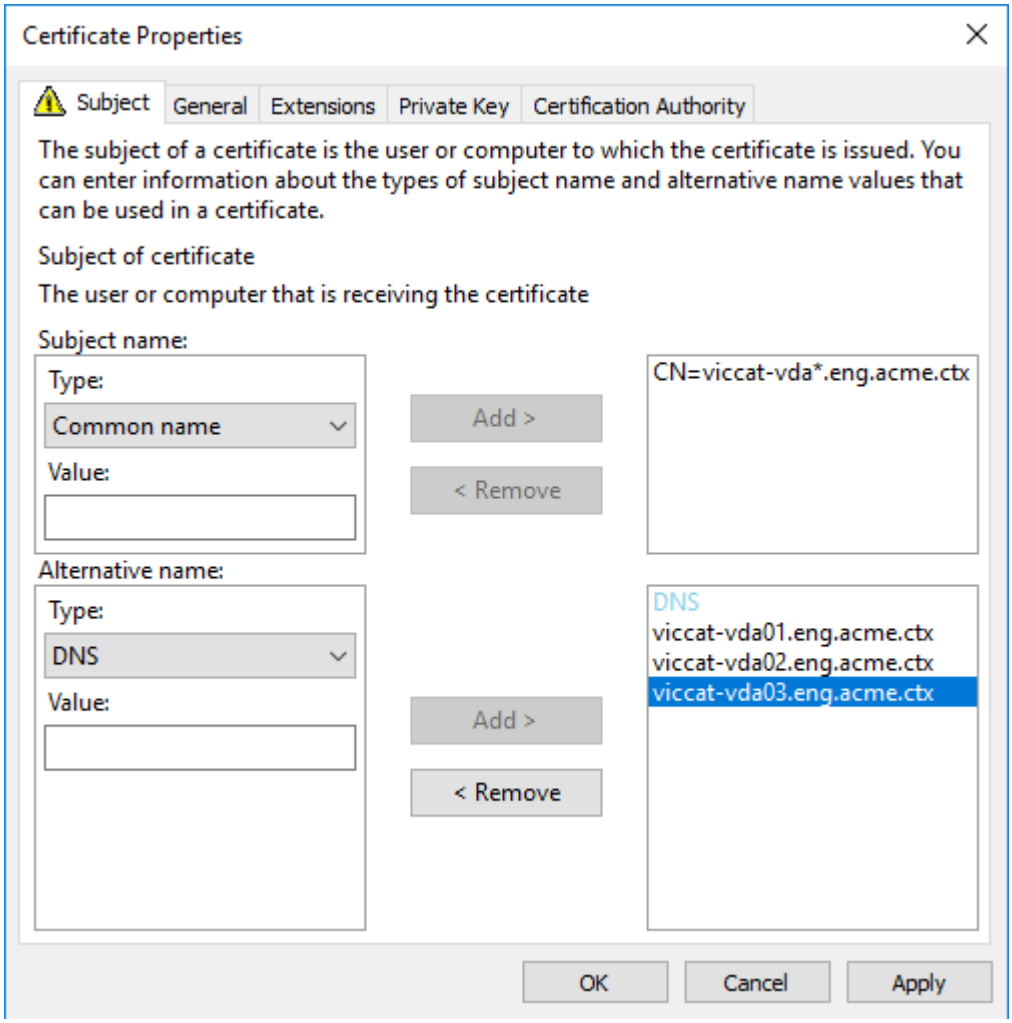
Alternative name —select type **DNS** and add the *.primary.domain of the VDAs



You can use SAN certificates to allow a single certificate to secure multiple specific VDAs:

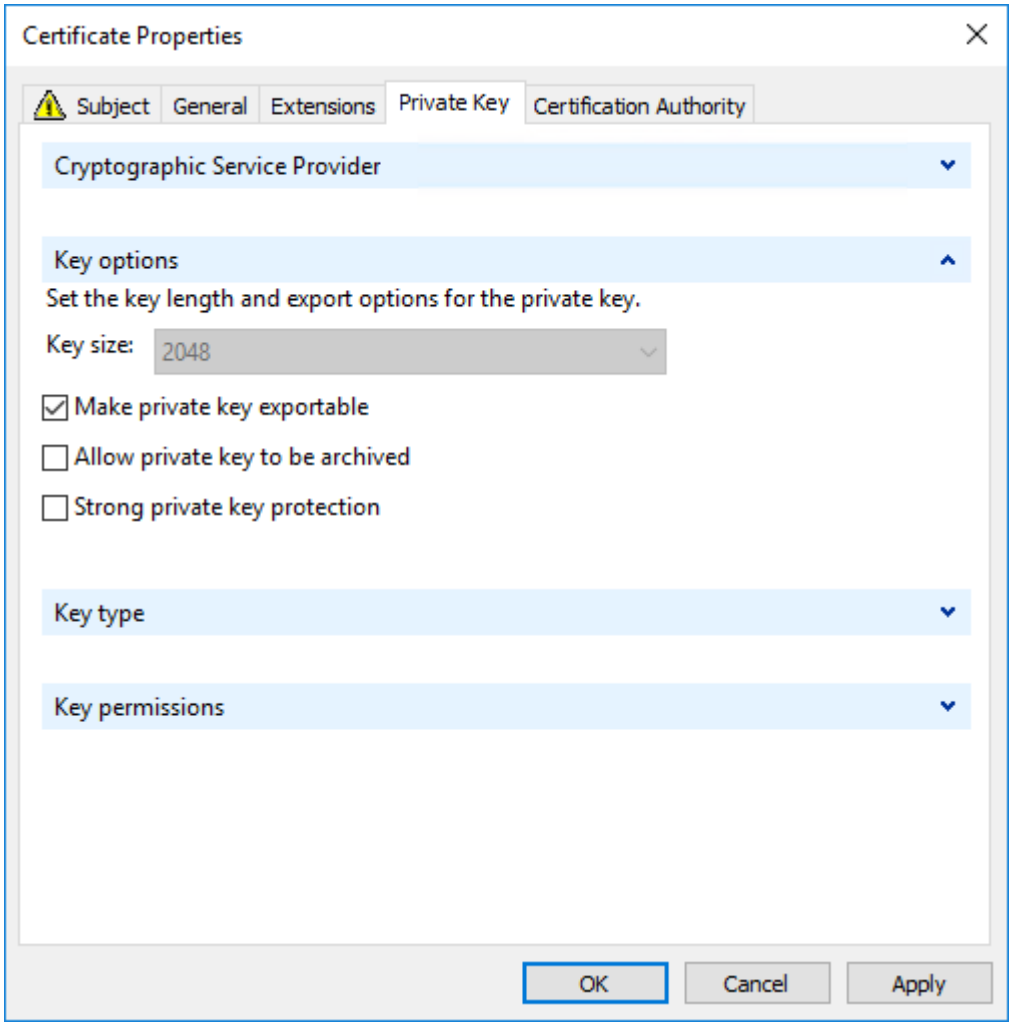
Subject name —select type **Common name** and enter a string to help identify the certificate usage

Alternative name —select type **DNS** and add an entry for the FQDN of each VDA. Keep the number of Alternative names to a minimum to ensure optimal TLS negotiation.



Note:

Both wildcard and SAN certificates require **Make private key exportable** on the Private Key tab to be selected:



Configure TLS on a VDA using the PowerShell script

Install the TLS Certificate in the Local Computer > Personal > Certificates area of the certificate store. If more than one certificate resides in that location, supply the thumbprint of the certificate to the PowerShell script.

> **Note:**
>
> Starting with XenApp and XenDesktop 7.16 LTSR, the PowerShell script finds the correct certificate based on the FQDN of the VDA. You do not need to supply the thumbprint when only a single certificate is present for the VDA FQDN.

The Enable-VdaSSL.ps1 script enables or disables the TLS listener on a VDA. This script is available in the *Support* > *Tools* > *SslSupport* folder on the installation media.

When you enable TLS, DHE cipher suites are disabled. ECDHE cipher suites are not affected.

When you enable TLS, the script disables all existing Windows Firewall rules for the specified TCP port. It then adds a new rule that allows the ICA Service to accept incoming connections only on the TLS TCP and UDP ports. It also disables the Windows Firewall rules for:

- Citrix ICA (default: 1494)
- Citrix CGP (default: 2598)
- Citrix WebSocket (default: 8008)

The effect is that users can only connect using TLS or DTLS. They cannot use ICA/HDX, ICA/HDX with Session Reliability, or HDX over WebSocket, without TLS or DTLS.

> **Note:**
>
> DTLS is not supported with ICA/HDX Audio over UDP Real-time Transport, or with ICA/HDX Framehawk.

See Network ports.

The script contains the following syntax descriptions, plus extra examples; you can use a tool such as Notepad++ to review this information.

> **Important:**
>
> Specify either the Enable or Disable parameter, and the CertificateThumbPrint parameter. The other parameters are optional.

Syntax `Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "\<thumbprint>"[–SSLPort \<port>] [-SSLMinVersion "\<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]`

Parameter	Description
Enable	Installs and enables the TLS listener on the VDA. Either this parameter or the Disable parameter is required.
Disable	Disables the TLS listener on the VDA. Either this parameter or the Enable parameter is required. If you specify this parameter, no other parameters are valid.

Parameter	Description
CertificateThumbPrint “”	Thumbprint of the TLS certificate in the certificate store, enclosed in quotation marks. The script uses the specified thumbprint to select the certificate you want to use. If this parameter is omitted, an incorrect certificate is selected.
SSLPort	TLS port. Default: 443
SSLMinVersion “”	Minimum TLS protocol version, enclosed in quotation marks. Valid values: “TLS_1.0” (default), “TLS_1.1”, and “TLS_1.2”.
SSLCipherSuite “”	TLS cipher suite, enclosed in quotation marks. Valid values: “GOV”, “COM”, and “ALL”(default).

Examples The following script installs and enables the TLS protocol version value. The thumbprint (represented as “12345678987654321”in this example) is used to select the certificate to use.

```
Enable-VdaSSL  – Enable -CertificateThumbPrint "12345678987654321"
```

The following script installs and enables the TLS listener, and specifies TLS port 400, the GOV cipher suite, and a minimum TLS 1.2 protocol value. The thumbprint (represented as “12345678987654321” in this example) is used to select the certificate to use.

```
Enable-VdaSSL  –  Enable
-CertificateThumbPrint "12345678987654321"
 – SSLPort 400  – SSLMinVersion "TLS_1.2"
 – SSLCipherSuite "All"
```

The following script disables the TLS listener on the VDA.

```
Enable-VdaSSL  – Disable
```

Manually configure TLS on a VDA

When configuring TLS on a VDA manually, you grant generic read access to the private key of the TLS certificate for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows Single-session OS, or NT SERVICE\TermService for a VDA for Windows Multi-session OS. On the machine where the VDA is installed:

STEP 1. Launch the Microsoft management console (MMC): Start > Run > mmc.exe.

STEP 2. Add the Certificates snap-in to the MMC:

1. Select File > Add/Remove Snap-in.
2. Select Certificates and then click Add.
3. When prompted with "This snap-in will always manage certificates for:"choose "Computer account"and then click Next.
4. When prompted with "Select the computer you want this snap-in to manage"choose "Local computer"and then click Finish.

STEP 3. Under Certificates (Local Computer) > Personal > Certificates, right–click the certificate and then select All Tasks > Manage Private Keys.

STEP 4. The Access Control List Editor displays "Permissions for (FriendlyName) private keys"where (FriendlyName) is the name of your TLS certificate. Add one of the following services and give it Read access:

- For a VDA for Windows Single-session OS, "PORTICASERVICE"
- For a VDA for Windows Multi-session OS, "TERMSERVICE"

STEP 5. Double-click the installed TLS certificate. In the certificate dialog, select the Details tab and then scroll to the bottom. Click Thumbprint.

STEP 6. Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Edit the SSL Thumbprint key and copy the value of the TLS certificate's thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as '0000'and special characters).
2. Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
3. If you want to change the default settings (optional), use the following in the same registry path:

   SSLPort DWORD –SSL port number. Default: 443.

   SSLMinVersion DWORD –1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Default: 2 (TLS 1.0).

   SSLCipherSuite DWORD –1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).

STEP 7. Ensure that the TLS TCP and UDP ports are that open in the Windows Firewall if they are not the default 443. (When you create the inbound rule in Windows Firewall, ensure its properties have the "Allow the connection"and "Enabled"entries selected.)

STEP 8. Ensure that no other applications or services (such as IIS) are using the TLS TCP port.

STEP 9. For VDAs for Windows Multi-session OS, restart the machine for the changes to take effect. (You do not need to restart machines containing VDAs for Windows Single-session OS.)

> **Important:**
>
> An extra step is necessary when the VDA is on Windows Server 2012 R2, Windows Server 2016, or Windows 10 Anniversary Edition or later supported release. This affects connections from Citrix Workspace app for HTML5, and Citrix Workspace app for Chrome. This also includes connections using Citrix Gateway.
>
> This step is also required for all connections using Citrix Gateway, for all VDA versions, if TLS between the Citrix Gateway and the VDA is configured.

On the VDA (Windows Server 2012 R2, Windows Server 2016, or Windows 10 Anniversary Edition or later), using the Group Policy Editor, go to Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order. Select the following order:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> **Note:**
>
> The first six items also specify the elliptic curve, P384 or P256. Ensure that "curve25519"is not selected. FIPS Mode does not prevent the use of "curve25519".

When this Group Policy setting is configured, the VDA selects a cipher suite only if appears in both lists: the Group Policy list and the list for the selected compliance mode (COM, GOV, or ALL). The cipher suite must also appear in the list sent by the client (Citrix Workspace app or StoreFront).

This Group Policy configuration also affects other TLS applications and services on the VDA. If your applications require specific cipher suites, you may need to add them to this Group Policy list.

> **Important:**
>
> Even though Group Policy changes are shown when they are applied, Group Policy changes for TLS configuration only take effect after an operating system restart. Therefore, for pooled desktops, apply the Group Policy changes for TLS configuration to the base image.

Configure TLS on Delivery Groups

Complete this procedure for each Delivery Group that contains VDAs you have configured for TLS connections.

1. From Studio, open the PowerShell console.
2. Run **asnp Citrix.*** to load the Citrix product cmdlets.

3. Run **Get-BrokerAccessPolicyRule -DesktopGroupName '*<delivery-group-name>*'| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Run **Set-BrokerSite -DnsResolutionEnabled $true**.

Troubleshooting

If a connection error occurs, check the system event log on the VDA.

When using Citrix Workspace app for Windows, if you receive a connection error that indicates a TLS error, disable Desktop Viewer and then try connecting again. Although the connection still fails an explanation of the underlying TLS issue might be provided. For example, you specified an incorrect template when requesting a certificate from the certificate authority.)

Most configurations that use HDX Adaptive Transport work successfully with DTLS, including those using the latest versions of Citrix Workspace app, Citrix Gateway, and the VDA. Some configurations which use DTLS between Citrix Workspace app and Citrix Gateway, and which use DTLS between Citrix Gateway and the VDA, require additional action.

Additional action is needed if either of the following also applies:

- the Citrix Gateway version supports DTLS to the VDA, but the VDA version does not support DTLS (version 7.15 or earlier),
- the VDA version supports DTLS (version 7.16 or later), but the Citrix Gateway version does not support DTLS to the VDA.

To avoid connections failing, do one of the following:

- update the Citrix Gateway to a version that supports DTLS to the VDA; or,
- update the VDA, to version 7.16 or later; or,
- disable DTLS at the VDA; or,
- disable HDX Adaptive Transport.

> **Note:**
>
> To disable DTLS at the VDA, modify the VDA firewall configuration to disable UDP port 443. See Network ports.

Communication between Controller and VDA

Windows Communication Framework (WCF) message-level protection secures communication between the Controller and the VDA. Extra transport-level protection using TLS is not required. The WCF configuration uses Kerberos for mutual authentication between the Controller and VDA. Encryption uses AES in CBC mode with a 256-bit key. Message integrity uses SHA-1.

According to Microsoft, the Security protocols used by WCF conform to standards from OASIS (Organization for the Advancement of Structured Information Standards), including WS-SecurityPolicy 1.2. Additionally, Microsoft states that WCF supports all algorithm suites listed in Security Policy 1.2.

Communication between the Controller and VDA uses the basic256 algorithm suite, whose algorithms are as stated above.

TLS and HTML5 video redirection, and browser content redirection

You can use HTML5 video redirection and browser content redirection to redirect HTTPS websites. The JavaScript injected into those websites must establish a TLS connection to the Citrix HDX HTML5 Video Redirection Service running on the VDA. To achieve this, the HTML5 Video Redirection Service generates two custom certificates in the certificate store on the VDA. Stopping the service removes the certificates.

The HTML5 video redirection policy is disabled by default.

The browser content redirection is enabled by default.

For more information on HTML5 video redirection, see Multimedia policy settings.

Transport Layer Security (TLS) on Universal Print Server

February 7, 2020

The Transport Layer Security (TLS) protocol is supported for TCP-based connections between the Virtual Delivery Agent (VDA) and the Universal Print Server.

> **Warning:**
>
> For tasks that include working in the Windows registry—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.

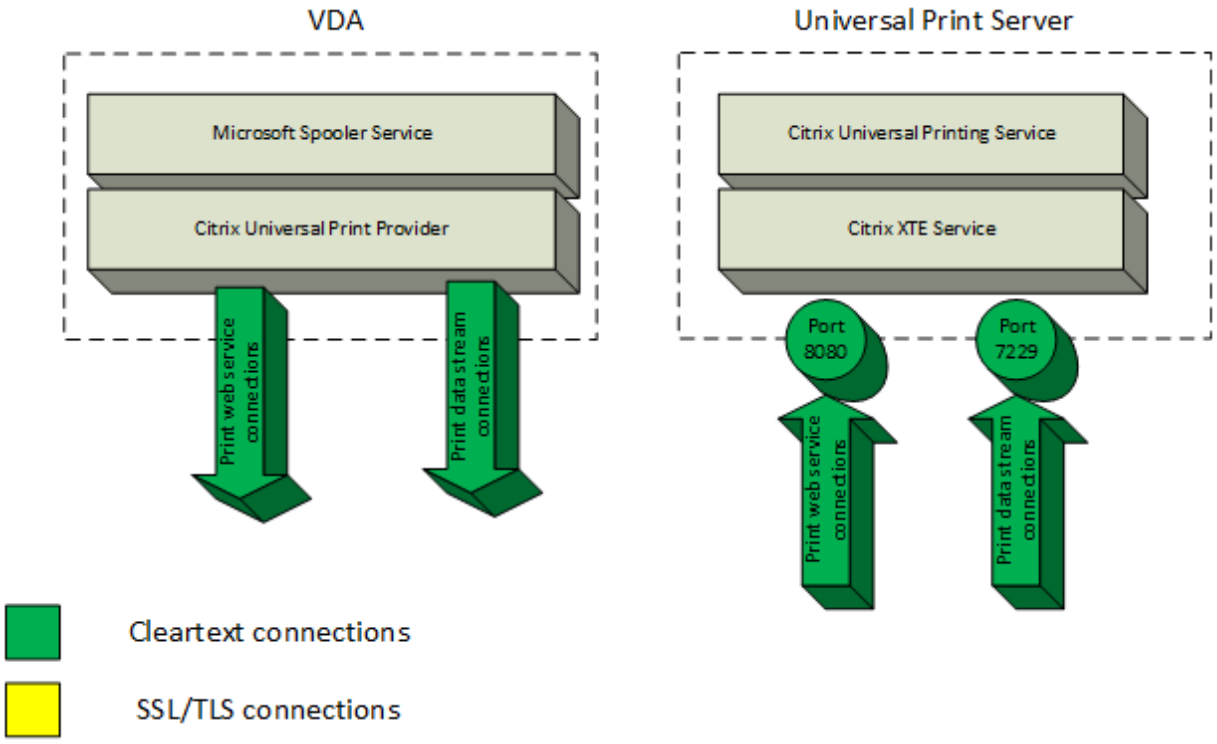
Types of printing connections between the VDA and Universal Print Server

Cleartext connections

The following connections related to printing originate from the VDA and connect to ports on the Universal Print Server. These connections are made only when the **SSL enabled** policy setting is set to **Disabled** (the default).

- Cleartext print web service connections (TCP port 8080)
- Cleartext print data stream (CGP) connections (TCP port 7229)

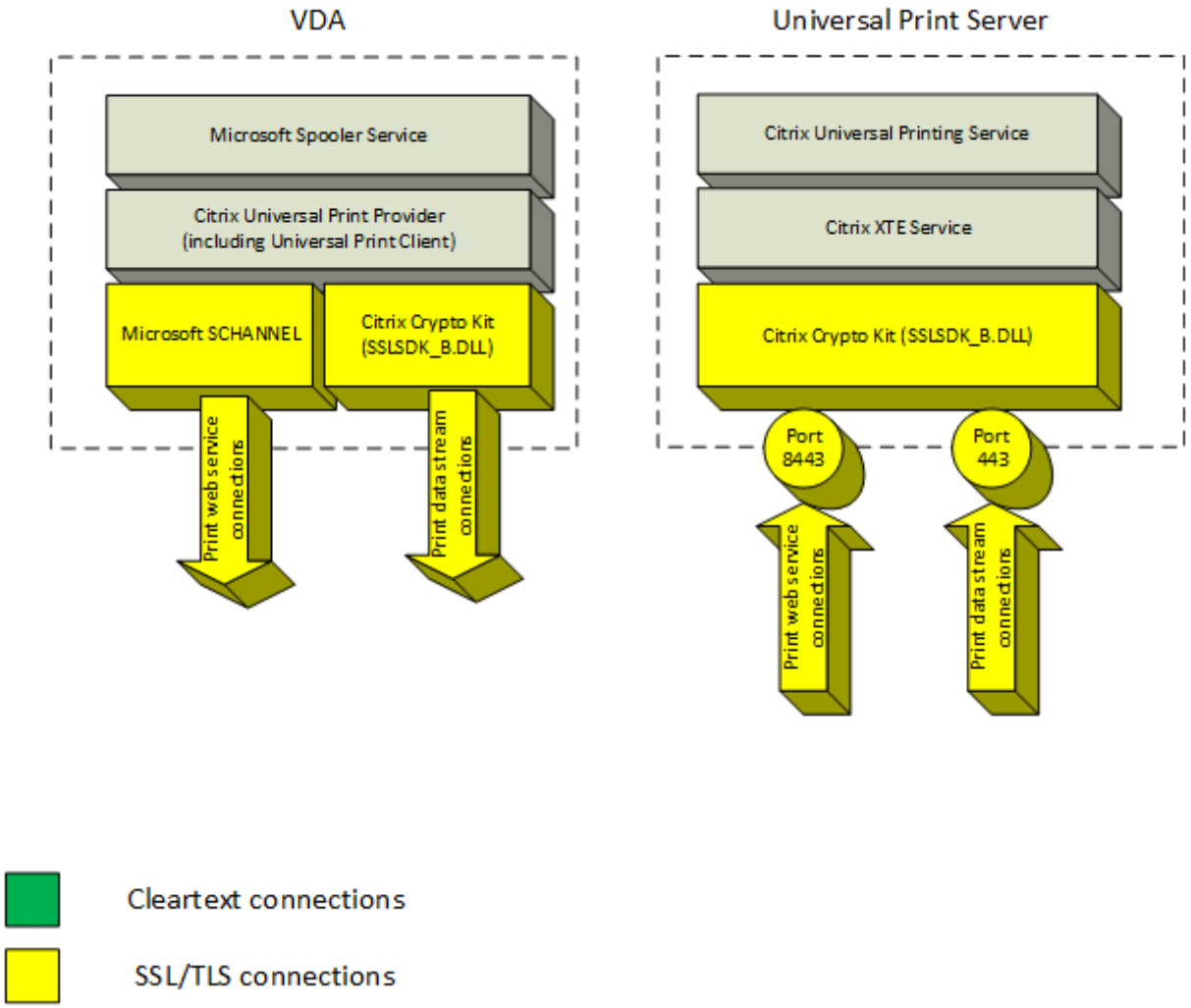
The Microsoft support article Service overview and network port requirements for Windows describes the ports used by the Microsoft Windows Print Spooler Service. The SSL/TLS settings in this document do not apply to the NETBIOS and RPC connections made by the Windows Print Spooler service. The VDA uses the Windows Network Print Provider (win32spl.dll) as a fallback if the **Universal Print Server enable** policy setting is set to **Enabled with fallback to Windows' native remote printing**.



Encrypted connections

These SSL/TLS connections related to printing originate from the VDA and connect to ports on the Universal Print Server. These connections are made only when the **SSL enabled** policy setting is set to **Enabled**.

- Encrypted print web service connections (TCP port 8443)
- Encrypted print data stream (CGP) connections (TCP port 443)



SSL/TLS client configuration

The VDA functions as the SSL/TLS client.

Use Microsoft Group Policy and the registry to configure Microsoft SCHANNEL SSP for encrypted print web service connections (TCP port 8443). The Microsoft support article TLS Registry Settings describes the registry settings for Microsoft SCHANNEL SSP.

Using the Group Policy Editor on the VDA (Windows Server 2016 or Windows 10), go to **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order**. Select the following order:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **Note:**
>
> When this Group Policy setting is configured, the VDA selects a cipher suite for encrypted print web service connections (default port: 8443) only if the connections appears in both SSL cipher suite lists:
>
> - Group Policy SSL cipher suite order list
> - List corresponding to the selected SSL Cipher Suite policy setting (COM, GOV, or ALL)
>
> This Group Policy configuration also affects other TLS applications and services on the VDA. If your applications require specific cipher suites, you might need to add them to this Group Policy Cipher Suite Order list.
>
> **Important:**
>
> Group Policy changes for TLS configuration take effect only after an operating system restart.
>
> Use a Citrix policy to configure SSL/TLS settings for encrypted print data stream (CGP) connections (TCP port 443).

SSL/TLS server configuration

The Universal Print Server functions as the SSL/TLS server.

Use the `Enable-UpsSsl.ps1` PowerShell script to configure SSL/TLS settings.

Install the TLS server certificate on the Universal Print Server

For HTTPS, the Universal Print Server supports TLS features by using server certificates. Client certificates are not used. Use Microsoft Active Directory Certificate Services or another certification authority to request a certificate for the Universal Print Server.

Keep in mind the following considerations when enrolling/requesting a certificate using Microsoft Active Directory Certificate Services:

1. Place the certificate in the Local Computer **Personal** certificate store.
2. Set the **Common Name** attribute of the Subject Distinguished Name (Subject DN) of the certificate to the fully qualified domain name (FQDN) of the Universal Print Server. Specify this in the certificate template.
3. Set the Cryptographic Service Provider (CSP) used to generate the certificate request and private key to **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Specify this in the certificate template.

4. Set the Key Size to at least 2048 bits. Specify this in the certificate template.

Configuring SSL on the Universal Print Server

The XTE Service on the Universal Print Server listens for incoming connections. It functions as an SSL server when SSL is enabled. The incoming connections have two types: print web service connections, which contain printing commands, and print data stream connections, which contain print jobs. SSL can be enabled on these connections. SSL protects the confidentiality and integrity of these connections. By default, SSL is disabled.

The PowerShell script used to configure SSL is on the installation media and has this file name: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

Configuring listening port numbers on the Universal Print Server

These are default ports for the XTE Service:

- Cleartext print web service (HTTP) TCP port: 8080
- Cleartext print data stream (CGP) TCP port: 7229
- Encrypted print web service (HTTPS) TCP port: 8443
- Encrypted print data stream (CGP) TCP port: 443

To change the ports used by the XTE Service on the Universal Print Server, run the following commands in PowerShell as administrator (see the later section for notes on the usage of the Enable-UpsSsl.ps1 PowerShell script):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` or `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

TLS settings on Universal Print Server

If you have multiple Universal Print Servers in a load-balanced configuration, ensure that the TLS settings are configured consistently across all Universal Print Servers.

When you configure TLS on Universal Print Server, permissions on the installed TLS certificate are changed, giving the Universal Printing Service read access to the certificate's private key, and informing the Universal Printing Service of the following:

- Which certificate in the certificate store to use for TLS.
- Which TCP port numbers to use for TLS connections.

The Windows Firewall (if enabled) must be configured to allow incoming connections on these TCP ports. This configuration is done for you when you use the Enable-UpsSsl.ps1 PowerShell script.

- Which versions of the TLS protocol to allow.

Universal Print Server supports TLS protocol versions 1.2, 1.1 and 1.0. Specify the minimum allowed version.

The default TLS protocol version is 1.2.

- Which TLS cipher suites to allow.

A cipher suite selects the cryptographic algorithms that are used for a connection. VDAs and Universal Print Server can support different sets of cipher suites. When a VDA connects and sends a list of supported TLS cipher suites, the Universal Print Server matches one of the client's cipher suites with one of the cipher suites in its own list of configured cipher suites, and accepts the connection. If there is no matching cipher suite, the Universal Print Server rejects the connection.

The Universal Print Server supports the following sets of cipher suites named GOV(ernment), COM(mercial), and ALL for the OPEN, FIPS and SP800-52 native Crypto Kit modes. The acceptable cipher suites also depend on the **SSL FIPS Mode** policy setting and on the Windows FIPS Mode. See this Microsoft support article for information about Windows FIPS mode.

Cipher suite (in decreasing priority order)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

Configure TLS on a Universal Print Server using the PowerShell script

Install the TLS Certificate in the **Local Computer > Personal > Certificates** area of the certificate store. If more than one certificate resides in that location, supply the thumbprint of the certificate to the `Enable-UpsSsl.ps1` PowerShell script.

> **Note:**
>
> The PowerShell script finds the correct certificate based on the FQDN of the Universal Print Server. You do not need to supply the certificate thumbprint when only a single certificate is present for the Universal Print Server FQDN.

The `Enable-UpsSsl.ps1` script enables or disables TLS connections originating from the VDA to the Universal Print Server. This script is available in the **Support > Tools > SslSupport** folder on the installation media.

When you enable TLS, the script disables all existing Windows Firewall rules for the Universal Print Server's TCP ports. It then adds new rules that allow the XTE Service to accept incoming connections only on the TLS TCP and UDP ports. It also disables the Windows Firewall rules for:

- Cleartext print web service connections (default: 8080)
- Cleartext print data stream (CGP) connections (default: 7229)

The effect is that the VDA can make these connections only when using TLS.

> **Note:**
>
> Enabling TLS does not affect Windows Print Spooler RPC/SMB connections originating from the VDA and going to the Universal Print Server.
>
> **Important:**
>
> Specify either **Enable** or **Disable** as the first parameter. The CertificateThumbprint parameter is optional if only one certificate in the Local Computer Personal certificate store has the Universal Print Server's FQDN. The other parameters are optional.

Syntax

```
1 Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
     HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
     SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
     FIPSMode <Boolean>] [-ComplianceMode <mode>]
2 Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

Parameter	Description
Enable	Enables SSL/TLS on the XTE Server. Either this parameter or the Disable parameter is required.
Disable	Disables SSL/TLS on the XTE Server. Either this parameter or the Enable parameter is required.

Parameter	Description
CertificateThumbprint "<thumbprint>"	Thumbprint of the TLS certificate in the Local Computer Personal certificate store, enclosed in quotation marks. The script uses the specified thumbprint to select the certificate you want to use.
HTTPPort <port>	Cleartext print web service (HTTP/SOAP) port. Default: 8080
CGPPort <port>	Cleartext print data stream (CGP) port. Default: 7229
HTTPSPort <port>	Encrypted print web service (HTTPS/SOAP) port. Default: 8443
CGPSSLPort <port>	Encrypted print data stream (CGP) port. Default: 443
SSLMinVersion "<version>"	Minimum TLS protocol version, enclosed in quotation marks. Valid values: “TLS_1.0”, “TLS_1.1”, and “TLS_1.2”. Default: TLS_1.2.
SSLCipherSuite “ <name>”	Name of TLS cipher suite package, enclosed in quotation marks. Valid values: “GOV”, “COM”, and “ALL”(default).
FIPSMode <Boolean>	Enables or disables FIPS 140 mode in the XTE Server. Valid values: $true to enable FIPS 140 mode, $false to disable FIPS 140 mode.

Examples

The following script enables TLS. The thumbprint (represented as “12345678987654321”in this example) is used to select the certificate to use.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

The following script disables TLS.

```
Enable-UpsSsl.ps1 –Disable
```

Configuring FIPS mode

Enabling US Federal Information Processing Standards (FIPS) mode ensures that only FIPS 140 compliant cryptography is used for Universal Print Server encrypted connections.

Configure FIPS mode on the server before configuring FIPS mode on the client.

Consult Microsoft's documentation site for enabling/disabling Windows FIPS mode.

Enabling FIPS mode on the client

On the Delivery Controller, run Citrix Studio and set the **SSL FIPS Mode** Citrix policy setting to **Enabled**. Enable the Citrix policy.

Do this on each VDA:

1. Enable Windows FIPS mode.
2. Restart the VDA.

Enabling FIPS mode on the server

Do this on each Universal Print Server:

1. Enable Windows FIPS mode.
2. Run this PowerShell command as Administrator: `stop-service CitrixXTEServer, UpSvc`
3. Run the `Enable-UpsSsl.ps1` script with the `-Enable -FIPSMode $true` parameters.
4. Restart the Universal Print Server.

Disabling FIPS mode on the client

On the Delivery Controller, run Citrix Studio and set the **SSL FIPS Mode** Citrix policy setting to **Disabled**. Enable the Citrix policy. You can also delete the **SSL FIPS Mode** Citrix policy setting.

Do this on each VDA:

1. Disable Windows FIPS mode.
2. Restart the VDA.

Disabling FIPS mode on the server

Do this on each Universal Print Server:

1. Disable Windows FIPS mode.
2. Run this PowerShell command as Administrator: `stop-service CitrixXTEServer, UpSvc`
3. Run the `Enable-UpsSsl.ps1` script with the `-Enable -FIPSMode $false` parameters.

4. Restart the Universal Print Server.

Configuring SSL/TLS protocol version

The default SSL/TLS protocol version is TLS 1.2. TLS 1.2 is the only recommended SSL/TLS protocol version for production use. For troubleshooting, it might be necessary to temporarily change the SSL/TLS protocol version in a non-production environment.

SSL 2.0 and SSL 3.0 are not supported on the Universal Print Server.

Setting SSL/TLS protocol version on the server

Do this on each Universal Print Server:

1. Run this PowerShell command as Administrator: `stop-service CitrixXTEServer, UpSvc`
2. Run the `Enable-UpsSsl.ps1` script with the `-Enable -SSLMinVersion` version parameters. Remember to set this back to TLS 1.2 when you are done testing.
3. Restart the Universal Print Server.

Setting SSL/TLS protocol version on the client

Do this on each VDA:

1. On the Delivery Controller, set the **SSL Protocol Version** policy setting to the desired protocol version and enable the policy.

2. The Microsoft support article TLS Registry Settings describes the registry settings for Microsoft SCHANNEL SSP. Enable the client-side **TLS 1.0, TLS 1.1 or TLS 1.2** using the registry settings.

> **Important:**
>
> Remember to restore the registry settings to their original values when you are done testing.

3. Restart the VDA.

Troubleshooting

If a connection error occurs, check the C:\Program Files (x86)\Citrix\XTE\logs\error.log log file on the Universal Print Server.

The error message **SSL handshake from client failed** appears in this log file if the SSL/TLS handshake fails. Such failures can occur if the SSL/TLS protocol version on the VDA and the Universal Print Server do not match.

Use the Universal Print Server FQDN in the following policy settings that contain Universal Print Server host names:

- Session printers
- Printer assignments
- Universal Print Servers for load balancing

Ensure that the system clock (date, time, and time zone) are correct on the Universal Print Servers and the VDAs.

Virtual channel security

November 5, 2021

By default, the Virtual channel allow list feature is disabled. When enabled, only Citrix virtual channels are allowed to open in 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.

Adding virtual channels to the allow list

To add a virtual channel to the allow list, you need:

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, these can be added separated by commas.

> **Note:**
>
> After making changes to the policy, reboot the VDA to ensure the changes take effect.

Using the previous examples, you would add the following to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

If there are multiple processes, you would add the following to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

Citrix virtual channel considerations

All built-in Citrix virtual channels are trusted and allowed to open without further configuration. However, there are two features that require explicit entries in the allow list due to external dependencies:

- Multimedia Redirection
- HDX RealTime Optimization Pack for Skype for Business

Multimedia Redirection

This 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

This 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`

Obtaining 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 third-party vendor that provided the virtual channel.

Alternatively, this information can be obtained 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 in the following event:
    - In a single-session VDA, event ID 2004 from source Picadd.
    - In a multi-session VDA, event ID 16 from source Rpm.
3. Log off from the session.
4. Add an entry in the Virtual channel allow list policy setting for the identified virtual channel, with just the virtual channel name.
5. Reboot the VDA.
6. Launch the virtual application or virtual desktop again.
7. In the VDA machine's System event log, look for the process that tried to open the virtual channel in the following event:
    - In a single-session VDA, event ID 2002 from source Picadd.
    - In a multi-session VDA, event ID 14 from source Rpm.
8. Log off from the session.
9. Edit the entry in the Virtual channel allow list policy setting to include the identified process.
10. Reboot the VDA.
11. Launch the virtual application or virtual desktop to validate that the custom virtual channel opens successfully.

Virtual channel allow list logging

The following events are logged in the single session VDA machine's event log:

Log Name	System
Id	2001

Source	Picadd
Level	Information
Description	Custom virtual channel <vcName> has been opened by process <processName>

Log Name	System
Id	2002
Source	Picadd
Level	Warning
Description	Custom virtual channel <vcName> cannot be opened by process <processName>

Log Name	System
Id	2003
Source	Picadd
Level	Information
Description	<username> opened custom virtual channel <vcName>

Log Name	System
Id	2004
Source	Picadd
Level	Warning

	Description	<username> tried to open custom virtual channel <vcName>

The following events are logged in the multi session VDA machine's event log:

	Log Name	System
	Id	13
	Source	Rpm
	Level	Information
	Description	Custom virtual channel <vcName> has been opened by process <processName>

	Log Name	System
	Id	14
	Source	Rpm
	Level	Warning
	Description	Custom virtual channel <vcName> cannot be opened by process <processName>

	Log Name	System
	Id	15
	Source	Rpm
	Level	Information

	Description	<username> opened custom virtual channel <vcName>

	Log Name	System
	Id	16
	Source	Rpm
	Level	Warning
	Description	<username> tried to open custom virtual channel <vcName>

Known third-party virtual channels

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
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- Epic Warp Drive
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings for VDI

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

February 6, 2020

HDX provides a high-definition user experience on any device, at any location. The articles in the Devices section describe these devices:

- Generic USB device
- Mobile and touch screen devices
- Serial devices
- Specialty keyboards
- TWAIN devices
- Webcams

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

Generic USB devices

February 6, 2020

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.

Mobile and touch screen devices

August 3, 2022

Tablet mode for touch screen devices using Windows Continuum

Continuum is a Windows 10 feature that adapts to the way the client device is used. This version of Continuum support, including dynamic change of modes, is available starting at VDA version 7.16 and Citrix Receiver for Windows version 4.10.

Windows 10 VDA detects the presence of a keyboard or mouse on a touch enabled client and puts the client in to desktop mode. If a keyboard or mouse is not present, Windows 10 VDA puts the client in to tablet/mobile mode. This detection occurs on connection and reconnection. It also occurs at dynamic attachment or detachment of the keyboard or mouse.

The feature is enabled by default. To disable this version of the feature, edit the Tablet mode toggle policy settings in the ICA policy settings article.

For the feature version included in XenApp 7.14 and 7.15 LTSR and XenDesktop 7.14 and 7.15 LTSR, use the registry settings to disable the feature. For more information, see Tablet mode for touch screen devices.

The **tablet mode** offers a user interface that is better suited to touch screens:

- Slightly larger buttons.
- The Start screen and any apps you start open in a full screen.
- Taskbar contains a back button.
- Icons deleted from the task bar.

You have access to the File Explorer.

The **desktop mode** offers the traditional user interface where you interact in the same manner as using PC and a keyboard and mouse.

Tablet mode requires a minimum of version Citrix Hypervisor 8.2 CU1 LTSR. Citrix Hypervisor integrates with the Citrix Virtual Desktops VDA, changing the hypervisor to enable the virtual firmware settings for 2-in-1 devices. Windows 10 loads the GPIO driver on the target virtual machine based on this updated BIOS. It is used for toggling between tablet and desktop modes within the virtual machine.

Citrix Workspace app for HTML5 (the light version) does not support Windows Continuum features.

Run the XenServer CLI command to allow laptop/tablet switching:
xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

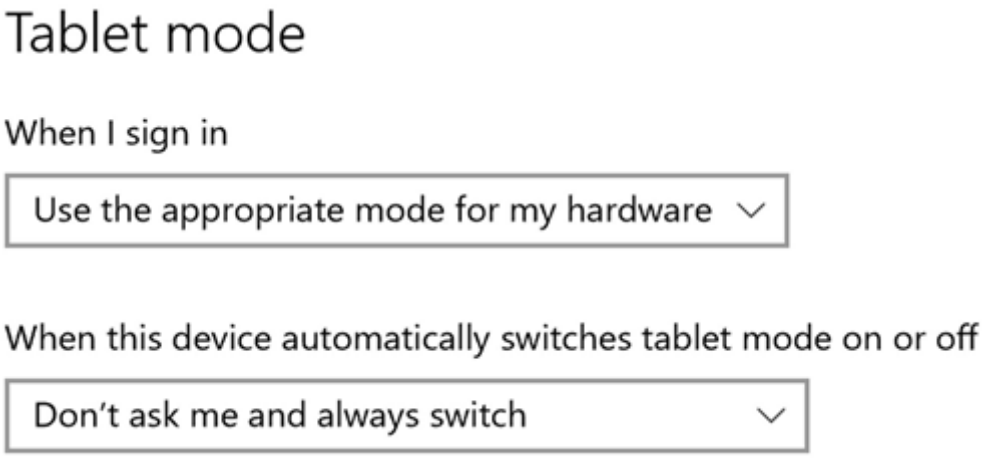
> **Important:**
> Updating the base image for an existing machine catalog after changing the metadata setting doesn't affect any previously provisioned VMs. After changing the XenServer VM base image, create a catalog, choose the base image, and provision a new Machine Creation Services (MCS) machine.

Before starting a session:

We recommend that you navigate to **Settings > System > Tablet Mode** on the VDA before starting a session and set the following options from the drop-down menus:

- Use the appropriate mode for my hardware
- Don't ask me and always switch

If you don't set these options before starting the session, set the options after you start the session and restart the VDA.



Microsoft Surface Pro and Surface Book pens

We support standard pen functionality with Windows Ink-based applications. This functionality requires a Virtual Delivery Agent running on a minimum of Microsoft Windows 10 version 1809 and client devices using a minimum of Citrix Workspace app for Windows version 1902. Support includes pointing, erasing, pen pressure, Bluetooth signals, and other features depending on the operating system firmware and pen model. For example, pen pressure can be up to 4096 levels. This feature is enabled by default.

For a demonstration of Windows Ink and the pen functionality, click this graphic:

System requirements

- Citrix Virtual Apps and Desktops minimum version 1903
- Citrix Workspace app for Windows minimum version 1902
- Microsoft Windows 10 minimum version 1809

Disable or enable

To disable or enable this feature, set the following registry:

HKEY_LOCAL_MACHINE\Software\ Citrix\Citrix Virtual Desktop Agent\PenApi

Name: DisablePen

Type: DWORD

Value:

1 - disables

0 - enables

Serial ports

February 24, 2023

Most new PCs don't have built-in serial (COM) ports. The ports are easy to add by using USB converters. Applications suited for serial ports often involve sensors, controllers, old check readers, pads, and

so forth. Some USB virtual COM-port devices use vendor-specific drivers in place of the Windows-provided drivers (usbser.sys). These drivers allow you to force the virtual COM port of the USB device so that it doesn't change even if connected to different USB sockets. This might be done from the **Device Manager > Ports (COM & LPT) > Properties** or from the application that controls the device.

Client COM port mapping allows devices attached to the COM ports on the user's endpoint to be used during virtual sessions. You can use these mappings like any other network mappings.

For each COM port, a driver in the operating system assigns a symbolic link name such as COM1 and COM2. The applications then use the link to access the port.

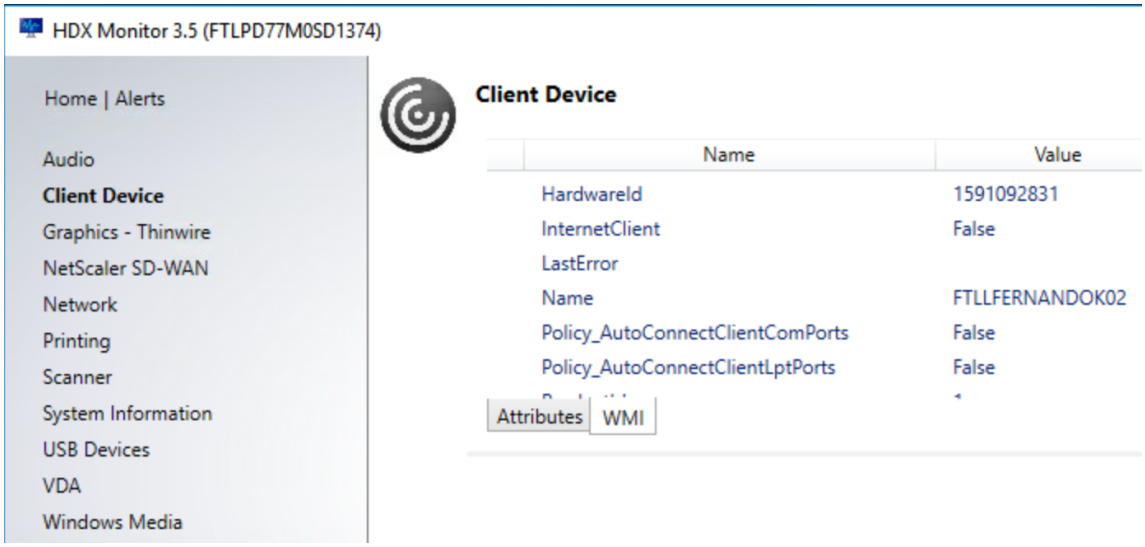
> **Important:**
> Because a device can attach to the endpoint by using USB directly, doesn't mean it can be redirected using generic USB redirection. Some USB devices function as virtual COM ports, which applications can access in the same way as physical serial port. The operating system can abstract COM ports and treat them like fileshares. Two common protocols for virtual COM are CDC ACM or MCT. When connected through an RS-485 port, applications might not work at all. Get an RS-485-to-RS232 converter to use RS-485 as a COM port.
> **Important:**
> Some applications recognize the device (for example, a signature pad) consistently only if it is connected to COM1 or COM2 on the client workstation.

Map a client COM port to a server COM port

You can map client COM ports to a Citrix session in three ways:

- Studio policies. For more information about policies, see Port redirection policy settings.
- VDA command prompt.
- Remote Desktop (Terminal Services) configuration tool.

1. Enable the **Client COM port redirection** and the **Auto connect client COM ports Studio** policies. After applied, some information is available in HDX Monitor.



2. If **Auto connect client COM ports** failed to map the port, you can map the port manually or use logon scripts. Log on to the VDA, and at a command prompt window, type:

   NET USE COMX: \\CLIENT\COMZ:

   Or

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   X is the number of the COM port on the VDA (ports 1 through 9 are available for mapping). **Z** is the number of the client COM port you want to map.

   To confirm that the operation was successful, type **NET USE** at a VDA command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.

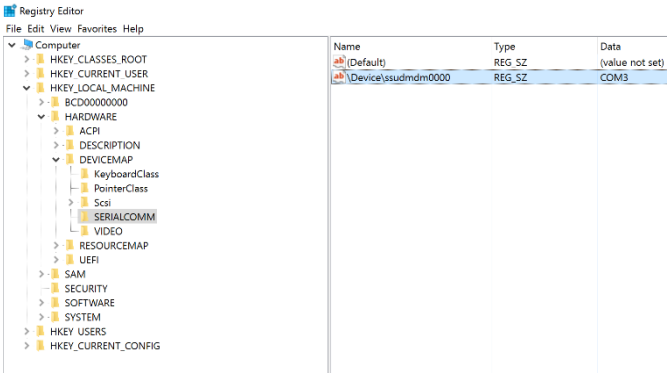
3. To use this COM port in a virtual desktop or application, install your user device application and point it to the mapped COM port name. For example, if you map COM1 on the client to COM3 on the server, install your COM port device application in the VDA and point it to COM3 during the session. Use this mapped COM port as you would a COM port on the user device.

> **Important:**
> COM port mapping is not TAPI-compatible. You can't map Windows Telephony Application Programming Interface (TAPI) devices to client COM ports. TAPI defines a standard way for applications to control telephone functions for data, fax, and voice calls. TAPI manages signaling, in-

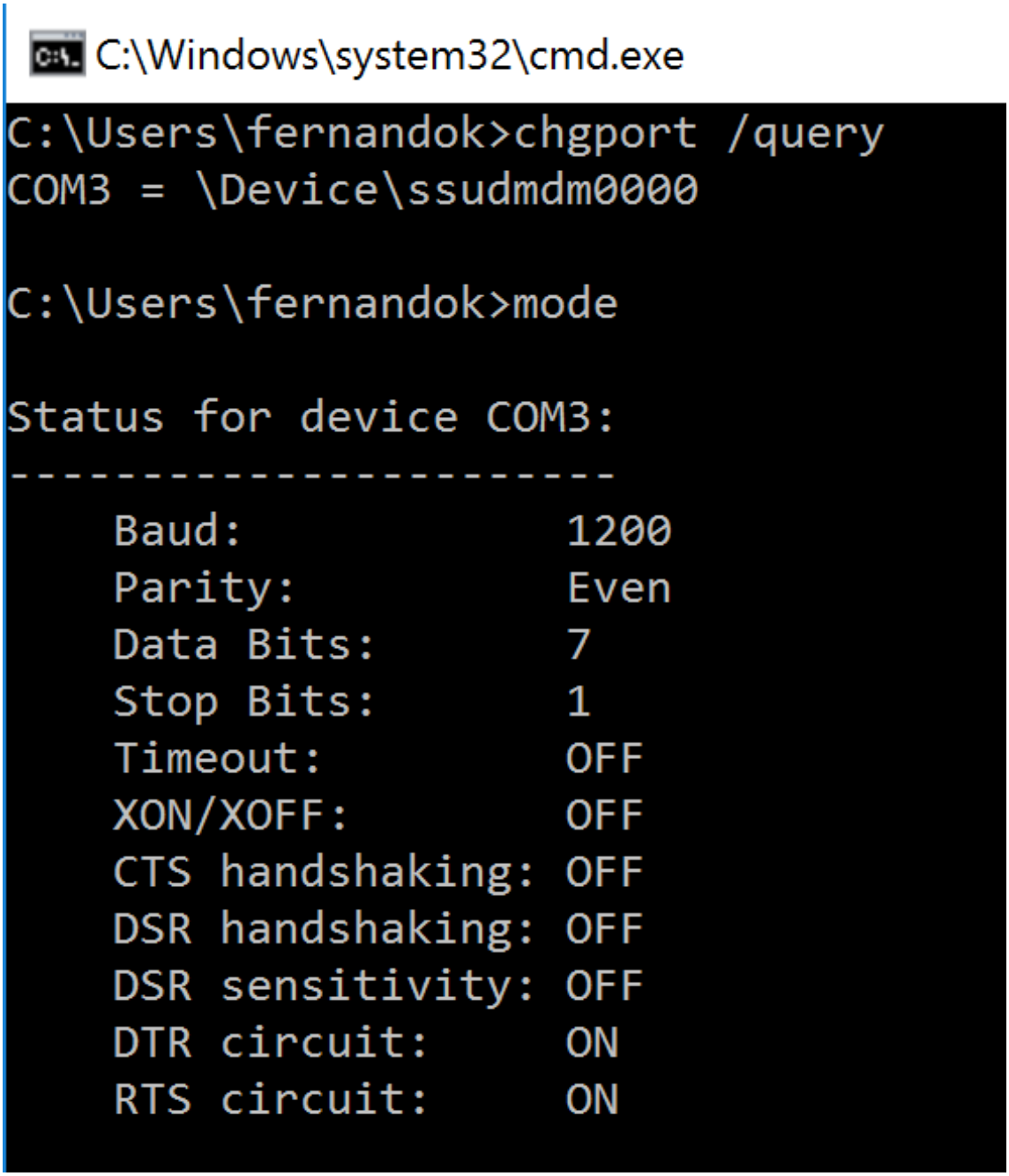
> cluding dialing, answering, and ending calls. Also, supplemental services such as holding, transferring, and conference calls.

Troubleshoot

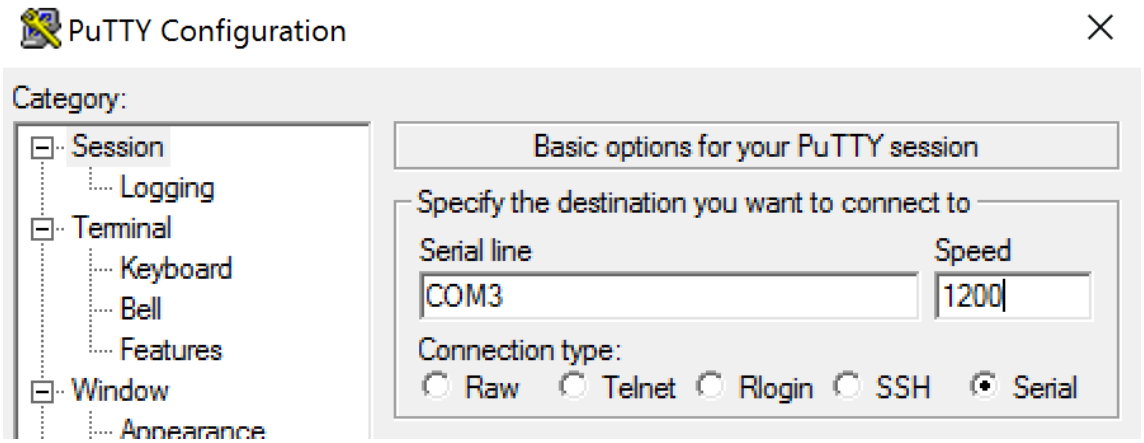
1. Ensure you can access the device directly from the endpoint, bypassing Citrix. While the port is not mapped to the VDA, you are not connected to a Citrix session. Follow any troubleshooting instructions that came with the device and verify that it works locally first.
   When a device is connected to a serial COM port, a registry key is created on the hive shown here:



   You can also find this information from the command prompt by running **chgport /query**.



If troubleshooting instructions for the device aren't available, try opening a PuTTY session. Choose **Session** and in **Serial line** specify your COM Port.



You can run **MODE** in a local command window. The output might display the COM port in use and the Baud/Parity/Data Bits/Stop Bits, which you need in your PuTTY session. If the PuTTY connection is successful, press **Enter** to see feedback from the device. Whatever characters you type might be repeated on the screen, or responded to. If this step is unsuccessful, you can't access the device from a virtual session.

2. Map the local COM port to the VDA (using policies or **NET USE COMX: \\CLIENT\COMZ:**) and repeat the same PuTTY procedures in the previous step, but this time from the VDA PuTTY. If PuTTY fails showing the error **Unable to open connection to COM1. Unable to open serial port**, another device might be using COM1.
3. Run **chgport /query**. If the built-in Windows serial driver on the VDA is auto-assigning \Device\Serial0 to a COM1 port of your VDA, do the following:
   A. Open CMD on the VDA and type **NET USE.**

   B. Delete any existing mapping (for example, COM1) on the VDA.

   NET USE COM1 /DELETE

   C. Map the device to the VDA.

   NET USE COM1: \\CLIENT\COM3:

   D. Point your application on the VDA to COM3.

   Lastly, try to map your local COM port (for example, COM3) to a different COM port on the VDA (other than COM1, for example COM3). Ensure that your application is pointing to it:
   NET USE COM3: \\CLIENT\COM3
4. If now you do see the port mapped, PuTTY is working but no data passing, it might be a race condition. The application might connect and open the port before it is mapped, locking it from being mapped. Try one of the following:

   - Open a second application published on the same server. Wait a few seconds for the port to be mapped, and then open the real application that tries to use the port.

- Enable the COM port redirection policies from the Group Policy Editor in Active Directory instead of Studio. Those policies are **Client COM port redirection** and **Auto connect client COM ports**. Policies applied this way might be processed before the Studio policies, guaranteeing that the COM port is mapped. Citrix policies are pushed to the VDA and stored in: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Use this logon script for the user or instead of publishing the application, publish a .bat script that first deletes any mapping on the VDA, remaps the virtual COM port, and then starts the application:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (or whatever value needed)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (or whatever value needed)
START C:\Program Files\<Your Software Path>\<your_software.exe>
```

5. Process Monitor from Sysinternals is the tool of last resort. When running the tool on the VDA, find and filter objects like COM3, picaser.sys, CdmRedirector, but especially <your_app>.exe. Any errors might appear as Access Denied or similar.

Limitations

- COM port devices must be connected before ICA session launch.
- COM port redirection during ICA reconnect doesn't provide dynamic COM port discovery.
- Connecting from a client with a COM port device connected, and then smooth roaming a new client without a COM port device connected, doesn't remove the existing COM port mapping.

Specialty keyboards

February 6, 2020

Bloomberg keyboards

> **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 Virtual Apps and Desktops support the Bloomberg model 4 Starboard keyboard (and earlier model 3). This keyboard enables customers in the financial sector to use the special features of the keyboard to access financial market data and perform trading quickly.

This keyboard is compatible with the KVM switch boxes and can work in two modes:

- PC (One USB cable with no KVM)
- KVM mode (Two USB Cables with one routed through KVM)

> **Important:**
> We recommend that you use the Bloomberg keyboard with only one session. We don't recommend using the keyboard with multiple concurrent sessions (one client to multiple sessions).

The Bloomberg keyboard 4 is a USB composite device comprising four USB devices in one physical shell:

- Keyboard.
- Fingerprint reader.
- Audio device with keys to increase and decrease volume and mute the speaker and the microphone. This device includes onboard speaker, microphone, and jack for the microphone and headset.
- USB hub to connect all of these devices to the system.

Requirements:

- The session to which Citrix Workspace app for Windows is connecting must support USB devices.
- Minimum of Citrix Workspace app 1808 for Windows or Citrix Receiver for Windows 4.8 to support Bloomberg keyboard model 3 and 4.
- Minimum of Citrix Workspace app 1808 for Windows or Citrix Receiver for Windows 4.12 to use KVM mode (two USB cables with one routed through KVM) for Model 4.

For information about configuring Bloomberg keyboards on Citrix Workspace app for Windows, see Configuring Bloomberg keyboards.

Enable Bloomberg keyboard support:

By default, the support for the enhanced Bloomberg keyboard is disabled. Enable this support by editing this registry entry on the client machine before you start a connection.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB

Name: **EnableBloombergHID** (dword)

Value: 0 = Disable 1 = Enable

Verify support:

To determine if Bloomberg keyboard support is enabled in Citrix Workspace app, check if the Desktop Viewer correctly reports the Bloomberg keyboard's devices.

Desktop scenario:

Open the Desktop Viewer. If support for Bloomberg keyboard is enabled, the Desktop Viewer shows see three devices under the USB icon:

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Seamless Application only scenario:

Open the Connection Center menu from the Citrix Workspace app notification area icon. If support for the Bloomberg keyboard is enabled, the three devices appear in the Devices menu.

The check mark against each of these devices indicates that they are remoted to the session.

TWAIN devices

February 6, 2020

Requirements

- The scanner must be TWAIN compliant.
- Install the TWAIN 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 TWAIN driver and not the Windows Image Acquisition service.
- 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.

For information about policy settings, see TWAIN devices policy settings.

Webcams

August 10, 2022

High definition webcam streaming

Webcams can be used by video conferencing applications running within the virtual session. The 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 video conferencing application. When the webcam and the application both support high-definition rendering, the application uses high-definition resolution. We support webcam resolutions up to 1920x1080.

This feature requires the Citrix Receiver for Windows, minimum version 4.10. For a list of Citrix Workspace app platforms that support HDX webcam redirection, see Citrix Workspace app feature matrix.

For more information about high definition webcam streaming, see HDX video conferencing and webcam video compression.

> **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 the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

You can use a registry key to disable the feature. The default resolution of 352x288 is used:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Name: Disable_HighDefWebcam

Type: REG_DWORD

Data: 1 = Disable the high definition webcam streaming

You can use registry keys on the client to configure a specific resolution. Ensure that the camera supports the specified resolution:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Name: DefaultWidth

Type: REG_DWORD

Data (decimal): desired width (for example 1280)

Name: DefaultHeight

Type: REG_DWORD

Data (decimal): desired height (for example 720)

Graphics

September 3, 2020

Citrix HDX graphics include an extensive set of graphics acceleration and encoding technologies that optimizes the delivery of rich graphics applications from Citrix Virtual Apps and Desktops. 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 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. 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 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.

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
- Framehawk
- Thinwire
- Text-based session watermark

HDX 3D Pro

July 8, 2020

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:

- Citrix Hypervisor

  - 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

June 25, 2020

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 Citrix Hypervisor 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 2016 and Windows Server 2012, 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, 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 following settings in the registry of the server running Windows Multi-session OS sessions:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001

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 following registry settings:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “CUDA” =dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “CUDA”=dword:00000001

To use the OpenCL acceleration POC features, enable the following registry settings:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL” =dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL”=dword:00000001

GPU acceleration for Windows single-session OS

March 17, 2021

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 Citrix Hypervisor, vSphere, and Hyper-V (passthrough only) hypervisors.

Using GPU Passthrough, you can create VMs with 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.

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 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.

  HDX 3D Pro also provides limited support for dual-monitor access to Windows XP desktops. For more information about this support, see VDAs on machines running Windows XP or Windows Vista.

- 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. Citrix Hypervisor and Hyper-V are supported with GPU passthrough. For more information, see AMD Virtualization Solution.

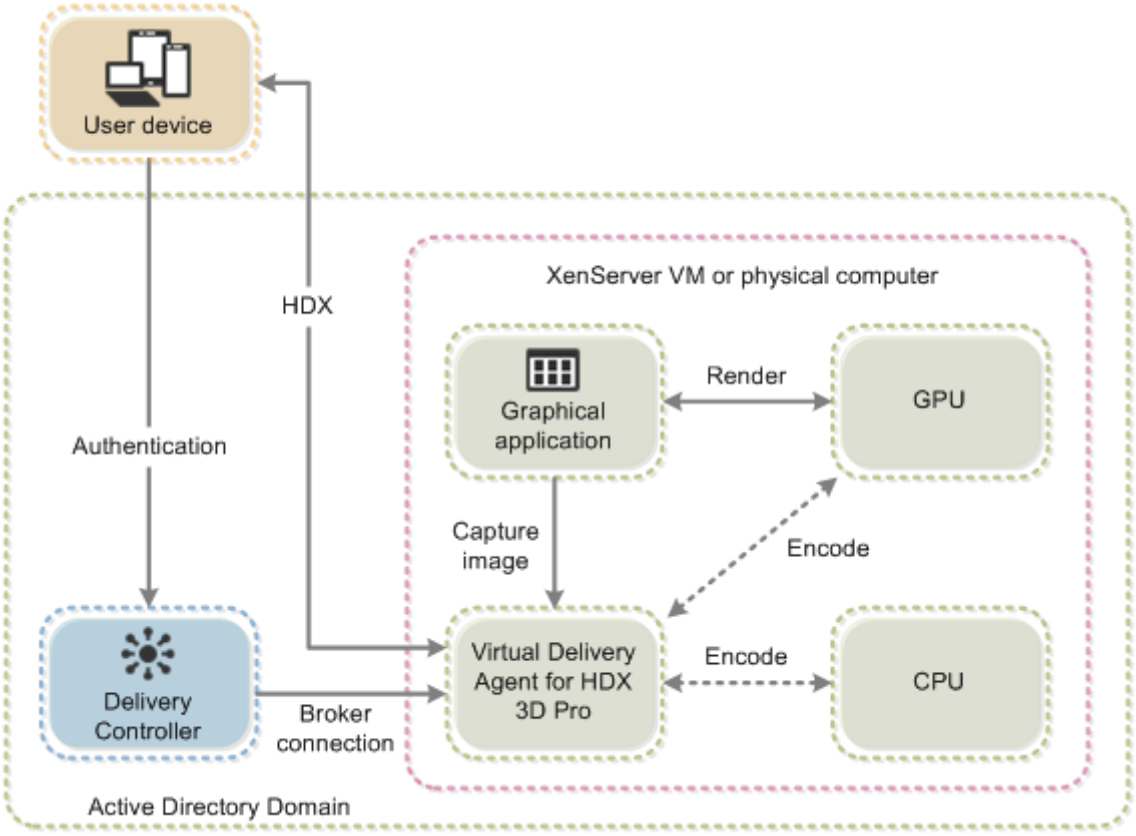
- Access to a high-performance video encoder for NVIDIA GPUs, AMD GPUs, and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature. The feature allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA 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

October 19, 2020

Introduction

Thinwire 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 should provide a highly interactive user experience that is similar to that of a local PC. Thinwire achieves this 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.

Thinwire

Thinwire should be used for delivering typical desktop workloads, for example, desktops, office productivity or browser-based applications. Thinwire is also recommended for multi-monitor, high resolution or high DPI scenarios, and for workloads with a mixture of video and non-video content.

HDX 3D Pro

In its default configuration, Thinwire can deliver 3D or highly interactive graphics. However, we recommend enabling HDX 3D Pro mode using the Citrix policy **Optimize for 3D graphics workload** for such scenarios when GPUs are present. The 3D Pro mode uses the GPU for hardware acceleration and configures Thinwire using optimal settings for graphics. This provides a more fluid experience for 3D professional graphics. For more information, see HDX 3D Pro and GPU acceleration for Windows Single-session OS.

Requirements and considerations

- Thinwire has been optimized for modern operating systems, including Windows Server 2012 R2, Windows Server 2016, Windows 7, 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 with Windows 7 and Windows 2008 R2.

- 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.

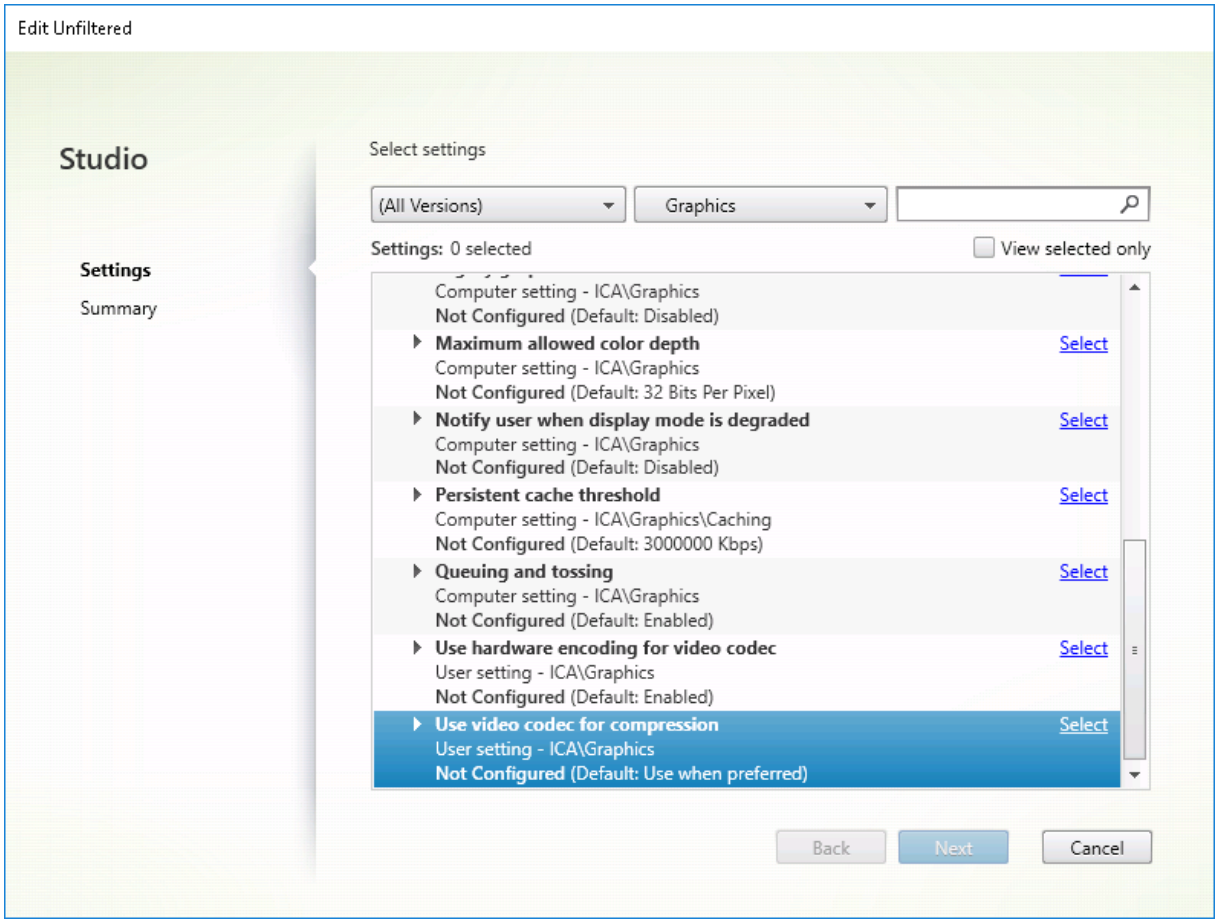
- All Citrix Workspace apps support Thinwire. Some Citrix Workspace apps may however support features of Thinwire that others do not, for example, 8 or 16-bit graphics for reduced bandwidth usage. Support for such features are automatically negotiated by Citrix Workspace app.
- Thinwire will use more 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 may increase as a result.
- In low bandwidth or high latency scenarios, you may consider enabling 8 or 16-bit graphics to improve interactivity, however visual quality will be affected, especially at 8-bit color depth.

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.
- Other options in this policy setting will continue to use Thinwire in combination 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, especially in cases with heavy use of 3D graphics.



A number of other policy settings, including the following Visual display policy settings can be used to fine tune the performance of display remoting technology and are all supported by Thinwire:

- 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.

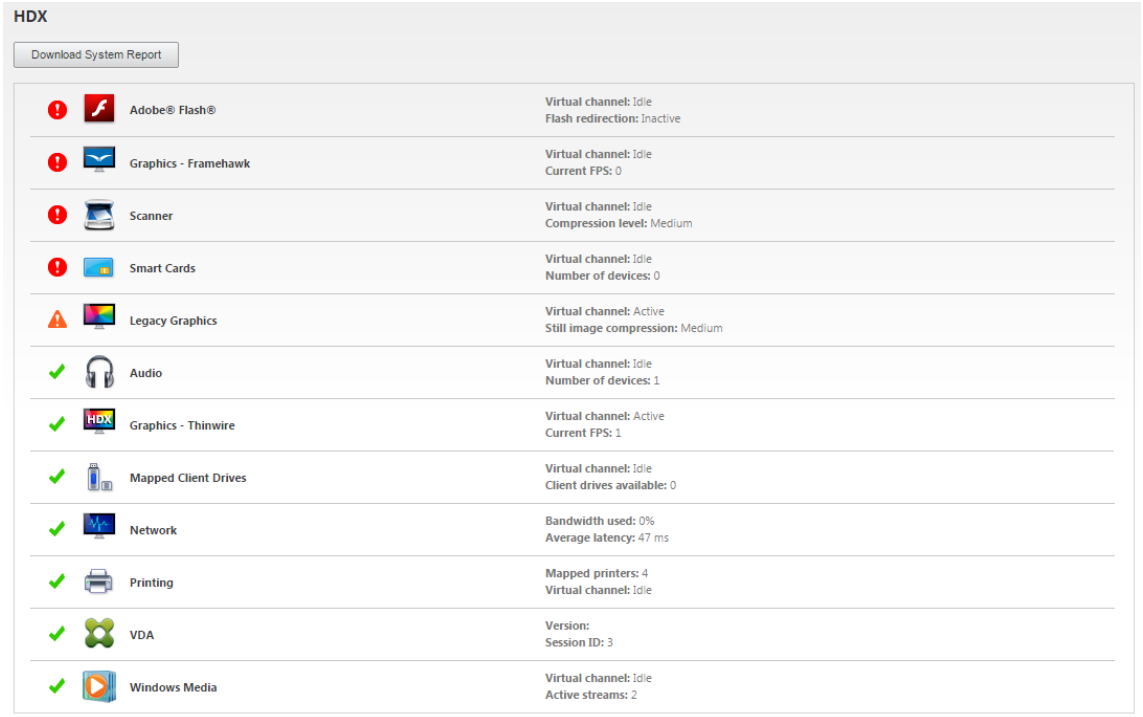
Monitoring Thinwire

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:

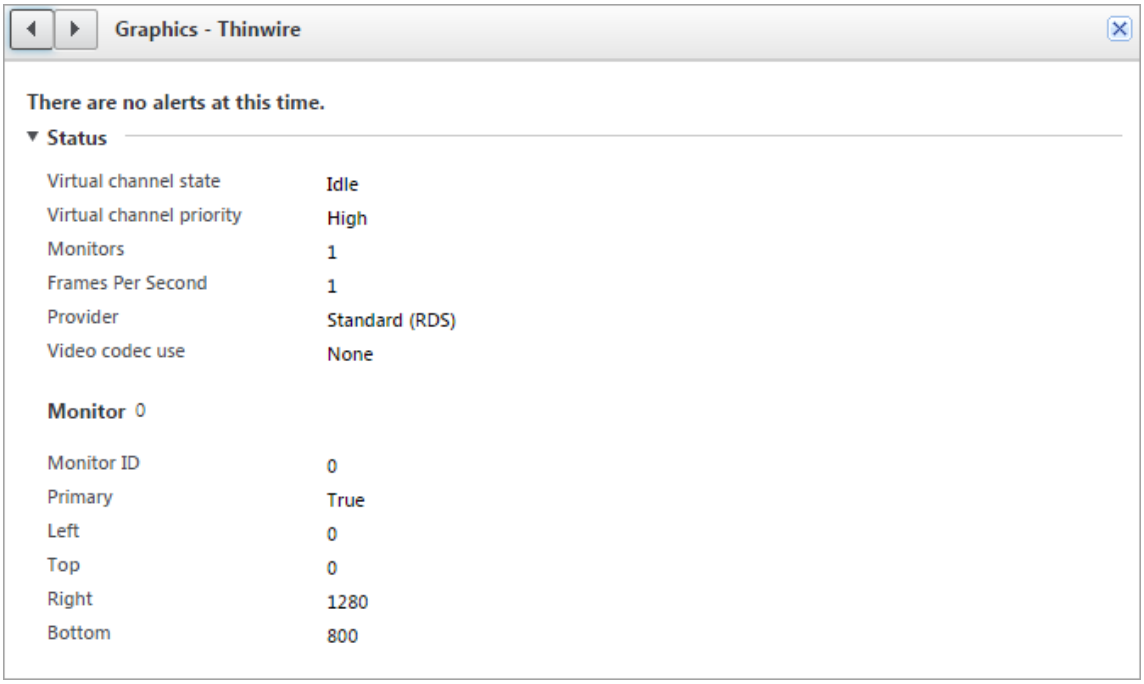
1. In Director, search for a user, machine or endpoint, open an active session and click **Details**. Or,

you can select **Filters** > **Sessions** > **All Sessions**, open an active session and click **Details**.

2. Scroll down to the **HDX** panel.



3. Select **Graphics - Thinwire**.



Encoding methods

In XenApp and XenDesktop 7.16 and earlier, there are three Thinwire bitmap encoding modes used for Multi-session OS and Single-session OS VDA graphics remoting:

- Full screen H.264
- Thinwire Plus
- Thinwire Plus with selective H.264

Legacy GDI remoting uses the XPDM remoting driver and not a Thinwire bitmap encoder.

In a typical desktop session, most of the imagery is simple graphics or text regions. When any of the three bitmap encoding modes listed are used, Thinwire 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.

Lossless compression codec (MDRLE)

In XenApp and XenDesktop 7.17, we've added a higher compression ratio MDRLE encoder that consumes less bandwidth in typical desktop sessions than the 2DRLE codec.

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

Session interactivity can degrade on low bandwidth or high latency links. For example, on a link with bandwidth < 2 Mbps or latency > 200 ms, scrolling on a web page can become slow, unresponsive, or bursty. Keyboard and mouse operations can lag behind graphics updates.

Through version 7.17, you might use policy settings to reduce bandwidth consumption by configuring the session to Low visual quality, or set a lower color depth (16 or 8-bit graphics). However, you needed to know that a user was on a weak connection. HDX Thinwire could not dynamically adjust static imagery quality, based on network conditions.
In 7.18, by default, HDX Thinwire switches to a progressive update mode when available bandwidth falls below 2 Mbps, or network latency exceeds 200ms. In this mode:

- All static images are heavily compressed.
- Text quality is reduced.

Transient imagery (video) is still managed with adaptive display or Selective H.264.

How progressive mode is used

By default, progressive mode is on standby for the Visual Quality policy settings: High, Medium (default), and Low.

Progressive mode is forced off (not used) when:

- Visual Quality = Always Lossless or Build to Lossless
- Preferred Colour Depth for Simple Graphics = 8-bit
- Use Video Codec = For the entire screen (when full-screen H.264 is desired)

When progressive mode is on standby, by default it is enabled when either of the following conditions occurs:

- Available bandwidth drops below 2 Mbps
- Network latency increases to above 200ms

After a mode switch occurs, a minimum of 10s is spent in that mode, even if the adverse network conditions are momentary.

Changing progressive mode behavior

You can change the progressive mode state with the following registry key:

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplay

Values:

0 = Always off (do not use in any circumstances)

1 = Automatic (toggle based on network conditions; this is the default)

2 = Always on

When in automatic mode (1), you can use the following registry key to change the thresholds at which progressive mode is toggled:

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayBandwidthThreshold

Value: <threshold in Kbps> (default = 2048)
Example: 4096 = toggle progressive mode on if bandwidth falls below 4 Mbps

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayLatencyThreshold

Value: <threshold in ms> (default = 200)
Example: 100 = toggle progressive mode on if network latency drops below 100ms.

Text-based session watermark

February 6, 2020

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 Thinwire and not the Framehawk or Desktop Composition Redirection (DCR) graphic modes.
- 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

February 7, 2020

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.

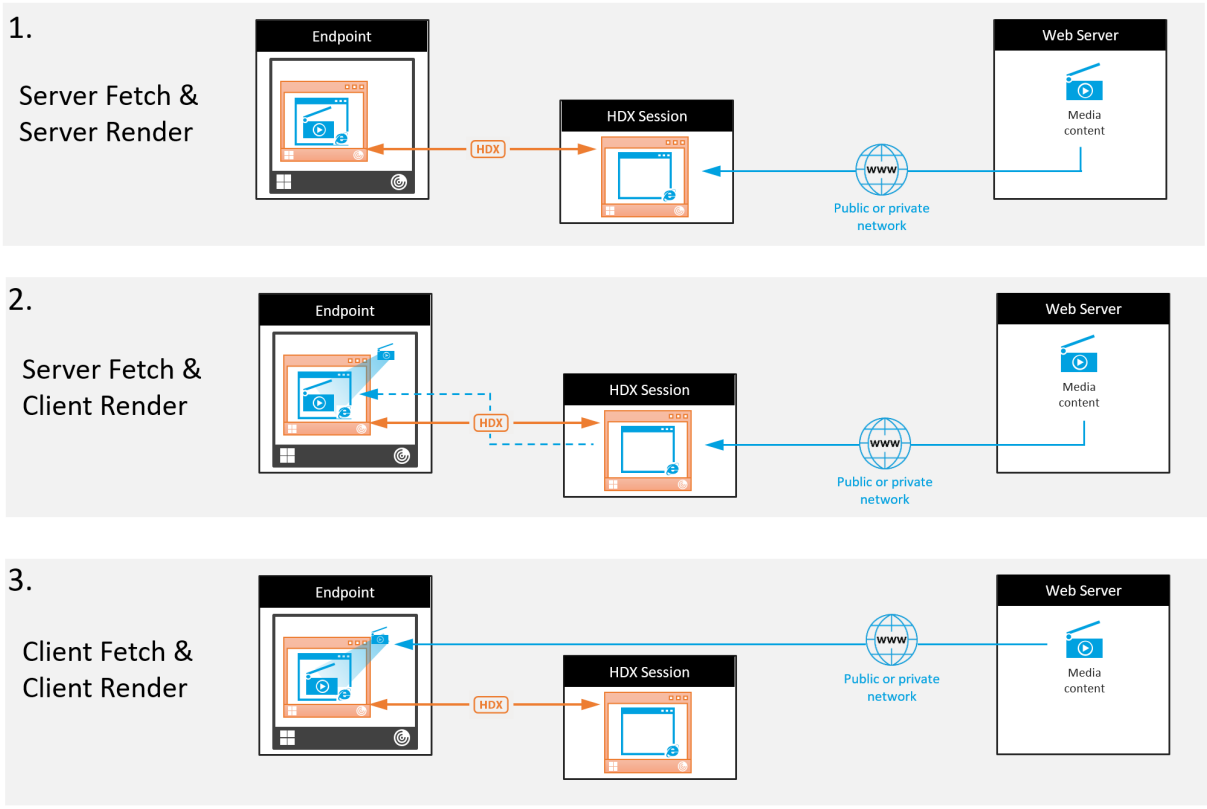
With server-rendered multimedia delivery, audio and video content is decoded and rendered on the Citrix Virtual Apps and Desktops server by the application. The content is then compressed and delivered using ICA protocol to Citrix Workspace app on the user device. This method provides the highest rate 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 RapidFire, 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 20, 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 rang 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.

> **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.

1. Using the Registry Editor on the user device, navigate to one of the following:
   - 32-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanc
   - 64-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Change the **Value data** field to FALSE.

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:
  - 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 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 executes 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 Studio 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

> **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.

You install an audio device on your client, enable the audio redirection, and start an RDS session. The audio files might fail to play and an error message appears.

As a workaround, add this registry key on the RDS machine, and then restart the machine:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig

Name: EnableSvchostMitigationPolicy

Type: REG_DWORD

Data: 0

Browser content redirection

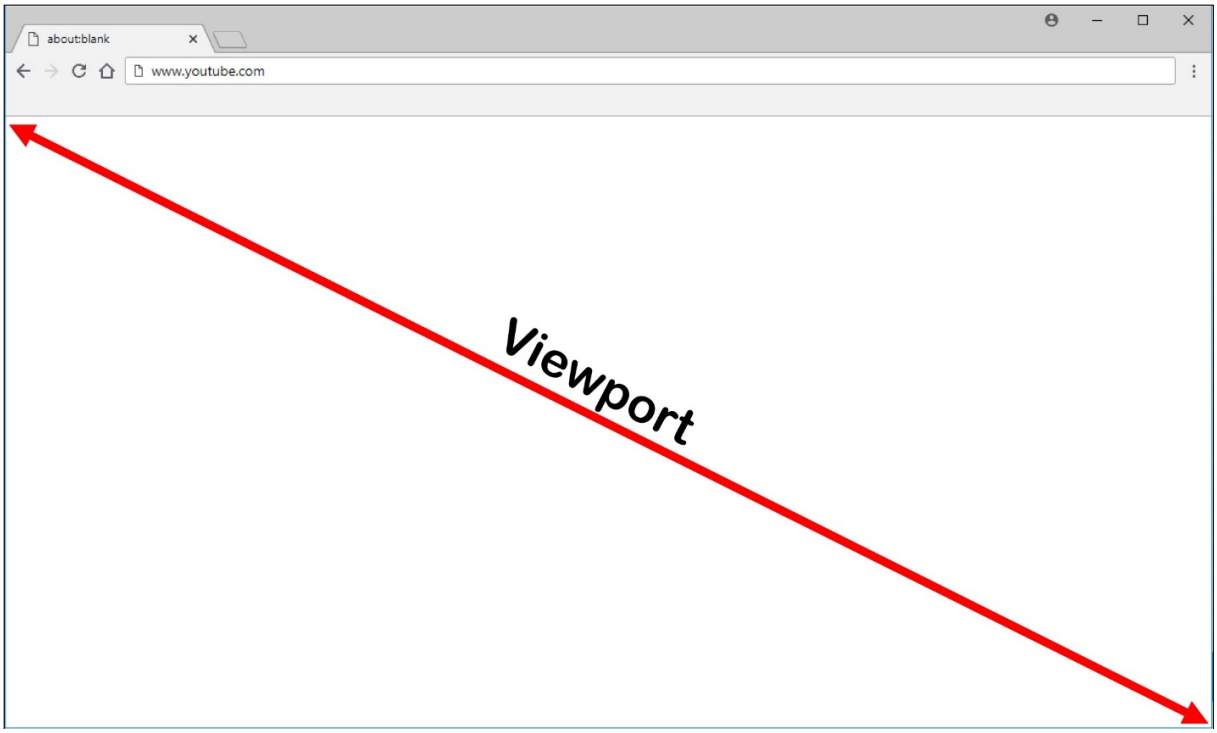
March 14, 2022

Browser content redirection prevents the rendering of whitelisted webpages 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 blacklist.

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.

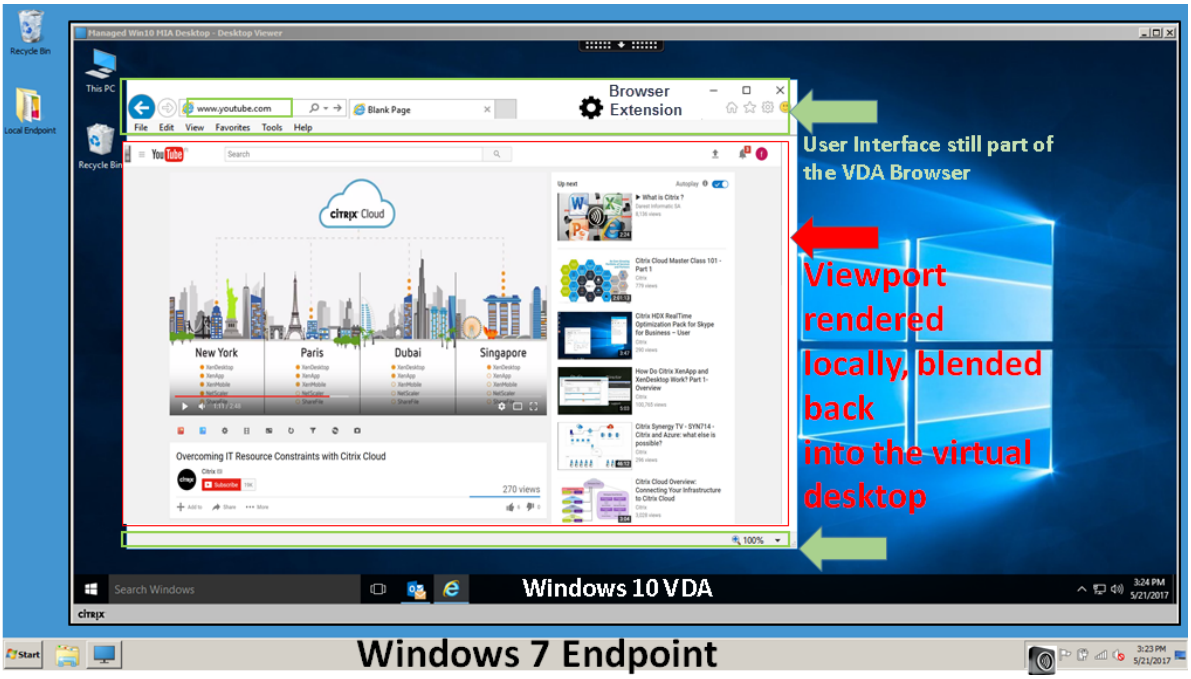


1. Configure a Studio policy that specifies an Access Control List containing the URLs whitelisted for redirection or the blacklist that disables redirection for specific URL paths. For the browser on the VDA to detect that the URL that the user is navigating to matches the whitelist or does not match a blacklist, 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 whitelist (for example `https://www.mycompany.com/`), and there is no match to a URL in the blacklist (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.



> **Important:**
>
> The following settings apply only to 1912 LTSR CU1 or later.

Here are scenarios of how Citrix Workspace app fetches content:

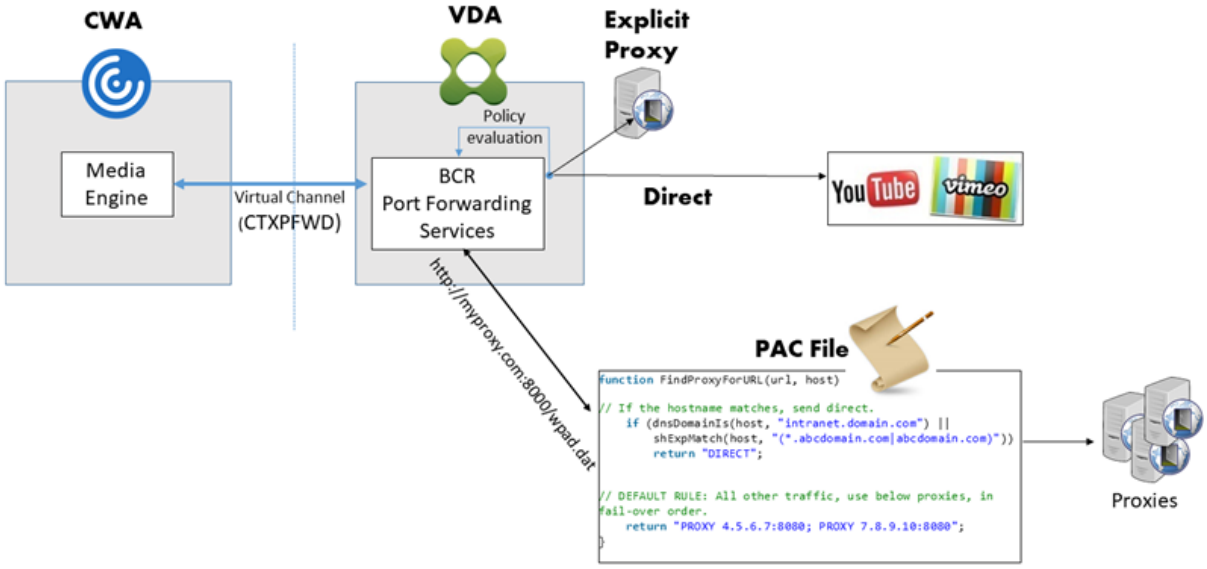
- **Server fetch and server render**: There is no redirection because you didn't whitelist the site or the redirection failed. We fall back to rendering the webpage on the VDA and use Thinwire to remote the graphics. Use policies to control the fallback behavior. High CPU, RAM, and bandwidth consumption 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:

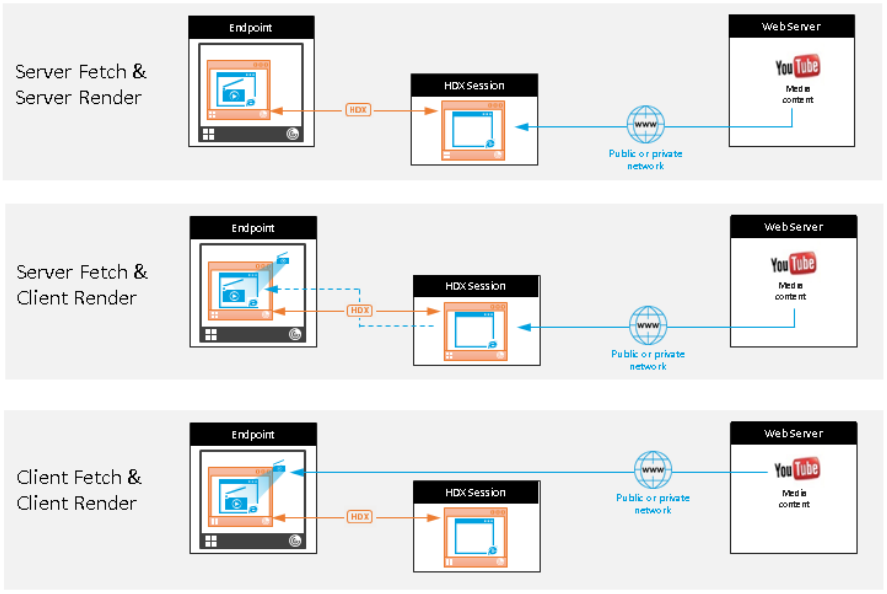
  - Explicit Proxy - If you have a single explicit proxy in your Datacenter. This routes browser content redirection traffic through the VDA and forwards it to the specified web proxy.
  - Direct or Transparent - If you do not have proxies, or if you use transparent proxies. This routes browser content redirection traffic through the VDA and forwards it directly to the web server hosting the content.

– 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. This routes browser content redirection traffic through the VDA and forwards it to the web proxy determined by evaluating the specified PAC file.



- **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 blacklist policy.

System Requirements:

Windows endpoints:

- Windows 7, 8.x, or 10
- Citrix Workspace app 1809 for Windows or later
- Citrix Receiver for Windows 4.10 or later

> **Note:**
>
> Citrix Workspace app 1912 LTSR for Windows as well as all cumulative updates to the Citrix Workspace app 1912 LTSR do not support browser content redirection.

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 https://support.citrix.com/article/CTX230052

Browser content redirection Chrome extension

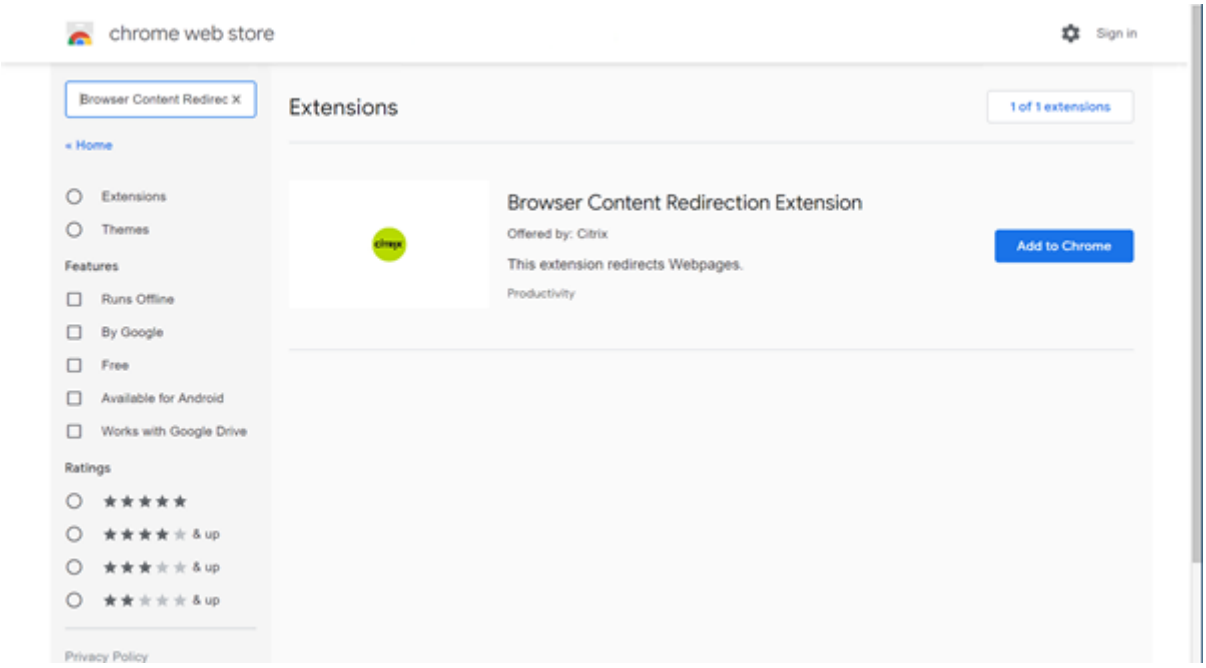
To use browser content redirection with Chrome, add the browser content redirection extension from the Chrome Web Store. Click **Add to Chrome** in the Citrix Virtual App and Desktop environment.

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

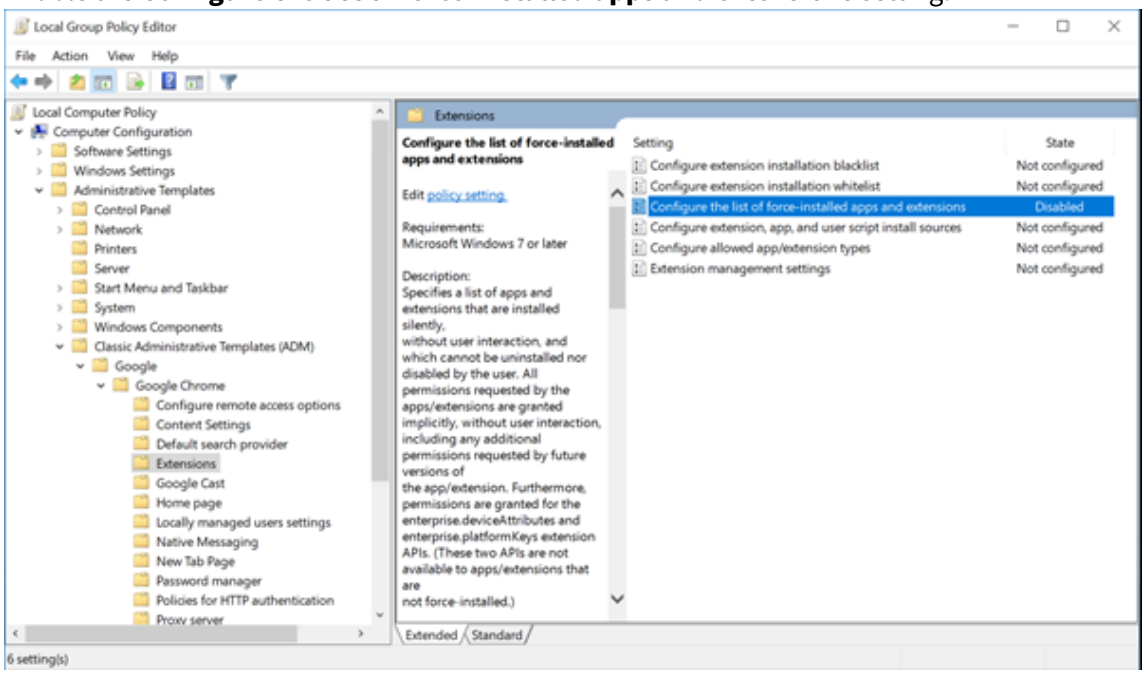
> **Note:**
>
> Citrix Workspace app 1912 LTSR for Windows as well as all cumulative updates to the Citrix Workspace app 1912 LTSR do not support browser content redirection.



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.

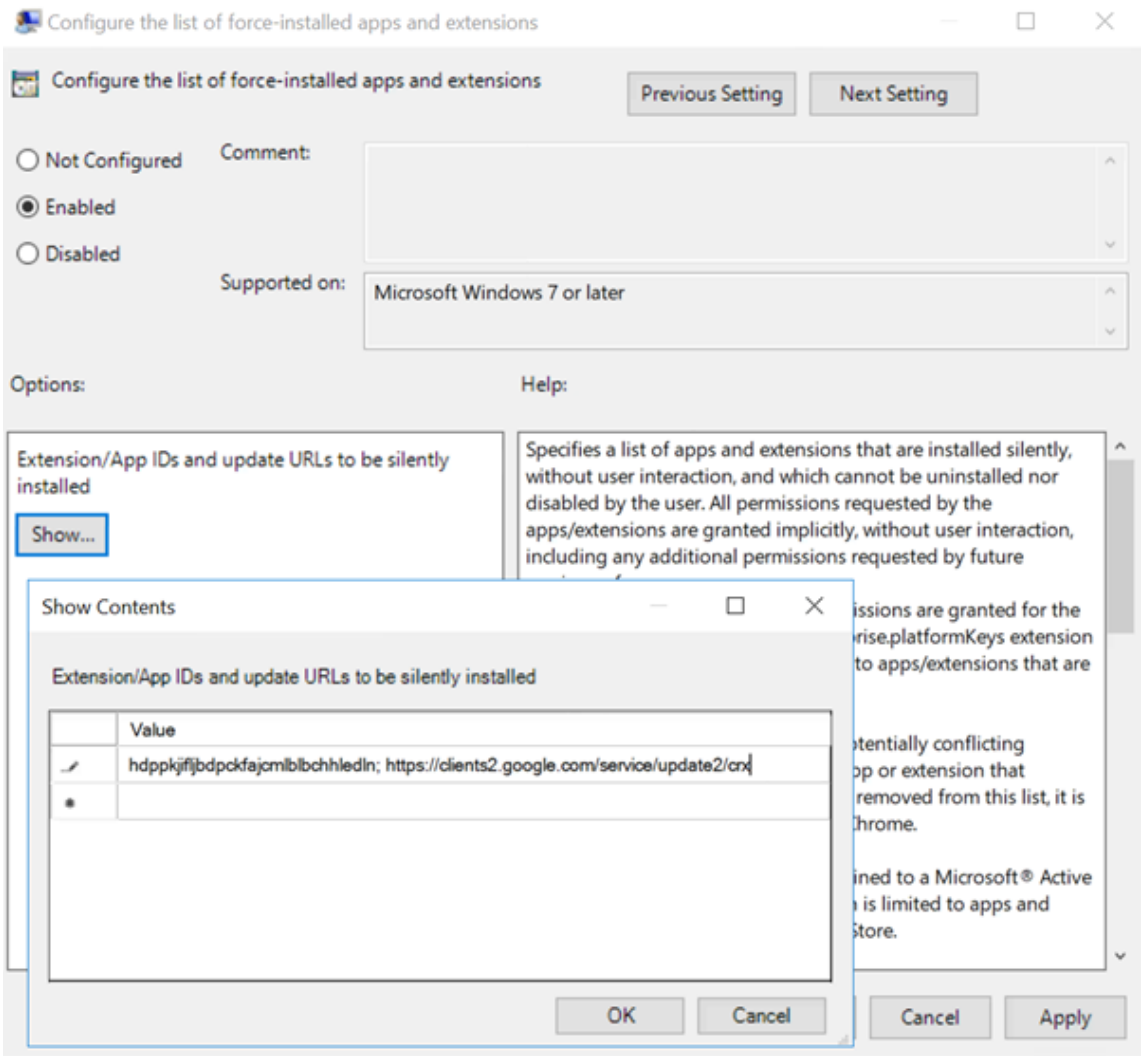
Deploy the extension using Group Policy

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 https://support.google.com/chrome/a/answer/187202?hl=en.
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.

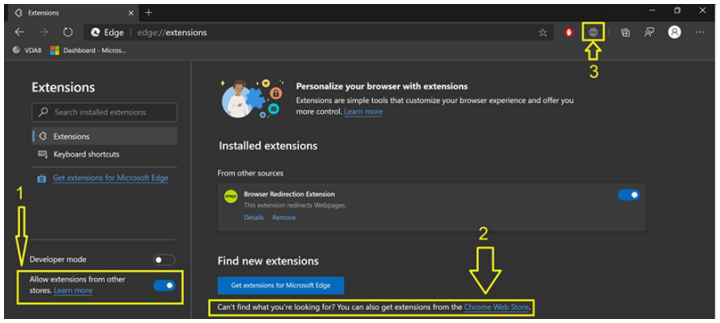
   If the **Configure the list of force-installed apps and extensions** setting is set to **Disabled**, the extension is automatically removed from Chrome for all users.

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

> **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.

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 following register key on the user's machine:

\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream

Name: GPU

Type: DWORD

Data: 0

HDX video conferencing and webcam video compression

August 27, 2020

> **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

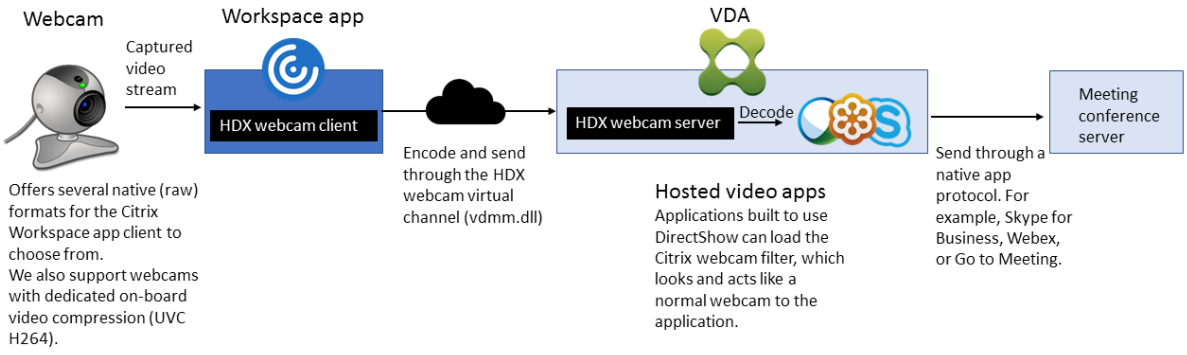
> of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

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.
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 uses the multimedia framework technology that is part of the client operating system to intercept video from capture devices and transcode and compress it. Manufacturers of capture devices supply 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 it's integrated giving 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, add the following DWORD key value to the registry key:

HKEY_CURRENT_USER\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1

HDX webcam video compression requirements

Supported clients: Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Workspace app for Chrome, and Citrix Workspace app for Linux.

> **Note:**
>
> Only Citrix Workspace app for Windows, Citrix Workspace app for Chrome, and Citrix Workspace app for Mac 2006 or later support webcam redirection for 64-bit apps.

Supported video conferencing applications (32 bit and 64 bit):

- Adobe Connect
- Cisco Webex and Webex for Teams
- GoToMeeting
- Google Hangouts and Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business 2015
- Microsoft Lync 2010 and 2013
- Microsoft Skype 7 or higher
- Media Foundation-based video applications on Windows 8.x or higher and Windows Server 2012 R2 and higher

To use Skype on a Windows client, edit the registry on the client and the server:

- Client registry key HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

  Name: DefaultHeight

  Type: REG_DWORD

  Data: 240

  Name: DefaultWidth, Type: REG_DWORD

  Data: 320

- Server registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

  Name: skype.exe,

  Type: REG_DWORD

  Data: Set to 0

Other user device requirements:

- Appropriate hardware to produce sound.
- DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding capable reduces client-side CPU usage.
- For HDX webcam video compression, install webcam drivers on the client, obtained from the camera manufacturer, if possible.

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 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 the feature. The default resolution of 352x288 is used:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Name: Enable_HighDefWebcam

Type: REG_DWORD

Data: 0 = Disable the high definition webcam streaming

You can use registry keys on the client to configure a specific resolution. Ensure that the camera supports the specified resolution:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Name: DefaultWidth

Type: REG_DWORD

Data (decimal): desired width (for example 1280)

Name: DefaultHeight

Type: REG_DWORD

Data (decimal): desired height (for example 720)

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 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 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 22, 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 7 x86 and x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Minimum VDA browser version	Windows OS version/build/SP
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 7 x86 and x64; Windows Server 2016 RTM 14393 (1607);Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows 7 x86 and x64; 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?

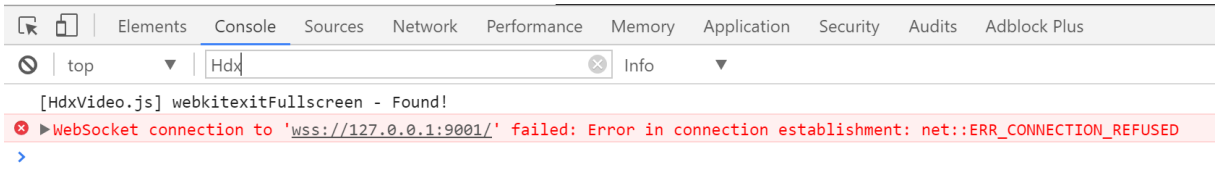
In this release, this feature is available for controlled webpages only. It requires the addition of the HdxVideo.js JavaScript (included in the Citrix Virtual Apps and Desktops Installation media) to the webpages where the HTML5 multimedia content is available. For example, videos on an internal training 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 execute 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

October 3, 2023

> **Important:**
>
> Optimization for Microsoft Teams requires a minimum of Microsoft Teams version 1.2.00.31357.

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).

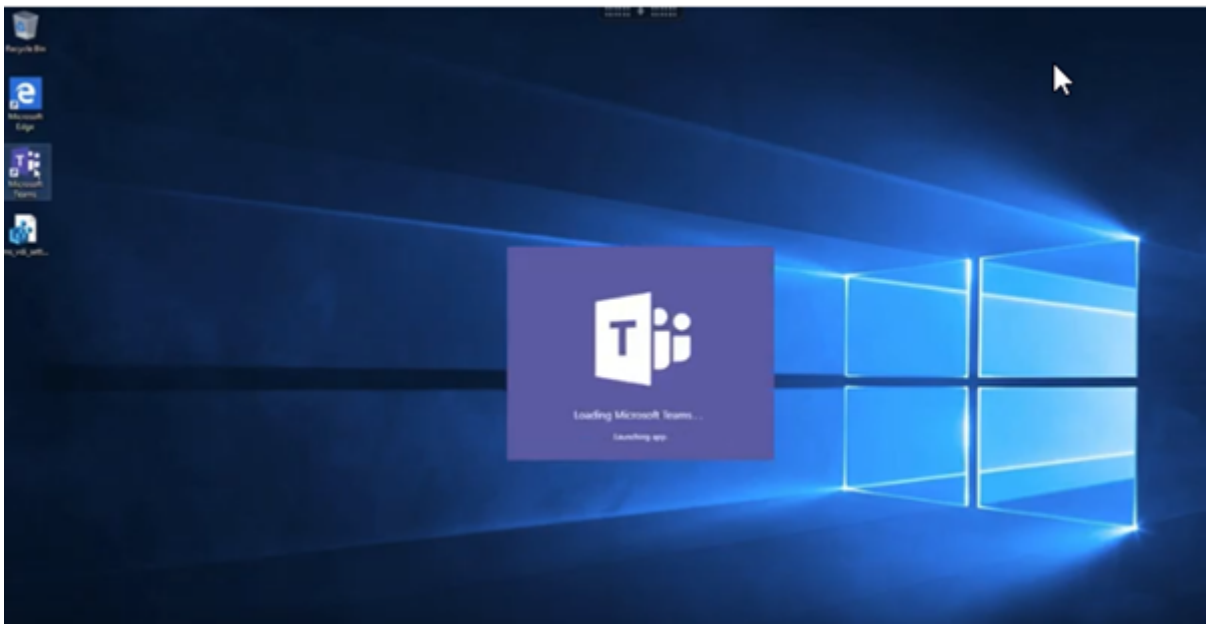
Our optimization for Microsoft Teams contains VDA-side HDX services and API to interface with the Microsoft Teams hosted app to receive commands. These components open a control virtual channel (CTXMTOP) to the Citrix Workspace app-side media engine. The endpoint decodes and renders the multimedia locally, moving the Citrix Workspace app window back into the hosted Microsoft Teams app.

Authentication and signaling occurs 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.

`CTXMTOP` is a command and control virtual channel. That means that media is not 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

> **Note:**
>
> We recommend installing the VDA before installing Teams in the golden image. This installation order is necessary for the **ALLUSER=1** flag to take effect. If the virtual machine had Teams installed before the VDA was installed, uninstall and reinstall Teams. If you are using App Layering, see the App Layering instructions at the end of this section for more details.

We recommend you follow the Microsoft Teams machine-wide installation guidelines and avoid using the .exe installer that installs 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 Teams Machine-Wide Installer appears in **Programs and Features** in the Control Panel and in **Apps & features** in Windows Settings for all users of the computer. All users can then uninstall 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 Teams application doesn't auto-update whenever there is a new version. We recommend this mode for non-persistent environments. For example, 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).

You have Windows 10 dedicated persistent VDI environments. You want the Teams application to auto-update and would prefer Teams to install per-user under `Appdata/Local`, use the `.exe` installer or the MSI without **ALLUSER=1**.

For App Layering:

> **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.

Create an empty registry key named `PortICA` (leave the default Name, Type, and Data).

If using Citrix App Layering to manage VDA and Microsoft Teams installations in different layers, deploy this registry key on Windows before installing Teams with **ALLUSER =1**:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

Or

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`

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 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.

Machine wide installer

The following is an example of folders, desktop shortcuts, and registries created by installing 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

Recommendations

- We recommend disabling auto-start by deleting the Teams registry keys. Doing so prevents "8AM logon storms"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 Teams **Settings** to improve performance. This setting ("disableGpu":**true**) is stored in %Appdata%\Microsoft\Teams inside the desktop-config.json file. 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 Teams.

> **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.

Per-user installer

When using the .exe installer, the installation process changes significantly, and 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 Teams with a non-persistent setup requires a profile caching manager for efficient Teams runtime data synchronization. Having a profile caching manager ensures that the appropriate user-specific information (for example, user data, profile, and settings) is cached during the user session. Make sure you synchronize the data in these two folders:

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

Teams cached content exclusion list for non-persistent setup:

Exclude the following items from the Teams caching folder, %AppData%/Microsoft/Teams. Excluding these items helps reduce the user caching size to further optimize your non-persistent setup.

Exclusion list –files

- Roaming\Microsoft\Teams* .txt

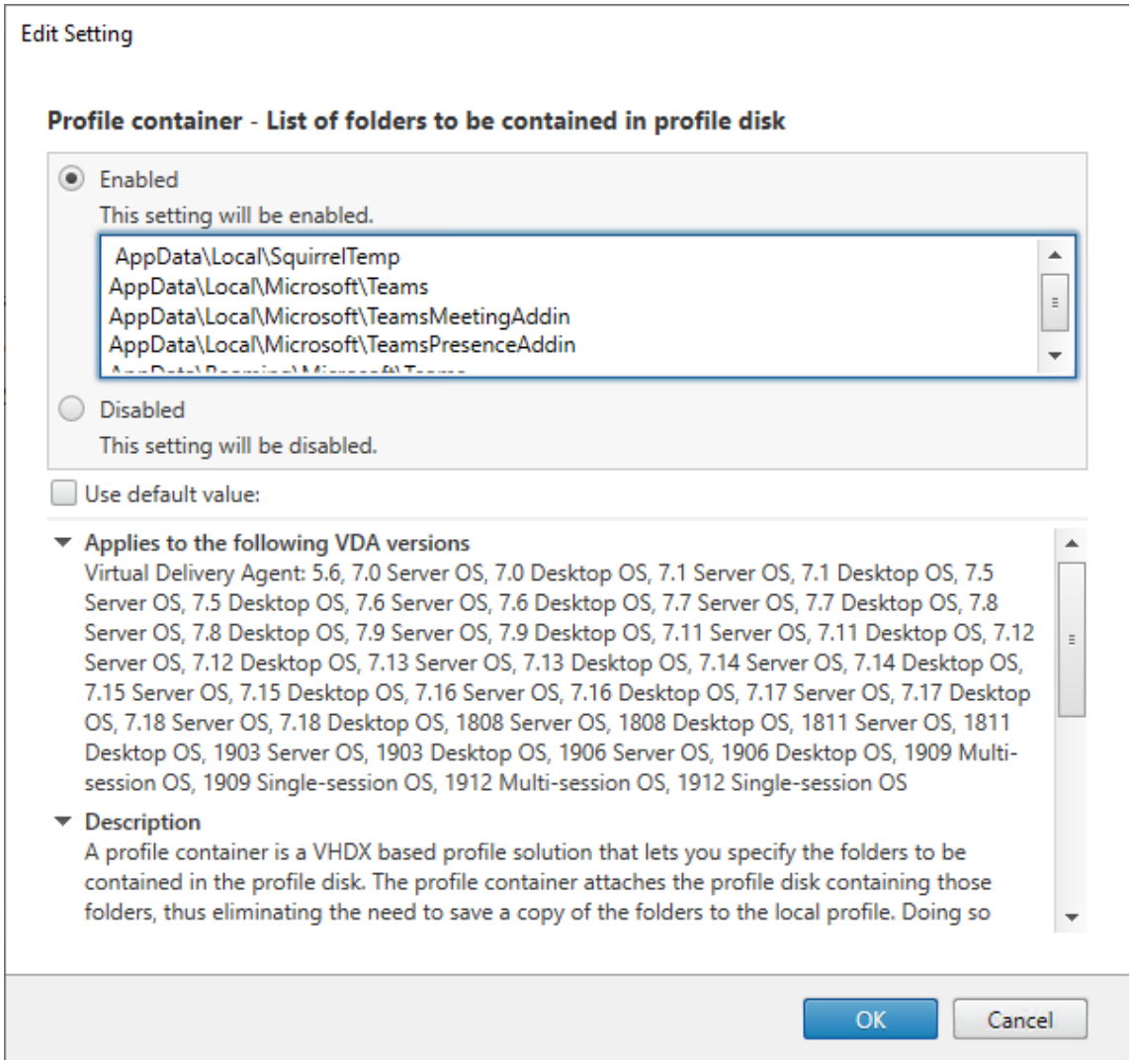
Exclusion list –directories

- Roaming\Microsoft\Teams\Logs
- Roaming\Microsoft\Teams\media-stack
- Roaming\Microsoft\Teams\Service Worker\CacheStorage
- Roaming\Microsoft\Teams\Application Cache
- Roaming\Microsoft\Teams\Cache
- Roaming\Microsoft\Teams\GPUCache
- Roaming\Microsoft\Teams\meeting-addin\Cache (Critical for issues where the Add-in is missing in Outlook)

Use case: single session scenario:

In this scenario, the end user uses Microsoft Teams in one location at a time. There is no need to run Teams in two different Windows sessions simultaneously. For instance, in a common virtual desktop deployment, each user is assigned to one desktop and Teams is deployed inside the virtual desktop as one application.
We recommend enabling Citrix Profile container and redirect the previously mentioned per-user directories 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 previously mentioned folders into this configuration. Alternatively, 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 2019, 2016, 2012R2 Standard and Datacenter Editions, and with the Server Core option

Minimum version - Virtual Delivery Agents (VDAs) 1906.2:

Supported operating systems:

- Windows 10 64-bit, versions 1607 and higher. (VM hosted apps are not supported).
- Windows Server 2019, 2016, and 2012 R2 (Standard and Datacenter Editions).

Requirements:

- BCR_x64.msi - the MSI that contains 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 2006.1 for Windows and Minimum version - Citrix Workspace app 1907 for Windows:

- Windows 7, 8, and 10 (32-bit and 64-bit editions, including Embedded editions)
- Windows 10 IoT Enterprise 2016 LTSB (v1607) and 2019 LTSC (v1809)
- Processor (CPU) architectures supported: x86 and x64 (ARM is not 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.
- 10ZiG Thin Clients verified: 4510 and 5810q.
- For a complete list of verified endpoints, see Thin Clients.
- Citrix Workspace app requires a minimum of 600 MB free disk space and 1 GB RAM.
- Microsoft .NET Framework minimum requirement is version 4.6.2. Citrix Workspace app automatically downloads and installs .NET Framework if it is not present in the system.

Minimum version - Citrix Workspace app 2006 for Linux:

For more information, see Optimization for Microsoft Teams in Citrix Workspace app for Linux documentation.

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 more information, see Prerequisites to install Citrix Workspace app.

Minimum version - Citrix Workspace app 2012 for Mac:

Supported operating systems

- macOS Catalina (10.15)
- macOS Big Sur Beta 8 in test environments only. Do not use in production environments.

Features supported:

- Audio
- Video
- Screen sharing optimization (incoming and outgoing)

Teams optimization works by default if the user has Citrix Workspace app 2012 or later and macOS 10.15.

If you want to disable Teams optimization, run this command in terminal and restart Workspace app:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

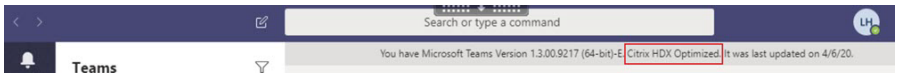
Enable optimization of Microsoft Teams

To enable optimization for Microsoft Teams, use the Studio policy described in Microsoft Teams redirection policy (it is **ON** by default). In addition to this policy being enabled, HDX checks to verify that the version of the Citrix Workspace app is equal to or greater than the minimum

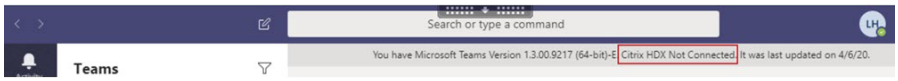
required version. If you enabled the policy and the Citrix Workspace app version is supported, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** is set to **1** automatically on the VDA. The Microsoft Teams application reads the key to load in VDI mode.

> **Note:**
>
> If you are using version 1906.2 VDAs or higher with older Controller versions (for example, version 7.15), which do not have the policy available in Studio, you can still be optimized because HDX optimization for Microsoft Teams is enabled by default in the VDA.

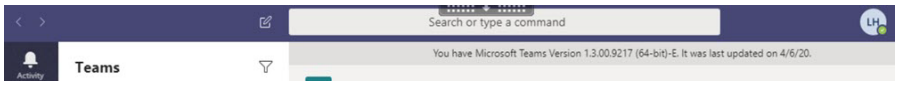
If you click **About > Version**, the **Citrix HDX Optimized** legend displays:



If you see **Citrix HDX Not Connected** instead, the Citrix API is loaded in Teams (which is the first step towards redirection), but there was an error in the subsequent 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, Teams failed to load the Citrix API. Exit Teams by right-clicking on the notification area icon and restart. Make sure the Studio policy is not set to **Prohibited**, and that the Citrix Workspace app version is supported.



Network requirements

Microsoft Teams relies on Media Processor servers in Office 365 for meetings or multiparty calls. Microsoft Teams relies on Office 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.

Therefore, the network health between the peer and the Office 365 cloud determines the performance of the call.

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 Office 365 network as directly as possible from the branch office.
- If you must use any of the following at the branch office, ensure that RTP/UDP Teams traffic is unhindered. HdxTeams.exe doesn't honor explicit proxies configured on the endpoint.
  - Bypass proxy servers
  - Network SSL intercept
  - Deep packet inspection devices
  - VPN hairpins (use split tunneling if possible)
- Plan and provide sufficient bandwidth.
- Check each branch office for network connectivity and quality.

The WebRTC media engine in the Workspace app (HdxTeams.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 by using symmetric keys (128 bit) to encrypt media and control messages, and uses the AES encryption cipher in counter mode.

The following metrics are recommended for guaranteeing a positive user experience:

Metric	Endpoint to Office 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.

In terms of bandwidth requirements, optimization for Microsoft Teams can use a wide variety of codecs for audio (OPUS/G.722/PCM G711) and video (H264/VP9).

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
Video (each way)	~ 2,500 kbps	VP9 720p @ 30 fps 16:9

Type	Bandwidth	Codec
Screen sharing	~ 300 kbps	H264 1080p @ 15 fps

* Opus supports constant and variable bitrate encoding from 6 kbps up to 510 kbps.

Opus and VP9 are the preferred codecs for peer-to-peer calls between two optimized VDI users.

G.722 and H264 are the preferred codecs for a VDI user joining a meeting.

Citrix Gateway

The presence of an on-premises Citrix Gateway or Citrix Gateway service as an HDX proxy doesn't have an impact on Microsoft Teams optimization. This is because there is only a command-and-control virtual channel established between the Workspace app and the VDA.

All the audio or video streams are offloaded to the client for local processing. As a result, there is no server-side rendering.

Depending on the configuration in your environment, the command-and-control virtual channel flows through the Citrix Gateway using either of the following:

- TLS for TCP
- DTLS for EDT

If you're also using the Citrix Gateway for VPN, make sure you're allowing the client machine to reach the O365 Microsoft Teams servers directly. You can achieve this through split tunneling or other methods.

Proxy servers

Depending on the location of the proxy, consider the following:

- Proxy configuration on the VDA:

  If you configure 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 make sure `127.0.0.1:9002` is bypassed.

  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 ensure 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, Citrix Workspace app for Windows version 2012 (Negotiate/Kerberos, NTLM, Basic, and Digest), Citrix Workspace app for Linux version 2101 (anonymous authentication), and Citrix Workspace app for Mac version 2104 (anonymous authentication) support proxy servers. Client devices with earlier releases of Citrix Workspace app cannot read proxy configurations. These devices send traffic directly to Office 365 TURN servers.

  > **Important:**
  >
  > Verify that the client device can connect to the DNS server to perform DNS resolutions. A client device must be able to resolve three Microsoft Teams TURN server's FQDNs: `worldaz.turn.teams.microsoft.com`, `usaz.turn.teams.microsoft.com`, and `euaz.turn.teams.microsoft.com`.

Call establishment and media flow paths

When possible, the HDX media engine in the Citrix Workspace app (HdxTeams.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 ports are blocked, the media engine falls back to TCP 443.

The HDX media engine supports ICE, Session Traversal Utilities for NAT (STUN), and Traversal Using Relays around NAT (TURN) for candidate discovery and connection establishment.

If there is no direct path between the two peers or between a peer and a conference server (if the user is joining a multi-party call or meeting), HdxTeams.exe uses a Microsoft Teams transport relay server in Office 365 to reach the other peer or the media processor (where meetings are hosted). The user's client machine must have access to two Office 365 subnet IP address ranges and 4 UDP ports. For more information, see the Architecture diagram in the "Call setup"section further down 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 contain both Transport Relays and media processors.
The Teams Transport Relays provide STUN and TURN functionality, but they are not ICE endpoints. Also, the Teams Transport Relays do not terminate media nor perform any transcoding. They can

bridge TCP (if HdxTeams.exe uses TCP) to UDP when they forward traffic to other peers or media processors.

HdxTeams.exe contacts the closest Microsoft Teams Transport Relay in the Office 365 cloud. HdxTeams.exe uses anycast IP and port 3478–3481 UDP (different UDP ports per workload, though multiplexing can happen) or 443 TCP TLSv1.2 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.

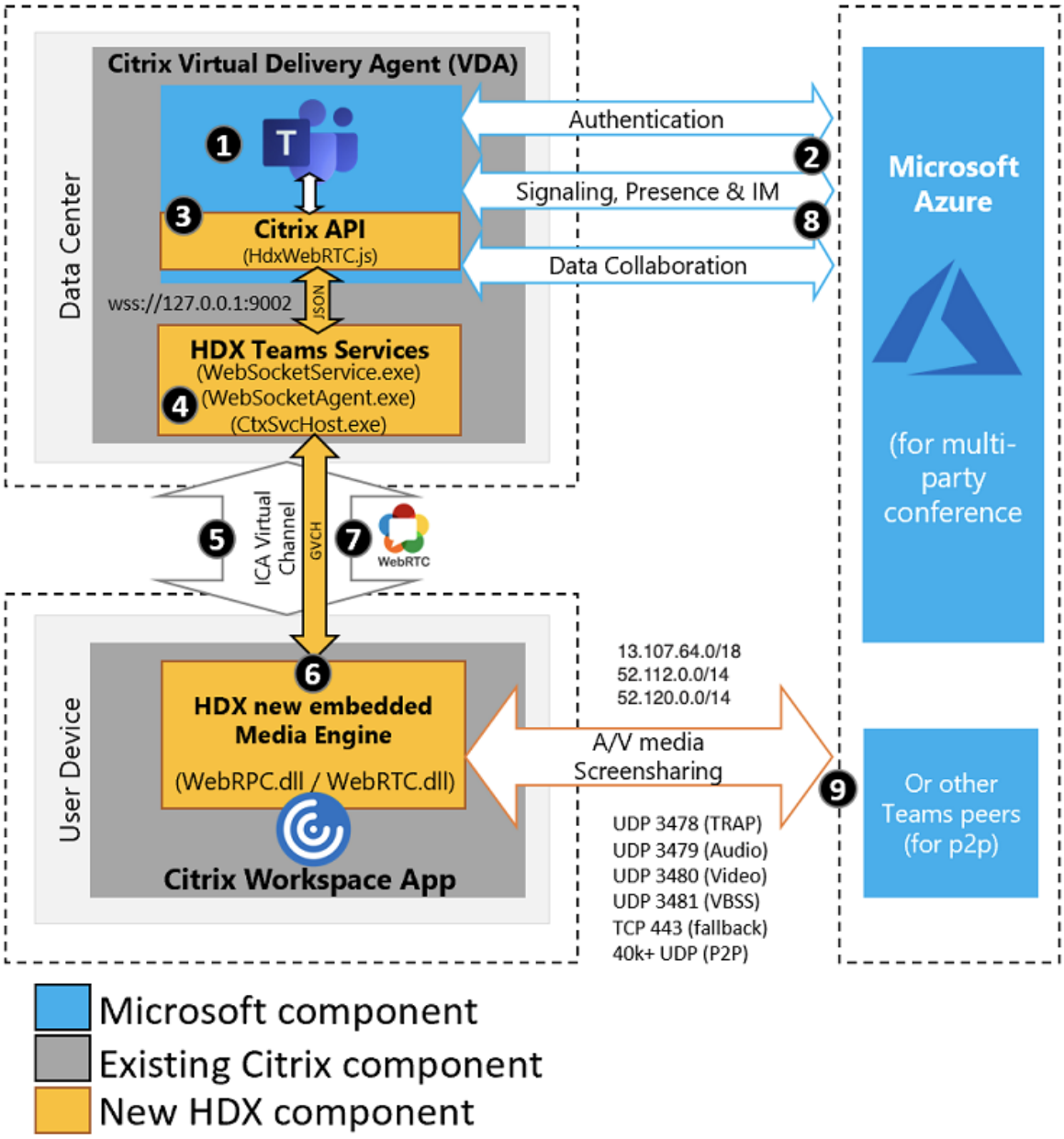
If Teams loaded in optimized mode and HdxTeams.exe is running on the endpoint, Interactive Connectivity Establishment (ICE) failures might cause a call setup failure or one-way-only audio/video. When a call cannot be completed or media streams are not full duplex, check the **Wireshark trace** on the endpoint first.

> **Note:**
>
> If the endpoints don't have internet access, it might still be possible for the user to make a peer-to-peer call only if they are on the same LAN. Meetings fail. In this case, there is 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. Launch Microsoft Teams.
2. Teams authenticates to O365. Tenant policies are pushed down to the Teams client, and relevant TURN and signaling channel information is relayed to the app.
3. Teams detects that it is running in a VDA and makes API calls to the Citrix JavaScript API.
4. Citrix JavaScript in Teams opens a secure WebSocket connection to WebSocketService.exe running on the VDA (127.0.0.1:9002), which spawns WebSocketAgent.exe inside the user session.
5. WebSocketAgent.exe instantiates a generic virtual channel by calling into the Citrix HDX Teams Redirection Service (CtxSvcHost.exe).

6. Citrix Workspace app's wfica32.exe (HDX engine) spawns a new process called HdxTeams.exe, which is the new WebRTC engine used for Teams optimization.
7. HdxTeams.exe and Teams.exe have a 2-way virtual channel path and can start processing multimedia requests.

   ——User calls——

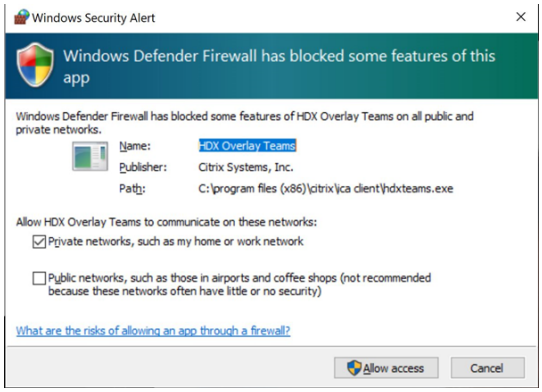
8. **Peer A** clicks the **call** button. Teams.exe communicates with the Teams services in Office 365 establishing an end-to-end signaling path with **Peer B**. Teams asks HdxTeams for a series of supported call parameters (codecs, resolutions, and so forth, which is known as a Session Description Protocol (SDP) offer). These call parameters are then relayed using the signaling path to the Teams services in Office 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 Session Traversal Utilities for NAT (STUN) bind requests) complete. Then, Secure Real-time Transport Protocol (SRTP) media flows directly between HdxTeams.exe and the other peer (or Office 365 conference servers if it is a meeting).

Microsoft Phone System

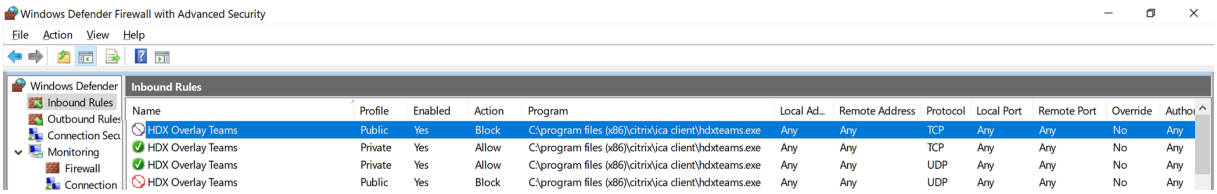
Phone System is Microsoft's technology that enables call control and PBX capabilities in the Office 365 cloud with Microsoft Teams. Optimization for Microsoft Teams supports Phone System, using Office 365 Calling Plans or Direct Routing. With Direct Routing, you connect your own supported session border controller to the Microsoft Phone System directly without any additional on-premises software.

Firewall considerations

When users initiate 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 (HDX Overlay 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 desired.

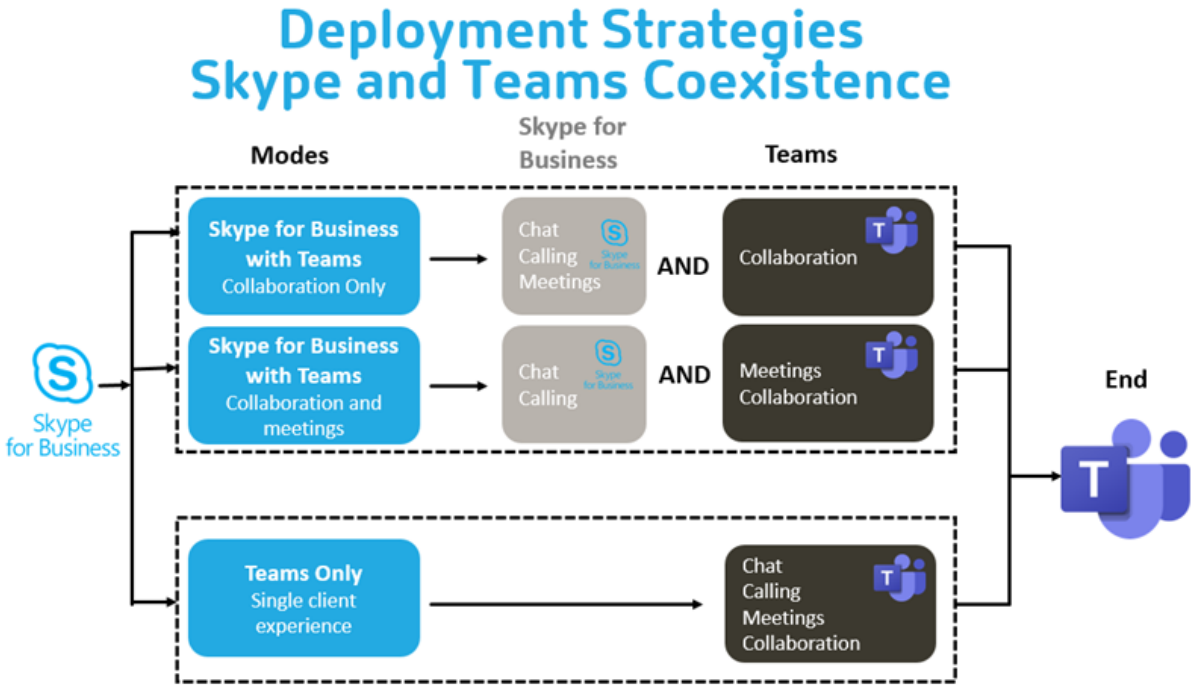


Microsoft Teams and Skype for Business Coexistence

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 Teams multimedia engines then honor whatever configuration is set in your environment (for example, island modes, Skype for Business with Teams collaboration, Skype for Business with 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 Teams.



Citrix SD-WAN: optimized network connectivity for Microsoft Teams

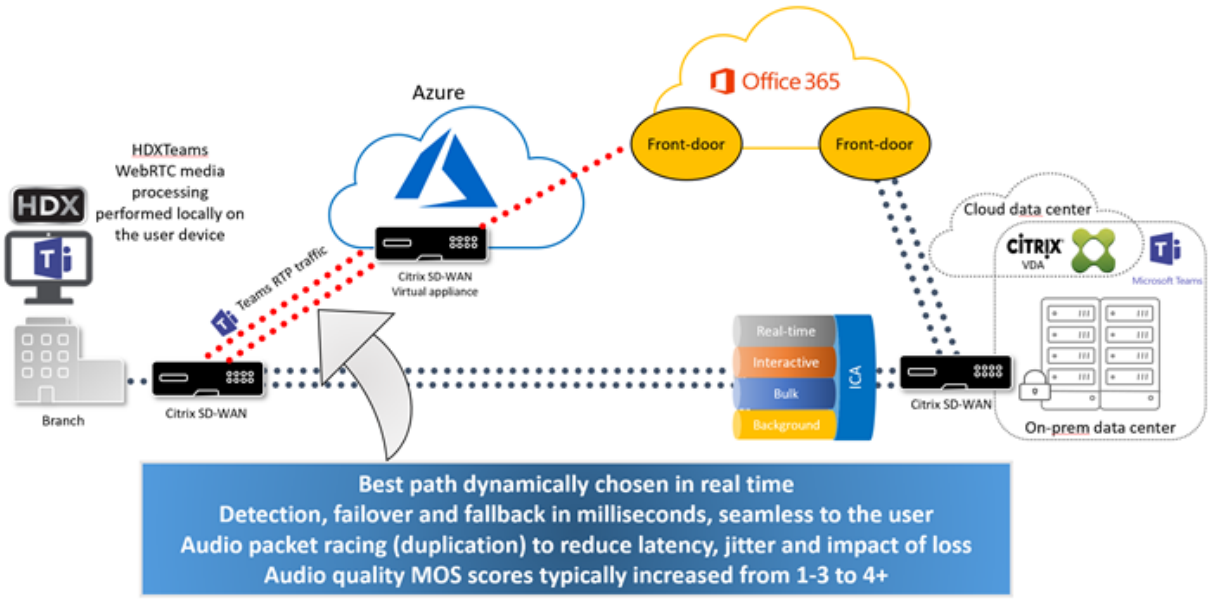
Optimal audio and video quality require a network connection to the Office 365 cloud that has low latency, low jitter, and low packet loss. Backhauling of Microsoft Teams audio-video RTP traffic from Citrix Workspace app users at branch office locations to a data center before going to the internet can add excessive latency and might also cause congestion on WAN links. Citrix SD-WAN optimizes connectivity for Microsoft Teams following Microsoft Office 365 network connectivity principles. Citrix SD-WAN uses the Microsoft REST-based Office 365 IP address and web service and proximate DNS 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.
- Alternatively, Citrix SD-WAN customers can connect to Office 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 is not a concern, it might be sufficient to minimize latency by steering Microsoft Teams traffic directly from the Citrix SD-WAN branch appliance to the nearest Office 365 front door. For more information, see Citrix SD-WAN Office 365 optimization.



Gallery view and active speakers in Microsoft Teams

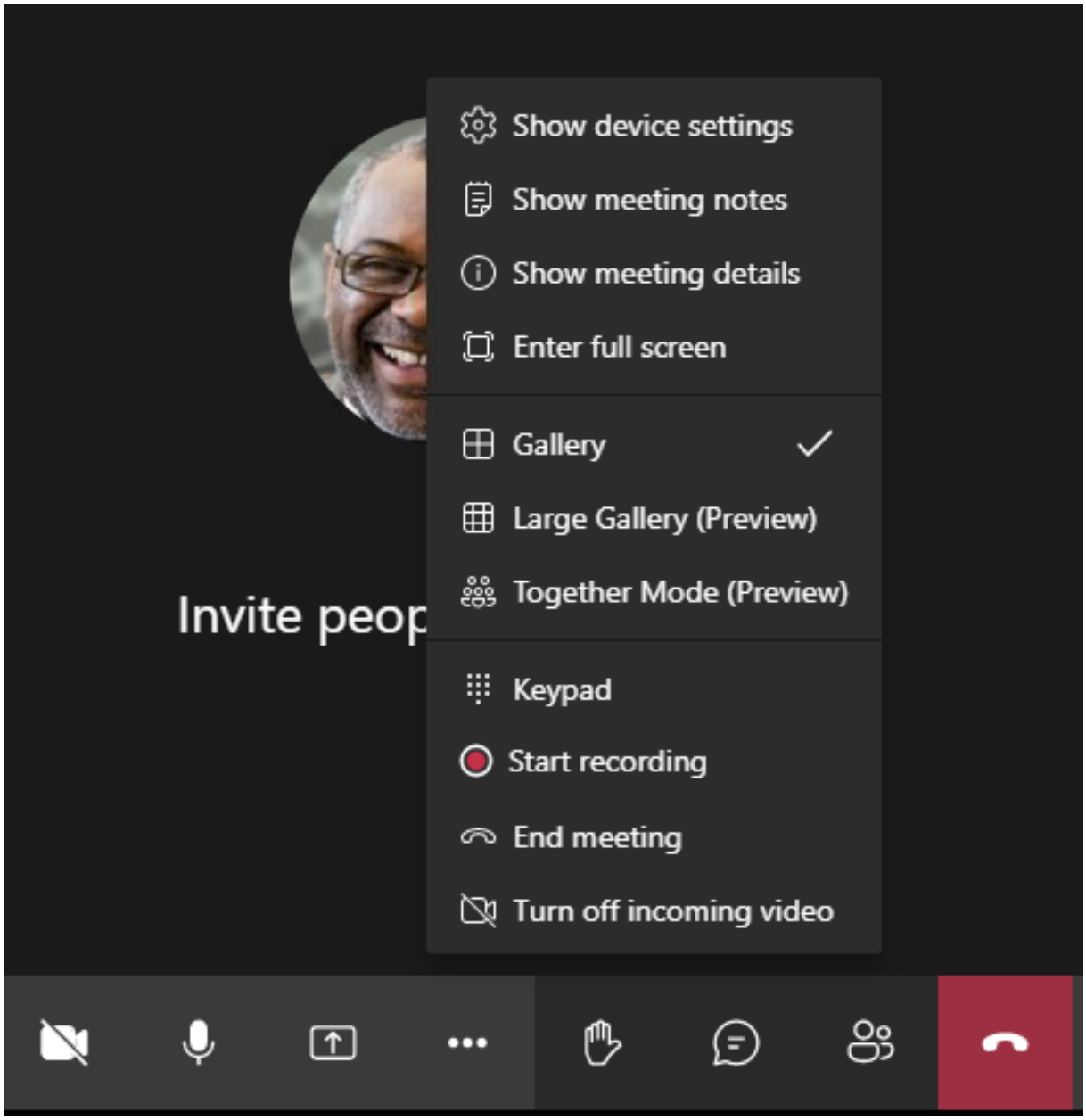
Microsoft Teams supports **Gallery**, **Large gallery**, and **Together mode** layouts.

Microsoft Teams displays a 2x2 grid with video streams of four participants (known as Gallery). In this case, Teams sends 4 individual video streams to the client device for decoding. When there are more than four participants sharing 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 Teams conference server composites a single video feed and sends it to the client device for decoding, resulting in lower CPU consumption. This single "Hollywood square"feed might include user's 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, 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.



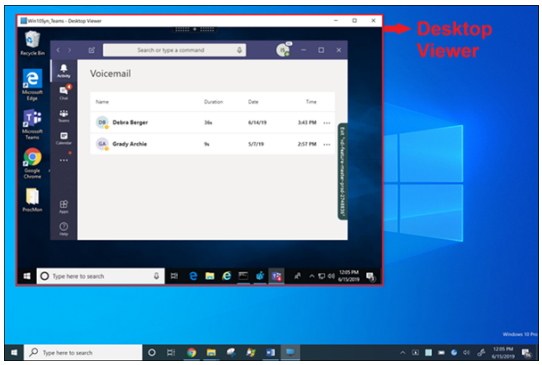
Screen sharing in Microsoft Teams

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. Therefore, if you are in the middle of a video call and the other peer starts to share the desktop, that original camera video feed is paused. Instead, the screen sharing video feed displays. The peer must then manually resume the camera sharing.

Outgoing screen sharing is also optimized and offloaded to the Citrix Workspace app (version 1907 or higher). In this case, HdxTeams.exe captures and transmits only the Citrix Desktop Viewer (CD-

Viewer.exe) window. If you want to share a local application running in your client machine, you can overlay it on top of CDViewer and it is also captured.

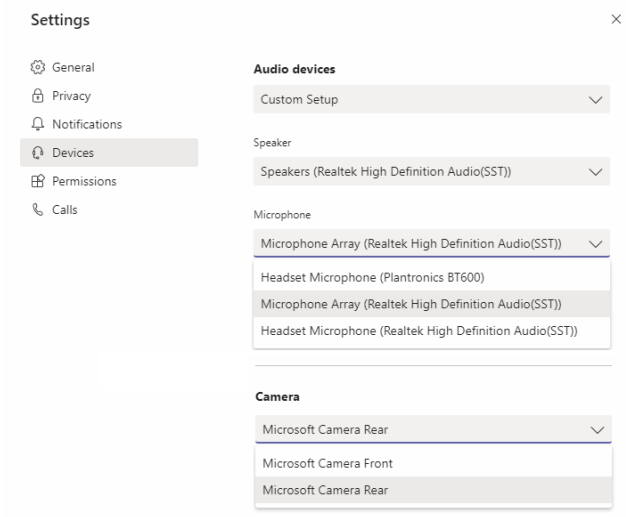
Multi-monitor: In cases where the CDViewer is in full screen mode and spanning across multi-monitor setups, only the primary monitor is shared. Users must drag the application of interest inside the virtual desktop to the primary monitor for the other peer on the call to see it.



> **Note:**
>
> If you are publishing Teams as a stand-alone seamless application, screen sharing captures the local desktop of your physical endpoint in Citrix Workspace app minimum version 1909.

Peripherals in Microsoft Teams

When optimization for Microsoft Teams is active, the Citrix Workspace app accesses the peripherals (headset, microphone, cameras, speakers, and so forth). Then the peripherals are properly enumerated in the Microsoft Teams UI (**Settings > Devices**).



Microsoft Teams does not access the devices directly. Instead, it relies on HdxTeams.exe for acquiring, capturing, and processing the media. Microsoft Teams lists the devices for the user to select.

Recommendations:

- Microsoft Teams certified headsets with built-in echo cancellation. In setups with multiple peripherals, where microphone and speakers are on separate devices an echo might be present. For example, 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 and 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.
- HdxTeams.exe cannot take advantage of CPU offloading with webcams that perform on-board H.264 encoding -UVC 1.1 and 1.5.

> **Note:**
>
> HdxTeams.exe 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 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, open the **Sound Control Panel** (mmsys.cpl), select the playback or recording device, go to **Properties > Advanced** and change the settings to a supported mode. Alternatively, disable the specific device.

Fallback mode

If Microsoft Teams fails to load in optimized VDI mode, the VDA falls back to legacy HDX technologies like Webcam redirection and client audio and microphone redirection. In the unoptimized 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.

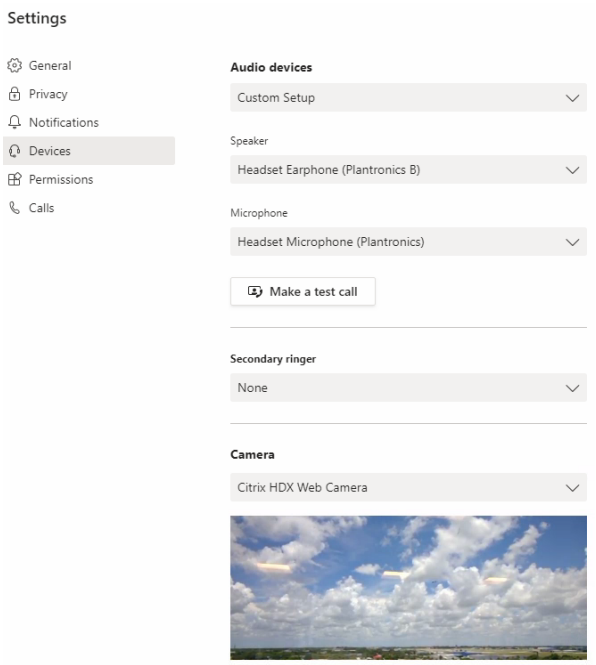
You can now granularly control the fallback mechanism by setting one of the following registry DWORD values in the VDA:

HKLM\SOFTWARE\Microsoft\Teams\DisableFallback

HKCU\SOFTWARE\Microsoft\Office\Teams\DisableFallback

To disable fallback mode, set the value to 1. To enable audio only, set the value to 2. If the value isn't present or is set to 0, fallback mode is enabled. This feature requires 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 Teams, the most significant 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 technologies 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:

- DTMF tones are not supported.
- HID buttons - Answer and end call are not supported. Volume up and down are supported.
- When doing screen sharing in multi-monitor setups, only the main monitor is shared.

- We support only one video stream from an incoming camera or screen share stream. When there's an incoming screen share, that screen share is shown it instead of the video of the dominant speaker.
- Secondary ringer (**Teams > Settings > Devices**) is not supported.
- QoS settings in Admin Center for Microsoft Teams do not apply for VDI users.
- App protection add-on feature for the Citrix Workspace app prevents outgoing screen sharing.
- The zoom in and zoom out function in Teams is not supported.

Limitation on the VDA:

- When you configure the Citrix Workspace app High DPI setting to **Yes** or to **No, use the native resolution**, the redirected video window appears out of place when the monitor's DPI scaling factor is set to anything above 100%.

Limitations on Citrix Workspace app and the VDA:

- Outgoing screen sharing: Application sharing is not supported.
- You can only control the volume of an optimized call using the volume bar on the client machine –not on the VDA.

Microsoft limitations

- The options to blur or customize the background aren't supported.
- A 3x3 gallery view is not supported. 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. Teams dependency –contact Microsoft for when to expect 1080p.
- PSTN call ringback tone is not supported.
- Media bypass for Direct Routing is not supported.

Citrix and Microsoft limitations

- When doing screen sharing, the option **include system audio** is not available.
- Pop out chat (also known as multi-window chat or the new meeting experience) is not supported.
- Breakout rooms are supported for VDI participants. Teams doesn't support breakout rooms if the organizer is a VDI user.
- Give control and take control: Not supported during a desktop screen sharing or application sharing session. Supported only during a PowerPoint sharing session.
- E911 and Location-Based Routing are not supported.

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, 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 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

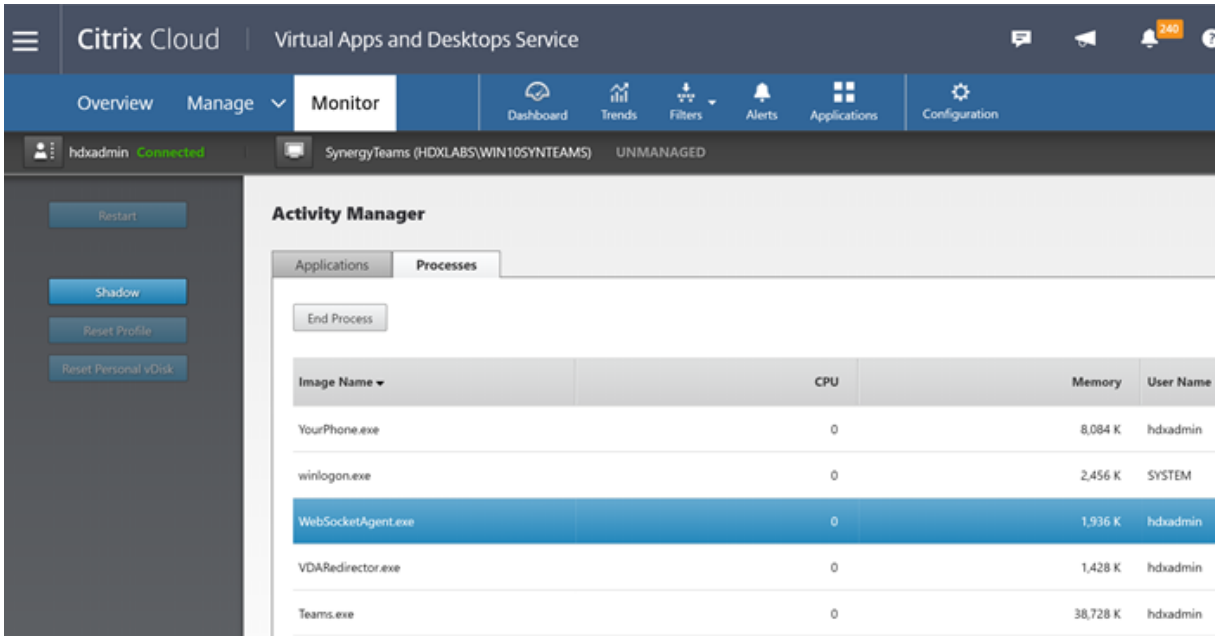
Monitor, troubleshoot, and support Microsoft Teams

March 7, 2022

Monitor Teams

This section provides guidelines for monitoring Microsoft Teams optimization with HDX.
If the user is running in optimized mode and `HdxTeams.exe` is running on the client machine, there

is a process in the VDA called `WebSocketAgent.exe` 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`.

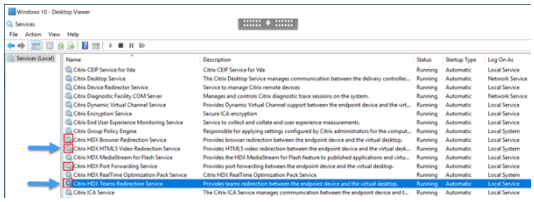
For more information, see *Monitoring* in the Knowledge Center article CTX253754.

Troubleshoot

This section provides troubleshooting tips for issues that you might encounter when using optimization for Microsoft Teams.
Further information can be found in 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.

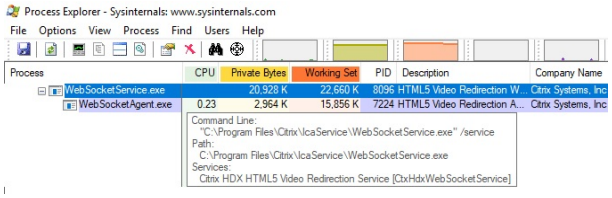


- **Citrix HDX Teams Redirection Service** establishes the virtual channel used in Microsoft Teams. The service relies on CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** runs as WebSocketService.exe listening on 127.0.0.1:9002 TCP. WebSocketService.exe performs two main functions:

  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.

Service	Path to executable in Windows Server OS	Log on as	Description
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 HdxTeams.exe. It does so when Microsoft Teams launches in the VDA and the user tries to call or access 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.

Linux logs:

You can locate Linux logs in the `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/` directory.

When establishing a call, these four ICE phases are required:

- Candidate gathering
- candidate exchange
- Connectivity checks (STUN bind requests)
- Candidate promotion

In the HdxTeams.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 this 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:

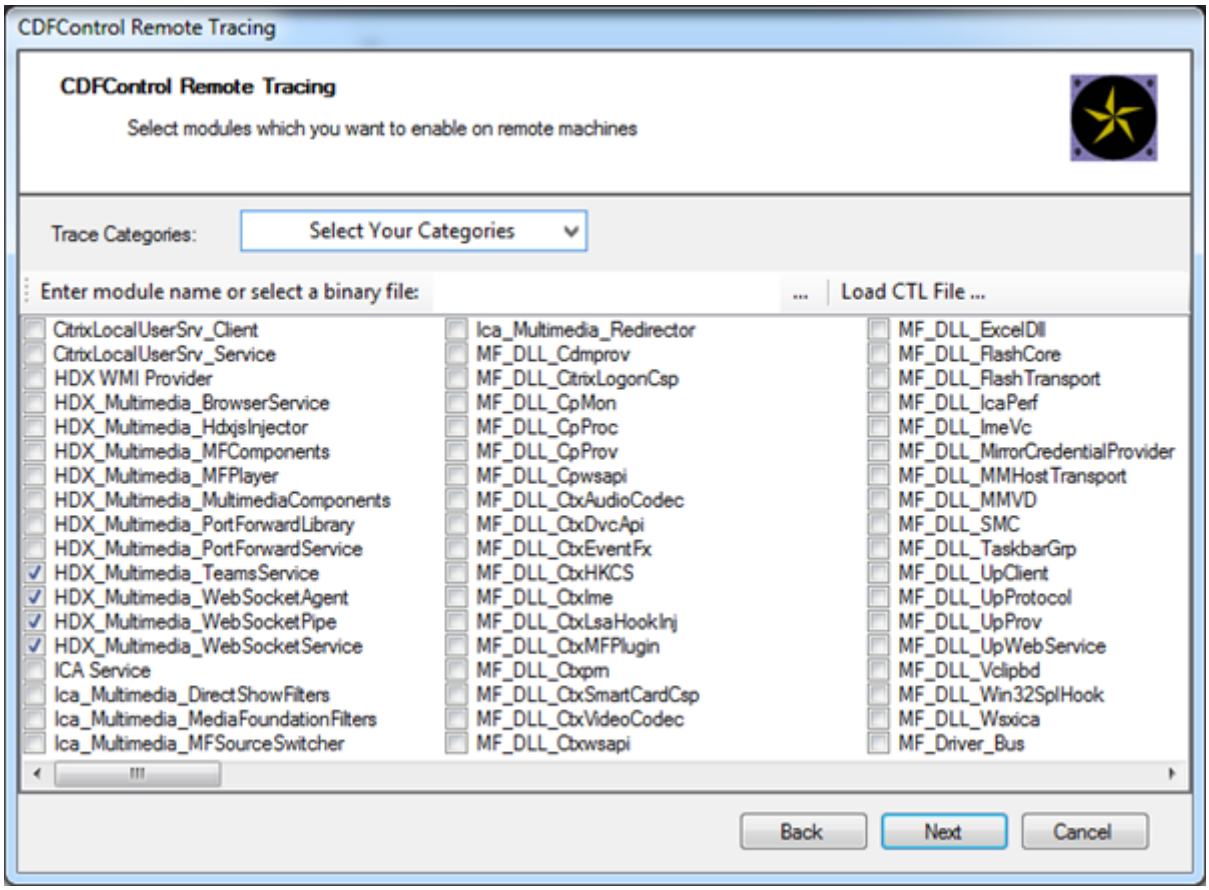
1. host
2. peer reflexive
3. server reflexive

4. transport relay

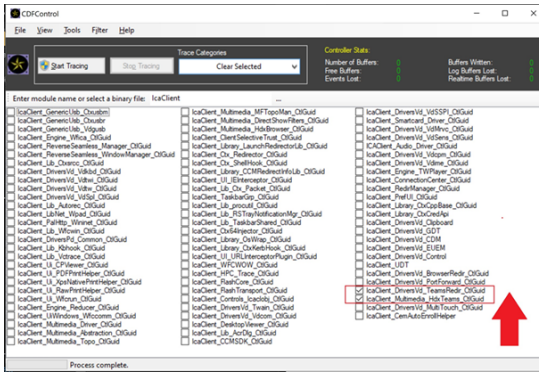
If you encounter an issue and can reproduce it consistently, we recommend clicking **Help > Report a problem** in Teams. Logs are shared between Citrix and Microsoft to resolve technical issues if you opened a case with Microsoft.
Capturing CDF traces before contacting Citrix Support is also beneficial. 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:



Windows Media redirection

February 6, 2020

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

February 6, 2020

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

February 6, 2020

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)

> **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.

1. On the server:
    a) Create a key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    b) Create a REG_DWORD value.
        - Name: CFROnlyModeAvailable
        - Type: REG_DWORD
        - Data: Set to 1
2. On the user device:

a) Ensure that the latest version of Citrix Workspace app is installed.
b) From the Citrix Workspace app installation directory, start CtxCFRUI.exe.
c) Choose the **Custom** radio button and add, edit, or remove folders.
d) Disconnect and reconnect your sessions for the setting to take effect.

Host to client redirection

July 20, 2021

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

February 4, 2022

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
- Internet Explorer 11

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.

The browser extension must be registered using the commands shown. Run the commands as needed on the VDA and client.

To register the browser extension 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 example:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

To unregister the browser extension use the `/unregIE` option as in the example shown:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

To register the browser extension on the client open a command prompt and run `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` with the same options as the examples shown.

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 considered 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

October 11, 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 blacklist) by selecting embedded links within a browser in a desktop session. If you navigate to a URL that is not present in the blacklist, 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 blacklist or whitelist 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 whitelist and URL blacklist 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:

- Internet Explorer 11. You can use Internet Explorer 8, 9, or 10, but Microsoft supports (and Citrix recommends using) version 11.
- Firefox 3.5 through 21.0
- Chrome 10

Citrix Viewer must also be enabled on the VDA.

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 whitelist and blacklist 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. Start Citrix Studio.
   - For on-premises deployments, open **Citrix Studio** from the **Start menu**.
   - For Cloud service deployments, go to **Citrix Cloud > Virtual Apps and Desktops service > Manage** tab.
2. In the Studio navigation pane, click **Policies**.
3. In the Actions pane, click **Create Policy**.

4. In the Create Policy window, type "Allow Local App Access"in the search box and then click **Select**.
5. 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.
6. In the Create Policy window, type "URL redirection white list"in the search box and then click **Select**. The URL redirection white list specifies URLs to open in the default browser of the remote session.
7. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.
8. In the Create Policy window, type "URL redirection black list"in the search box and then click **Select**. The URL redirection black list specifies URLs that are redirected to the default browser running on the endpoint.
9. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.
10. On the Settings page, click **Next**.
11. On the Users and Machines page, assign the policy to the applicable Delivery Groups and then click **Next**.
12. 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.
> - 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/CitrixBase.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 one of the following two ways:

Use the Registry Editor.

1. On the server where Citrix Studio is installed, run regedit.exe.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`.
3. Add the REG_DWORD entry `ClientHostedAppsEnabled` and a value of 1. (A 0 value disables Local App Access.)

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 Cloud service 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. Open **Citrix Studio** from the **Start** menu.

2. In the Studio navigation pane, click **Applications**.
3. In the upper middle pane, right-click the blank area and select **Add Local App Access Application** from the context 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**.
4. 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\System32\VDARedirector.exe /regAll

URL interception across browsers

- By default, Internet Explorer redirects the specified URL. If the URL is not in the blacklist 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 blacklist.

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.

1. On the hosted desktop, run **regedit.msc**.

2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State`.

   For a 64-bit system, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State`.

3. Add the REG_DWORD entry **Terminate** and one of the values:

   - 1 - Local applications continue to run when a user logs off or disconnects from the virtual desktop. Upon reconnection, local applications are reintegrated if they are available in the virtual desktop.
   - 3 - Local applications close when a user logs off or disconnects from the virtual desktop.

Generic USB redirection and client drive considerations

August 10, 2022

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 that 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 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.

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 or Windows Server 2016.
- 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:

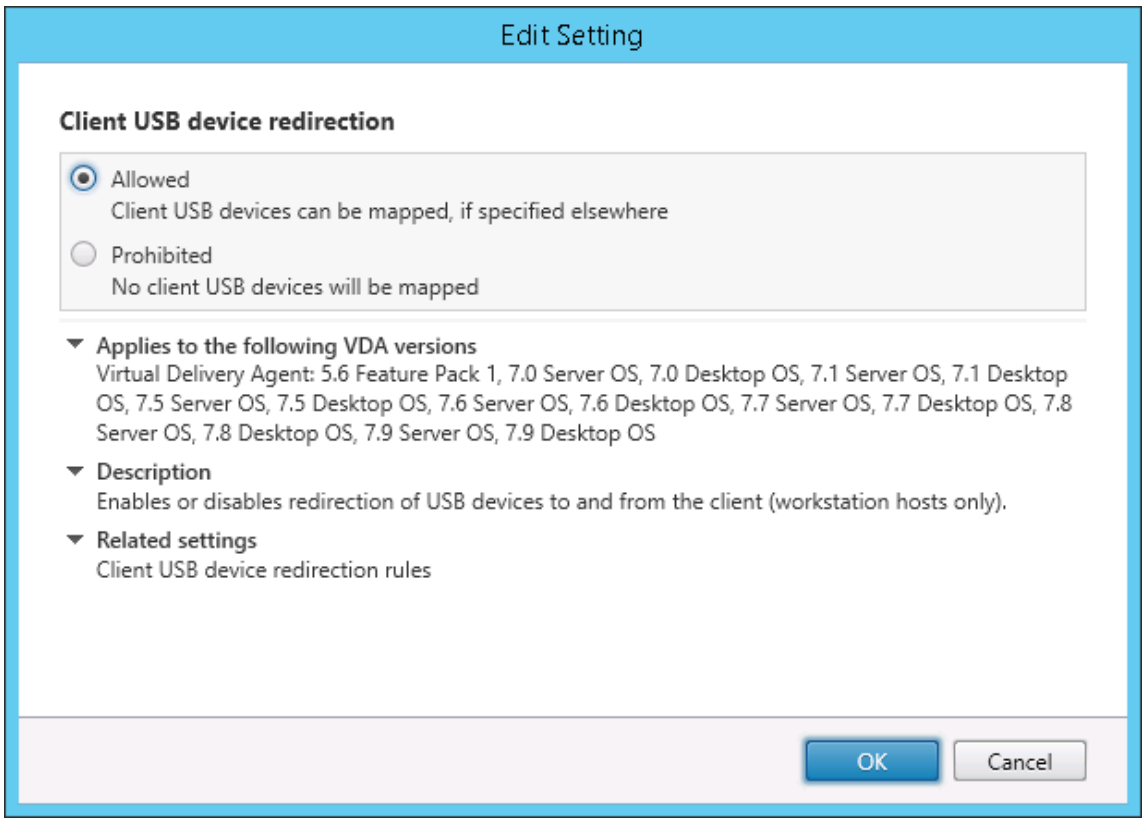
- If two different organizations or departments are responsible for Citrix Workspace app and VDA, they can enforce control separately. This configuration applies when a user in one organization accesses an application in another organization.
- Citrix policy settings can control USB devices that are 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:

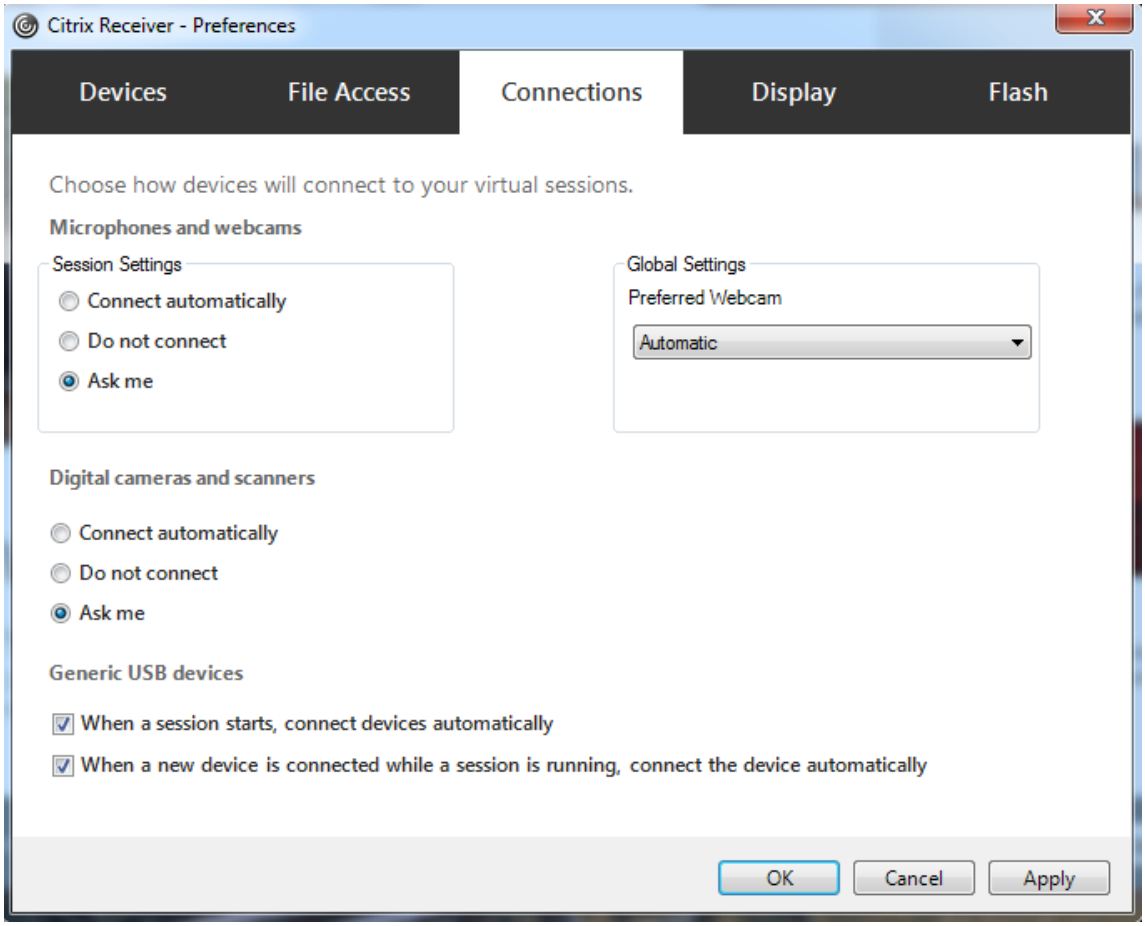
1. Add the Client USB device redirection to a policy and set its value to **Allowed**.



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.



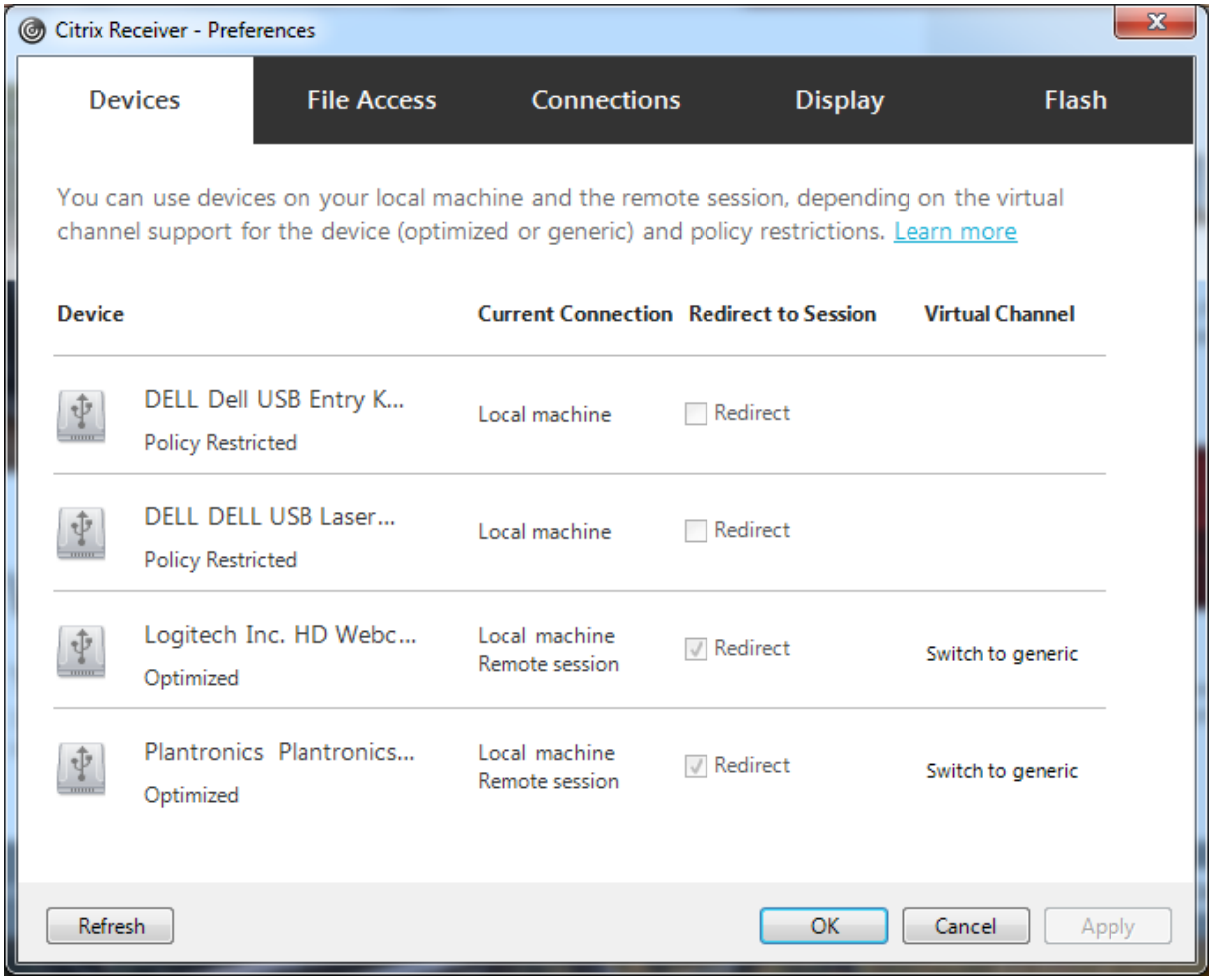
If you specified USB policy rules for the VDA in the previous step, specify those same policy rules for Citrix Workspace app.

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.

Control file access with client drive mapping

You can control whether users can copy files from their virtual environments to their user devices. By default, files and folders on mapped client-drives are available in read/write mode from within the session.

To prevent users from adding or changing files and folders on mapped client-devices, enable the **Read-only client drive access** policy setting. When adding this setting to a policy, ensure that the Client drive redirection setting is set to **Allowed** and is also added to the policy.

Print

March 7, 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.

Printing concepts

Before you begin planning your deployment, make sure that you understand these core concepts for printing:

- The types of printer provisioning available
- How print jobs are routed
- The basics of printer driver management

Printing concepts build on Windows printing concepts. To configure and successfully manage printing in your environment, you must understand how Windows network and client printing works and how this translates into printing behavior in this environment.

Print process

In this environment, all printing is initiated (by the user) on machines hosting applications. Print jobs are redirected through the network print server or user device to the printing device.

There is no persistent workspace for users of virtual desktops and applications. When a session ends the user's workspace is deleted, thus all settings need to be rebuilt at the beginning of each session. As a result, each time a user starts a new session, the system must rebuild the user's workspace.

When a user prints:

- Determines what printers to provide to the user. This is known as printer provisioning.
- Restores the user's printing preferences.
- Determines which printer is the default for the session.

You can customize how to perform these tasks by configuring options for printer provisioning, print job routing, printer property retention, and driver management. Be sure to evaluate how the various option settings might change the performance of printing in your environment and the user experience.

Printer provisioning

The process that makes printers available in a session is known as provisioning. Printer provisioning is typically handled dynamically. That is, the printers that appear in a session are not predetermined and stored. Instead, the printers are assembled, based on policies, as the session is built during log on and reconnection. As a result, the printers can change according to policy, user location, and network changes, provided they are reflected in policies. Thus, users who roam to a different location might see changes to their workspace.

The system also monitors client-side printers and dynamically adjusts in-session auto-created printers based on additions, deletions, and changes to the client-side printers. This dynamic printer discovery benefits mobile users as they connect from various devices.

The most common methods of printer provisioning are:

- **Universal Print Server** - The Citrix Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal print driver. This solution enables you to use a single driver on a Multi-session OS machine to allow network printing from any device.

Citrix recommends the Citrix Universal Print Server for remote print server scenarios. The Universal Print Server transfers the print job over the network in an optimized and compressed format, thus minimizing network use and improving the user experience.

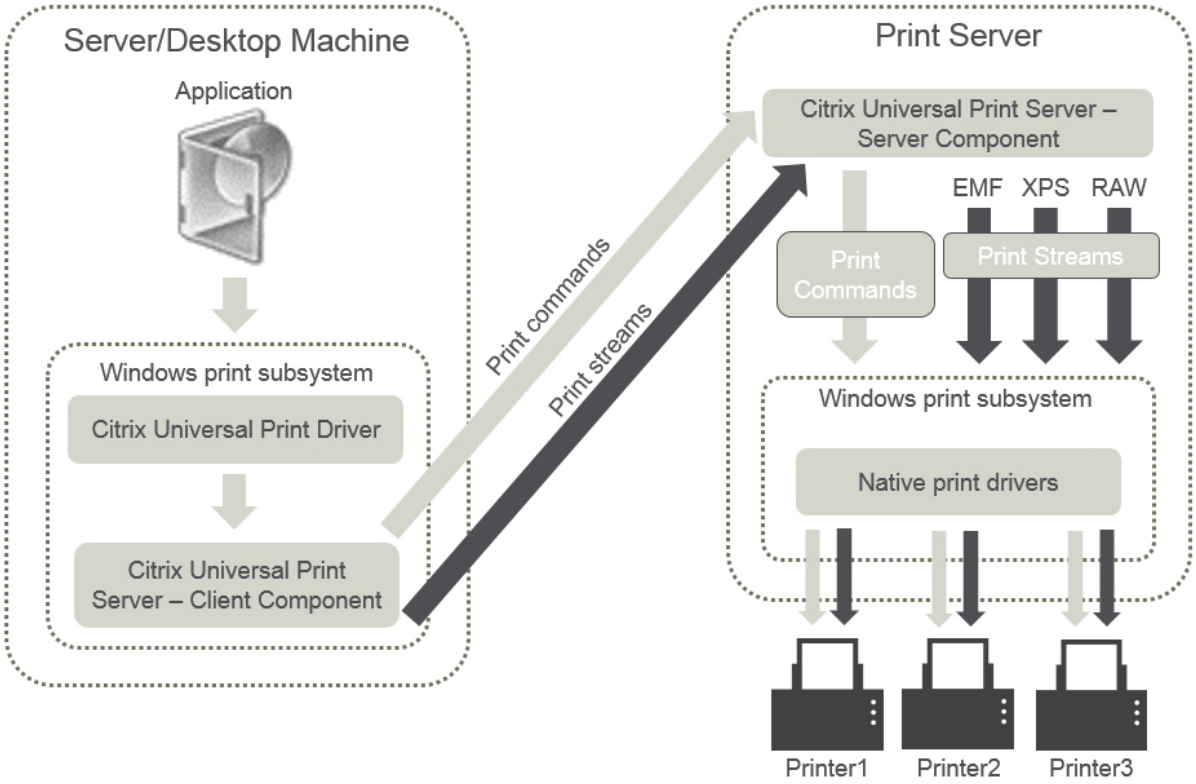
The Universal Print Server feature comprises:

A client component, **UPClient** - Enable the UPClient on each Multi-session OS machine that provisions session network printers and uses the Universal print driver.

A server component, **UPServer** - Install UPServer on each print server that provisions session network printers and uses the Universal print driver for the session printers (whether or not the session printers are centrally provisioned).

For Universal Print Server requirements and setup details, refer to the system requirements and installation articles.

The following illustration shows the typical workflow for a network based printer in an environment that uses Universal Print Server.



When you enable the Citrix Universal Print Server, all connected network printers leverage it automatically through auto-discovery.

> **Note:**
> The Universal Print Server is also supported for VDI-in-a-Box 5.3. For information about installing Universal Print Server with VDI-in-a-Box, refer to the VDI-in-a-Box documentation.

- **Autocreation** - *Autocreation* refers to printers automatically created at the beginning of each session. Both remote network printers and locally attached client printers can be auto-created. Consider auto-creating only the default client printer for environments with a large number of printers per user. Auto-creating a smaller number of printers uses less overhead (memory and CPU) on Multi-session OS machines. Minimizing auto-created printers can also reduce user logon times.

  Auto-created printers are based on:

  - The printers installed on the user device.
  - Any policies that apply to the session.

    Autocreation policy settings enable you to limit the number or type of printers that are auto-created. By default, the printers are available in sessions when configuring all printers on the user device automatically, including locally attached and network printers.

  After the user ends the session, the printers for that session are deleted.

Client and network printer autocreation has associated maintenance. For example, adding a printer requires that you:

- Update the Session printers policy setting.
- Add the driver to all Multi-session OS machines using the Printer driver mapping and compatibility policy setting.

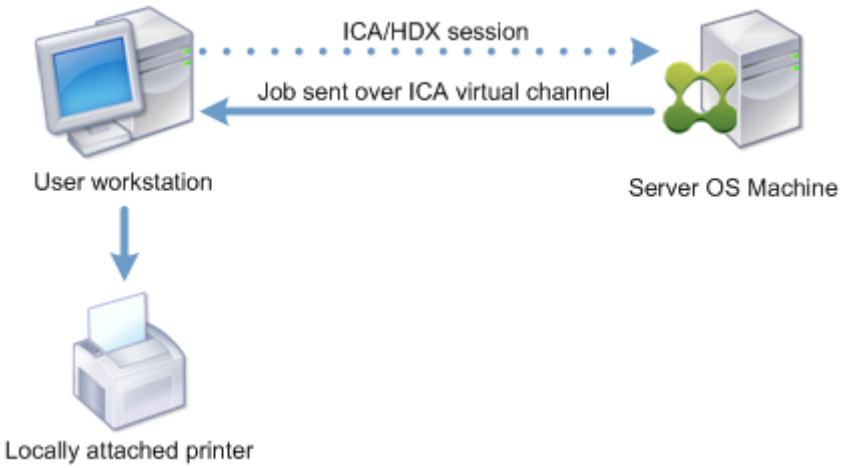
Print job routing

The term printing pathway encompasses both the path by which print jobs are routed and the location where print jobs are spooled. Both aspects of this concept are important. Routing affects network traffic. Spooling affects utilization of local resources on the device that processes the job.

In this environment, print jobs can take two paths to a printing device: through the client or through a network print server. Those paths are referred to as the client printing pathway and the network printing pathway. Which path is chosen by default depends on the kind of printer used.

Locally attached printers

The system routes jobs to locally attached printers from the Multi-session OS machine, through the client, and then to the print device. The ICA protocol optimizes and compresses the print job traffic. When a printing device is attached locally to the user device, print jobs are routed over the ICA virtual channel.



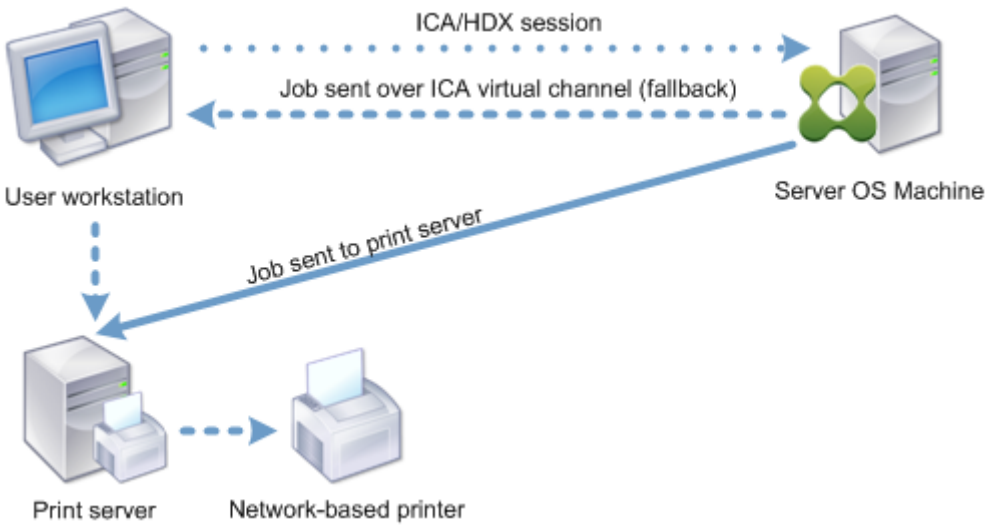
Network-based printers

By default, all print jobs destined for network printers route from the Multi-session OS machine, across the network, and directly to the print server. However, print jobs are automatically routed over the ICA connection in the following situations:

- If the virtual desktop or application cannot contact the print server.
- If the native printer driver is not available on the Multi-session OS machine.

If the Universal Print Server is not enabled, configuring the client printing pathway for network printing is useful for low bandwidth connections, such as wide area networks, that can benefit from the optimization and traffic compression that results from sending jobs over the ICA connection.

The client printing pathway also lets you limit traffic or restrict bandwidth allocated for print jobs. If routing jobs through the user device is not possible, such as for thin clients without printing capabilities, Quality of Service should be configured to prioritize ICA/HDX traffic and ensure a good in-session user experience.



Print driver management

The Citrix Universal Printer Driver (UPD) is a device-independent print driver, which is compatible with most printers. The Citrix UPD consists of two components:

Server component. The Citrix UPD is installed as part of the Citrix Virtual Apps and Desktops VDA installation. The VDA installs the following drivers with Citrix UPD: "Citrix Universal Printer"(EMF driver) and the "Citrix XPS Universal Printer"(XPS driver).

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

The VDA installers no longer offer options to control Universal Print Server PDF printer driver installation. The PDF printer driver is now always installed automatically. When you upgrade to the 7.17 VDA (or a later supported version), any previously installed Citrix PDF printer driver is automatically removed and replaced with the latest version.

When a print job is initiated the driver records the output of the application and sends it, without any modification to the end-point device.

Client component. The Citrix UPD is installed as part of the Citrix Workspace app installation. It fetches the incoming print stream for the Citrix Virtual Apps and Desktops session. It then forwards the print stream to the local printing subsystem where the print job is rendered using the device specific printer drivers.

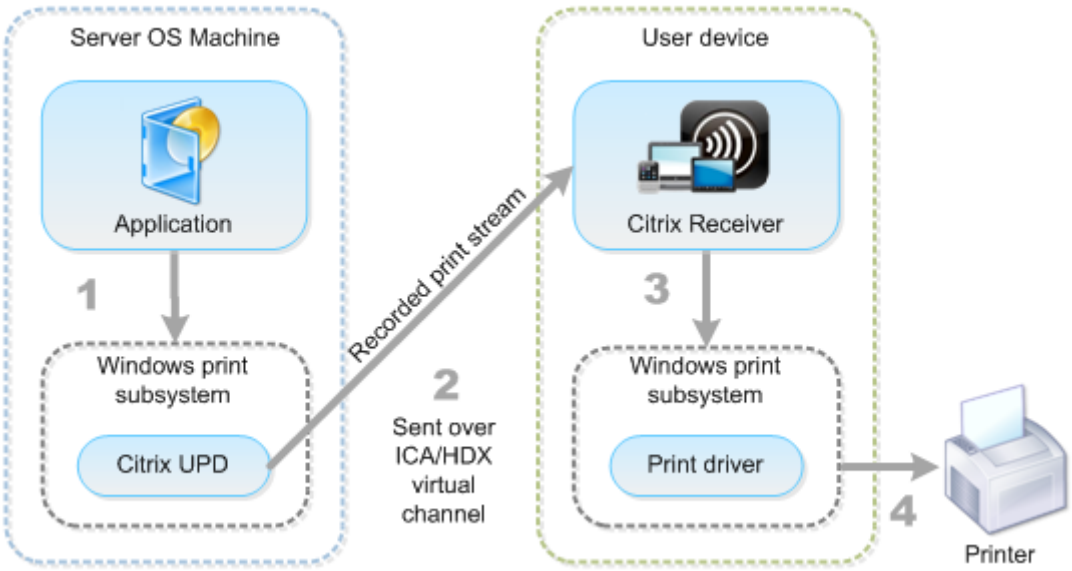
The Citrix UPD supports the following print formats:

- Enhanced Metafile Format (**EMF**), default. EMF is the 32-bit version of the Windows Metafile (WMF) format. The EMF driver can only be used by Windows-based clients.
- XML Paper Specification (**XPS**). The XPS driver uses XML to create a platform-independent "electronic paper"similar to Adobe PDF format.
- Printer Command Language (**PCL5c** and **PCL4**). PCL is a printing protocol developed originally by Hewlett-Packard for inkjet printers. It is used for printing basic text and graphics and is widely supported on HP LaserJet and multifunction peripherals.
- PostScript (**PS**). PostScript is a computer language that can be used for printing text and vector graphics. The driver is widely used in low-cost printers and multifunction peripherals.

The PCL and PS drivers are best suited when using non-Windows based devices such as a Mac or UNIX client. The order in which Citrix UPD attempts to use the drivers can be changed using the Universal driver preference policy setting.

The Citrix UPD (EMF and XPS drivers) supports advanced printing features such as stapling and paper source selection. These features are available if the native driver makes them available using the Microsoft Print Capability technology. The native driver should use the standardized Print Schema Keywords in the Print Capabilities XML. If non-standard keywords are used, the advanced printing features are not available using Citrix Universal print driver.

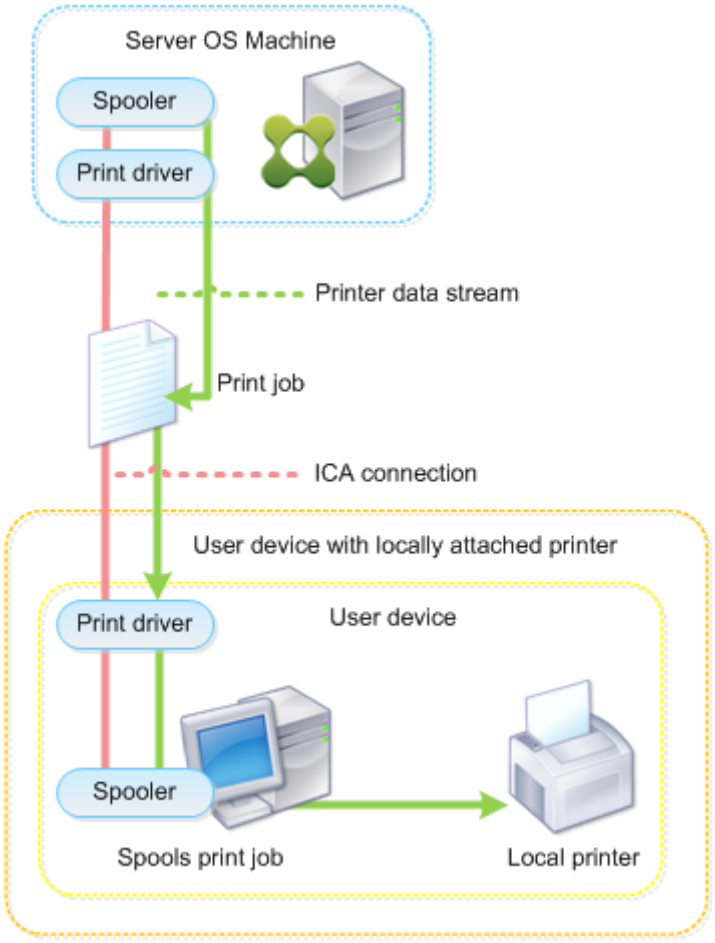
The following illustration shows the Universal print driver components and a typical workflow for a printer locally attached to a device.



When planning your driver management strategy, determine if you will support the Universal print driver, device-specific drivers, or both. If you support standard drivers, you must determine:

During printer autocreation, if the system detects a new local printer connected to a user device, it checks the Multi-session OS machine for the required printer driver. By default, if a Windows-native driver is not available, the system uses the Universal print driver.

The printer driver on the Multi-session OS machine and the driver on the user device must match for printing to succeed. The illustration that follows shows how a printer driver is used in two places for client printing.



- The types of drivers to support.
- Whether to install printer drivers automatically when they are missing from Multi-session OS machines.
- Whether to create driver compatibility lists.

Related content

- Printing configuration example
- Best practices, security considerations, and default operations
- Print policies and preferences
- Provision printers
- Maintain the printing environment

Printing configuration example

March 7, 2022

Choosing the most appropriate printing configuration options for your needs and environment can simplify administration. Although the default print configuration enables users to print in most environments, the defaults might not provide the expected user experience or the optimum network usage and management overhead for your environment.

Your printing configuration depends upon:

- Your business needs and your existing printing infrastructure.

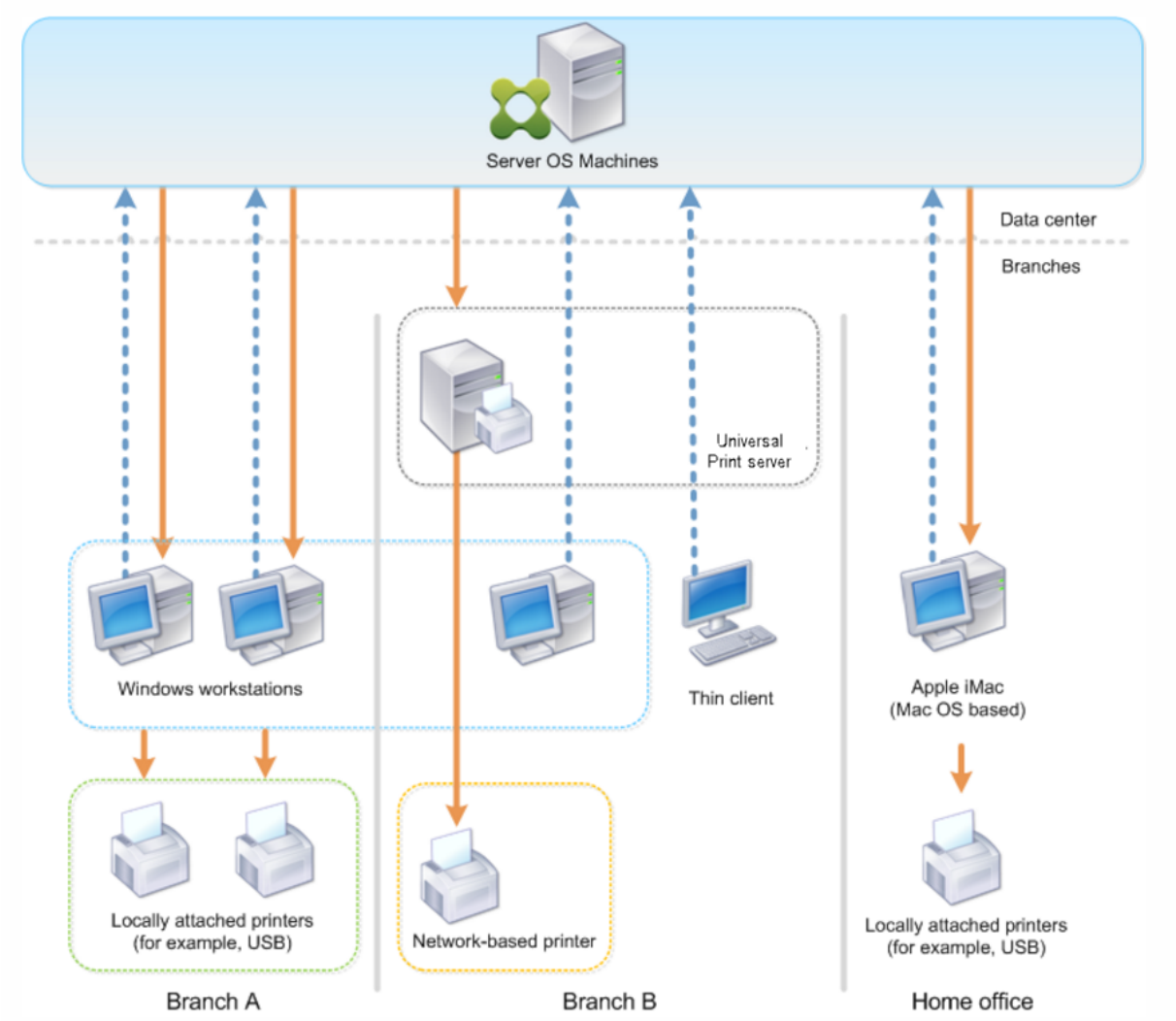
  Design your printing configuration around the needs of your organization. Your existing printing implementation (whether users can add printers, which users have access to what printers, and so on) might be a useful guide when defining your printing configuration.
- Whether your organization has security policies that reserve printers for certain users (for example, printers for Human Resources or payroll).
- Whether users need to print while away from their primary work location, such as workers who move between workstations or travel on business.

When designing your printing configuration, try to give users the same experience in a session as they have when printing from local user devices.

Example print deployment

The following illustration shows the print deployment for these use cases:

- **Branch A** - A small overseas branch office with a few Windows workstations. Every user workstation has a locally attached, private printer.
- **Branch B** - A large branch office with thin clients and Windows-based workstations. For increased efficiency, the users of this branch share network-based printers (one per floor). Windows-based print servers located within the branch manage the print queues.
- **Home office** - A home office with a Mac OS-based user device that accesses the company's Citrix infrastructure. The user device has a locally attached printer.



The following sections describe the configurations which minimize the complexity of the environment and simplify its management.

Auto-created client printers and Citrix Universal printer driver

In Branch A, all users work on Windows-based workstations, therefore auto-created client printers and the Universal printer driver are used. Those technologies provide these benefits:

- Performance - Print jobs are delivered over the ICA printing channel, thus the print data can be compressed to save bandwidth.

  To ensure that a single user printing a large document cannot degrade the session performance of other users, a Citrix policy is configured to specify the maximum printing bandwidth.

  An alternative solution is to leverage a multi-stream ICA connection, in which the print traffic is transferred within a separate low priority TCP connection. Multi-stream ICA is an option when

Quality of Service (QoS) is not implemented on the WAN connection.

- Flexibility - Use of the Citrix Universal printer driver ensures that all printers connected to a client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center.

Citrix Universal Print Server

In Branch B, all printers are network-based and their queues are managed on a Windows print server, thus the Citrix Universal Print Server is the most efficient configuration.

All required printer drivers are installed and managed on the print server by local administrators. Mapping the printers into the virtual desktop or application session works as follows:

- For Windows-based workstations - The local IT team helps users connect the appropriate network-based printer to their Windows workstations. This enables users to print from locally-installed applications.

  During a virtual desktop or application session, the printers configured locally are enumerated through autocreation. The virtual desktop or application then connects to the print server as a direct network connection if possible.

  The Citrix Universal Print Server components are installed and enabled, thus native printer drivers are not required. If a driver is updated or a printer queue is modified, no additional configuration is required in the data center.

- For thin clients - For thin client users, printers must be connected within the virtual desktop or application session. To provide users with the simplest printing experience, administrators configure a single Citrix Session Printer policy per floor to connect a floor's printer as the default printer.

  To ensure the correct printer is connected even if users roam between floors, the policies are filtered based on the subnet or the name of the thin client. That configuration, referred to as proximity printing, allows for local printer driver maintenance (according to the delegated administration model).

  If a printer queue needs to be modified or added, Citrix administrators must modify the respective Session printer policy within the environment.

Because the network printing traffic will be sent outside the ICA virtual channel, QoS is implemented. Inbound and outbound network traffic on ports used by ICA/HDX traffic are prioritized over all other network traffic. That configuration ensures that user sessions are not impacted by large print jobs.

Auto-created client printers and Citrix Universal printer driver

For home offices where users work on non-standard workstations and use non-managed print devices, the simplest approach is to use auto-created client printers and the Universal printer driver.

Deployment summary

In summary, the sample deployment is configured as follows:

- No printer drivers are installed on Multi-session OS machines. Only the Citrix Universal printer driver is used. Fallback to native printing and the automatic installation of printer drivers are disabled.
- A policy is configured to auto-create all client printers for all users. Multi-session OS machines will directly connect to the print servers by default. The only configuration required is to enable the Universal Print Server components.
- A session printer policy is configured for every floor of Branch B and applied to all thin clients of the respective floor.
- QoS is implemented for Branch B to ensure excellent user experience.

Best practices, security considerations, and default operations

February 6, 2020

Best practices

Many factors determine the best printing solution for a particular environment. Some of these best practices might not apply to your Site.

- Use the Citrix Universal Print Server.
- Use the Universal printer driver or Windows-native drivers.
- Minimize the number of printer drivers installed on Multi-session OS machines.
- Use driver mapping to native drivers.
- Never install untested printer drivers on a production site.
- Avoid updating a driver. Always attempt to uninstall a driver, restart the print server, and then install the replacement driver.

- Uninstall unused drivers or use the Printer driver mapping and compatibility policy to prevent printers from being created with the driver.
- Try to avoid using version 2 kernel-mode drivers.
- To determine if a printer model is supported, contact the manufacturer or see the Citrix Ready product guide at www.citrix.com/ready.

  In general, all of the Microsoft-supplied printer drivers are tested with Terminal Services and guaranteed to work with Citrix. However, before using a third-party printer driver, consult your printer driver vendor so that the driver is certified for Terminal Services by the Windows Hardware Quality Labs (WHQL) program. Citrix does not certify printer drivers.

Security considerations

Citrix printing solutions are secure by design.

- The Citrix Print Manager Service constantly monitors and responds to session events such as logon and logoff, disconnect, reconnect, and session termination. It handles service requests by impersonating the actual session user.
- Citrix printing assigns each printer a unique namespace in a session.
- Citrix printing sets the default security descriptor for auto-created printers to ensure that client printers auto-created in one session are inaccessible to users running in other sessions. By default, administrative users cannot accidentally print to another session's client printer, even though they can see and manually adjust permissions for any client printer.

Default print operations

By default, if you do not configure any policy rules, printing behavior is as follows:

- The Universal Print Server is disabled.
- All printers configured on the user device are created automatically at the beginning of each session.

  This behavior is equivalent to configuring the Citrix policy setting Auto-create client printers with the Auto-create all client printers option.
- The system routes all print jobs queued to printers locally attached to user devices as client print jobs (that is, over the ICA channel and through the user device).
- The system routes all print jobs queued to network printers directly from Multi-session OS machines. If the system cannot route the jobs over the network, it will route them through the user device as a redirected client print job.

This behavior is equivalent to disabling the Citrix policy setting Direct connection to print servers.

- The system attempts to store printing properties, a combination of the user's printing preferences and printing device-specific settings, on the user device. If the client does not support this operation, the system stores printing properties in user profiles on the Multi-session OS machine.

  This behavior is equivalent to configuring the Citrix policy setting Printer properties retention with the Held in profile only if not saved on client option.

- In VDAs version 7.16 and later, the Citrix policy setting "Automatic installation of inbox printer drivers"does not have any effect on Windows 8 and later Windows operating systems versions because V3 in-box printer drivers are not included in the operating system.

- In VDAs earlier than 7.16, the system uses the Windows version of the printer driver if it is available on the Multi-session OS machine. If the printer driver is not available, the system attempts to install the driver from the Windows operating system. If the driver is not available in Windows, it uses a Citrix Universal print driver.

  This behavior is equivalent to enabling the Citrix policy setting "Automatic installation of in-box printer drivers"and configuring the Universal printing setting with the "Use universal printing only if requested driver is unavailable".

  Enabling "Automatic installation of in-box printer drivers"might result in the installation of a large number of native printer drivers.

> **Note:**
>
> If you are unsure about what the shipping defaults are for printing, display them by creating a new policy and setting all printing policy rules to Enabled. The option that appears is the default.

Always-On logging

An Always-On logging feature is available for the print server and printing subsystem on the VDA.

To collate the logs as a ZIP for emailing, or to automatically upload logs to Citrix Insight Services, use the **Start-TelemetryUpload** PowerShell cmdlet.

Printing policies and preferences

February 6, 2020

When users access printers from published applications, you can configure Citrix policies to specify:

- How printers are provisioned (or added to sessions)
- How print jobs are routed
- How printer drivers are managed

You can have different printing configurations for different user devices, users, or any other objects on which policies are filtered.

Most printing functions are configured through the Citrix Printing policy settings. Printing settings follow standard Citrix policy behavior.

The system can write printer settings to the printer object at the end of a session or to a client printing device, provided the user's network account has sufficient permissions. By default, Citrix Workspace app uses the settings stored in the printer object in the session, before looking in other locations for settings and preferences.

By default, the system stores, or retains, printer properties on the user device (if supported by the device) or in the user profile on the Multi-session OS machine. When a user changes printer properties during a session, those changes are updated in the user profile on the machine. The next time the user logs on or reconnects, the user device inherits those retained settings. That is, printer property changes on the user device do not impact the current session until after the user logs off and then logs on again.

Printing preference locations

In Windows printing environments, changes made to printing preferences can be stored on the local computer or in a document. In this environment, when users modify printing settings, the settings are stored in these locations:

- **On the user device itself** - Windows users can change device settings on the user device by right-clicking the printer in the Control Panel and selecting Printing Preferences. For example, if Landscape is selected as page orientation, landscape is saved as the default page orientation preference for that printer.
- **Inside of a document** - In word-processing and desktop-publishing programs, document settings, such as page orientation, are often stored inside documents. For example, when you queue a document to print, Microsoft Word typically stores the printing preferences you specified, such as page orientation and the printer name, inside the document. These settings appear by default the next time you print that document.
- **From changes a user made during a session** - The system keeps only changes to the printing settings of an auto-created printer if the change was made in the Control Panel in the session; that is, on the Multi-session OS machine.
- **On the Multi-session OS machine** - These are the default settings associated with a particular printer driver on the machine.

The settings preserved in any Windows-based environment vary according to where the user made the changes. This also means that the printing settings that appear in one place, such as in a spreadsheet program, can be different than those in others, such as documents. As result, printing settings applied to a specific printer can change throughout a session.

Hierarchy of user printing preferences

Because printing preferences can be stored in multiple places, the system processes them according to a specific priority. Also, it is important to note that device settings are treated distinctly from, and usually take precedence over, document settings.

By default, the system always applies any printing settings a user modified during a session (that is, the retained settings) before considering any other settings. When the user prints, the system merges and applies the default printer settings stored on the Multi-session OS machine with any retained or client printer settings.

Saving user printing preferences

Citrix recommends that you do not change where the printer properties are stored. The default setting, which saves the printer properties on the user device, is the easiest way to ensure consistent printing properties. If the system is unable to save properties on the user device, it automatically falls back to the user profile on the Multi-session OS machine.

Review the Printer properties retention policy setting if these scenarios apply:

- If you use legacy plug-ins that do not allow users to store printer properties on a user device.
- If you use mandatory profiles on your Windows network and want to retain the user's printer properties.

Provision printers

March 7, 2022

Citrix Universal Print Server

When determining the best print solution for your environment, consider the following:

- The Universal Print Server provides features not available for the Windows Print Provider: Image and font caching, advanced compression, optimization, and QoS support.

- The Universal print driver supports the public device-independent settings defined by Microsoft. If users need access to device settings that are specific to a print driver manufacturer, the Universal Print Server paired with a Windows-native driver might be the best solution. With that configuration, you retain the benefits of the Universal Print Server while providing users access to specialized printer functionality. A trade-off to consider is that Windows-native drivers require maintenance.
- The Citrix Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal print driver, a single driver on the Multi-session OS machine that allows local or network printing from any device, including thin clients and tablets.

To use the Universal Print Server with a Windows-native driver, enable the Universal Print Server. By default, if the Windows-native driver is available, it is used. Otherwise, the Universal print driver is used. To specify changes to that behavior, such as to use only the Windows-native driver or only the Universal print driver, update the Universal print driver usage policy setting.

Install the Universal Print Server

To use the Universal Print Server, install the UpsServer component on your print servers, as described in the installation documents, and configure it. For more information, see Install core components and Install using the command line.

For environments where you want to deploy the UPClient component separately, for example with **XenApp 6.5**:

1. Download the Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) standalone package for Windows Single-session OS or Windows Multi-session OS.
2. Extract the VDA using the command line instructions described in Install using the command line.
3. Install the pre-requisites from the \Image-Full\Support\VcRedist_2013_RTM
    - Vcredist_x64 / vcredist_x86
        - Run x86 for 32-bit only, and both for 64-bit deployments
4. Install the cdf prerequisite from the \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
    - Cdf_x64 / Cdf_x86
        - x86 for 32-bit, x64 for 64-bit
5. Find the UPClient component in \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
6. Install the UPClient component by extracting and then launching the component's MSI.
7. A restart is required after installing the UPClient component.

Opt out of CEIP for the Universal Print Server

You are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP) when you install the Universal Print Server. The first upload of data occurs after seven days from the date and time of installation.

To opt out of CEIP, edit the registry key **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** and set the **DWORD** value to **0**.

To opt back in, set the DWORD value to 1.

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.

For more information, see Citrix Insight Services.

Configure the Universal Print Server

Use the following Citrix policy settings to configure the Universal Print Server. For more information, refer to the on-screen policy settings help.

- **Universal Print Server enable**. Universal Print Server is disabled by default. When you enable Universal Print Server, you choose whether to use the Windows Print Provider if the Universal Print Server is unavailable. After you enable the Universal Print Server, a user can add and enumerate network printers through the Windows Print Provider and Citrix Provider interfaces.
- **Universal Print Server print data stream (CGP) port**. Specifies the TCP port number used by the Universal Print Server print data stream CGP (Common Gateway Protocol) listener. Defaults to **7229**.
- **Universal Print Server web service (HTTP/SOAP) port**. Specifies the TCP port number used by the Universal Print Server listener for incoming HTTP/SOAP requests. Defaults to **8080**.

To change the default port of HTTP 8080 for Universal Print Server communication to Citrix Virtual Apps and Desktops VDAs, the following registry must also be created and the port number value modified on the Universal Print Server computer(s):

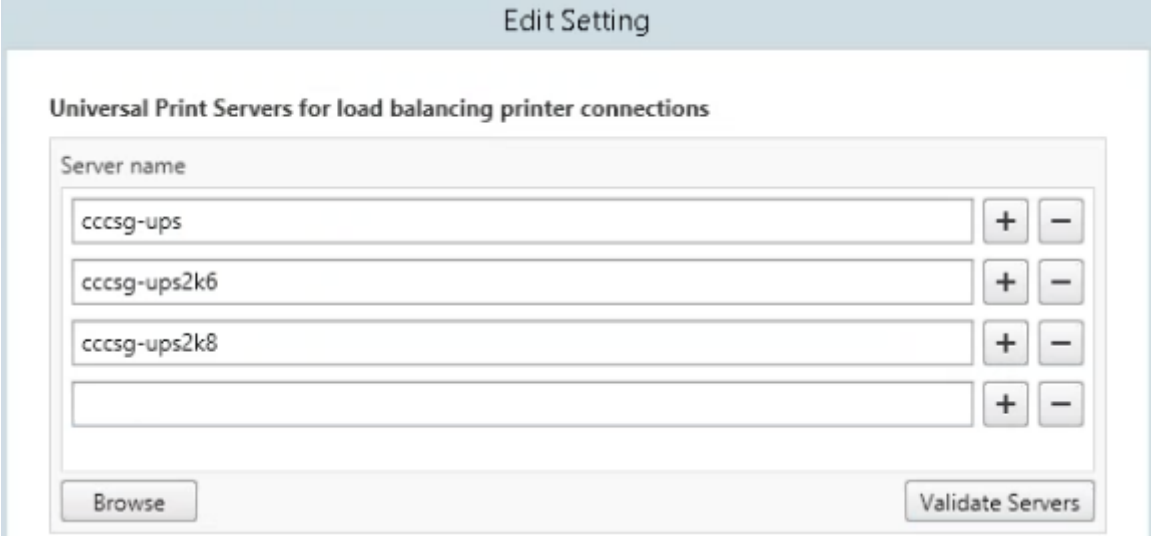
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
“UpsHttpPort”=DWORD:<portnumber>

This port number must match the HDX Policy, Universal Print Server web service (HTTP/SOAP) port, in Studio.

- **Universal Print Server print stream input bandwidth limit (kbps)**. Specifies the upper bound (in kilobits-per-second) for the transfer rate of print data delivered from each print job

to the Universal Print Server using CGP. Defaults to 0 (unlimited).

- **Universal Print Servers for load balancing**. This setting lists the Universal Print Servers to be used to load balance printer connections established at session launch, after evaluating other Citrix printing policy settings. To optimize printer creation time, Citrix recommends that all print servers have the same set of shared printers.



- **Universal Print Servers out-of-service threshold**. Specifies how long the load balancer should wait for an unavailable print server to recover before it determines that the server is permanently offline and redistributes its load to other available print servers. Default is 180 (seconds).

Once the printing policies are modified on the Delivery Controller, it can take a few minutes for the policy changes to be applied to the VDAs.

Interactions with other policy settings - The Universal Print Server honors other Citrix printing policy settings and interacts with them as noted in the following table. The information provided assumes that the Universal Print Server policy setting is enabled, the Universal Print Server components are installed, and the policy settings are applied.

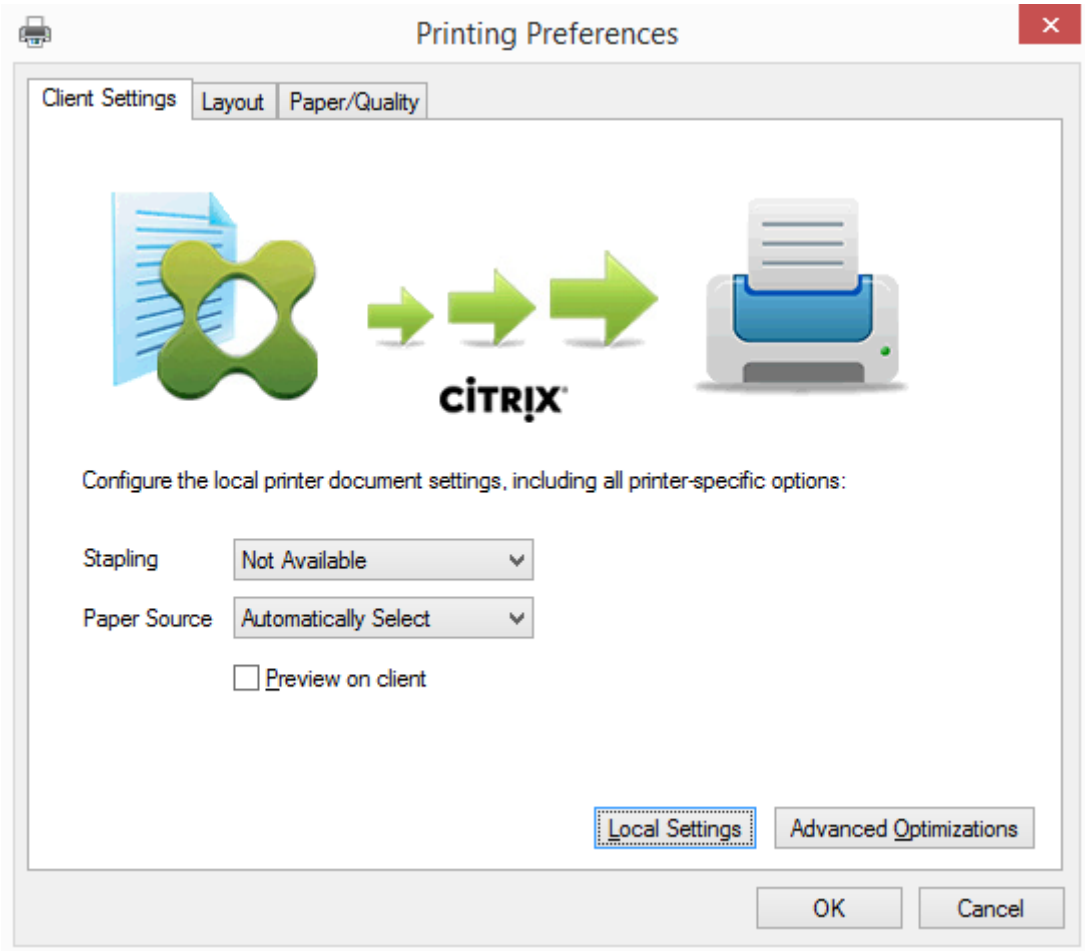
Policy setting	Interaction
Client printer redirection, Auto-create client printers	After the Universal Print Server is enabled, client network printers are created using the Universal print driver instead of the native drivers. Users see the same printer name as before.

Session printers	When you use the Citrix Universal Print Server solution, Universal print driver policy settings are honored.
Direct connections to print server	When the Universal Print Server is enabled and the Universal print driver usage policy setting is configured to use universal printing only, a direct network printer connection can be created to the print server, using the Universal print driver.
UPD preference	Supports EMF and XPS drivers.

Effects on user interfaces - The Citrix Universal print driver used by the Universal Print Server disables the following user interface controls:

- In the Printer Properties dialog box, the Local Printer Settings button
- In the Document Properties dialog box, the Local Printer Settings and Preview on client buttons

The Citrix Universal print driver (EMF and XPS drivers) supports advanced printing features such as stapling and paper source. The user can select Stapling or Paper Source options from the custom UPD print dialog if the client or network printers which are mapped to the UPD in the session support these features.



To set non-standard printer settings such as stapling and secure PIN, select **Local Settings** in the customer UPD print dialog for any client mapped printers that use either the Citrix UPD EMF or XPS drivers. The **Printing Preferences** dialog of the mapped printer is displayed outside the session on the client, allowing the user to change any printer option, and the modified printer settings are used in the active session when printing that document.

These features are available if the native driver makes them available using the Microsoft Print Capability technology. The native driver should use the standardized Print Schema Keywords in the Print Capabilities XML. If non-standard keywords are used, the advanced printing features will not be available using Citrix Universal print driver.

When using the Universal Print Server, the Add Printer Wizard for the Citrix Print Provider is the same as the Add Printer Wizard for the Windows Print Provider, with the following exceptions:

- When adding a printer by name or address, you can provide an HTTP/SOAP port number for the print server. That port number becomes a part of the printer name and appears in displays.
- If the Citrix Universal print driver usage policy setting specifies that universal printing must be used, the Universal print driver name appears when selecting a printer. The Windows Print Provider cannot use the Universal print driver.

The Citrix Print Provider does not support client-side rendering.

For more information about the Universal Print Server, see CTX200328.

Auto-created client printers

These universal printing solutions are provided for client printers:

- **Citrix Universal Printer** - A generic printer created at the beginning of sessions that is not tied to a printing device. The Citrix Universal Printer is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. The Universal Printer can print to any client-side printing device.

  The Citrix Universal Printer might not work for all user devices or Citrix Workspace apps in your environment. The Citrix Universal Printer requires a Windows environment and does not support the Citrix Offline Plug-in or applications that are streamed to the client. Consider using auto-created client printers and the Universal print driver for such environments.

  To use a universal printing solution for non-Windows Citrix Workspace apps, use one of the other Universal print drivers that are based on postscript/PCL and installed automatically.

- **Citrix Universal print drivers** - A device-independent printer driver. If you configure a Citrix Universal print driver, the system uses the EMF-based Universal print driver by default.

  The Citrix Universal print driver might create smaller print jobs than older or less advanced printer drivers. However, a device-specific driver might be needed to optimize print jobs for a specialized printer.

Configure universal printing - Use the following Citrix policy settings to configure universal printing. For more information, refer to the on-screen policy settings help.

- Universal print driver usage. Specifies when to use universal printing.
- Auto-create generic universal printer. Enables or disables auto-creation of the generic Citrix Universal Printer object for sessions when a user device compatible with Universal Printing is in use. By default, the generic Universal Printer object is not auto-created.
- Universal driver preference. Specifies the order in which the system attempts to use Universal print drivers, beginning with the first entry in the list. You can add, edit, or remove drivers and change the order of the drivers in the list.
- Universal printing preview preference. Specifies whether to use the print preview function for auto-created or generic universal printers.
- Universal printing EMF processing mode. Controls the method of processing the EMF spool file on the Windows user device. By default, EMF records are spooled directly to the printer. Spooling directly to the printer allows the spooler to process the records faster and uses fewer CPU resources.

For more policies, see Optimize printing performance. To change the defaults for settings such as paper size, print quality, color, duplex, and the number of copies, see CTX113148.

Auto-create printers from the user device - At the start of a session, the system auto-creates all printers on the user device by default. You can control what, if any, types of printers are provisioned to users and prevent autocreation.

Use the Citrix policy setting
Auto-create client printers to control autocreation. You can specify that:

- All printers visible to the user device, including network and locally attached printers, are created automatically at the start of each session (default)
- All local printers physically attached to the user device is created automatically
- Only the default printer for the user device is created automatically
- Autocreation is disabled for all client printers

The Auto-create client printers setting requires that the Client printer redirection setting is Allowed (the default).

Assign network printers to users

By default, network printers on the user device are created automatically at the beginning of sessions. The system enables you to reduce the number of network printers that are enumerated and mapped by specifying the network printers to be created within each session. Such printers are referred to as session printers.

You can filter session printer policies by IP address to provide proximity printing. Proximity printing enables users within a specified IP address range to automatically access the network printing devices that exist within that same range. Proximity printing is provided by the Citrix Universal Print Server and does not require the configuration described in this section.

Proximity printing might involve the following scenario:

- The internal company network operates with a DHCP server which automatically designates IP addresses to users.
- All departments within the company have unique designated IP address ranges.
- Network printers exist within each department's IP address range.

When proximity printing is configured and an employee travels from one department to another, no additional printing device configuration is required. Once the user device is recognized within the new department's IP address range, it will have access to all network printers within that range.

Configure specific printers to be redirected in sessions - To create administrator-assigned printers, configure the Citrix policy setting Session printers. Add a network printer to that policy using one of the following methods:

- Enter the printer UNC path using the format \\servername\printername.
- Browse to a printer location on the network.
- Browse for printers on a specific server. Enter the server name using the format \\servername and click Browse.

Important: The server merges all enabled session printer settings for all applied policies, starting from the highest to lowest priorities. When a printer is configured in multiple policy objects, custom default settings are taken from only the highest priority policy object in which that printer is configured.

Network printers created with the Session printers setting can vary according to where the session was initiated by filtering on objects such as subnets.

Specify a default network printer for a session - By default, the user's main printer is used as the default printer for the session. Use the Citrix policy setting Default printer to change how the default printer on the user device is established in a session.

1. On the Default printer settings page, select a setting for Choose client's default printer:
    - Network printer name. Printers added with the Session printers policy setting appear in this menu. Select the network printer to use as the default for this policy.
    - Do not adjust the user's default printer. Uses the current Terminal Services or Windows user profile setting for the default printer. For more information, refer to the on-screen policy settings help.
2. Apply the policy to the group of users (or other filtered objects) you want to affect.

Configure proximity printing - Proximity printing is also provided by the Citrix Universal Print Server, which does not require the configuration described here.

1. Create a separate policy for each subnet (or to correspond with printer location).
2. In each policy, add the printers in that subnet's geographic location to the Session printers setting.
3. Set the Default printer setting to Do not adjust the user's default printer.
4. Filter the policies by client IP address. Be sure to update these policies to reflect changes to the DHCP IP address ranges.

Maintain the printing environment

February 6, 2020

Maintaining the printing environment includes:

- Managing printer drivers

- Optimizing printing performance
- Displaying printer and managing print queues

Manage printer drivers

To minimize administrative overhead and the potential for print driver issues, Citrix recommends use of the Citrix Universal print driver.

If auto-creation fails, by default, the system installs a Windows-native printer driver provided with Windows. If a driver is not available, the system falls back to the Universal print driver. For more information about printer driver defaults, refer to Best practices, security considerations, and default operations.

If the Citrix Universal print driver is not an option for all scenarios, map printer drivers to minimize the amount of drivers installed on Multi-session OS machines. In addition, mapping printer drivers enables you to:

- Allow specified printers to use only the Citrix Universal print driver
- Allow or prevent printers to be created with a specified driver
- Substitute good printer drivers for outdated or corrupted drivers
- Substitute a driver that is available on Windows server for a client driver name

Prevent the automatic installation of printer drivers - The automatic installation of print drivers should be disabled to ensure consistency across Multi-session OS machines. This can be achieved through Citrix policies, Microsoft policies, or both. To prevent the automatic installation of Windows-native printer drivers, disable the Citrix policy setting Automatic installation of in-box printer drivers.

Map client printer drivers - Each client provides information about client-side printers during logon, including the printer driver name. During client printer autocreation, Windows server printer driver names are selected that correspond to the printer model names provided by the client. The autocreation process then uses the identified, available printer drivers to construct redirected client print queues.

Here is the general process for defining driver substitution rules and editing print settings for mapped client printer drivers:

1. To specify driver substitution rules for auto-created client printers, configure the Citrix policy setting Printer driver mapping and compatibility by adding the client printer driver name and selecting the server driver that you want to substitute for the client printer driver from the Find printer driver menu. You can use wildcards in this setting. For example, to force all HP printers to use a specific driver, specify HP* in the policy setting.
2. To ban a printer driver, select the driver name and choose the Do not create setting.

3. As needed, edit an existing mapping, remove a mapping, or change the order of driver entries in the list.
4. To edit the printing settings for mapped client printer drivers, select the printer driver, click Settings, and specify settings such as print quality, orientation, and color. If you specify a printing option that the printer driver does not support, that option has no effect. This setting overrides retained printer settings the user set during a previous session.
5. Citrix recommends testing the behavior of the printers in detail after mapping drivers, since some printer functionality can be available only with a specific driver.

When users log on the system checks the client printer driver compatibility list before it sets up the client printers.

Optimize printing performance

To optimize printing performance, use the Universal Print Server and Universal print driver. The following policies control printing optimization and compression:

- Universal printing optimization defaults. Specifies default settings for the Universal Printer when it is created for a session:
  - Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
  - Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.
  - Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached.
  - Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.
- Universal printing image compression limit. Defines the maximum quality and the minimum compression level available for images printed with the Universal print driver. By default, the image compression limit is set to Best Quality (lossless compression).
- Universal printing print quality limit. Specifies the maximum dots per inch (dpi) available for generating printed output in the session. By default, no limit is specified.

By default, all print jobs destined for network printers route from the Multi-session OS machine, across the network, and directly to the print server. Consider routing print jobs over the ICA connection if the

network has substantial latency or limited bandwidth. To do that, disable the Citrix policy setting Direct connections to print servers. Data sent over the ICA connection is compressed, so less bandwidth is consumed as the data travels across the WAN.

Improve session performance by limiting printing bandwidth - While printing files from Multi-session OS machines to user printers, other virtual channels (such as video) may experience decreased performance due to competition for bandwidth especially if users access servers through slower networks. To prevent such degradation, you can limit the bandwidth used by user printing. By limiting the data transmission rate for printing, you make more bandwidth available in the HDX data stream for transmission of video, keystrokes, and mouse data.

> **Important:**
>
> The printer bandwidth limit is always enforced, even when no other channels are in use.

Use the following Citrix policy bandwidth printer settings to configure printing bandwidth session limits. To set the limits for the site, perform this task using Studio. To set the limits for individual servers, perform this task using the Group Policy Management Console in Windows locally on each Multi-session OS machine.

- The Printer redirection bandwidth limit setting specifies the bandwidth available for printing in kilobits per second (kbps).
- The Printer redirection bandwidth limit percent setting limits the bandwidth available for printing to a percentage of the overall bandwidth available.

  Note: To specify bandwidth as a percentage using the Printer redirection bandwidth limit percent setting, enable the Overall session bandwidth limit as well.

  If you enter values for both settings, the most restrictive setting (the lower value) is applied.

To obtain real-time information about printing bandwidth, use Citrix Director.

Load balance Universal Print Servers

The Universal Print Server solution can scale by adding more print servers into the load balance solution. There is no single point of failure as each VDA has its own load balancer to distribute the printing load to all print servers.

Use the policy settings, Universal Print Servers for load balancing and Universal Print Servers out-of-service threshold, to distribute the printing load across all the print servers in the load balance solution.

If there is an unforeseen failure of a print server, the failover mechanism of the load balancer in each VDA automatically redistributes the printer connections allocated on the failed print servers to the

other available print servers such that all existing and incoming sessions function normally without affecting the user experience and without requiring the immediate administrator intervention.

Administrators can monitor the activity of the load balanced print servers using a set of performance counters to track the following on the VDA:

- List of load balanced print servers on the VDA and their state (available, unavailable)
- Number of printer connections accepted by each print server
- Number of printer connections failed on each print server
- Number of active printer connection on each print server
- Number of pending printer connections on each print server

Display and manage print queues

The following table summarizes where you can display printers and manage print queues in your environment.

		Printing Pathway
Client printers (Printers attached to the user device)	Client printing pathway	UAC Enabled On: Print Management snap-in located in the Microsoft Management Console; UAC Enabled Off: Pre-Windows 8: Control Panel, Windows 8: Print Management snap-in
Network printers (Printers on a network print server)	Network printing pathway	UAC Enabled On: Print Server > Print Management snap-in located in the Microsoft Management Console; UAC Enabled Off: Print Server > Control Panel
Network printers (Printers on a network print server)	Client printing pathway	UAC Enabled On: Print Server > Print Management snap-in located in the Microsoft Management Console; UAC Enabled Off: Pre-Windows 8: Control Panel, Windows 8: Print Management snap-in

		Printing Pathway
Local network server printers (Printers from a network print server that are added to a Multi-session OS machine)	Network printing pathway	UAC Enabled On: Print Server > Control Panel; UAC Enabled Off: Print Server > Control Panel

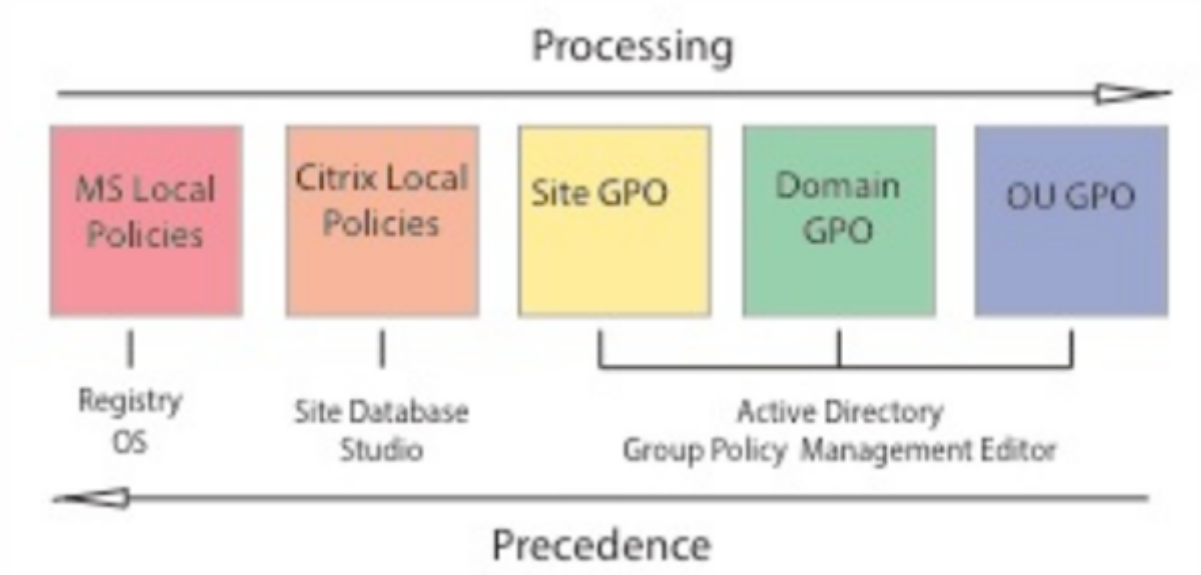
> **Note:**
>
> Print queues for network printers that use the network printing pathway are private and cannot be managed through the system.

Policies

February 7, 2020

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 physical and virtual machines or to users. You can apply settings to individual users at the local level or in security groups in Active Directory. The configurations define specific criteria and rules. If you don't specifically assign the policies, the settings are applied to all connections.



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, which override any conflicting policies on both the Microsoft and Citrix Local Policies levels.

All Citrix Local Policies are created and managed in the Citrix 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 Active Directory. Microsoft Local Policies are created in the Windows Operating System and are stored in the registry.

Studio uses a Modeling Wizard to help administrators compare configuration settings within templates and policies to help eliminate conflicting and redundant settings. Administrators can set GPOs using the GPMC to configure settings and apply them to a target set of users at different levels of the network.

These GPOs are saved in Active Directory, and access to the management of these settings is restricted for most of IT for security.

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.

Local 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. The end user logs on to a machine using domain credentials.
2. Credentials are sent to the domain controller.
3. Active Directory applies all policies (end user, endpoint, organizational unit, and domain).
4. The end user logs on to Citrix Workspace app and accesses an application or desktop.
5. Citrix and Microsoft policies are processed for the end user and machine hosting the resource.
6. Active Directory determines precedence for policy settings. It then applies them to the registries of the endpoint device and to the machine hosting the resource.
7. The end user logs off from the resource. Citrix policies for the end user and endpoint device are no longer active.
8. The end user logs off the user device, which releases the GPO user policies.
9. The end user turns off the device, which releases the GPO machine policies.

When creating policies for groups of users, devices, and machines, some members might have different requirements and would need exceptions to some policy settings. Exceptions are made by way of filters in Studio and the GPMC that determine who or what the policy affects.

> **Note:**
> We do not support mixing Windows and Citrix policies in the same GPO.

Work with policies

March 14, 2022

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

You can use the following tools to work with Citrix policies.

- **Studio** - If you are a Citrix administrator without permission to manage group policy, use Studio to create policies for your site. Policies created using Studio are stored in the site database and updates are pushed to the virtual desktop either when that virtual desktop registers with the broker or when a user connects to that virtual desktop.
- **Local Group Policy Editor** (Microsoft Management Console snap-in) - If your network environment uses Active Directory and you have permission to manage group policy, you can use the Local Group Policy Editor to create policies for your Site. The settings you configure affect the Group Policy Objects (GPOs) you specify in the Group Policy Management Console.

> **Important**
>
> You must use the Local Group Policy Editor to configure some policy settings, including those related to registering VDAs with a Controller and those related to Microsoft App-V servers.

Policy processing order and precedence

Group policy settings are processed in the following order:

1. Local GPO
2. XenApp or XenDesktop Site GPO (stored in the Site database)
3. Site-level GPOs
4. Domain-level GPOs
5. Organizational Units

However, if a conflict occurs, policy settings that are processed last can overwrite those that are processed earlier. This means that policy settings take precedence in the following order:

1. Organizational Units
2. Domain-level GPOs
3. Site-level GPOs
4. XenApp or XenDesktop Site GPO (stored in the Site database)
5. Local GPO

For example, a Citrix administrator uses Studio to create a policy (Policy A) that enables client file redirection for the company's sales employees. Meanwhile, another administrator uses the Group Policy Editor to create a policy (Policy B) that disables client file redirection for sales employees. When the sales employees log on to the virtual desktops, Policy B is applied and Policy A is ignored because Policy B was processed at the domain level and Policy A was processed at the XenApp or XenDesktop Site GPO level.

However, when a user launches an ICA or Remote Desktop Protocol (RDP) session, Citrix session settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical RDP client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging.

When using multiple policies, you can prioritize policies that contain conflicting settings; see Compare, prioritize, model, and troubleshoot policies for details.

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.

Navigate Citrix policies and settings

In the Local Group Policy Editor, policies and settings appear in two categories: Computer Configuration and User Configuration. Each category has a Citrix Policies node. See the Microsoft documentation for details about navigating and using this snap-in.

In Studio, policy settings are sorted into categories based on the functionality or feature they affect. For example, the Profile management section contains 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 when connecting using ICA. User policies are applied when a user connects or reconnects using ICA. User policies are not applied if a user connects using RDP or logs on directly to the console.

  To access policies, settings, or templates, select Policies in the Studio navigation pane.

  - The **Policies** tab lists all policies. When you select a policy, tabs to the right display: Overview (name, priority, enabled/disabled status, and description), Settings (list of configured settings), and Assigned to (user and machine objects to which the policy is currently assigned). For more information, see Create policies.
  - The **Templates** tab lists Citrix-provided and custom templates you created. When you select a template, tabs to the right display: Description (why you might want to use the template) and 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 in other policies or templates. For example, you might want to verify setting values to ensure compliance with best practices. For more information, see Compare, prioritize, model, and troubleshoot policies.
  - From the **Modelling** tab, you can simulate connection scenarios with Citrix policies. For more information, see Compare, prioritize, model, 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 in the Actions pane.
  3. On the Settings page, begin to type the name of the setting.

  You can refine your search by selecting a specific product version, selecting a category (for example, Bandwidth), or by selecting the View selected only check box or selecting to search only the settings that have been added to the selected policy. For an unfiltered search, select All Settings.

- To search for a setting within a policy :

  1. Select the policy.
  2. Select the Settings tab, begin to type the name of the setting.

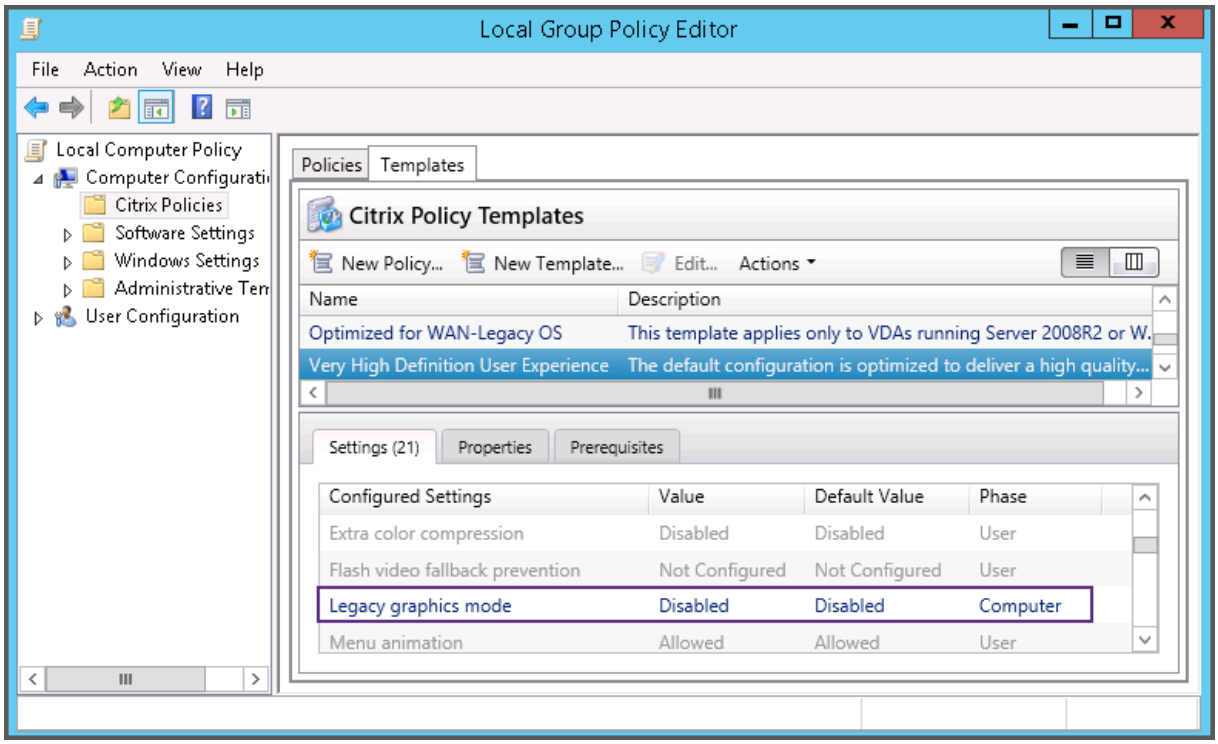
You can refine your search by selecting a specific product version or by selecting a category. For an unfiltered search, select All Settings.

A policy, once created, is completely independent of the template used. You can use the Description field on a new policy to keep track of the source template used.

In Studio, policies and templates are displayed in a single list regardless of whether they contain user, computer or both types of settings and can be applied using both user and computer filters.

In Group Policy Editor, Computer and User settings must be applied separately, even if created from a template that contains both types of settings. In this example choosing to use Very High Definition User Experience in Computer Configuration:

- Legacy Graphics mode is a Computer setting that will be used in a policy created from this template.
- The User settings, grayed out, will not be used in a policy created from this template.



Policy templates

April 5, 2024

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 by importing or exporting templates.

Policy templates can be imported and exported.

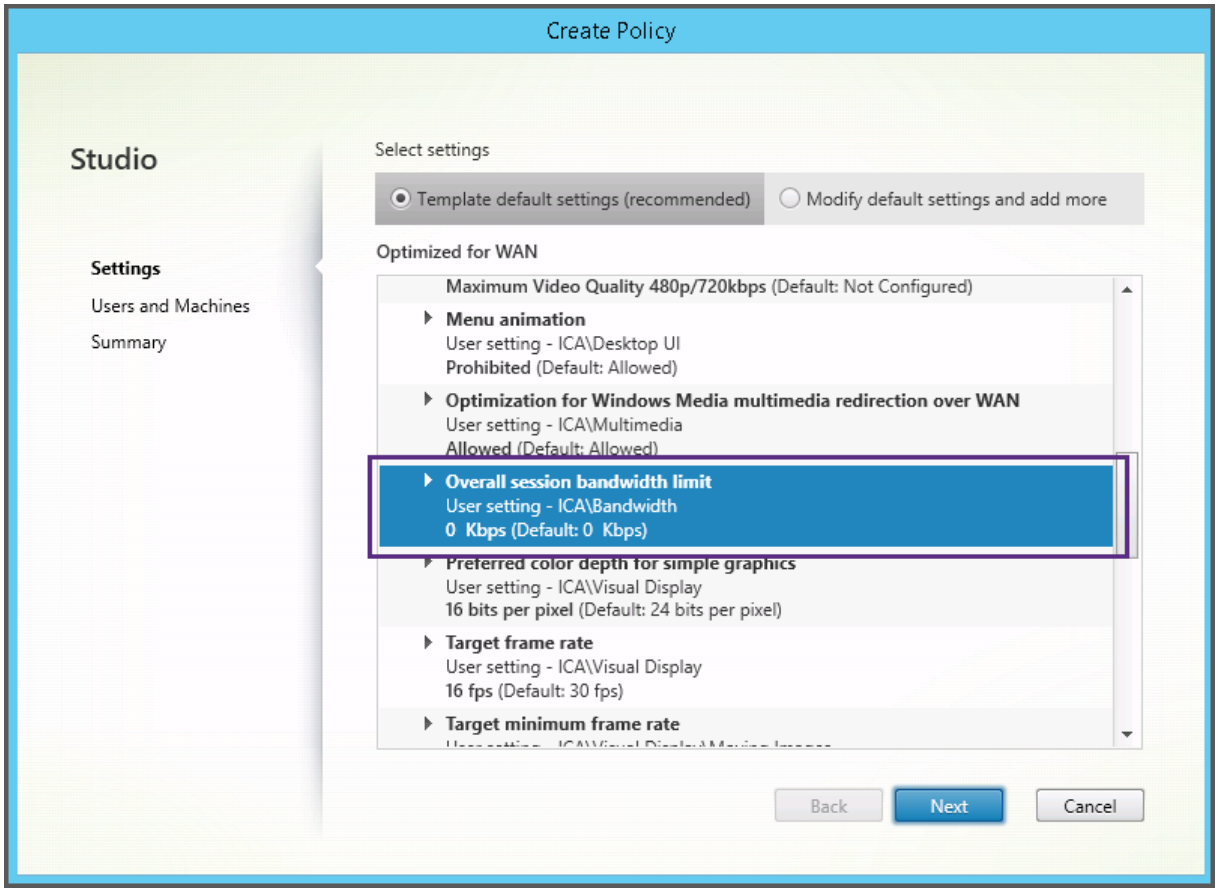
For considerations when using templates to create policies, see the Knowledge Center article CTX202330. To download the PDF, log in using your credentials.

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 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 is intended for task workers in branch offices using a shared WAN connection or remote locations with low bandwidth connections accessing 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 *Optimized for WAN* 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 Virtual Apps and Desktops. This template includes settings that disable access to printing, clipboard, peripheral devices, drive mapping, port redirection, and 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.



If you are working with a deployment (policy management and VDAs) earlier than XenApp and XenDesktop 7.6 FP3, and require High Server Scalability and Optimized for WAN templates, 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 Studio

To create a template based on a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select the template from which you will create the template.
3. Select **Create Template** in the Actions pane.
4. Select and configure the policy settings to include in the template. Remove any existing settings that don't belong. Enter a name for the template.

After you click **Finish**, the new template appears on the **Templates** tab.

To create a template based on a policy:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Policies** tab and then select the policy from which you will create the template.
3. Select **Save as Template** in the Actions pane.
4. Select and configure any new policy settings to include in the template. Remove any existing settings that don't belong. Enter a name and description for the template, and then click **Finish**.

To import a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select **Import Template**.
3. Select the template file to import and then click **Open**. If you import a template with the same name as an existing template, you can choose to overwrite the existing template or save the template with a different name that is generated automatically.

To export a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select **Export Template**.
3. Select the location where you want to save the template and then click **Save**.

A `.gpt` file is created in the specified location.

Create and manage templates using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the **Policies** node and then select **Citrix Policies**. Choose the appropriate action.

Task	Instruction
Create a template from an existing policy	On the **Policies** tab, select the policy and then select **Actions > Save as Template**.
Create a policy from an existing template	On the **Templates** tab, select the template and then click **New Policy**.
Create a template from an existing template	On the **Templates** tab, select the template and then click **New Template**.
Import a template	On the **Templates** tab, select **Actions > Import**.
Export a template	On the **Templates** tab, select **Actions > Export**.
View template settings	On the **Templates** tab, select the template and then click the **Settings** tab.
View a summary of template properties	On the **Templates** tab, select the template and then click the **Properties** tab.

Task	Instruction
View template prerequisites	On the **Templates** tab, select the template and then click the **Prerequisites** tab.

Templates and Delegated Administration

Policy templates are stored on the machine where the policy management package was installed. This machine is either the Delivery Controller machine or the Group Policy Objects management machine - not the Citrix Virtual Apps and Desktops Site's database. This means that the Windows administrative permissions control the policy template files rather than Site's Delegated Administration roles and scopes.

As a result, an administrator with read-only permission in the Site can, for example, create templates. However, because templates are local files, no changes are made to your environment.

Custom templates are only visible to the user account that creates them and stored in the user's Windows profile. To expose a custom template further, create a policy from it or export it to a shared location.

Create policies

April 22, 2020

Before creating a policy, decide which group of users or devices it should affect. You may want to create a policy based on user job function, connection type, user device, or geographic location. Alternatively, you can use the same criteria that you use for Windows Active Directory group policies.

If you already created a policy that applies to a group, consider editing that policy and configuring the appropriate settings, instead of creating another policy. Avoid creating a new policy solely to enable a specific setting or to exclude the policy from applying to certain users.

When you create a new policy, you can base it on settings in a policy template and customize settings as needed, or you can 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 checkbox is explicitly checked.

Policy settings

Policy settings can be enabled, disabled, or not configured. By default, policy settings are not configured, which means they are not added to a policy. Settings are applied only when they are added to a policy.

Some policy settings can be in one of the following states:

- Allowed or Prohibited allows or prevents the action controlled by the setting. In some cases, 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 or not users are allowed to access the drives on their devices. To allow users to access their network drives, both this setting and the Client network drives setting must be added to the policy. If the Client drive redirection setting is disabled, users cannot 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. If you are using Active Directory, policy settings are updated when Active Directory reevaluates policies at 90-minute intervals and applied either when the virtual desktop restarts or when a user logs on.

For some policy settings, you can enter or select a value when you add the setting to a policy. You can limit configuration of the setting by selecting Use default value. This disables configuration of the setting and allows only the setting's default value to be used when the policy is applied, 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.
- Do not enable conflicting or overlapping settings in Remote Desktop Session Host Configuration. In some cases, Remote Desktop Session Host Configuration provides similar functionality to Citrix policy settings. When possible, keep all settings consistent (enabled or disabled) for ease of troubleshooting.
- Disable unused policies. Policies with no settings added create unnecessary processing.

Policy assignments

When creating a policy, you assign it to certain user 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.

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.
Netscaler SD-WAN	Whether or not a user session is launched through Netscaler SD-WAN. Note: You can add only one Netscaler 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. **Note:** Private desktop and shared desktop filter options are available only for Citrix Virtual Apps and Desktops 7.x. For more information, see CTX219153.
Organizational Unit (OU)	Organizational unit.
Tag	Tags. **Note:** Apply this policy to all tagged machines. Note that application tags are not included.

Assignment name	Applies a policy based on
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 may not be applied as expected. For more information, see CTX127461

A policy named "Unfiltered"is provided by default.

- If you use Studio to manage Citrix policies, settings you add to the Unfiltered policy are applied to all servers, desktops, and connections in a Site.
- If you use the Local Group Policy Editor to manage Citrix policies, settings you add to the Unfiltered policy are applied to all Sites and connections that are within the scope of the Group Policy Objects (GPOs) that contain the policy. For example, the Sales OU contains 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 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 is not 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 in order 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 is not applied because the connection does not satisfy Assignment F.

Create a new policy based on a template, using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Templates tab and select a template.
3. Select Create Policy from Template in the Actions pane.
4. By default, the new policy uses all the default settings in the template (the Use template default settings radio button is selected). If you want to change settings, select the Modify defaults and add more settings radio button, and then add or remove settings.
5. Specify how to apply the policy by selecting one of the following:

   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
   - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.

6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.

The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create a new policy based on a template, using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Templates tab and select a template.
3. Select Create Policy from Template in the Actions pane.
4. By default, the new policy uses all the default settings in the template (the Use template default settings radio button is selected). If you want to change settings, select the Modify defaults and add more settings radio button, and then add or remove settings.
5. Specify how to apply the policy by selecting one of the following:
   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
   - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.

   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create a new policy using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Policies tab.
3. Select Create Policy in the Actions pane.
4. Add and configure policy settings.
5. Specify how to apply the policy by choosing one of the following:
   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.

- Assign to all objects in a site to apply the policy to all user and machine objects in the Site.

6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.

   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create and manage policies using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the Policies node and then select Citrix Policies. Choose the appropriate action below.

Task	Instruction
Create a new policy	On the Policies tab, click New.
Edit an existing policy	On the Policies tab, select the policy and then click Edit.
Change the priority of an existing policy	On the Policies tab, select the policy and then click either Higher or Lower.
View summary information about a policy	On the Policies tab, select the policy and then click the Summary tab.
View and amend policy settings	On the Policies tab, select the policy and then click the Settings tab.
View and amend policy filters	On the Policies tab, select the policy and then click the Filters tab. When you add more than one filter to a policy, all the filter conditions must be met for the policy to be applied.
Enable or disable a policy	On the Policies tab, select the policy and then select either Actions > Enable or Actions > Disable.
Create a new policy from an existing template	On the Templates tab, select the template and then click New Policy.

Compare, prioritize, model, and troubleshoot policies

February 6, 2020

You can use multiple policies to customize your environment to meet users' needs based on their job functions, geographic locations, or connection types. For example, for security you may need to place restrictions on user groups who regularly work with sensitive data. You can create a policy that prevents users from saving sensitive files on their local client drives. However, if some people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence.

When using multiple policies, you must determine how to prioritize them, how to create exceptions, and how to view the effective policy when policies conflict.

In general, policies override similar settings configured for the entire Site, for specific Delivery Controllers, or on the user device. The exception to this principle is security. The highest encryption setting in your environment, including the operating system and the most restrictive shadowing setting, always overrides other settings and policies.

Citrix policies interact with policies you set in your operating system. In a Citrix environment, Citrix settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical Remote Desktop Protocol (RDP) client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging. For some policy settings, such as Secure ICA, the settings in policies must match the settings in the operating system. If a higher priority encryption level is set elsewhere, the Secure ICA policy settings that you specify in the policy or when you are delivering application and desktops can be overridden.

For example, the encryption settings that you specify when creating Delivery Groups should be at the same level as the encryption settings you specified throughout your environment.

Note: In the second hop of double-hop scenarios, when a Single-session OS VDA connects to Multi-session OS VDA, Citrix policies act on the Single-session OS VDA as if it were the user device. For example, if policies are set to cache images on the user device, the images cached for the second hop in a double-hop scenario are cached on the Single-session OS VDA machine.

Compare policies and templates

You can compare settings in a policy or template with those in other policies or templates. For example, you might need to verify setting values to ensure compliance with best practices. You might also want to compare settings in a policy or template with the default settings provided by Citrix.

1. Select Policies in the 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.

Prioritize policies

Prioritizing policies allows you to define the precedence of policies when they contain conflicting settings. 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.

You prioritize policies by giving them different priority numbers in Studio. By default, new policies are given the lowest priority. If policy settings conflict, a policy with a higher priority (a priority number of 1 is the highest) overrides a policy with a lower priority. Settings are merged according to priority and the setting's condition; for example, whether the setting is disabled or enabled. Any disabled setting overrides a lower-ranked setting that is enabled. Policy settings that are not configured are ignored and do not override the settings of lower-ranked settings.

1. Select Policies in the Studio navigation pane. Make sure the Policies tab is selected.
2. Select a policy.
3. Select Lower Priority or Higher Priority in the Actions pane.

Exceptions

When you create policies for groups of users, user devices, or machines, you may find that some members of the group require exceptions to some policy settings. You can create exceptions by:

- Creating a policy only for those group members who need the exceptions and then ranking the 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 do not match the assignment criteria. For example, a policy contains 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 is applied to all users who log on to the Site with IP addresses in the range specified in Assignment A. However, the policy is not applied to the user logging on to the Site with the user account specified in Assignment B, even though the user's computer is assigned an IP address in the range specified in Assignment A.

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 determine how final policy settings are merged for a connection by calculating the Resultant Set of Policy.

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 domain controller, users, Citrix policy assignment evidence values, and simulated environment settings such as slow network connection. The report that the wizard produces lists the Citrix policies that would likely take effect in the scenario. If you are logged on to the Controller as a domain user, the wizard calculates the Resultant Set of Policy using both site policy settings and Active Directory Group Policy Objects (GPOs).
- Use Group Policy Results to produce a report describing the Citrix policies in effect for a given user and controller. The Group Policy Results tool helps you evaluate the current state of GPOs in your environment and generates a report that describes how these objects, including Citrix policies, are currently being applied to a particular user and controller.

You can launch the Citrix Group Policy Modeling Wizard from the Actions pane in Studio. You can launch either tool from the Group Policy Management Console in Windows.

If you run the Citrix Group Policy Modeling Wizard or Group Policy Results tool from the Group Policy Management Console, site policy settings created using Studio are not included in the Resultant Set of Policy.

To ensure you obtain the most comprehensive Resultant Set of Policy, Citrix recommends launching the Citrix Group Policy Modeling wizard from Studio, unless you create policies using only the Group Policy Management Console.

Use the Citrix Group Policy Modeling Wizard

Open the Citrix Group Policy Modeling Wizard using one of the following:

- Select Policies in the Studio navigation pane, select the Modeling tab, and then select Launch Modeling Wizard in the Actions pane.

- Launch the Group Policy Management Console (gpmc.msc), right-click Citrix Group Policy Modeling in the tree pane, and then select Citrix Group Policy Modeling Wizard.

Follow the wizard instructions to select the domain controller, users, computers, environment settings, and Citrix assignment criteria to use in the simulation. After you click Finish, the wizard produces a report of the modeling results. In Studio, the report appears in the middle pane under the Modeling tab.

To view the report, select View Modeling Report.

Troubleshoot policies

Users, IP addresses, and other assigned objects can have multiple policies that apply simultaneously. This can result in conflicts where a policy may not behave as expected. When you run the Citrix Group Policy Modeling Wizard or the Group Policy Results tool, you might discover that no policies are applied to user connections. When this happens, users connecting to their applications and desktops under conditions that match the policy evaluation criteria are not affected by any policy settings. This occurs when:

- No policies have assignments that match the policy evaluation criteria.
- Policies that match the assignment do not 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.

Default policy settings

August 4, 2021

The following tables list policy settings, their default, and the Virtual Delivery Agent (VDA) versions to which they apply.

ICA

Name	Default setting	VDA
Adaptive transport	Off; Use when preferred	VDA 7.13–7.15; VDA 7.16 through current
Client clipboard redirection	Allowed	All VDA versions
Desktop launches	Prohibited	VDA for Multi-session OS 7 through current
ICA listener port number	1494	All VDA version
Launching of non-published programs during client connection	Prohibited	VDA for Multi-session OS 7 through current
Client clipboard write allowed formats	No formats are specified	VDA 7.6 through current
Rendezvous protocol	Disabled	Applies only to HDX sessions established through Citrix Cloud.
Restrict client clipboard write	Prohibited	VDA 7.6 through current
Restrict session clipboard write	Prohibited	VDA 7.6 through current
Session clipboard write allowed formats	No formats are specified	VDA 7.6 through current
Tablet mode toggle	Enabled	VDA 7.16 through current; for VDA 7.14 and 7.15 LTSR, configure this setting using the registry.
Virtual channel allow list	Disabled	VDA 1912

ICA/Adobe Flash delivery/Flash redirection

Name	Default setting	VDA
Flash video fallback prevention	Not configured	VDA 7.6 FP3 through current
Flash video fallback prevention error *.swf		VDA 7.6 FP3 through current

ICA/Audio

Name	Default setting	VDA
Audio Plug N Play	Allowed	VDA for Multi-session OS 7 through current
Audio quality	High - high definition audio	All VDA versions
Client audio redirection	Allowed	All VDA versions
Client microphone redirection	Allowed	All VDA versions

ICA/Auto client reconnect

Name	Default setting	VDA
Audio over UDP real-time transport	Allowed	All VDA versions
Auto client reconnect	Allowed	All VDA versions
Auto client reconnect authentication	Do not require authentication	All VDA versions
Auto client reconnect logging	Do not log auto-reconnect events	All VDA versions
Auto client reconnect timeout	120 seconds	VDA 7.13 through current
Reconnect UI transparency level	80%	VDA 7.13 through current

ICA/Bandwidth

Name	Default setting	VDA
Audio redirection bandwidth limit	0 Kbps	All VDA versions
Audio redirection bandwidth limit percent	0	All VDA versions
Client USB device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

Name	Default setting	VDA
Client USB device redirection bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Clipboard redirection bandwidth limit	0 Kbps	All VDA versions
Clipboard redirection bandwidth limit percent	0	All VDA versions
COM port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
COM port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
File redirection bandwidth limit	0 Kbps	All VDA versions
File redirection bandwidth limit percent	0	All VDA versions
HDX MediaStream Multimedia Acceleration bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 and VDA for Single-session OS 7 through current VDA for Multi-session OS and VDA for Single-session OS
HDX MediaStream Multimedia Acceleration bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
LPT port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
LPT port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Overall session bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit	0 Kbps	All VDA versions

Name	Default setting	VDA
Printer redirection bandwidth limit percent	0	All VDA versions
TWAIN device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
TWAIN device redirection bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Bidirectional content redirection

Name	Default setting	VDA
Allow bidirectional content redirection	Prohibited	VDA 7.13 through current
Allowed URLs to be redirected to client	empty	VDA 7.13 through current
Allowed URLs to be redirected to VDA	empty	VDA 7.13 through current
Client to host (VDA) and client to client bidirectional content redirection		Use the Citrix Workspace App Group Policy Object administrative template

ICA/Browser content redirection

Name	Default setting	VDA
Browser content redirection	Allowed	VDA 7.16 through current
Browser content redirection ACL configuration	`https://www.youtube.com/*`	VDA 7.16 through current
Browser content redirection proxy configuration	empty	VDA 7.16 through current

ICA/Client sensors

Name	Default setting	VDA
Allow applications to use the physical location of the client device	Prohibited	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Desktop UI

Name	Default setting	VDA
Desktop Composition Redirection	Disabled (7.6 FP3 through current);Enabled (5.6 through 7.6 FP2)	VDA 5.6, VDA for Single-session OS 7 through 7.15
Desktop Composition Redirection graphics quality	Medium	VDA 5.6, VDA for Single-session OS 7 through 7.15
Desktop wallpaper	Allowed	All VDA versions
Menu animation	Allowed	All VDA versions
View window contents while dragging	Allowed	All VDA versions

ICA/End user monitoring

Name	Default setting	VDA
ICA round trip calculation	Enabled	All VDA versions
ICA round trip calculation interval	15 seconds	All VDA versions
ICA round trip calculations for idle connections	Disabled	All VDA versions

ICA/Enhanced desktop experience

Name	Default setting	VDA
Enhanced Desktop Experience	Allowed	VDA for Multi-session OS 7 through current

ICA/File redirection

Name	Default setting	VDA
Auto connect client drives	Allowed	All VDA versions
Client drive redirection	Allowed	All VDA versions
Client fixed drives	Allowed	All VDA versions
Client floppy drives	Allowed	All VDA versions
Client network drives	Allowed	All VDA versions
Client optical drives	Allowed	All VDA versions
Client removable drives	Allowed	All VDA versions
Host to client redirection	Disabled	VDA for Multi-session OS 7 through current
Preserve client drive letters	Disabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Read-only client drive access	Disabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Special folder redirection	Allowed	Web Interface deployments only; VDA for Multi-session OS 7 through current
Use asynchronous writes	Disabled	All VDA versions

ICA/Graphics

Name	Default setting	VDA
Allow visually lossless compression	Disabled	VDA 7.6 through current
Display memory limit	65536 Kb	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Display mode degrade preference	Degrade color depth first	All VDA versions
Dynamic windows preview	Enabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Image caching	Enabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Legacy graphics mode	Disabled	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Maximum allowed color depth	32 bits per pixel	All VDA versions
Notify user when display mode is degraded	Disabled	VDA for Multi-session OS 7 through current
Optimize for 3D graphics workload	Disabled	VDA 7.17 through current
Queuing and tossing	Enabled	All VDA versions
Use video codec for compression	Use video codec when preferred	VDA 7.6 FP3 through current
Use hardware encoding for video codec	Enabled	VDA 7.11 through current

ICA/Graphics/Caching

Name	Default setting	VDA
Persistent cache threshold	3000000 Kbps	VDA for Multi-session OS 7 through current

ICA/Graphics/Framehawk

Name	Default setting	VDA
Framehawk display channel	Disabled	VDA 7.6 FP2 through current
Framehawk display channel port range	3224,3324	VDA 7.6 FP2 through current

ICA/Keep alive

Name	Default setting	VDA
ICA keep alive timeout	60 seconds	All VDA versions
ICA keep alives	Do not send ICA keep alive messages	All VDA versions

ICA/Local App Access

Name	Default setting	VDA
Allow Local App Access	Prohibited	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
URL redirection black list	No sites are specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
URL redirection white list	No sites are specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Mobile experience

Name	Default setting	VDA
Automatic keyboard display	Prohibited	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Launch touch-optimized desktop	Allowed	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current. This setting is disabled and not available for Windows 10 and Windows Server 2016 machines.
Remote the combo box	Prohibited	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Multimedia

Name	Default setting	VDA
HTML5 video redirection	Prohibited	VDA 7.12 through current
Limit video quality	Not configured	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Microsoft Teams redirection	Allowed	VDA for Multi-session OS 1906 through current, VDA for Single-session OS 1906 through current.
Multimedia conferencing	Allowed	All VDA versions
Optimization for Windows Media multimedia redirection over WAN	Allowed	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

Name	Default setting	VDA
Use GPU for optimizing Windows Media multimedia redirection over WAN	Prohibited	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Windows Media fallback prevention	Not configured	VDA 7.6 FP3 through current
Windows Media client-side content fetching	Allowed	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Windows Media redirection	Allowed	All VDA versions
Windows Media redirection buffer size	5 seconds	VDA 5, 5.5, 5.6 FP1 through current
Windows Media redirection buffer size use	Disabled	VDA 5, 5.5, 5.6 FP1 through current

ICA/Multi-Stream Connections

Name	Default setting	VDA
Audio over UDP	Allowed	VDA for Multi-session OS 7 through current
Audio UDP port range	16500, 16509	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Port policy	Primary port (2598) has High Priority	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Stream computer setting	Disabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

Name	Default setting	VDA
Multi-Stream user setting	Disabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Stream virtual channel stream assignment setting	See Multi-Stream virtual channel assignment settings for default stream assignments	VDA 1912

ICA/Port Redirection

Name	Default setting	VDA
Auto connect client COM ports	Disabled	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Auto connect client LPT ports	Disabled	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Client COM port redirection	Prohibited	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Client LPT port redirection	Prohibited	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry

ICA/Printing

Name	Default setting	VDA
Client printer redirection	Allowed	All VDA versions
Default printer	Set default printer to the client's main printer	All VDA versions
Printer assignments	User's current printer is used as the default printer for the session	All VDA versions

Name	Default setting	VDA
Printer auto-creation event log preference	Log errors and warnings	All VDA versions
Session printers	No printers are specified	All VDA versions
Wait for printers to be created (desktop)	Disabled	All VDA versions

ICA/Printing/Client Printers

Name	Default setting	VDA
Auto-create client printers	Auto-create all client printers	All VDA versions
Auto-create generic universal printer	Disabled	All VDA versions
Client printer names	Standard printer names	VDA 5.6
Direct connections to print servers	Enabled	All VDA versions
Printer driver mapping and compatibility	No rules are specified	All VDA versions
Printer properties retention	Held in profile only if not saved on client	All VDA versions
Retained and restored client printers	Allowed	VDA 5, 5,5, 5.6 FP1

ICA/Printing/Drivers

Name	Default setting	VDA
Automatic installation of in-box printer drivers	Enabled	All VDA versions
Universal driver preference	EMF; XPS; PCL5c; PCL4; PS	All VDA versions
Universal print driver usage	Use universal printing only if requested driver is unavailable	All VDA versions

ICA/Printing/Universal Print Server

Name	Default setting	VDA
Universal Print Server enable	Disabled	All VDA versions
Universal Print Server print data stream (CGP) port	7229	All VDA version
Universal Print Server print stream input bandwidth limit (kpbs)	0	All VDA versions
Universal Print Server web service (HTTP/SOAP) port	8080	All VDA versions
Universal Print Servers for load balancing		VDA versions 7.9 through current
Universal Print Server out-of-service threshold	180 (seconds)	VDA versions 7.9 through current

ICA/Printing/Universal Printing

Name	Default setting	VDA
Universal printing EMF processing mode	Spool directly to printer	All VDA versions
Universal printing image compression limit	Best quality (lossless compression)	All VDA versions
Universal printing optimization defaults	Image Compression: Desired image quality = Standard quality, Enable heavyweight compression = False; Image and Font Caching: Allow caching of embedded images = True; Allow non-administrators to modify these settings = False;	All VDA versions
Universal printing preview preference	Do not use print preview for auto-created or generic universal printers	All VDA versions

Name	Default setting	VDA
Universal printing print quality limit	No limit	All VDA versions

ICA/Security

Name	Default setting	VDA
SecureICA minimum encryption level	Basic	VDA for Multi-session OS 7 through current

ICA/Server Limits

Name	Default setting	VDA
Server idle timer interval	0 milliseconds	VDA for Multi-session OS 7 through current

ICA/Session Limits

Name	Default setting	VDA
Disconnected session timer	Disabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Disconnected session timer interval	1440 minutes	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session connection timer	Disabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session connection timer interval	1440 minutes	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current

Name	Default setting	VDA
Session idle timer	Enabledf	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session idle timer interval	1440 minutes	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current

ICA/Session Reliability

Name	Default setting	VDA
Session reliability connections	Allowed	All VDA versions
Session reliability port number	2598	All VDA versions
Session reliability timeout	180 seconds	All VDA versions

ICA/Time Zone Control

Name	Default setting	VDA
Estimate local time for legacy clients	Enabled	VDA for Multi-session OS 7 through current
Restore Single-session OS time zone on session disconnect or logoff	Enabled	Current VDA version
Use local time of client	Use server time zone	All VDA versions

ICA/TWAIN Devices

Name	Default setting	VDA
Client TWAIN device redirection	Allowed	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
TWAIN compression level	Medium	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/USB Devices

Name	Default setting	VDA
Client USB device optimization rules	Enabled (VDA 7.6 FP3 through current); Disabled (VDA 7.11 through current); By default, no rules are specified	VDA 7.6 FP3 through current
Client USB device redirection	Prohibited	All VDA versions
Client USB device redirection rules	No rules are specified	All VDA versions
Client USB Plug and Play device redirection	Allowed	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Visual Display

Name	Default setting	VDA
Preferred color depth for simple graphics	24 bits per pixel	VDA 7.6 FP3 through current
Target frame rate	30 fps	All VDA versions

Name	Default setting	VDA
Visual quality	Medium	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Visual Display/Moving Images

Name	Default setting	VDA
Minimum image quality	Normal	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Moving image compression	Enabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Progressive compression level	None	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Progressive compression threshold value	2147483647 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Target minimum frame rate	10 fps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Visual Display/Still Images

Name	Default setting	VDA
Extra color compression	Disabled	All VDA versions

Name	Default setting	VDA
Extra color compression threshold	8192 Kbps	All VDA versions
Heavyweight compression	Disabled	All VDA versions
Lossy compression level	Medium	All VDA versions
Lossy compression threshold value	2147483647 Kbps	All VDA versions

ICA/WebSockets

Name	Default setting	VDA
WebSockets connections	Prohibited	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
WebSockets port number	8008	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
WebSockets trusted origin server list	The wildcard, *, is used to trust all Receiver for Web URLs	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

Load Management

Name	Default setting	VDA
Concurrent logon tolerance	2	VDA for Multi-session OS 7 through current
CPU usage	Disabled	VDA for Multi-session OS 7 through current
CPU usage excluded process priority	Below Normal or Low	VDA for Multi-session OS 7 through current

Name	Default setting	VDA
Disk usage	Disabled	VDA for Multi-session OS 7 through current
Maximum number of sessions	250	VDA for Multi-session OS 7 through current
Memory usage	Disabled	VDA for Multi-session OS 7 through current
Memory usage base load	Zero load: 768MB	VDA for Multi-session OS 7 through current

Profile Management/Advanced settings

Name	Default setting	VDA
Disable automatic configuration	Disabled	All VDA versions
Log off user if a problem is encountered	Disabled	All VDA versions
Number of retries when accessing locked files	5	All VDA versions
Process Internet cookie files on logoff	Disabled	All VDA versions

Profile Management/Basic settings

Name	Default setting	VDA
Active write back	Disabled	All VDA versions
Enable Profile Management	Disabled	All VDA versions
Excluded groups	Disabled. Members of all user groups are processed.	All VDA versions
Offline profile support	Disabled	All VDA versions
Path to user store	Windows	All VDA versions
Process logons of local administrators	Disabled	All VDA versions

Name	Default setting	VDA
Processed groups	Disabled. Members of all user groups are processed.	All VDA versions

Profile Management/Cross-Platform Settings

Name	Default setting	VDA
Cross-platform settings user groups	Disabled. All user groups specified in Processed groups are processed	All VDA versions
Enable cross-platform settings	Disabled	All VDA versions
Path to cross-platform definitions	Disabled. No path is specified.	All VDA versions
Path to cross-platform settings store	Disabled. Windows\PM_CM is used.	All VDA versions
Source for creating cross-platform settings	Disabled	All VDA versions

Profile Management/File System/Exclusions

Name	Default setting	VDA
Exclusion list - directories	Disabled. All folders in the user profile are synchronized.	All VDA versions
Exclusion list - files	Disabled. All files in the user profile are synchronized.	All VDA versions

Profile Management/File System/Synchronization

Name	Default setting	VDA
Directories to synchronize	Disabled. Only non-excluded folders are synchronized.	All VDA versions

Name	Default setting	VDA
Files to synchronize	Disabled. Only non-excluded files are synchronized.	All VDA versions
Folders to mirror	Disabled. No folders are mirrored.	All VDA versions

Profile Management/Folder Redirection

Name	Default setting	VDA
Grant administrator access	Disabled	All VDA versions
Include domain name	Disabled	All VDA versions

Profile Management/Folder Redirection/AppData(Roaming)

Name	Default setting	VDA
AppData(Roaming) path	Disabled. No location is specified.	All VDA versions
Redirection settings for AppData(Roaming)	Contents are redirected to the UNC path specified in the AppData(Roaming) path policy settings	All VDA versions

Profile Management/Folder Redirection/Contacts

Name	Default setting	VDA
Contacts path	Disabled. No location is specified.	All VDA versions
Redirection settings for Contacts	Contents are redirected to the UNC path specified in the Contacts path policy settings	All VDA versions

Profile Management/Folder Redirection/Desktop

Name	Default setting	VDA
Desktop path	Disabled. No location is specified.	All VDA versions
Redirection settings for Desktop	Contents are redirected to the UNC path specified in the Desktop path policy settings	All VDA versions

Profile Management/Folder Redirection/Documents

Name	Default setting	VDA
Documents path	Disabled. No location is specified.	All VDA versions
Redirection settings for Documents	Contents are redirected to the UNC path specified in the Documents path policy settings	All VDA versions

Profile Management/Folder Redirection/Downloads

Name	Default setting	VDA
Downloads path	Disabled. No location is specified.	All VDA versions
Redirection settings for Downloads	Contents are redirected to the UNC path specified in the Downloads path policy settings	All VDA versions

Profile Management/Folder Redirection/Favorites

Name	Default setting	VDA
Favorites path	Disabled. No location is specified.	All VDA versions

Name	Default setting	VDA
Redirection settings for Favorites	Contents are redirected to the UNC path specified in the Favorites path policy settings	All VDA versions

Profile Management/Folder Redirection/Links

Name	Default setting	VDA
Links path	Disabled. No location is specified.	All VDA versions
Redirection settings for Links	Contents are redirected to the UNC path specified in the Links path policy settings	All VDA versions

Profile Management/Folder Redirection/Music

Name	Default setting	VDA
Music path	Disabled. No location is specified.	All VDA versions
Redirection settings for Music	Contents are redirected to the UNC path specified in the Music path policy settings	All VDA versions

Profile Management/Folder Redirection/Pictures

Name	Default setting	VDA
Pictures path	Disabled. No location is specified.	All VDA versions
Redirection settings for Pictures	Contents are redirected to the UNC path specified in the Pictures path policy settings	All VDA versions

Profile Management/Folder Redirection/Saved Games

Name	Default setting	VDA
Saved Games path	Disabled. No location is specified.	All VDA versions
Redirection settings for Saved Games	Contents are redirected to the UNC path specified in the Saved Games path policy settings	All VDA versions

Profile Management/Folder Redirection/Searches

Name	Default setting	VDA
Searches path	Disabled. No location is specified.	All VDA versions
Redirection settings for Searches	Contents are redirected to the UNC path specified in the Searches path policy settings	All VDA versions

Profile Management/Folder Redirection/Start Menu

Name	Default setting	VDA
Start Menu path	Disabled. No location is specified.	All VDA versions
Redirection settings for Start Menu	Contents are redirected to the UNC path specified in the Start Menu path policy settings	All VDA versions

Profile Management/Folder Redirection/Video

Name	Default setting	VDA
Video path	Disabled. No location is specified.	All VDA versions
Redirection settings for Video	Contents are redirected to the UNC path specified in the Video path policy settings	All VDA versions

Profile Management/Log settings

Name	Default setting	VDA
Active Directory actions	Disabled	All VDA versions
Common information	Disabled	All VDA versions
Common warnings	Disabled	All VDA versions
Enable logging	Disabled	All VDA versions
File system actions	Disabled	All VDA versions
File system notifications	Disabled	All VDA versions
Logoff	Disabled	All VDA versions
Logon	Disabled	All VDA versions
Maximum size of the log file	1048576	All VDA versions
Path to log file	Disabled. Log files are saved in the default location; %SystemRoot%\System32\Logfiles\UserProfileManager.	All VDA versions
Personalized user information	Disabled	All VDA versions
Policy values at logon and logoff	Disabled	All VDA versions
Registry actions	Disabled	All VDA versions
Registry differences at logoff	Disabled	All VDA versions

Profile Management/Profile handling

Name	Default setting	VDA
Delay before deleting cached profiles	0	All VDA versions
Delete locally cached profiles on logoff	Disabled	All VDA versions
Local profile conflict handling	Use local profile	All VDA versions
Migration of existing profiles	Local and roaming	All VDA versions
Path to the template profile	Disabled. New user profiles are created from the default user profile on the device where a user first logs on.	All VDA versions
Template profile overrides local profile	Disabled	All VDA versions
Template profile overrides roaming profile	Disabled	All VDA versions
Template profile used as a Citrix mandatory profile for all logons	Disabled	All VDA versions

Profile Management/Registry

Name	Default setting	VDA
Exclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions
Inclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions

Profile Management/Streamed user profiles

Name	Default setting	VDA
Always cache	Disabled	All VDA versions
Always cache size	0 Mb	All VDA versions

Name	Default setting	VDA
Profile streaming	Disabled	All VDA versions
Streamed user profile groups	Disabled. All user profiles within an OU are processed normally.	All VDA versions
Timeout for pending area lock files (days)	1 day	All VDA versions

Receiver

Name	Default setting	VDA
StoreFront accounts list	No stores are specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

User personalization layer

Name	Default setting	VDA
User Layer Repository Path	Disabled. No path specified.	VDA 19.12 and later versions
User Layer Size in GB	0 GB (Defaults to minimum layer size of 10 GB)	VDA 19.12 or later versions

Virtual Delivery Agent

Name	Default setting	VDA
Controller registration IPv6 netmask	No netmask is specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Controller registration port	80	All VDA versions
Controller SIDs	No SIDs are specified	All VDA versions

Name	Default setting	VDA
Controllers	No controllers are specified	All VDA versions
Enable auto update of controllers	Enabled	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Only use IPv6 controller registration	Disabled	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Site GUID	No GUID is specified	All VDA versions

Virtual Delivery Agent/HDX 3D Pro

Name	Default setting	VDA
Enable lossless	Enabled	VDA 5.5, 5.6 FP1
HDX 3D Pro quality settings		VDA 5.5, 5.6 FP1

Virtual Delivery Agent/Monitoring

Name	Default setting	VDA
Enable process monitoring	Disabled	VDA 7.11 through current
Enable resource monitoring	Enabled	VDA 7.11 through current

Virtual IP

Name	Default setting	VDA
Virtual IP loopback support	Disabled	VDA 7.6 through current
Virtual IP virtual loopback programs list	None	VDA 7.6 through current

Policy settings reference

February 7, 2020

Policies contain settings that are applied when the policy is enforced. Descriptions in this section also indicate if more settings are required to enable a feature or are similar to a setting.

Quick reference

The following tables list the settings you can configure within a policy. Find the task you want to complete in the left column, then locate its corresponding setting in the right column.

A full listing of all policy settings is available in .CHM (Compiled HTML) format and .CSV format. These files are available in the `\program files\citrix\grouppolicy` folder on the server where the broker (delivery controller) is installed. You can also download the latest version of the policy settings by clicking here.

Audio

For this task	Use this policy setting
Control whether to allow the use of multiple audio devices	Audio Plug N Play
Control whether to allow audio input from microphones on the user device	Client microphone redirection
Control audio quality on the user device	Audio quality
Control audio mapping to speakers on the user device	Client audio redirection

Bandwidth for user devices

To limit bandwidth used for	Use this policy setting
Client audio mapping	Audio redirection bandwidth limit or Audio redirection bandwidth limit percent
Cut-and-paste using local clipboard	Clipboard redirection bandwidth limit or Clipboard redirection bandwidth limit percent

To limit bandwidth used for	Use this policy setting
Access in a session to local client drives	File redirection bandwidth limit or File redirection bandwidth limit percent
HDX MediaStream Multimedia Acceleration	HDX MediaStream Multimedia Acceleration bandwidth limit or HDX MediaStream Multimedia Acceleration bandwidth limit percent
Client session	Overall session bandwidth limit
Printing	Printer redirection bandwidth limit or Printer redirection bandwidth limit percent
TWAIN devices (such as a camera or scanner)	TWAIN device redirection bandwidth limit or TWAIN device redirection bandwidth limit percent
USB devices	Client USB device redirection bandwidth limit or Client USB device redirection bandwidth limit percent

Redirection of client drives and user devices

For this task	Use this policy setting
Control whether or not drives on the user device are connected when users log on to the server	Auto connect client drives
Control cut-and-paste data transfer between the server and the local clipboard	Client clipboard redirection
Control how drives map from the user device	Client drive redirection
Control whether users' local hard drives are available in a session	Client fixed drives and Client drive redirection
Control whether users' local floppy drives are available in a session	Client floppy drives and Client drive redirection
Control whether users' network drives are available in a session	Client network drives and Client drive redirection
Control whether users' local CD, DVD, or Blu-ray drives are available in a session	Client optical drives and Client drive redirection
Control whether users' local removable drives are available in a session	Client removable drives and Client drive redirection

For this task	Use this policy setting
Control whether users' TWAIN devices, such as scanners and cameras, are available in a session and control compression of image data transfers	Client TWAIN device redirection; TWAIN compression redirection
Control whether USB devices are available in a session	Client USB device redirection and Client USB device redirection rules
Improve the speed of writing and copying files to a client disk over a WAN	Use asynchronous writes

Content redirection

For this task	Use this policy setting
Control whether to use content redirection from the server to the user device	Host to client redirection

Desktop UI

For this task	Use this policy setting
Control whether or not Desktop wallpaper is used in users' sessions	Desktop wallpaper
View window contents while a window is dragged	View window contents while dragging

Graphics and multimedia

> **Important:**
>
> The Flash policy remains only to allow customers with older VDAs to use newer controllers (for example, version 1912 controllers) and still use Flash. This VDA version does not support Flash.

For this task	Use this policy setting
Control the maximum number of frames per second sent to user devices from virtual desktops	Target frame rate
Control the visual quality of images displayed on the user device	Visual quality
Control whether websites can display Flash content when accessed in sessions	Flash server-side content fetching URL list; Flash URL compatibility list; Flash video fallback prevention policy setting; Flash video fallback prevention error *.swf
Control compression of server-rendered video	Use video codec for compression; Use hardware encoding for video codec
Control the delivery of HTML5 multimedia web content to users	HTML5 video redirection

Prioritize Multi-Stream network traffic

For this task	Use this policy setting
Specify ports for ICA traffic across multiple connections and establish network priorities	Multi-Port policy
Enable support for multi-stream connections among servers and user devices	Multi-Stream (computer and user settings)

Print

For this task	Use this policy setting
Control creation of client printers on the user device	Auto-create client printers and Client printer redirection
Control the location where printer properties are stored	Printer properties retention
Control whether the client or the server processes the print requests	Direct connections to print servers
Control whether users can access printers connected to their user devices	Client printer redirection

For this task	Use this policy setting
Control installation of native Windows drivers when automatically creating client and network printers	Automatic installation of in-box printer drivers
Control when to use the Universal Printer Driver	Universal print driver usage
Choose a printer based on a roaming user session information	Default printer
Load balance and set failover threshold for Universal Print Servers	Universal Print Servers for load balancing; Universal Print Servers out-of-service threshold

> **Note:**
> Policies cannot be used to enable a screen saver in a desktop or application session. For users who require screen savers, the screen saver can be implemented on the user device.

ICA policy settings

November 24, 2020

Adaptive transport

This setting allows or prevents data transport over EDT as primary and fallback to TCP.

By default, adaptive transport is enabled (**Preferred**), and EDT is used when possible, with fallback to TCP. If it's been disabled and you want to enable it, follow this procedure.

1. In Studio, enable the policy setting, HDX adaptive transport. We also recommend that you do not enable this feature as a universal policy for all objects in the Site.
2. To enable the policy setting, set the value to **Preferred**, then click **OK**.

Preferred. Adaptive transport over EDT is used when possible, with fallback to TCP.

Diagnostic mode. EDT is forced on and fallback to TCP is disabled. We recommend this setting only for troubleshooting.

Off. TCP is forced on, and EDT is disabled.

For more information, see Adaptive transport.

Application launch wait timeout

This setting specifies the wait timeout value in milliseconds for a session to wait for the first application to start. If the start of the application exceeds this time period, the session ends.

You can choose the default time (10000 milliseconds) or specify a number in milliseconds.

Client clipboard redirection

This setting allows or prevents the clipboard on the user device being mapped to the clipboard on the server.

By default, clipboard redirection is allowed.

To prevent cut-and-paste data transfer between a session and the local clipboard, select **Prohibit**. Users can still cut and paste data between applications running in sessions.

After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection. Use the **Clipboard redirection bandwidth limit** or the **Clipboard redirection bandwidth limit percent** settings.

Client clipboard write allowed formats

When the **Restrict client clipboard write** setting is **Enabled**, host clipboard data cannot be shared with the client endpoint. You can use this setting to allow specific data formats to be shared with the client endpoint clipboard. To use this setting, enable it and add the specific formats to be allowed.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE

- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

The following custom formats are predefined in XenApp and XenDesktop and Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML format is disabled by default. To enable this feature:

- Ensure that **Client clipboard redirection** is set to **Allowed**.
- Ensure that **Restrict client clipboard write** is set to **Enabled**.
- Add an entry for **CF_HTML** (and any other formats you want supported) in **Client clipboard write allowed formats**.

You can add more custom formats. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either **Client clipboard redirection** or **Restrict client clipboard write** is set to **Prohibited**.

> **Note**
>
> Enabling HTML format clipboard copy support (CF_HTML) copies any scripts from the source of the copied content to the destination. Check that you trust the source before proceeding to copy. If you do copy content containing scripts, they are live only if you save the destination file as an HTML file and execute it.

Restrict client clipboard write

If this setting is **Allowed**, host clipboard data cannot be shared with the client endpoint. You can allow specific formats by enabling the **Client clipboard write allowed formats** setting.

By default, this setting is Prohibited.

Restrict session clipboard write

When this setting is **Allowed**, client clipboard data cannot be shared within the user session. You can allow specific formats by enabling the **Session clipboard write allowed formats** setting.

By default, this setting is Prohibited.

Session clipboard write allowed formats

When the **Restrict session clipboard write** setting is **Allowed**, client clipboard data cannot be shared with session applications. You can use this setting to allow specific data formats to be shared with the session clipboard.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

The following custom formats are predefined in XenApp and XenDesktop and Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML format is disabled by default. To enable this feature:

- Ensure that **Client clipboard redirection** is set to **Allowed**.
- Ensure that **Restrict session clipboard write** is set to **Enabled**.
- Add an entry for **CF_HTML** (and any other formats you want supported) in **Session clipboard write allowed formats**.

You can add more custom formats. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either the Client clipboard redirection setting or Restrict session clipboard write setting is set to Prohibited.

> **Note**
>
> Enabling HTML format clipboard copy support (CF_HTML) copies any scripts from the source of the copied content to the destination. Check that you trust the source before proceeding to copy. If you do copy content containing scripts, they are live only if you save the destination file as an HTML file and execute it.

Desktop starts

This setting allows or prevents connects to a session on that VDA using an ICA connection by non-administrative users in a VDA Direct Access Users group.

By default, non-administrative users cannot connect to these sessions.

This setting doesn't affect non-administrative users in a VDA Direct Access Users group who are using an RDP connection. These users can connect to the VDA whether this setting is enabled or disabled. This setting has no affect on non-administrative users that are not in a VDA Direct Access Users group. These users cannot connect to the VDA whether this setting is enabled or disabled.

ICA listener connection timeout

This setting specifies the maximum wait time for a connection using the ICA protocol to be completed.

By default, the maximum wait time is 120000 milliseconds, or two minutes.

ICA listener port number

This setting specifies the TCP/IP port number used by the ICA protocol on the server.

By default, the port number is set to 1494.

Valid port numbers must be in the range of 0-65535 and must not conflict with other well-known port numbers. If you change the port number, restart the server for the new value to take effect. If you change the port number on the server, you must also change it on every Citrix Workspace app or plug-in that connects to the server.

Keyboard and Input Method Editor (IME)

> **Note:**
>
> This policy applies only to 1912 LTSR CU2 and later.

This setting enables or disables dynamic keyboard layout synchronization, Input Method Editor (IME), Unicode keyboard layout mapping, and hides or shows the keyboard layout switch notification dialog message.

1. In Studio, select **Keyboard and IME**.
2. Select **Client keyboard layout synchronization and IME improvement** to control the dynamic keyboard layout synchronization and generic client Input Method Editor (IME) features in the VDA. You can configure:

   Disabled - dynamic keyboard layout synchronization and generic client Input Method Editor (IME).

   Support dynamic client keyboard layout synchronization - enables dynamic keyboard layout synchronization.

   Support dynamic client keyboard layout synchronization and IME improvement - enables both dynamic keyboard layout synchronization and generic client Input Method Editor (IME).
3. Select **Enable Unicode keyboard layout mapping** to enable or disable Unicode keyboard mapping.
4. Select **Hide keyboard layout switch pop-up message box** to allow or prohibit whether a message displays that the keyboard layout is synchronizing when the user changes the client keyboard layout.

Default settings:

- **Client keyboard layout synchronization and IME improvement**
  - Disabled in Windows Server 2016 and Windows Server 2019.

  - Support dynamic client keyboard layout synchronization and IME improvement in Windows Server 2012 and Windows 2010.

- **Disable Unicode keyboard layout mapping**
- **Show keyboard layout switch pop-up message box**

This policy replaces the registry settings that are listed in the **Description** section of the policy settings.

Logoff checker startup delay

This setting specifies the duration to delay the logoff checker startup. Use this policy to set the time (in seconds) that a client session waits before disconnecting the session.

This setting also increases the time it takes for a user to log off the server.

Rendezvous protocol

This setting changes how HDX sessions are proxied when using the Citrix Gateway Service. When enabled, HDX traffic no longer flows through the Citrix Cloud Connector. Instead, the VDA establishes an outbound connection directly to the Citrix Gateway Service (enhancing Cloud Connector scalability).

> **Important:**
>
> This feature is controlled by a feature toggle in Citrix Cloud as well as an HDX policy setting. The Citrix Cloud feature toggle is enabled by default while the HDX setting is disabled by default. The HDX setting affects only HDX sessions established though the Citrix Gateway Service. Sessions established directly between client and VDA or through an on-premises Citrix Gateway are not affected by this setting.

For information, see Rendezvous protocol.

Starting of non-published programs during client connection

This setting specifies whether to allow starting initial applications through RDP on the server.

By default, starting initial applications through RDP on the server is not allowed.

Tablet mode toggle policy settings

Tablet mode toggle optimizes the look and behavior of Store apps, Win32 apps, and the Windows shell on the VDA. It does so by automatically toggling the virtual desktop to Tablet mode when connecting from small form factor devices like phones and tablets, or any touch enabled device.

If this policy is disabled, the VDA is in the mode the user sets it to and maintains the same mode throughout, irrespective of the type of client.

Auto client reconnect policy settings

February 6, 2020

The auto client reconnect section contains policy settings for controlling the automatic reconnection of sessions.

Auto client reconnect

This setting allows or prevents automatic reconnection by the same client after a connection has been interrupted.

For Citrix Receiver for Windows 4.7 and later and Citrix Workspace app 1808 and later, auto client reconnect uses only the policy settings from Citrix Studio. Updates to these policies in Studio synchronize auto client reconnect from server to client. With older versions of Citrix Receiver for Windows, to configure auto client reconnect, use a Studio policy and change the registry or the default.ica file.

Allowing automatic client reconnect allows users to resume working where they were interrupted when a connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

If the Citrix Workspace app cookie containing the key to the session ID and credentials isn't used, automatic reconnection might result in a new session being started. That is, instead of reconnecting to an existing session. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be reentered. If users intentionally disconnect, auto client reconnect is not triggered.

A session window is grayed out when a reconnection is in progress. A countdown timer displays the time remaining before the session is reconnected. When a session times out, it is disconnected.

For application sessions, when automatic reconnect is allowed, a countdown timer appears in the notification area specifying the time remaining before the session is reconnected. Citrix Workspace

app tries to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For user sessions, when automatic reconnect is allowed, Citrix Workspace app tries to reconnect to the session for a specified period, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period is two minutes. To change this period, edit the policy.

By default, automatic client reconnect is allowed.

To disable auto client reconnect:

1. Start Citrix Studio.
2. Open the **Auto client reconnect** policy.
3. Set the policy to **Prohibited**.

Auto client reconnect authentication

This setting requires authentication for automatic client reconnections.

When a user initially logs on, the credentials are encrypted, stored in memory, and a cookie is created containing the encryption key. The cookie is sent to Citrix Workspace app. When this setting is configured, cookies are not used. Instead, a dialog box is displayed to users requesting credentials when Citrix Workspace app attempts to reconnect automatically.

By default, authentication is not required.

To change auto client reconnect authentication:

1. Start Citrix Studio.
2. Open the **Auto client reconnect authentication** policy.
3. Enable or disable authentication.
4. Choose **OK**.

Auto client reconnect logging

This setting enables or disables the recording of auto client reconnections in the event log.

When logging is enabled, the server System Log captures information about successful and failed automatic reconnection events. A site does not provide a combined log of reconnection events for all servers.

By default, logging is disabled.

To change auto client reconnect logging:

1. Start Citrix Studio.

2. Open the **Auto client reconnect logging** policy.
3. Enable or disable logging.
4. Choose **OK**.

Auto client reconnect timeout

By default, auto client reconnect timeout is set to 120 seconds, the maximum configurable value for an auto client reconnect timeout is 300 seconds.

To change auto client reconnect timeout:

1. Start Citrix Studio.
2. Open the **Auto client reconnect timeout** policy.
3. Edit the timeout value.
4. Choose **OK**.

Reconnect UI transparency level

You can use Studio policy to configure the opacity level applied to the XenApp or XenDesktop session window during session reliability reconnection time.

By default, Reconnect UI transparency is set to 80%.

To change the reconnect user interface opacity level:

1. Start Citrix Studio.
2. Open the **Reconnect UI transparency level** policy.
3. Edit the value.
4. Choose **OK**.

Audio policy settings

February 6, 2020

The Audio section contains policy settings that permit user devices to send and receive audio in sessions without reducing performance.

Audio over UDP real-time transport

This setting allows or prevents the transmission and receipt of audio between the VDA and user device over RTP using the User Datagram Protocol (UDP). When this setting is disabled, audio is sent and received over TCP.

By default, audio over UDP is allowed.

Audio Plug N Play

This setting allows or prevents the use of multiple audio devices to record and play sound.

By default, the use of multiple audio devices is allowed.

This setting applies only to Windows Multi-session OS machines.

Audio quality

This setting specifies the quality level of sound received in user sessions.

By default, sound quality is set to High - high definition audio.

To control sound quality, choose one of the following options:

- Select Low - for low speed connections for low-bandwidth connections. Sounds sent to the user device are compressed up to 16 Kbps. This compression results in a significant decrease in the quality of the sound but allows reasonable performance for a low-bandwidth connection.
- Select Medium - optimized for speech to deliver Voice over Internet Protocol applications, to deliver media applications in challenging network connections with lines less than 512 Kbps, or significant congestion and packet loss. This codec offers fast encode time, making it ideal for use with softphones and Unified Communications applications when you require server-side media processing.

  Audio sent to the user device is compressed up to 64 Kbps. This compression results in a moderate decrease in the quality of the audio played on the user device, while providing low latency and consuming low bandwidth. If Voice over Internet Protocol quality is unsatisfactory, ensure that the Audio over UDP Real-time Transport policy setting is set to Allowed.

  Now, Real-time Transport (RTP) over UDP is only supported when this audio quality is selected. Use this audio quality even for delivering media applications for challenging network connections like low (fewer than 512 Kbps) lines and when there is congestion and packet loss in the network.

- Select High - high definition audio for connections where bandwidth is plentiful and sound quality is important. Clients can play sound at its native rate. Sounds are compressed at a high quality level maintaining up to CD quality, and using up to 112 Kbps of bandwidth. Transmitting this amount of data can result in increased CPU usage and network congestion.

Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption doubles.

To specify the maximum amount of bandwidth, configure the Audio redirection bandwidth limit or the Audio redirection bandwidth limit percent settings.

Client audio redirection

This setting specifies whether applications hosted on the server can play sounds through a sound device installed on the user device. This setting also specifies whether users can record audio input.

By default, audio redirection is allowed.

After allowing this setting, you can limit the bandwidth consumed by playing or recording audio. Limiting the amount of bandwidth consumed by audio can improve application performance but might also degrade audio quality. Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption doubles. To specify the maximum amount of bandwidth, configure the Audio redirection bandwidth limit or the Audio redirection bandwidth limit percent settings.

On Windows Multi-session OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

Important: Prohibiting Client audio redirection disables all HDX audio functionality.

Client microphone redirection

This setting enables or disables client microphone redirection. When enabled, users can use microphones to record audio input in a session.

By default, microphone redirection is allowed.

For security, users are alerted when servers that are not trusted by their devices try to access microphones. Users can choose to accept or not accept access. Users can disable the alert on Citrix Workspace app.

On Windows Multi-session OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

If the Client audio redirection setting is disabled on the user device, this rule has no effect.

Bandwidth policy settings

February 6, 2020

The Bandwidth section contains policy settings to avoid performance problems related to client session bandwidth use.

Important: Using these policy settings with the Multi-Stream policy settings might produce unexpected results. If you use Multi-Stream settings in a policy, ensure these bandwidth limit policy settings are not included.

Audio redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for playing or recording audio in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Audio redirection bandwidth limit percent setting, the most restrictive setting (lower value) is applied.

Audio redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for playing or recording audio as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Audio redirection bandwidth limit setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Client USB device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for the redirection of USB devices to and from the client.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Client USB device redirection bandwidth limit percent setting, the most restrictive setting (the lower value) is applied.

Client USB device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for the redirection of USB devices to and from the client as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Client USB device redirection bandwidth limit setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Clipboard redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for data transfer between a session and the local clipboard.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Clipboard redirection bandwidth limit percent setting, the most restrictive setting (the lower value) is applied.

Clipboard redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for data transfer between a session and the local clipboard as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Clipboard redirection bandwidth limit setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

COM port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the maximum allowed bandwidth in kilobits per second for accessing a COM port in a client connection. If you enter a value for this setting and a value for the COM port redirection bandwidth limit percent setting, the most restrictive setting (the lower value) is applied.

COM port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the maximum allowed bandwidth for accessing COM ports in a client connection as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified

If you enter a value for this setting and a value for the COM port redirection bandwidth limit setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions

File redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for accessing a client drive in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the File redirection bandwidth limit percent setting, the most restrictive setting (the lower value) takes effect.

File redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for accessing client drives as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the File redirection bandwidth limit setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

HDX MediaStream Multimedia Acceleration bandwidth limit

This setting specifies the maximum allowed bandwidth limit, in kilobits per second, for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the HDX MediaStream Multimedia Acceleration bandwidth limit percent setting, the most restrictive setting (the lower value) takes effect.

HDX MediaStream Multimedia Acceleration bandwidth limit percent

This setting specifies the maximum allowed bandwidth for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the HDX MediaStream Multimedia Acceleration bandwidth limit setting, the most restrictive setting (the lower value) takes effect.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

LPT port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the maximum allowed bandwidth, in kilobits per second, for print jobs using an LPT port in a single user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the LPT port redirection bandwidth limit percent setting, the most restrictive setting (the lower value) is applied.

LPT port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the bandwidth limit for print jobs using an LPT port in a single client session as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the LPT port redirection bandwidth limit setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Overall session bandwidth limit

This setting specifies the total amount of bandwidth available, in kilobits per second, for user sessions.

The maximum enforceable bandwidth cap is 10 Mbps (10,000 Kbps). By default, no maximum (zero) is specified.

Limiting the amount of bandwidth consumed by a client connection can improve performance when other applications outside the client connection are competing for limited bandwidth.

Printer redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for accessing client printers in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Printer redirection bandwidth limit percent setting, the most restrictive setting (the lower value) is applied.

Printer redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for accessing client printers as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Printer redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

TWAIN device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for controlling TWAIN imaging devices from published applications.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the TWAIN device redirection bandwidth limit percent setting, the most restrictive setting (the lower value) is applied.

TWAIN device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for controlling TWAIN imaging devices from published applications as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the TWAIN device redirection bandwidth limit setting, the most restrictive setting (having the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Bidirectional content redirection policy settings

March 7, 2022

Allow Bidirectional Content Redirection

Set this policy to **Allowed** to enable redirection between server (VDA) and client. It's set to **Prohibited** by default.

Use the **Allowed URLs to be redirected to Client** policy to configure the list of URLs for VDA to client redirection.

> **Note:**
>
> This policy must be set with the **Bidirectional Content Redirection** policy on the client for redirection to be allowed.

Allowed URLs to be redirected to Client

Specifies the list of URLs to open on the client when bidirectional content redirection is allowed.

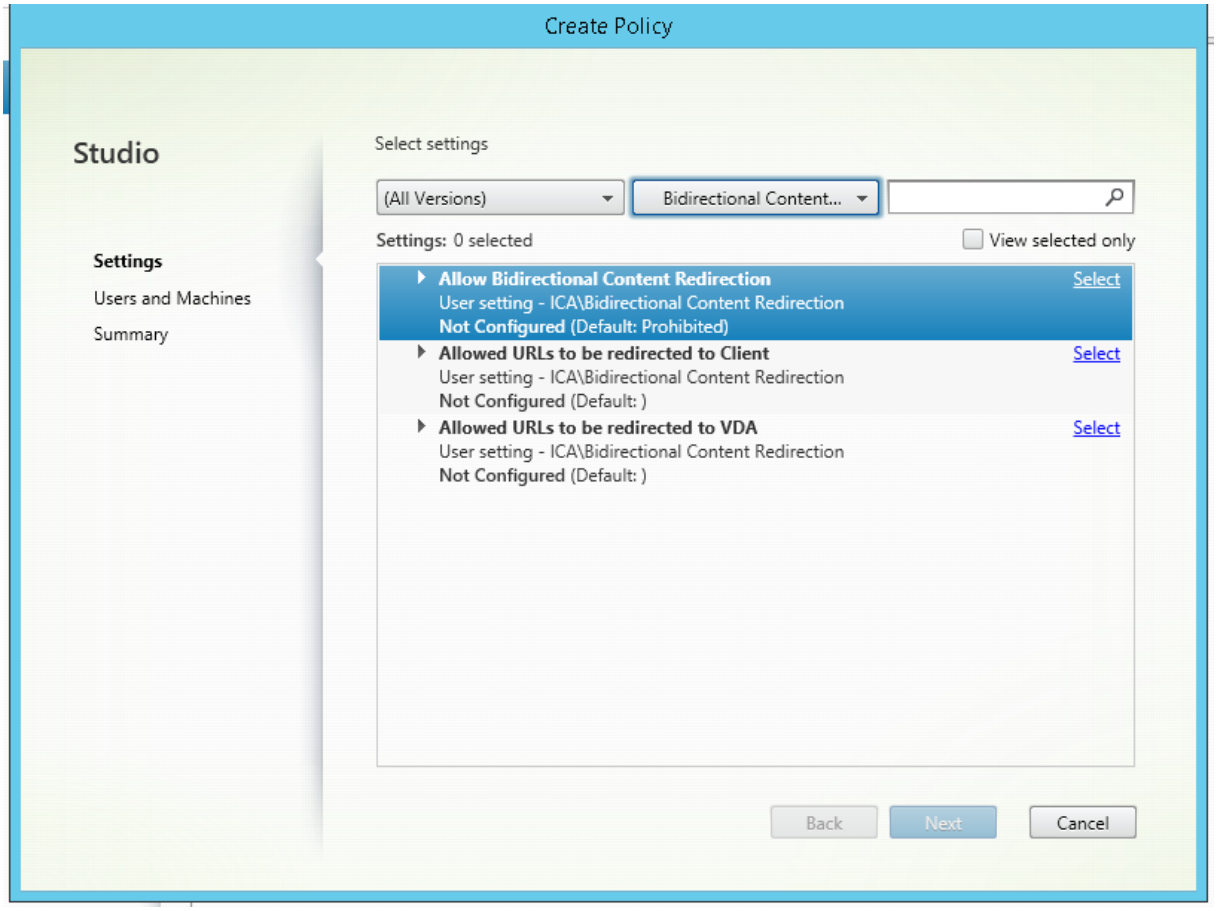
A semi-colon (;) is the delimiter. An asterisk (*) can be used as a wild card. For example:

To enable bidirectional content redirection

When you include URLs, you can specify one URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard in the domain name. For example:

http://*.citrix.com; http://www.google.com

1. Start Citrix Studio.
2. Open the **Bidirectional Content Redirection** policy.
3. Select **Allow Bidirectional Content Redirection**, choose **Allowed**, and **OK**. If you do not allow this option, you are unable to complete this procedure.
4. Select **Allowed URLs to be redirected to Client** and specify a URL, a list of URLs, or choose the default value.
5. Select **Allowed URLs to be redirected to VDA** and specify a URL, a list of URLs, or choose the default value.



For information about the client-side bidirectional content redirection configuration on the Citrix Workspace app, see Bidirectional content redirection in the Citrix Workspace app for Windows documentation.

Copy and paste between session and client

To configure copy and paste functionality from a session to client, set the following policies:

- Client Clipboard redirection to allowed.
- Restrict Client Clipboard Write to restrict pasting all formats from clipboard to the client.

- Client Clipboard Write Allowed Formats to make an exception for pasting files from clipboard to the client (Use format CFX_FILE to allow the feature).
- Restrict Session Clipboard Write to restrict pasting all formats from the clipboard into the VDA session.
- Session Clipboard Write Allowed Formats to make an exception for pasting files from clipboard to the VDA (Use format CFX_FILE to allow the feature).

Register browser add-ons

The Internet Explorer browser add-on is required for bidirectional content redirection.

You can use the following commands to register and unregister the Internet Explorer add-on:

- To register the Internet Explorer add-on on a client device: <client-installation-folder>\redirector.exe /regIE
- To unregister the Internet Explorer add-on on a client device: <client-installation-folder>\redirector.exe /unregIE
- To register the Internet Explorer add-on on a VDA: <VDAinstallation-folder>\VDARedirector.exe /regIE
- To unregister the Internet Explorer add-on on a VDA: <VDAinstallation-folder>\VDARedirector.exe /unregIE

For example, the following command registers the Internet Explorer add-on on a device running Citrix Workspace app.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

The following command registers the Internet Explorer add-on on a Windows Multi-session OS VDA.

C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regIE

Browser content redirection policy settings

March 7, 2022

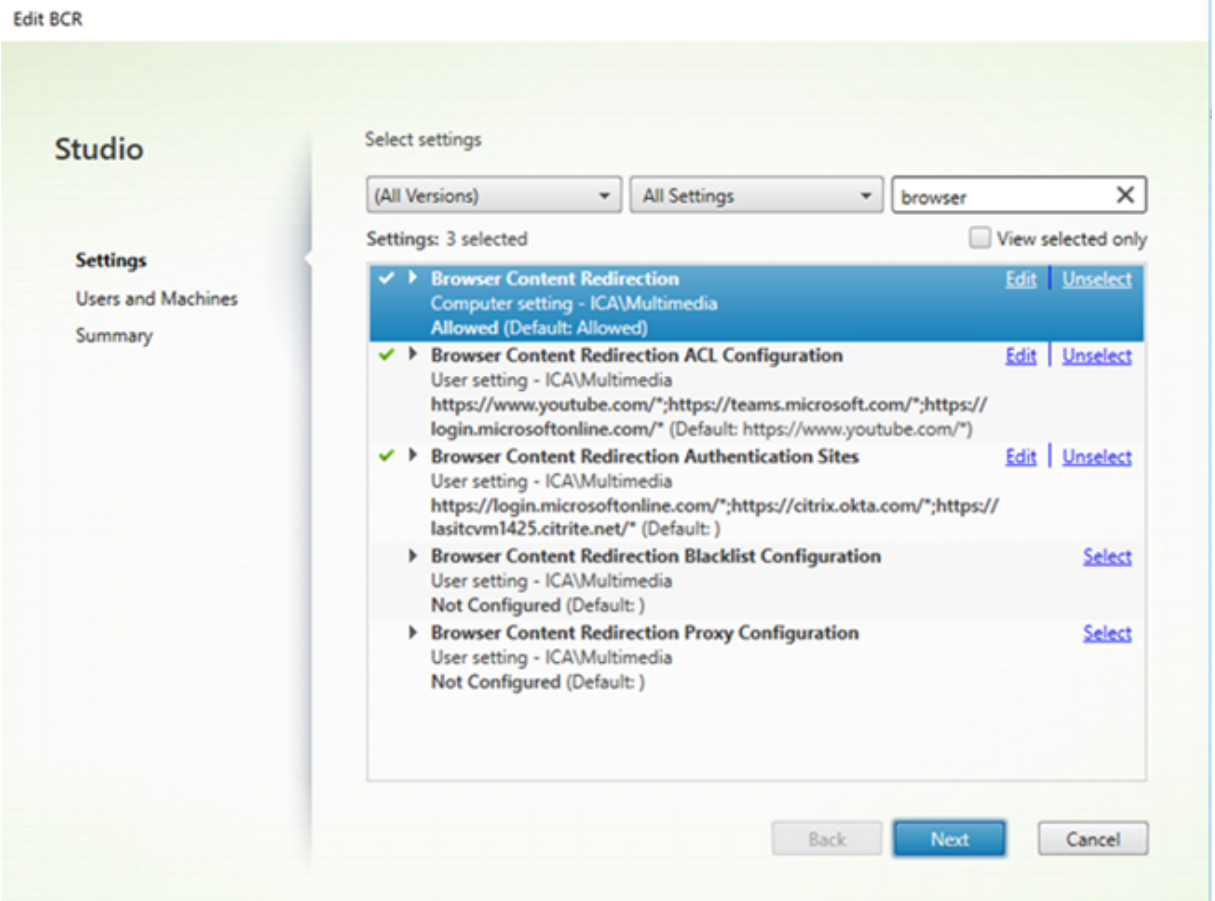
The browser content redirection section contains policy settings to configure this feature.

Browser content redirection controls and optimizes the way Citrix Virtual Apps and Desktops deliver any web browser content (for example, HTML5) to users. Only the visible area of the browser where content is displayed is redirected.

HTML5 video redirection and browser content redirection are independent features. The HTML5 video redirection policies are not needed for this feature to work, but the Citrix HDX HTML5 Video Redirection Service is used for browser content redirection. For more information, see Browser content redirection.

Policy settings:

The following policy settings are available for the browser content redirection feature in Citrix Studio. These policies can be overridden with registry keys on the VDA, but registry keys are optional.



TLS and browser content redirection

You can use browser content redirection to redirect HTTPS websites. The JavaScript injected into those websites must establish a TLS connection to the Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) running on the VDA. To achieve this redirection and maintain the TLS integrity of the webpage, the Citrix HDX HTML5 Video Redirection Service generates two custom certificates in the certificate store on the VDA.

HdxVideo.js uses Secure Websockets to communicate with WebSocketService.exe running on the VDA. This process runs on the Local System, and performs SSL termination and user session mapping.

WebSocketService.exe is listening on 127.0.0.1 port 9001.

Browser content redirection

By default, Citrix Workspace app tries client fetch and client render. If client fetch client and render fails, server-side rendering is tried. If you also enable the browser content redirection proxy configuration policy, Citrix Workspace app tries only server fetch and client render.

By default, this setting is Allowed.

Browser content redirection server fetch web proxy authentication setting

> **Note:**
>
> This policy is available only on 1912 CU3 and later.

This setting routes HTTP traffic originating at an overlay through a downstream web proxy. The downstream web proxy authorizes and authenticates HTTP traffic using the VDA user's domain credentials through the Negotiate authentication scheme.

You must configure browser content redirection for server fetch mode in the PAC file using the Browser content redirection proxy configuration policy. In the PAC script, provide instructions to route the overlay traffic through a downstream web proxy. Then configure the downstream web proxy to authenticate the VDA users through the Negotiate authentication scheme.

When set to **Allowed**, the web proxy responds with a 407 Negotiate challenge, containing a **Proxy-Authenticate: Negotiate** header. Browser content redirection then obtains a Kerberos service ticket by using the VDA user's domain credentials and includes the service ticket in subsequent requests to the web proxy.

When set to **Prohibited**, browser content redirection proxies all TCP traffic between the overlay and the web proxy without interfering. The overlay uses basic authentication credentials or any other available credentials to authenticate to the web proxy.

By default, this setting is Prohibited.

Browser content redirection Access Control List (ACL) policy settings

Use this setting to configure an Access Control List (ACL) of URLs that can use browser content redirection or are denied access to browser content redirection.

Authorized URLs are the whitelisted URLs whose content is redirected to the client.

The wildcard * is permitted, but it isn't permitted within the protocol or the domain address part of the URL.

Allowed: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Not allowed: `http://*.xyz.com/`

You can achieve better granularity by specifying paths in the URL. For example, if you specify `https://www.xyz.com/sports/index.html`, only the index.html page is redirected.

By default, this setting is set to `https://www.youtube.com/*`

For more information, see the Knowledge Center article CTX238236.

Browser content redirection authentication sites

Use this setting to configure a list of URLs. Sites redirected by using browser content redirection use the list to authenticate a user. The setting specifies the URLs for which browser content redirection remains active (redirected) when navigating away from a whitelisted URL.

A classic scenario is a website that relies on an Identity Provider (IdP) for authentication. For example, website `www.xyz.com` must be redirected to the endpoint, but a third party IdP, like Okta (`www.xyz.okta.com`) handles the authentication portion. The administrator uses the browser content redirection ACL configuration policy to whitelist `www.xyz.com`, and then uses browser content redirection authentication sites to whitelist `www.xyz.okta.com`.

For more information, see the Knowledge Center article CTX238236.

Browser content redirection blacklist setting

This setting works along with the browser content redirection ACL configuration setting. If URLs are present in the browser content redirection ACL configuration setting and the blacklist configuration setting, the blacklist configuration takes precedence and the browser content of the URL isn't redirected.

Unauthorized URLs: Specifies the blacklisted URLs whose browser content isn't redirected to the client, but rendered on the server.

The wildcard * is permitted, but it isn't permitted within the protocol or the domain address part of the URL.

Allowed: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Not allowed: `http://*.xyz.com/`

You can achieve better granularity by specifying paths in the URL. For example, if you specify `https://www.xyz.com/sports/index.html`, only index.html is blacklisted.

Browser content redirection proxy setting

> **Important:**
>
> The following settings apply only to 1912 LTSR CU1 or later.

This setting provides configuration options for proxy settings on the VDA for browser content redirection. If enabled with a valid proxy address and port number, PAC / WPAD URL, or Direct/Transparent setting, Citrix Workspace app tries only server fetch and client rendering.

If disabled or not configured and using a default value, Citrix Workspace app tries client fetch and client rendering.

By default, this setting is Prohibited.

Allowed pattern for an explicit proxy:

`http://\<hostname/ip address\>:\<port\>`

Example:

```
http://proxy.example.citrix.com:80
http://10.10.10.10:8080
```

Allowed patterns for PAC/WPAD files:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

Example: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

Example: `http://10.10.10.10/configuration/pac/wpad.dat`

Allowed patterns for direct or transparent proxies:

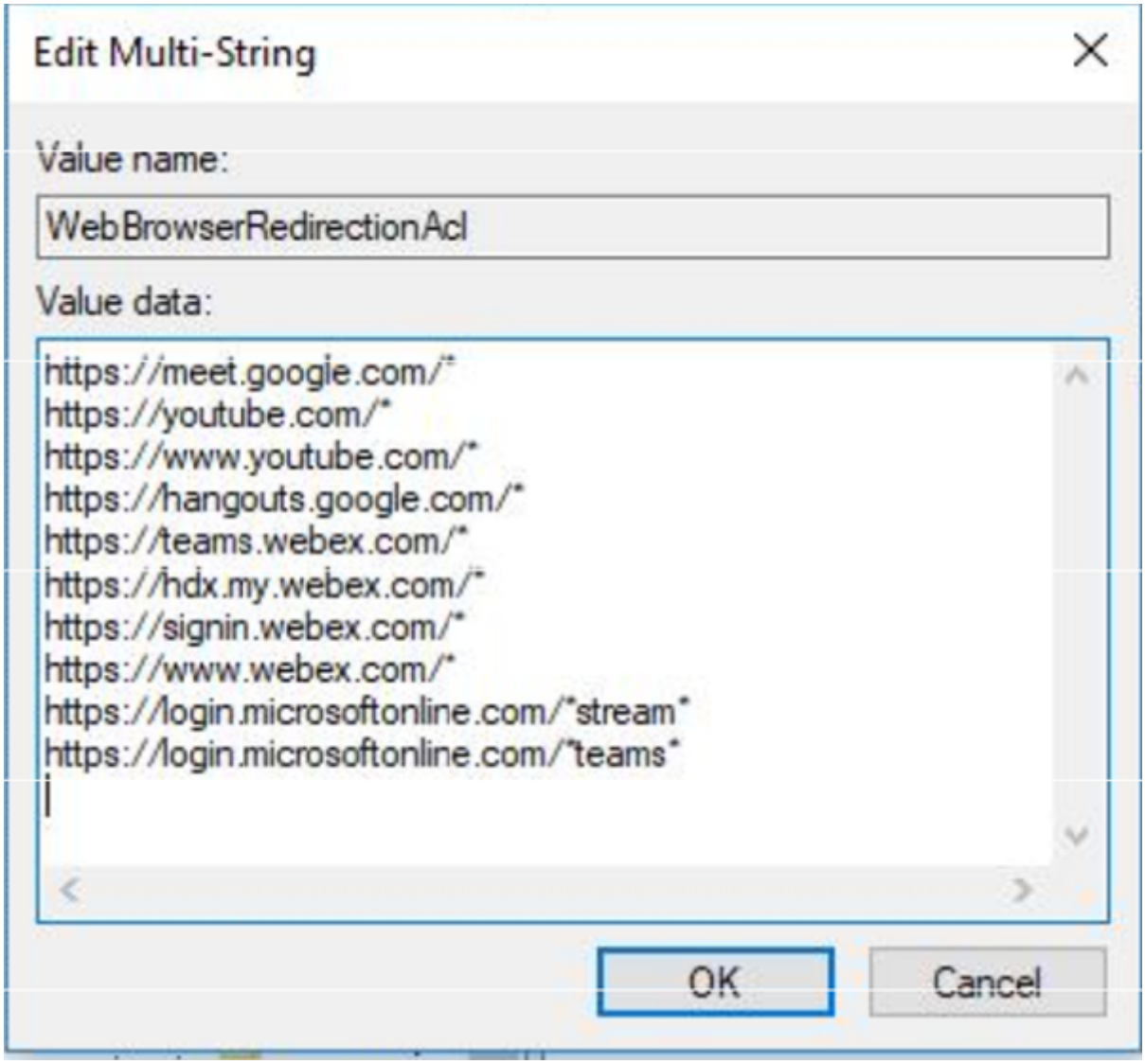
Type the word **DIRECT** in the policy text box.

Browser content redirection registry key overrides

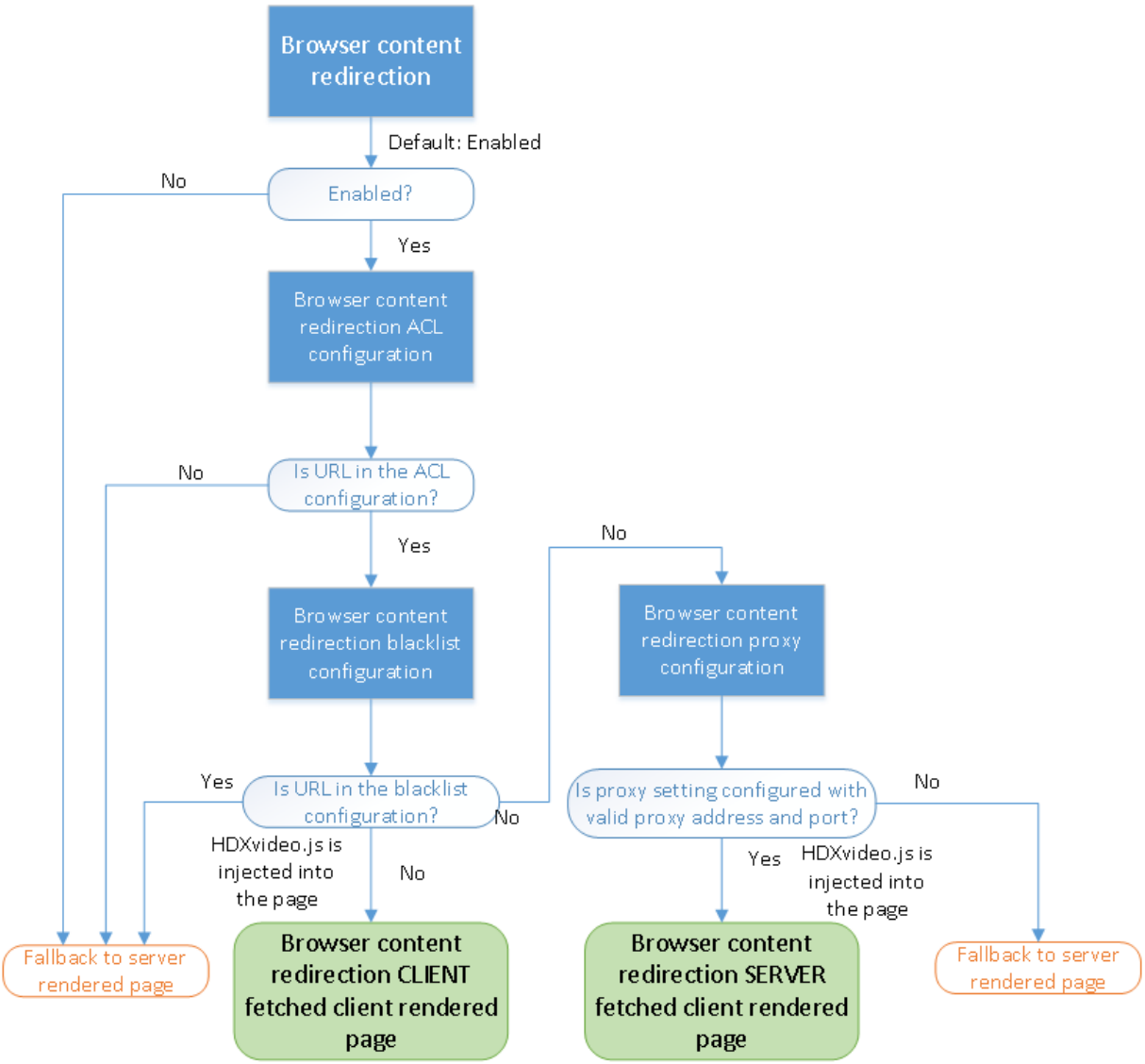
> **Warning**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
>
> Registry override options for policy settings:

```
\HKLM \SOFTWARE\Wow6432Node\Citrix\HdxMediastream
```


Name	Type	Value
WebBrowserRedirection	DWORD	1=Allowed, 0=Prohibited
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationMethod	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` or `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



HDXVideo.js insertion for browser content redirection



HdxVideo.js is injected on the webpage by using the browser content redirection Chrome extension or the Internet Explorer Browser Helper Object (BHO). The BHO is a plug-in model for Internet Explorer. It provides hooks for browser APIs and allows the plug-in to access the Document Object Model (DOM) of the page to control navigation.

The BHO decides whether to inject HdxVideo.js on a given page. The decision is based on the administrative policies shown in the previous flow chart.

After it decides to inject the JavaScript and redirect browser content to the client, the webpage on the Internet Explorer browser on the VDA is blanked out. Setting the **document.body.innerHTML** to empty removes the entire body of the webpage on the VDA. The page is ready to be sent to the client to be displayed on the overlay browser (Hdxbrowser.exe) on the client.

Client sensors policy settings

February 6, 2020

The Client Sensors section contains policy settings for controlling how mobile device sensor information is handled in a user session.

Allow applications to use the physical location of the client device

This setting determines whether applications running in a session on a mobile device are allowed to use the physical location of the user device.

By default, the use of location information is prohibited

When this setting is prohibited, attempts by an application to retrieve location information return a ‘‘permission denied’’value.

When this setting is allowed, a user can prohibit use of location information by denying a Citrix Workspace app request to access the location. Android and iOS devices prompt at the first request for location information in each session.

When developing hosted applications that use the Allow applications to use the physical location of the client device setting, consider the following:

- Ensure a location-enabled application doesn’t rely on location information being available because:
  - A user might not allow access to location information.
  - The location might not be available or might change while the application is running.
  - A user might connect to the application session from a different device that does not support location information.
- A location-enabled application must:
  - Have the location feature off by default.
  - Provide a user option to allow or disallow the feature while the application is running.
  - Provide a user option to clear location data that the application caches. (Citrix Workspace app does not cache location data.)
- A location-enabled application must manage the granularity of the location information so that the data acquired is appropriate to the purpose of the application and conforms to regulations in all relevant jurisdictions.
- Enforce a secure connection (for example, using TLS or a VPN) when using location services. Connect Citrix Workspace app to trusted servers.
- Consider obtaining legal advice regarding the use of location services.

Desktop UI policy settings

February 6, 2020

The Desktop UI section contains policy settings that control visual effects such as desktop wallpaper, menu animations, and drag-and-drop images, to manage the bandwidth used in client connections. You can improve application performance on a WAN by limiting bandwidth usage.

> **Important**
>
> We do not support legacy graphics mode and Desktop Composition Redirection (DCR) in this release. This policy is included only for backward compatibility when using XenApp 7.15 LTSR, XenDesktop 7.15 LTSR, and previous VDA releases with Windows 7 and Windows 2008 R2.

Desktop Composition Redirection

This setting specifies whether to use the processing capabilities of the graphics processing unit (GPU) or integrated graphics processor (IGP) on the user device for local DirectX graphics rendering to provide users with a more fluid Windows desktop experience. When enabled, Desktop Composition Redirection delivers a highly responsive Windows experience while maintaining high scalability on the server.

By default, Desktop Composition Redirection is disabled.

To deselect Desktop Composition Redirection and reduce the bandwidth required in user sessions, select Disabled when adding this setting to a policy.

Desktop Composition Redirection graphics quality

This setting specifies the quality of graphics used for Desktop Composition Redirection.

The default is High.

Choose from High, Medium, Low, or Lossless quality.

Desktop wallpaper

This setting allows or prevents wallpaper showing in user sessions.

By default, user sessions can show wallpaper.

To deselect desktop wallpaper and reduce the bandwidth required in user sessions, select Prohibited when adding this setting to a policy.

Menu animation

This setting allows or prevents menu animation in user sessions.

By default, menu animation is allowed.

Menu animation is a Microsoft personal preference setting for ease of access. When enabled, it causes a menu to appear after a short delay, either by scrolling or fading in. An arrow icon appears at the bottom of the menu. The menu appears when you point to that arrow.

Menu animation is enabled on a desktop if this policy setting is set to Allowed and the menu animation Microsoft personal preference setting is enabled.

Note: Changes to the menu animation Microsoft personal preference setting are changes to the desktop. If the desktop is set to discard changes when the session ends, a user who has enabled menu animations in a session might not have menu animation available in subsequent sessions on the desktop. For users who require menu animation, enable the Microsoft setting in the master image for the desktop or ensure that the desktop retains user changes.

View window contents while dragging

This setting allows or prevents the display of window contents when dragging a window across the screen.

By default, viewing window contents is allowed.

When set to Allowed, the entire window appears to move when you drag it. When set to Prohibited, only the window outline appears to move until you drop it.

End user monitoring policy settings

February 6, 2020

The End User Monitoring section contains policy settings for measuring session traffic.

ICA round trip calculation

This setting determines whether ICA round trip calculations are performed for active connections.

By default, calculations for active connections are enabled.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

ICA round trip calculation interval

This setting specifies the frequency, in seconds, at which ICA round trip calculations are performed.

By default, ICA round trip is calculated every 15 seconds.

ICA round trip calculations for idle connections

This setting determines whether ICA round trip calculations are performed for idle connections.

By default, calculations are not performed for idle connections.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

Enhanced desktop experience policy setting

February 6, 2020

The Enhanced Desktop Experience policy setting sessions running on server operating systems to look like local Windows 7 desktops, providing users with an enhanced desktop experience.

By default, this setting is allowed.

If a user profile with Windows Classic theme exists on the virtual desktop, enabling this policy does not provide an enhanced desktop experience for that user. If a user with a Windows 7 theme user profile logs on to a virtual desktop running Windows Server 2012 for which this policy is either not configured or disabled, that user sees an error message indicating failure to apply the theme.

In both cases, resetting the user profile resolves the issue.

If the policy changes from enabled to disabled on a virtual desktop with active user sessions, the look and feel of those sessions is inconsistent with both the Windows 7 and Windows Classic desktop experience. To avoid this inconsistency, ensure you restart the virtual desktop after changing this policy setting. You must also delete any roaming profiles on the virtual desktop. Citrix also recommends deleting any other user profiles on the virtual desktop to avoid inconsistencies between profiles.

If you are using roaming user profiles in your environment, ensure the Enhanced Desktop Experience feature is enabled or disabled for all virtual desktops that share a profile.

Citrix does not recommend sharing roaming profiles between virtual desktops running server operating systems and client operating systems. Profiles for client and server operating systems differ and sharing roaming profiles across both types can lead to inconsistencies in profile properties when a user moves between the two.

File Redirection policy settings

February 6, 2020

The File Redirection section contains policy settings relating to client drive mapping and client drive optimization.

Auto connect client drives

This setting allows or prevents automatic connection of client drives when users log on.

By default, automatic connection is allowed.

When adding this setting to a policy, ensure to enable the settings for the drive types you want automatically connected. For example, to allow automatic connection of users' CD-ROM drives, configure this setting and the Client optical drives setting.

The following policy settings are related:

- Client drive redirection
- Client floppy drives
- Client optical drives
- Client fixed drives
- Client network drives
- Client removable drives

Client drive redirection

This setting enables or disables file redirection to and from drives on the user device.

By default, file redirection is enabled.

> **Note:**
>
> Client drive redirection policy settings do not apply to drives mapped to sessions using generic USB redirection.

When enabled, users can save files to all their client drives. When disabled, all file redirection is prevented, regardless of the state of the individual file redirection settings such as Client floppy drives and Client network drives.

The following policy settings are related:

- Client floppy drives

- Client optical drives
- Client fixed drives
- Client network drives
- Client removable drives

Client fixed drives

This setting allows or prevents users from accessing or saving files to fixed drives on the user device.

By default, accessing client fixed drives is allowed.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client fixed drives are not mapped and users cannot access these drives manually, regardless of the state of the Client fixed drives setting.

To ensure that fixed drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client floppy drives

This setting allows or prevents users from accessing or saving files to floppy drives on the user device.

By default, accessing client floppy drives is allowed.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client floppy drives are not mapped and users cannot access these drives manually, regardless of the state of the Client floppy drives setting.

To ensure that floppy drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client network drives

This setting allows or prevents users from accessing and saving files to network (remote) drives through the user device.

By default, accessing client network drives is allowed.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client network drives are not mapped and users cannot access these drives manually, regardless of the state of the Client network drives setting.

To ensure that network drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client optical drives

This setting allows or prevents users from accessing or saving files to CD-ROM, DVD-ROM, and BD-ROM drives on the user device.

By default, accessing client optical drives is allowed.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client optical drives are not mapped and users cannot access these drives manually, regardless of the state of the Client optical drives setting.

To ensure that optical drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client removable drives

This setting allows or prevents users from accessing or saving files to USB drives on the user device.

By default, accessing client removable drives is allowed.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client removable drives are not mapped and users cannot access these drives manually, regardless of the state of the Client removable drives setting.

To ensure that removable drives are automatically connected when users log on, configure the Auto connect client drives setting.

Host to client redirection

This setting enables or disables file type associations for URLs and some media content to be opened on the user device. When disabled, content opens on the server.

By default, file type association is disabled.

These URL types are opened locally when you enable this setting:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Real Player and QuickTime (RTSP)
- Real Player and QuickTime (RTSPU)
- Legacy Real Player (PNM)
- Microsoft Media Server (MMS)

Preserve client drive letters

This setting enables or disables mapping of client drives to the same drive letter in the session.

By default, client drive letters are not preserved.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed.

Read-only client drive access

This setting allows or prevents users and applications from creating or changing files or folders on mapped client drives.

By default, files and folders on mapped client drives can be changed.

If set to Enabled, files and folders are accessible with read-only permissions.

When adding this setting to a policy, ensure the Client drive redirection setting is present and set to Allowed.

Special folder redirection

This setting allows or prevents Citrix Workspace app and Web Interface users to see their local Documents and Desktop special folders from a session.

By default, special folder redirection is allowed.

This setting prevents any objects filtered through a policy from having special folder redirection, regardless of settings that exist elsewhere. When this setting is prohibited, any related settings specified for StoreFront, Web Interface, or Citrix Workspace app are ignored.

To define which users can have special folder redirection, select Allowed and include this setting in a policy filtered on the users you want to have this feature. This setting overrides all other special folder redirection settings.

Because special folder redirection must interact with the user device, policy settings that prevent users from accessing or saving files to their local hard drives also prevent special folder redirection from working.

When adding this setting to a policy, ensure that the Client fixed drives setting is present and set to Allowed.

Use asynchronous writes

This setting enables or disables asynchronous disk writes.

By default, asynchronous writes are disabled.

Asynchronous disk writes can improve the speed of file transfers and writing to client disks over WANs, which relatively high bandwidth and high latency typically characterize. However, if there is a connection or disk fault, the client file or files being written might end in an undefined state. If this undefined state occurs, a pop-up window informs the user of the files affected. The user can then take remedial action such as restarting an interrupted file transfer on reconnection or when the disk fault is corrected.

We recommend enabling asynchronous disk writes only for users requiring remote connectivity having good file access speed and who can easily recover files or data lost if there is a connection or disk failure.

When adding this setting to a policy, ensure that the Client drive redirection setting is present and set to Allowed. If this setting is disabled, asynchronous writes don't occur.

Graphics policy settings

February 6, 2020

The Graphics section contains policy settings for controlling how images are handled in user sessions.

Allow visually lossless compression

This setting allows visually lossless compression to be used instead of true lossless compression for graphics. Visually lossless improves performance over true lossless, but has minor loss that is unnoticeable by sight. This setting changes the way the values of the Visual quality setting are used.

By default this setting is disabled.

Graphics status indicator

This setting configures the graphics status indicator to run in the user session. This indicator allows the user to see details on the graphics mode in use, including graphics provider, encoder, hardware encoding, image quality, progressive display status, and lossless text.

By default graphics status indicator is disabled. This setting replaces the lossless indicator. Previous releases of Citrix Virtual Apps and Desktops enable the lossless indicator instead.

Limitation due to Microsoft quiet time:

After enabling the graphics status indicator, there might be an issue the **first** time a user logs on to Citrix Virtual Apps and Desktops. Four hours elapse before the status indicator icon appears in the notification area.

Display memory limit

This setting specifies the maximum video buffer size in kilobytes for the session.

By default, the display memory limit is 65536 kilobytes.

Specifies the maximum video buffer size in kilobytes for the session. Specify an amount in kilobytes from 128 to 4,194,303. The maximum value of 4,194,303 does not limit the display memory. By default, the display memory is 65536 kilobytes. Using more color depth and higher resolution for connections requires more memory. In legacy graphics mode, if the memory limit is reached, the display degrades according to the "Display mode degrade preference"setting.

For connections requiring more color depth and higher resolution, increase the limit. Calculate the maximum memory required using the equation:

Memory depth in bytes = (color-depth-in-bits-per-pixel) / 8) x (vertical-resolution-in-pixels) x (horizontal-resolution-in-pixels).

For example, with a color depth of 32, vertical resolution of 600, and a horizontal resolution of 800, the maximum memory required is (32 / 8) x (600) x (800) = 1920000 bytes, which yields a display memory limit of 1920 KB.

Color depths other than 32-bit are available only if the Legacy graphics mode policy setting is enabled.

HDX allocates only the amount of display memory needed for each session. So, if only some users require more than the default, there is no negative impact on scalability by increasing the display memory limit.

Display mode degrade preference

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies whether color depth or resolution degrades first when the session display memory limit is reached.

By default, color depth is degraded first.

When the session memory limit is reached, you can reduce the quality of displayed images by choosing whether color depth or resolution is degraded first. When color depth is degraded first, displayed images use fewer colors. When resolution is degraded first, displayed images use fewer pixels per inch.

To notify users when either color depth or resolution is degraded, configure the Notify user when display mode is degraded setting.

Dynamic windows preview

This setting enables or disables the display of seamless windows in:

- Flip-
- Flip 3D
- Taskbar preview
- Windows peek

Windows Aero preview option	Description
Taskbar Preview	When the user hovers over a window's taskbar icon, an image of that window appears above the taskbar.
Windows Peek	When the user hovers over a taskbar preview image, a full-sized image of the window appears on the screen.
Flip	When the user presses ALT+TAB, small preview icons are shown for each open window.
Flip 3D	When the user presses TAB+Windows logo key, large images of the open windows cascade across the screen.

By default, this setting is enabled.

Image caching

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting enables or disables the caching and retrieving of sections of images in sessions. Caching images in sections and retrieving these sections when needed makes scrolling smoother, reduces the amount of data transmitted over the network, and reduces the processing required on the user device.

By default, the image caching setting is enabled.

> **Note:**
>
> The image caching setting controls how images are cached and retrieved. The setting does not control whether images are cached. Images are cached if the Legacy graphics mode setting is enabled.

Legacy graphics mode - not supported. For backward compatibility only

> **Important:**
>
> We do not support legacy graphics mode and Desktop Composition Redirection (DCR) in this release. This policy is included only for backward compatibility when using XenApp 7.15 LTSR, XenDesktop 7.15 LTSR, and previous VDA releases with Windows 7 and Windows 2008 R2.

This setting disables the rich graphics experience. Use this setting to revert to the legacy graphics experience, reducing bandwidth consumption over a WAN or mobile connection. Bandwidth reductions introduced in XenApp and XenDesktop 7.13 make this mode obsolete.

By default, this setting is disabled and users are provided with the rich graphics experience.

Legacy graphics mode is supported with Windows 7 and Windows Server 2008 R2 VDAs.

Legacy graphics mode is not supported on Windows 8.x, 10 or Windows Server 2012, 2012 R2, and 2016.

See CTX202687 for more on optimizing graphics modes and policies in XenApp and XenDesktop 7.6 FP3 or higher.

Maximum allowed color depth

> **Note:**

> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies the maximum color depth allowed for a session.

By default, the maximum allowed color depth is 32 bits per pixel.

This setting applies only to Thinwire drivers and connections. It does not apply to VDAs that have a non-ThinWire driver as the primary display driver, such as VDAs that use a Windows Display Driver Model (WDDM) driver as the primary display driver. For Single-session OS VDAs using a WDDM driver as the primary display driver, such as Windows 8, this setting has no effect. For Windows Multi-session OS VDAs using a WDDM driver, such as Windows Server 2012 R2, this setting might prevent users from connecting to the VDA.

Setting a high color depth requires more memory. To degrade color depth when the memory limit is reached, configure the **Display mode degrade preference** setting. When color depth is degraded, displayed images use fewer colors.

Notify user when display mode is degraded

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting displays a brief explanation to the user when the color depth or resolution is degraded.

By default, notifying users is disabled.

Optimize for 3D graphics workload

This setting configures the appropriate default settings that best suit graphically intense workloads. Enable this setting for users whose workload focuses on graphically intense applications. Apply this policy only in cases where a GPU is available to the session. Any other settings that explicitly override the default settings set by this policy take precedence.

By default, optimize for 3D graphics workload is disabled.

Queuing and tossing

> **Note:**

> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting discards queued images that another image replaces.

By default, queuing and tossing is enabled.

This setting improves response when graphics are sent to the user device. Configuring this setting can cause animations to become choppy because of dropped frames.

Use video codec for compression

Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When **For the entire screen** is chosen the video codec is applied as the default codec for all. When **For actively changing regions** is selected the video codec is used for areas where there is constant change on the screen, other data uses still image compression and bitmap caching. When video decoding is not available on the endpoint, or when you specify **Do not use video codec**, a combination of still image compression and bitmap caching is used. When **Use when preferred** is selected, the system chooses, based on various factors. The results might vary between versions as the selection method is enhanced.

Select **Use when preferred** to allow the system to make its best effort to choose appropriate settings for the current scenario.

Select **For the entire screen** to optimize for improved user experience and bandwidth, especially in cases with heavy use of server-rendered video and 3D graphics.

Select **For actively changing regions** to optimize for improved video performance, especially in low bandwidth, while maintaining scalability for static and slowly changing content. This setting is supported in multi-monitor deployments.

Select **Do not use video codec** to optimize for server CPU load and for cases that do not have numerous server-rendered videos or other graphically intense applications.

The default is **Use when preferred**.

Use hardware encoding for video

This setting allows the use of graphics hardware, if available, to compress screen elements with video codec. If such hardware is not available, the VDA falls back to CPU-based encoding using the software video codec.

The default option for this policy setting is **Enabled**.

Multiple monitors are supported.

Any Citrix Workspace app that supports video decoding can be used with hardware encoding.

NVIDIA

For NVIDIA GRID GPUs, hardware encoding is supported with VDAs for Multi-session OS and Single-session OS.

NVIDIA GPUs must support NVENC hardware encoding. See NVIDIA video codec SDK for a list of supported GPUs.

NVIDIA GRID requires driver version 3.1 or higher. NVIDIA Quadro requires driver version 362.56 or higher. Citrix recommends drivers from the NVIDIA Release R361 branch.

Lossless text is not compatible with NVENC hardware encoding. If you enabled lossless text, lossless text takes priority over NVENC hardware encoding.

Selective use of the H.264 hardware codec for actively changing regions is supported.

Visually lossless (YUV 4:4:4) compression is supported. Visually lossless (graphics policy setting, Allow visually lossless compression) requires Citrix Workspace app 1808 or higher or Citrix Receiver for Windows 4.5 or higher.

Intel

For Intel Iris Pro graphics processors, hardware encoding is supported with VDAs for Single-session OS and Multi-session OS.

Intel Iris Pro graphics processors in the Intel Broadwell processor family and later are supported. Intel Remote Displays SDK version 1.0 is required and can be downloaded from Intel website: Remote Displays SDK.

Lossless text is supported only when Video codec policy is set for the entire screen and the **Optimize for 3D graphics workload** policy is disabled.

Visually lossless (YUV 4:4:4) is not supported.

The Intel encoder provides a good user experience for up to eight encoding sessions (for example one user using eight monitors or eight users using a monitor each). If more than eight encoding sessions are required, check how many monitors the virtual machine connects with. To maintain a good user experience, the administrator can decide to configure this policy setting on a per user or per machine basis.

AMD

For AMD, hardware encoding is supported with VDAs for Single-session OS.

AMD GPUs must support the RapidFire SDK. For example, the AMD Radeon Pro or FirePro GPUs.

For encoding to work, install the latest AMD drivers. You can download those drivers from https://www.amd.com/en/support.

Lossless text is not compatible with AMD hardware encoding. If you enabled lossless text, lossless text takes priority over AMD hardware encoding.

Selective use of the H.264 hardware codec for actively changing regions is supported.

Caching policy settings

February 6, 2020

The Caching section contains policy settings that enable caching image data on user devices when client connections are limited in bandwidth.

Persistent cache threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting caches bitmaps on the hard drive of the user device. This enables re-use of large, frequently-used images from previous sessions.

By default, the threshold is 3000000 bits per second.

The threshold value represents the point below which the Persistent Cache feature will take effect. For example, using the default value, bitmaps are cached on the hard drive of the user device when bandwidth falls below 3000000 bps.

Framehawk policy settings

February 6, 2020

> **Important:**
>
> As of Citrix Virtual Apps and Desktops 7 1903, Framehawk is no longer supported. Instead, use Thinwire with adaptive transport enabled.

The Framehawk section contains policy settings that enable and configure the Framehawk display channel on the server.

Framehawk display channel

When enabled, the server attempts to use the Framehawk display channel for the user's graphics and input remoting. That display channel will use UDP to provide a better user experience on networks with high loss and latency characteristics; however, it may also use more server resources and bandwidth than other graphics modes.

By default, the Framehawk display channel is disabled.

Framehawk display channel port range

This policy setting specifies the range of UDP port numbers (in the form *lowest port number,highest port number)* the VDA uses to exchange Framehawk display channel data with the user device. The VDA attempts to use each port, starting with the lowest port number and incrementing for each subsequent attempt. The port handles inbound and outbound traffic.

By default, the port range is 3224,3324.

Keep alive policy settings

February 6, 2020

The Keep Alive section contains policy settings for managing ICA keep-alive messages.

ICA keep alive timeout

This setting specifies the number of seconds between successive ICA keep-alive messages.

By default, the interval between keep-alive messages is 60 seconds.

Specify an interval between 1-3600 seconds in which to send ICA keep-alive messages. Do not configure this setting if your network monitoring software is responsible for closing inactive connections.

ICA keep alives

This setting enables or disables sending ICA keep-alive messages periodically.

By default, keep-alive messages are not sent.

Enabling this setting prevents broken connections from being disconnected. If the server detects no activity, this setting prevents Remote Desktop Services (RDS) from disconnecting the session. The

server sends keep-alive messages every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

ICA keep-alive does not work if you are using session reliability. Configure ICA keep-alive only for connections that are not using Session Reliability.

Related policy settings: Session reliability connections.

Local App Access policy settings

February 10, 2021

The Local App Access section contains policy settings that manage the integration of users' locally installed applications with hosted applications in a hosted desktop environment.

Allow Local App Access

This setting allows or prevents the integration of users' locally installed applications with hosted applications within a hosted desktop environment.

When a user starts a locally installed application, that application appears to run within their virtual desktop, even though it is actually running locally.

If you set the **Allow local app access** policy setting to **Enabled**, browser content redirection isn't supported.

By default, Local App Access is prohibited.

URL redirection block list

This setting specifies websites that are redirected to and started in the local Web browser. These websites might include websites requiring locale information, such as msn.com or newsgoogle.com, or websites containing rich media content that are better rendered on the user device.

By default, no sites are specified.

URL redirection allow list

This setting specifies websites that are rendered in the environment in which they are started.

By default, no sites are specified.

Mobile experience policy settings

February 6, 2020

The Mobile Experience section contains policy settings for handling the Citrix Mobility Pack.

Automatic keyboard display

This setting enables or disables the automatic display of the keyboard on mobile device screens.

By default, the automatic display of the keyboard is disabled.

Launch touch-optimized desktop

This setting is disabled and not available for Windows 10 or Windows Server 2016 machines.

This setting determines the overall Citrix Workspace app interface behavior by allowing or prohibiting a touch-friendly interface that is optimized for tablet devices.

By default, a touch-friendly interface is used.

To use only the Windows interface, set this policy setting to Prohibited.

Remote the combo box

This setting determines the types of combo boxes you can display in sessions on mobile devices. To display the device-native combo box control, set this policy setting to Allowed. When this setting is allowed, a user can change a Citrix Workspace app for iOS session setting to use the Windows combo box.

By default, the Remote the combo box feature is prohibited.

Multimedia policy settings

May 22, 2024

The Multimedia section contains policy settings for managing streaming HTML5 and Windows audio and video in user sessions.

> **Warning**
>
> 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.

Multimedia policies

By default, all multimedia policies set on the Delivery Controller are stored in these registries:

Machine policies:

```
HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies
```

User policies:

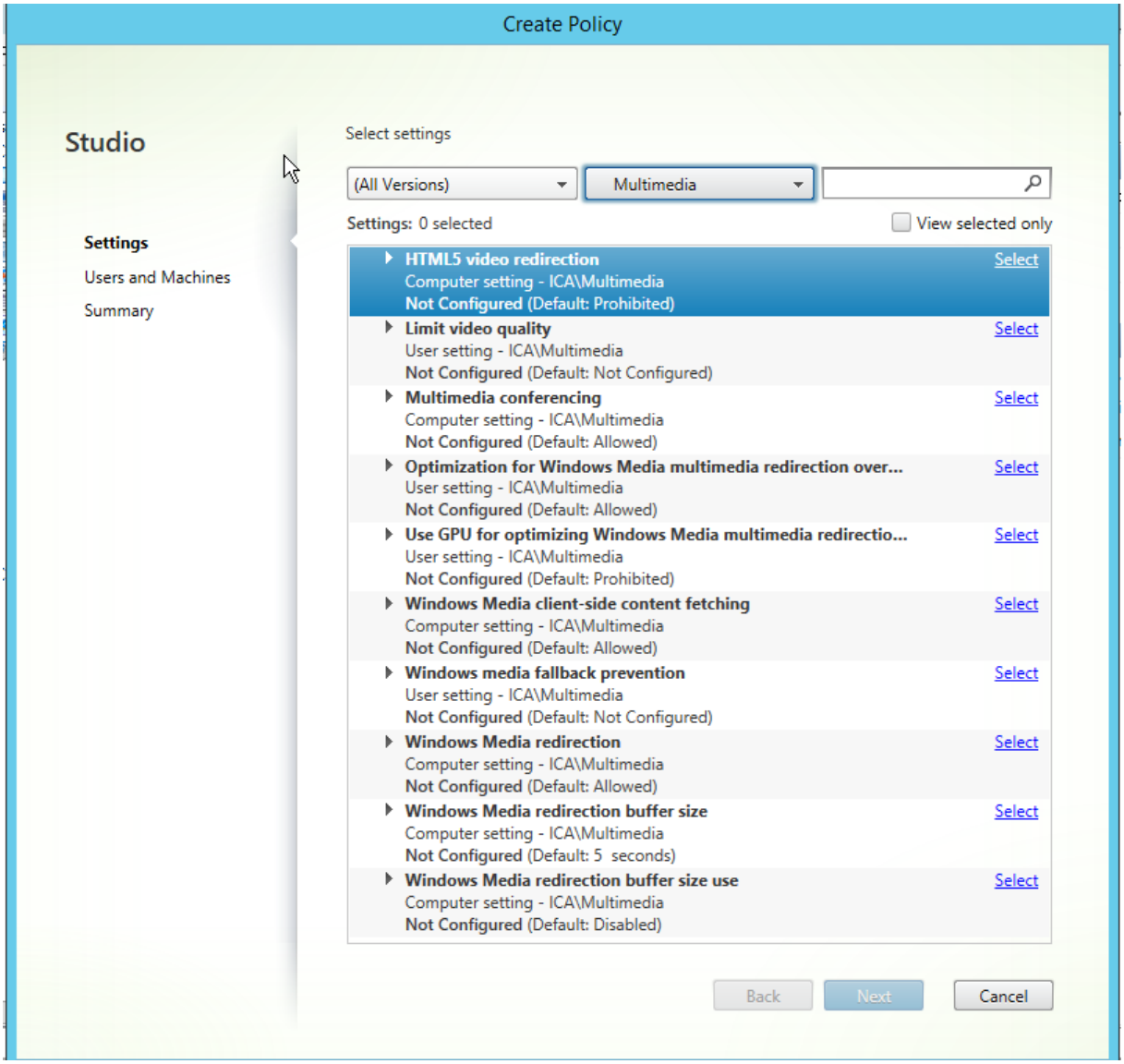
```
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ User Session ID } \User\
MultimediaPolicies
```

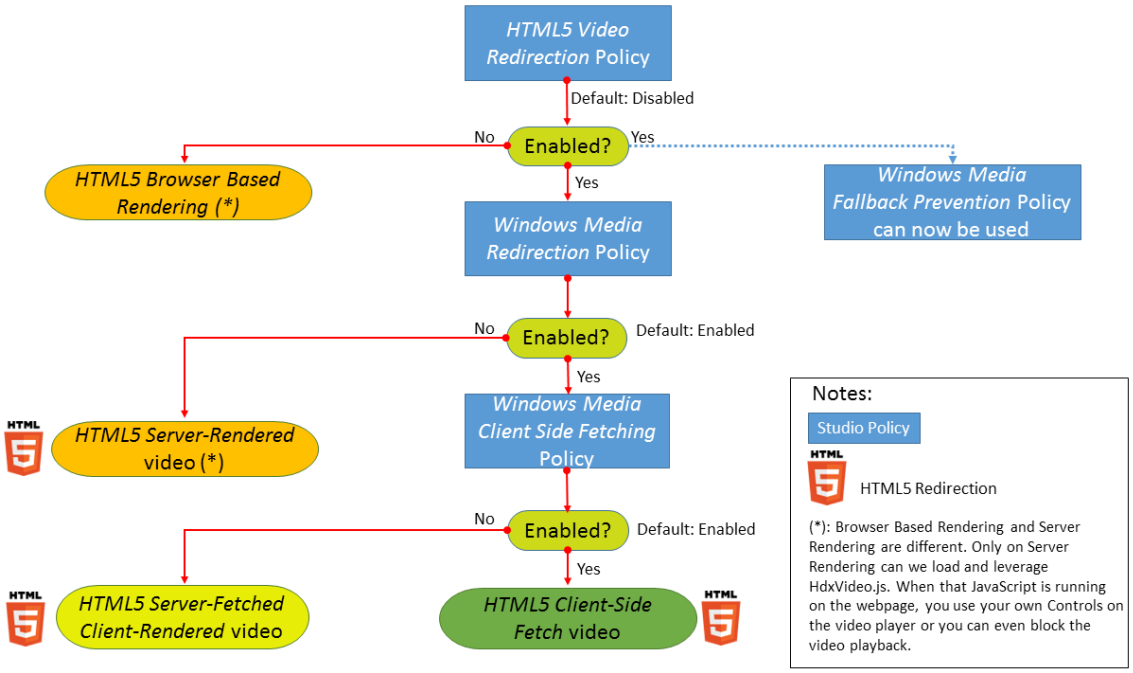
To locate the current user session ID, issue the **qwinsta** command on the Windows command line.

HTML5 video redirection

Controls and optimizes the way Citrix Virtual Apps and Desktops servers deliver HTML5 multimedia web content to users.

By default, this setting is disabled.





In this release, this feature is available for controlled web pages only. It requires the addition of JavaScript to the web pages where the HTML5 multimedia content is available, for example, videos on an internal training site.

To configure HTML5 video redirection:

1. Copy the file, **HdxVideo.js**, from %Program Files%/Citrix/ICA Service/HTML5 Video Redirection on the VDA install to the location of your internal web page.
2. Insert this line into your web page (if your web page has other scripts, include **HdxVideo.js** before those scripts):
   ```
   <script src="HdxVideo.js"type="text/javascript"\></script>
   ```

Note: If HdxVideo.js is not in the same location as your web page, use the **src** attribute to specify the full path to it.

If the JavaScript has not been added to your controlled web pages and the user plays an HTML5 video, Citrix Virtual Apps and Desktops default to the server-side rendering.

For redirection of HTML5 videos to work, allow ***Windows Media Redirection***. This policy is mandatory for Server Fetch Client Render, and necessary for Client Side Fetching (which in turn also requires *Windows Media client-side content fetching* to be Allowed).

Microsoft Edge doesn't support this feature.

HdxVideo.js replaces the browser HTML5 Player controls with its own. To check that the HTML5 video redirection policy is in effect on a certain website, compare the player controls to a scenario where the **HTML5 video redirection** policy is Prohibited:

(Citrix custom controls when the policy is Allowed)

(Native webpage controls when the policy is Prohibited or not configured)

The following video controls are supported:

- play
- pause
- seek
- repeat
- audio
- full screen

You can view an HTML5 video redirection test page at https://www.citrix.com/solutions/html5-redirect.html.

TLS, HTML5 video redirection, and browser content redirection

You can use HTML5 video redirection to redirect videos from HTTPS websites or browser content redirection to redirect the entire website. The JavaScript injected into those websites must establish a TLS connection to the Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) running on the VDA. To achieve this redirection and maintain the TLS integrity of the webpage, two custom certificates are generated by the Citrix HDX HTML5 Video Redirection Service in the certificate store on the VDA.

HdxVideo.js uses Secure Websockets to communicate with WebSocketService.exe running on the VDA. This process runs as a Local System account, and performs SSL termination and user session mapping.

WebSocketService.exe is listening on 127.0.0.1 port 9001.

Limit video quality

This setting applies only to Windows Media and not to HTML5. It requires you enable **Optimization for Windows Media multimedia redirection over WAN**.

This setting specifies the maximum video quality level allowed for an HDX connection. When configured, maximum video quality is limited to the specified value, ensuring that multimedia Quality of Service (QoS) is maintained within an environment.

By default, this setting is not configured.

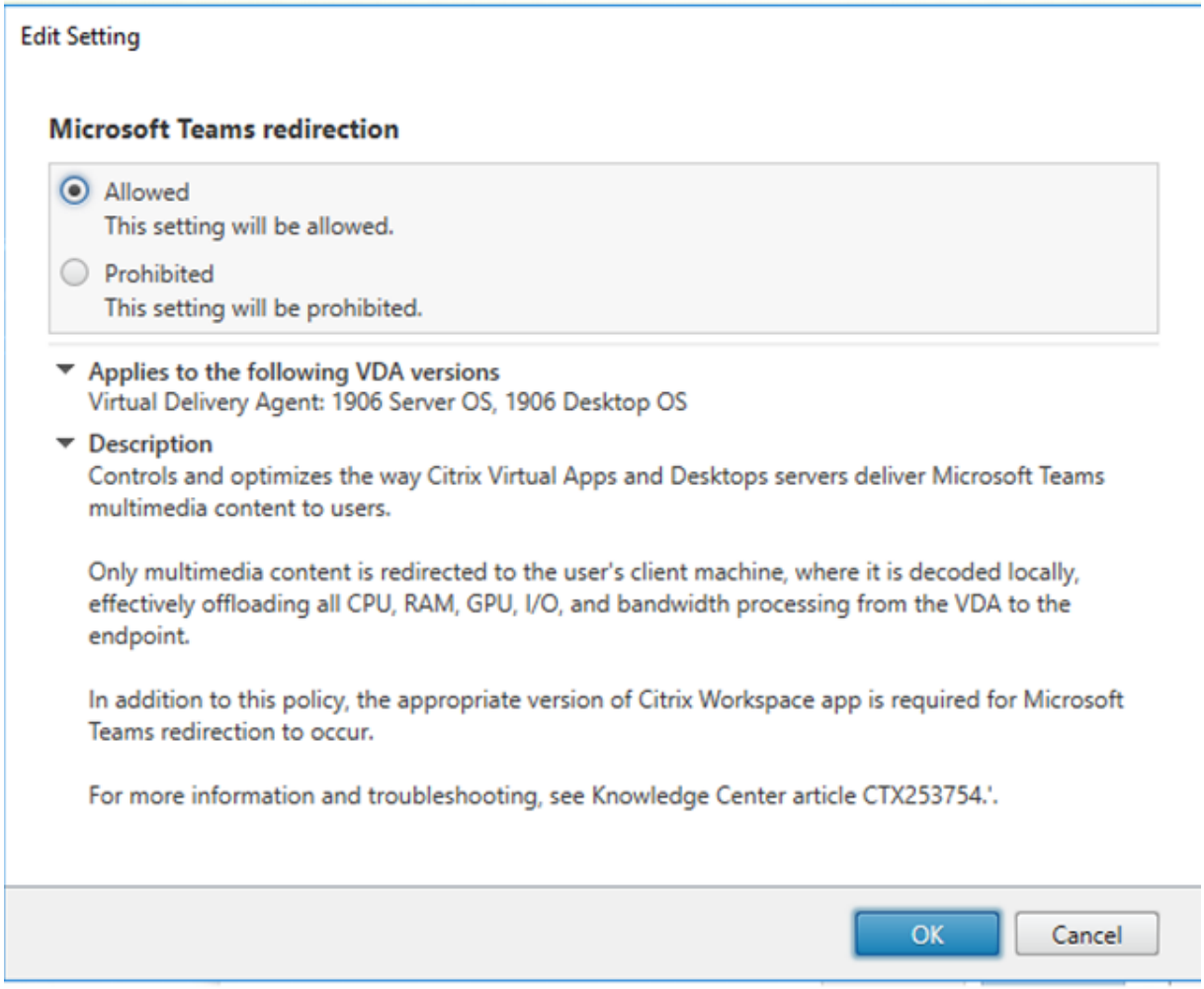
To limit the maximum video quality level allowed, choose one of the following options:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Playing multiple videos simultaneously on the same server consumes large amounts of resources and may impact server scalability.

Microsoft Teams redirection

This setting enables optimization of Microsoft Teams, based on the HDX technology.



If this policy is enabled, and you're using a supported version of Citrix Workspace app, this registry key is set to **1** on the VDA. The Microsoft Teams application reads the key to load in VDI mode. Please note it is not required to set the registry key manually.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Name: MSTeamsRedirSupport

Value: DWORD (1 - on, 0 - off)

> **Note:**
>
> If you are using version 1906.2 VDAs or higher with older Controller versions (for example, version 7.15), which do not have the policy available in Studio, HDX optimization is enabled by default in the VDA. If the Workspace app version is 1907 or higher, Teams launches in optimized mode.
>
> In this case, to disable the feature for specific users, you can override the registry setting by using a group policy to apply a logon script to the user's organizational unit.

By default, Microsoft Teams redirection is enabled.

Multimedia conferencing

This setting allows or prevents the use of optimized webcam redirection technology by video conferencing applications.

By default, video conferencing support is allowed.

When adding this setting to a policy, ensure that the Windows Media redirection setting is present and set to Allowed (the default).

When using multimedia conferencing, ensure that the following conditions are met:

- Manufacturer-supplied drivers for the webcam used for multimedia conferencing are installed on the client.
- Connect the webcam to the user device before initiating a video conferencing session. The server uses only one installed webcam at any given time. If multiple webcams are installed on the user device, the server attempts to use each webcam in succession until a video conferencing session is created successfully.

This policy is not needed when redirecting the web cam using Generic USB redirection. In that case, install the webcam drivers on the VDA.

Optimization for Windows Media multimedia redirection over WAN

This setting applies only to Windows Media and not to HTML5. The setting enables real-time multimedia transcoding, allowing audio and video media streaming to mobile devices over degraded net-

works, and enhancing the user experience by improving how Windows Media content is delivered over a WAN.

By default, the delivery of Windows Media content over the WAN is optimized.

When adding this setting to a policy, make sure the **Windows Media Redirection** setting is present and set to **Allowed**.

When this setting is enabled, real-time multimedia transcoding is deployed automatically as needed to enable media streaming, providing a seamless user experience even in extreme network conditions.

Use GPU for optimizing Windows Media multimedia redirection over WAN

This setting applies only to Windows Media and enables real-time multimedia transcoding to be done in the Graphics Processing Unit (GPU) on the Virtual Delivery Agent (VDA). It improve server scalability. GPU transcoding is available only if the VDA has a supported GPU for hardware acceleration. Otherwise, transcoding falls back to the CPU.

Note: GPU transcoding is supported only on NVIDIA GPUs.

By default, using the GPU on the VDA to optimize the delivery of Windows Media content over the WAN is prohibited.

When adding this setting to a policy, make sure the Windows Media Redirection and Optimization for Windows Media multimedia redirection over WAN settings are present and set to Allowed.

Windows media fallback prevention

This setting applies to browser content redirection, HTML5, and Windows Media. For it to work with HTML5, set the **HTML5 video redirection** policy to **Allowed**.

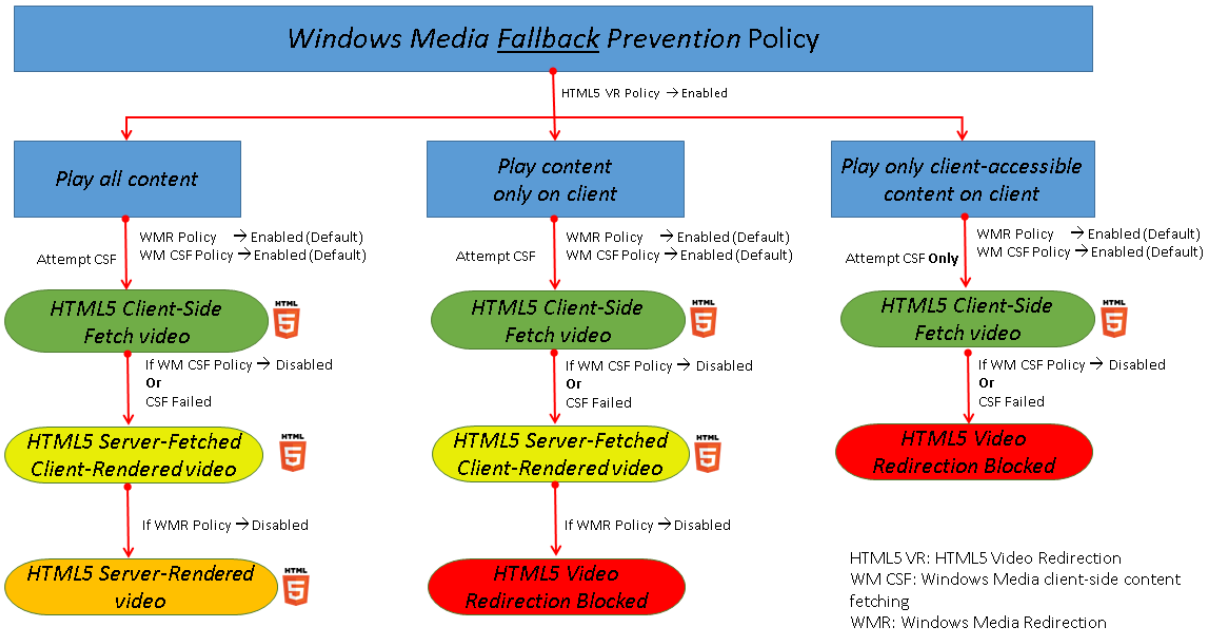
Administrators can use the Windows media fallback prevention policy setting to specify the methods that will be attempted to deliver streamed content to users.

By default, this setting is not configured. When the setting is set to Not Confgured, the behavior is the same as **Play all content**.

To configure this setting, choose one of the following options:

- **Play all content**. Attempt client-side content fetching, then Windows Media Redirection. If unsuccessful, play content on the server.
- **Play all content only on client**. Attempt client-side fetching, then Windows Media Redirection. If unsuccessful, the content does not play.
- **Play only client-accessible content on client**. Attempt only client-side fetching. If unsuccessful, the content does not play.

When the content does not play, the error message “Company has blocked video because of lack of resources”displays in the player window (for a default duration of 5 seconds).



The duration of this error message can be customized with the following registry key on the VDA. If the registry entry does not exist, the duration defaults to 5 seconds.

The registry path varies depending on architecture of the VDA:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

or

\HKLM\SOFTWARE\Citrix\HdxMediastream

Registry key:

Name: VideoLoadManagementErrDuration

Type: DWORD

Range: 1 - up to DWORD limit (default = 5)

Unit: seconds

Windows Media client-side content fetching

This setting applies to both HTML5 and Windows Media. The setting enables a user device to stream multimedia files directly from the source provider on the internet or intranet, rather than through the XenApp or XenDesktop host server.

By default, this setting is **Allowed**. Allowing this setting improves network usage and server scalability by moving any processing on the media from the host server to the user device. It also removes the requirement that an advanced multimedia framework such as Microsoft DirectShow or Media Foundation be installed on the user device. the user device requires only the ability to play a file from a URL

When adding this setting to a policy, make sure the **Windows Media Redirection** setting is present and set to **Allowed**. If **Windows Media Redirection** is disabled, the streaming of multimedia files to the user device direct from the source provider is also disabled.

Windows Media redirection

This setting applies to both HTML5 and Windows Media and controls and optimizes the way servers deliver streaming audio and video to users.

By default, this setting is **Allowed**. For HTML5, this setting doesn't take effect if the policy **HTML5 video redirection** is **Prohibited**.

Allowing this setting increases the quality of audio and video rendered from the server to a level that compares with audio and video played locally on a user device. The server streams multimedia to the client in the original, compressed form and allows the user device to decompress and render the media.

Windows Media redirection optimizes multimedia files that are encoded with codecs that adhere to Microsoft DirectShow, DirectX Media Objects (DMO), and Media Foundation standards. To play back a given multimedia file, a codec compatible with the encoding format of the multimedia file must be present on the user device.

By default, audio is disabled on Citrix Workspace app. To allow users to run multimedia applications in ICA sessions, turn on audio or give users permission to turn on audio in their Citrix Workspace app interface.

Select **Prohibited** only if playing media using Windows Media redirection appears worse than when rendered using basic ICA compression and regular audio. This is rare but can happen under low bandwidth conditions, for example, with media with a very low frequency of key frames.

Windows Media Redirection buffer size

This setting is a legacy and does not apply to HTML5.

This setting specifies a buffer size from 1 to 10 seconds for multimedia acceleration.

By default, the buffer size is 5 seconds.

Windows Media Redirection buffer size use

This setting is a legacy and does not apply to HTML5.

This setting enables or disables using the buffer size specified in the **Windows Media Redirection buffer size** setting.

By default, the buffer size specified is not used.

If this setting is disabled or if the Windows Media Redirection buffer size setting is not configured, the server uses the default buffer size value (five seconds).

Multi-stream connections policy settings

December 29, 2020

The Multi-Stream Connections section contains policy settings for managing Quality of Service prioritization for multiple ICA connections in a session.

Audio over UDP

This setting allows or prevents audio over UDP on the server.

By default, audio over UDP is allowed on the server.

When enabled, this setting opens a UDP port on the server to support all connections configured to use Audio over UDP Real-time Transport.

Audio UDP port range

This setting specifies the range of port numbers (lowest port number, highest port number) used by the Virtual Delivery Agent (VDA) to exchange audio packet data with the user device. The VDA attempts to use each UDP port pair to exchange data with the user device, starting with the lowest and incrementing by two for each subsequent attempt. Each port handles both inbound and outbound traffic.

By default, this range is set to 16500,16509.

Multi-Port policy

This setting specifies the TCP ports to be used for ICA traffic and establishes the network priority for each port.

By default, the primary port (2598) has a High priority.

When you configure ports, you can assign the following priorities:

- Very High - for real-time activities, such as webcam conferences
- High - for interactive elements, such as screen, keyboard, and mouse
- Medium - for bulk processes, such as client drive mapping
- Low - for background activities, such as printing

Each port must have a unique priority. For example, you cannot assign a Very High priority to both CGP port 1 and CGP port 3.

To remove a port from prioritization, set the port number to 0. You cannot remove the primary port and you cannot change its priority level.

When configuring this setting, restart the server. This setting takes effect only when the Multi-Stream computer setting policy setting is enabled.

Multi-Stream computer setting

This setting enables or disables Multi-Stream on the server.

By default, Multi-Stream is disabled. Configure the Multi-Stream computer policy setting if you use Citrix SD-WAN or third-party routers to achieve the desired Quality of Service.

When configuring this setting, reboot the server to ensure that changes take effect.

> **Important:**
>
> Using this policy setting with bandwidth limit policy settings such as Overall session bandwidth limit might produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

Multi-Stream user setting

This setting enables or disables Multi-Stream on the user device.

By default, Multi-Stream is disabled for all users. Configure the Multi-Stream user setting if you use Citrix SD-WAN or third-party routers to achieve the desired Quality of Service.

This setting takes effect only on hosts where the Multi-Stream computer setting policy setting is enabled.

> **Important:**
>
> Using this policy setting with bandwidth limit policy settings such as Overall session bandwidth limit might produce unexpected results. When including this setting in a policy, ensure that band-

> width limit settings are not included.

Multi-Stream virtual channel assignment settings

> **Important:**
>
> The following settings apply only to 1912 LTSR CU1 or later.

This setting specifies the ICA stream the virtual channels are assigned to when multi-stream is used.

If you do not configure these settings, virtual channels are kept in their default stream. To assign a virtual channel to an ICA stream, select the desired stream number (0, 1, 2, 3) from the **Stream Number** list next to the virtual channel name.

If there is a custom virtual channel in use in the environment, click **Add**, specify the virtual channel name in the text box under **Virtual Channels**, and select the desired stream number from the **Stream Number** list next to it. The name you specify must be the actual virtual channel name and not a friendly name. For example, CTXSBR instead of Citrix Browser Acceleration.

These settings take effect only when you've enabled the multi-stream computer setting.

By default, the virtual channels and their stream assignments are:

- Audio: 0
- Browser Content Redirection: 2
- Client COM Port Mapping: 3
- Client Drive Mapping: 2
- Client Printer Mapping: 3
- Clipboard: 2
- CTXDND: 1
- DVC plug-ins (Static VC name auto-generated from DVC plug-in Friendly Name, or admin-assigned): 2
- End User Experience Monitoring: 1
- File Transfer (HTML5 Receiver): 2
- Generic Data Transfer: 2
- ICA Control: 1
- Input Method Editor: 1
- Legacy Client Printer Mapping (COM1): 1, 3
- Legacy Client Printer Mapping (COM2): 2, 3
- Legacy Client Printer Mapping (LPT1): 1, 3
- Legacy Client Printer Mapping (LPT2): 2, 3
- License Management: 1
- Microsoft Teams/WebRTC Redirection: 1

- Mobile Receiver: 1
- MultiTouch: 1
- Port Forwarding: 2
- Remote Audio and Video Extensions (RAVE): 2
- Seamless (Transparent Window Integration): 1
- Sensor and Location: 1
- Smart Card: 1
- Thinwire Graphics: 1
- Transparent UI Integration/Logon Status: 2
- TWAIN Redirection: 2
- USB: 2
- Zero Latency Font and Keyboard: 2
- Zero Latency Data Channel: 2

For more information on virtual channel assignments and priorities, see the Knowledge Center article CTX131001.

Port redirection policy settings

February 6, 2020

The Port Redirection section contains policy settings for client LPT and COM port mapping.

For Virtual Delivery Agent versions **earlier than 7.0**, use the following policy settings to configure port redirection. For VDA versions **7.0 through 7.8**, configure these settings using the registry; see Configure COM Port and LPT Port Redirection settings using the registry. For VDA version **7.9**, use the following policy settings.

Auto connect client COM ports

This setting enables or disables automatic connection of COM ports on user devices when users log on to a site.

By default, client COM ports are not automatically connected.

Auto connect client LPT ports

This setting enables or disables automatic connection of LPT ports on user devices when users log on to a site.

By default, client LPT ports are not connected automatically.

Client COM port redirection

This setting allows or prevents access to COM ports on the user device.

By default, COM port redirection is prohibited.

The following policy settings are related:

- COM port redirection bandwidth limit
- COM port redirection bandwidth limit percent

Client LPT port redirection

This setting allows or prevents access to LPT ports on the user device.

By default, LPT port redirection is prohibited.

LPT ports are used only by legacy applications that send print jobs to the LPT ports and not to the print objects on the user device. Most applications today can send print jobs to printer objects. This policy setting is necessary only for servers that host legacy applications that print to LPT ports.

Note, although Client COM port redirection is bi-directional, LPT port redirection is output only and limited to \\client\LPT1 and \\client\LPT2 within an ICA session.

The following policy settings are related:

- LPT port redirection bandwidth limit
- LPT port redirection bandwidth limit percent

Printing policy settings

February 6, 2020

The Printing section contains policy settings for managing client printing.

Client printer redirection

This setting controls whether client printers are mapped to a server when a user logs on to a session.

By default, client printer mapping is allowed. If this setting is disabled, the PDF printer for the session is not auto-created.

Related policy settings: auto-create client printers

Default printer

This setting specifies how the default printer on the user device is established in a session.

By default, the user's current printer is used as the default printer for the session.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do not adjust the user's default printer. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session is the first printer auto-created in the session, which is either:

- The first printer added locally to the Windows server in **Control Panel > Devices** and **Printers**.
- The first auto-created printer, if there are no printers added locally to the server.

You can use this option to present users with the nearest printer through profile settings (known as proximity printing).

Printer assignments

This setting provides an alternative to the Default printer and Session printers settings. Use the individual Default printer and Session printers settings to configure behaviors for a site, large group, or organizational unit. Use the **Printer assignments** setting to assign a large group of printers to multiple users.

This setting specifies how the default printer on the listed user devices is established in a session.

By default, the user's current printer is used as the default printer for the session.

It also specifies the network printers to be auto-created in a session for each user device. By default, no printers are specified.

- When setting the default printer value:

  To use the current default printer for the user device, select Do not adjust.

  To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do no adjust. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session is the first printer auto-created in the session, which is either:

  - The first printer added locally to the Windows server in Control Panel > Devices and Printers.
  - The first auto-created printer, if there are no printers added locally to the server.

- When setting the session printers value: to add printers, type the UNC path of the printer you want to auto-create. After adding the printer, you can apply customized settings for the current session at every logon.

Printer auto-creation event log preference

This setting specifies the events that are logged during the printer auto-creation process. You can choose to log no errors or warnings, only errors, or errors and warnings.

By default, errors and warnings are logged.

An example of a warning is an event in which a printer's native driver could not be installed and the Universal print driver is installed instead. To use the Universal print driver in this scenario, configure the Universal print driver usage setting to Use universal printing only or Use universal printing only if requested driver is unavailable.

Session printers

This setting specifies the network printers to be auto-created in a session. Inside the ICA/HDX session, the Citrix Print Manager service (CpSvc.exe) creates a network printer connection during the session logon for each network printer specified in the **Session Printer** policy setting. It deletes the printers during the session logoff. By default, no printers are specified.

In the **Session Printer** policy setting, the network printers can reside on a Windows Print Server or a Citrix Universal Print Server.

- **Windows Print Server:** Shares one or more network printers. It also has the native printer drivers required to use the network printers.
- **Universal Print Server:** A Windows Print Server where the Citrix Universal Print Server software has been installed.

When using a Windows Print Server, the Citrix Print Manager service creates the network printer connections using native printer drivers. The Citrix Virtual Apps server must have the native printer drivers installed on it.

When using a Citrix Universal Print Server, the Citrix Print Manager service creates the network printer connections using either native printer drivers, Citrix Universal Printer Driver, or Citrix Universal XPS Printer Driver. The driver that you use is controlled by the Universal Print Driver usage policy setting.

All Windows printer drivers currently fall within either the v3 or v4 driver version. For more information, see Support for the Microsoft V3 and V4 Printer Driver Architectures.

To add session printers and verify if they appear in the sessions, complete the following procedure:

1. In Citrix Studio, navigate to the **Policies** tab.
2. Enable the session printing policy in the **Edit Policy** dialog box.
3. In the policy, add the session printer. To add printers, type the UNC path of the printer you want to auto-create. After adding the printer, you can apply customized settings for the current session at every logon. The session printer must display in the list.

4. After the policy has been set, the published application might not display session printers. This issue might occur because the printer driver is missing from the Citrix Virtual Apps server or the policy has been created but not enabled.

   > Note:
   >
   > If the printer driver has not been installed on the Citrix Virtual Apps server, you might experience the most common mistake with session printers where administrators forget to install the printer driver on the Citrix Virtual Apps server.

5. Start the published desktop and manually add the session printer in **Devices and Printers > Control Panel**.
6. If this fails, investigate the communication between the Citrix Virtual Apps server and print server. Consider running a test with RDP.

Wait for printers to be created (server desktop)

This setting allows or prevents a delay in connecting to a session so that server desktop printers can be auto-created.

By default, a connection delay does not occur.

Client printers policy settings

July 13, 2021

The Client Printers section contains policy settings for client printers, including settings to auto-create client printers, retain printer properties, and connect to print servers.

Auto-create client printers

This setting specifies the client printers that are auto-created. This setting overrides default client printer auto-creation settings.

By default, all client printers are auto-created.

This setting takes effect only if the Client printer redirection setting is present and set to Allowed.

When adding this setting to a policy, select an option:

- Auto-create all client printers automatically creates all printers on a user device.

- Auto-create the client's default printer only automatically creates only the printer selected as the default printer on the user device.
- Auto-create local (non-network) client printers only automatically creates only printers directly connected to the user device through an LPT, COM, USB, TCP/IP, or other local port.
- Do not auto-create client printers turns off autocreation for all client printers when users log on. This causes the Remote Desktop Services (RDS) settings for autocreating client printers to override this setting in lower priority policies.

Auto-create generic universal printer

This setting enables or disables auto-creation of the generic Citrix Universal Printer object for sessions where a user device compatible with Universal Printing is in use.

By default, the generic Universal Printer object is not auto-created.

The following policy settings are related:

- Universal print driver usage
- Universal driver preference

Auto-create PDF universal printer

This setting enables or disables auto-creation of the Citrix PDF printer for sessions using Citrix Workspace app for Windows (starting from VDA 7.19), Citrix Workspace app for HTML5, or Citrix Workspace app for Chrome.

By default, the Citrix PDF printer is not auto-created.

Client printer names

This setting selects the naming convention for auto-created client printers.

By default, standard printer names are used.

Select Standard printer names to use printer names such as "HPLaserJet 4 from clientname in session 3."

Select Legacy printer names to use old-style client printer names and preserve backward compatibility for users or groups using MetaFrame Presentation Server 3.0 or earlier. An example of a legacy printer name is "Client/clientname#/HPLaserJet 4."This option is less secure.

Note: This option is provided only for backwards compatibility with legacy versions of XenApp and XenDesktop.

Direct connections to print servers

This setting enables or disables direct connections from the virtual desktop or server hosting applications to a print server for client printers hosted on an accessible network share.

By default, direct connections are enabled.

Enable direct connections if the network print server is not across a WAN from the virtual desktop or server hosting applications. Direct communication results in faster printing if the network print server and the virtual desktop or server hosting applications are on the same LAN.

Disable direct connections if the network is across a WAN or has substantial latency or limited bandwidth. Print jobs are routed through the user device where they are redirected to the network print server. Data sent to the user device is compressed, so less bandwidth is consumed as the data travels across the WAN.

If two network printers have the same name, the printer on the same network as the user device is used.

Printer driver mapping and compatibility

This setting specifies the driver substitution rules for auto-created client printers.

This setting is configured to exclude Microsoft OneNote and XPS Document Writer from the auto-created client printers list.

When you define driver substitution rules, you can allow or prevent printers to be created with the specified driver. Additionally, you can allow created printers to use only universal print drivers. Driver substitution overrides or maps printer driver names the user device provides, substituting an equivalent driver on the server. This gives server applications access to client printers that have the same drivers as the server, but different driver names.

You can add a driver mapping, edit an existing mapping, override custom settings for a mapping, remove a mapping, or change the order of driver entries in the list. When adding a mapping, enter the client printer driver name and then select the server driver you want to substitute.

Printer properties retention

This setting specifies whether or not to store printer properties and where to store them.

By default, the system determines if printer properties are stored on the user device, if available, or in the user profile.

When adding this setting to a policy, select an option:

- Saved on the client device only is for user devices that have a mandatory or roaming profile that is not saved. Choose this option only if all the servers in your farm are running XenApp 5 and above and your users are using Citrix online plug-in versions 9 through 12.x, or Citrix Receiver 3.x.
- Retained in user profile only is for user devices constrained by bandwidth (this option reduces network traffic) and logon speed or for users with legacy plug-ins. This option stores printer properties in the user profile on the server and prevents any properties exchange with the user device. Use this option with MetaFrame Presentation Server 3.0 or earlier and MetaFrame Presentation Server Client 8.x or earlier. Note that this is applicable only if a Remote Desktop Services (RDS) roaming profile is used.
- Held in profile only if not saved on client allows the system to determine where printer properties are stored. Printer properties are stored either on the user device, if available, or in the user profile. Although this option is the most flexible, it can also slow logon time and use extra bandwidth for system-checking.
- Do not retain printer properties prevents storing printer properties.

Retained and restored client printers

This setting enables or disables the retention and re-creation of printers on the user device. By default, client printers are auto-retained and auto-restored.

Retained printers are user-created printers that are created again, or remembered, at the start of the next session. When Citrix Virtual Apps recreates a retained printer, it considers all policy settings except the Auto-create client printers setting.

Restored printers are printers fully customized by an administrator, with a saved state that is permanently attached to a client port.

Citrix PDF Universal Printer driver

The Citrix PDF Universal Printer driver enables users to print documents opened with hosted applications or applications running on virtual desktops delivered by Citrix Virtual Apps and Desktops. When a user selects the Citrix PDF Printer option, the driver converts the file to PDF and transfers the PDF to the local device. The PDF is then opened for viewing and printing from a locally attached printer. PDF is one of the formats supported with Citrix Universal Printing (in addition to EMF and XPS).
The PDF printer can be enabled, configured, and set as default using Citrix Policy. The Citrix PDF Printer option is available to users of Citrix Workspace app for Windows, Chrome, and HTML5.

> **Note:**
>
> A PDF viewer is required for Windows endpoints. The client must have an application that has

> file type association registered on Windows to open PDF files.

Drivers policy settings

February 6, 2020

The Drivers section contains policy settings related to printer drivers.

Automatic installation of in-box printer drivers

> **Note**
>
> This policy does not support VDAs in this release.

This setting enables or disables the automatic installation of printer drivers from the Windows in-box driver set or from driver packages staged on the host using pnputil.exe /a.

By default, these drivers are installed as needed.

Universal driver preference

This setting specifies the order in which universal printer drivers are used, beginning with the first entry in the list.

By default, the preference order is:

- EMF
- XPS
- PCL5c
- PCL4
- PS

You can add, edit, or remove drivers, and change the order of drivers in the list.

Universal print driver usage

This setting specifies when to use universal printing.

By default, universal printing is used only if the requested driver is unavailable.

Universal printing employs generic printer drivers instead of standard model-specific drivers, potentially simplifying the burden of driver management on host computers. The availability of universal

print drivers depends on the capabilities of the user device, host, and print server software. In certain configurations, universal printing might not be available.

When adding this setting to a policy, select an option:

- Use only printer model specific drivers specifies that the client printer uses only the standard model-specific drivers that are auto-created at logon. If the requested driver is unavailable, the client printer cannot be auto-created.
- Use universal printing only specifies that no standard model-specific drivers are used. Only universal print drivers are used to create printers.
- Use universal printing only if requested driver is unavailable uses standard model-specific drivers for printer creation if they are available. If the driver is not available on the server, the client printer is created automatically with the appropriate universal driver.
- Use printer model specific drivers only if universal printing is unavailable uses the universal print driver if it is available. If the driver is not available on the server, the client printer is created automatically with the appropriate model-specific printer driver.

Universal Print Server policy settings

February 6, 2020

The Universal Print Server section contains policy settings for handling the Universal Print Server.

SSL cipher suite

This setting specifies the set of SSL/TLS cipher suites used by the Universal Print Client for encrypted print data stream (CGP) connections.

To control the cipher suite package used by the Universal Print Client for encrypted print web service (HTTPS/SOAP) connections, see [SCHANNEL].

Default value: ALL

This setting has the following values: ALL, COM or GOV.

The cipher suites corresponding to each value are listed below:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL compliance mode

This setting specifies the level of compliance with NIST Special Publication 800-52 that is used by the Universal Print Client for encrypted print data stream (CGP) connections.

Default value: None.

This setting has the following values:

None.

The encrypted print data stream (CGP) connections use the default compliance mode.

SP800-52.

The encrypted print data stream (CGP) connections use the NIST Special Publication 800-52 compliance mode.

SSL enabled

This setting specifies whether SSL/TLS is used by the Universal Print Client for print data stream (CGP) connections and for web service (HTTP/SOAP) connections.

When you set **Universal Print Server enable** to **Enabled with fallback to Windows' native remote printing**, fallback connections are made by the Microsoft Windows Network Print Provider. This setting does not affect these fallback connections.

Default value: Disabled

This setting has the following values:

Enabled.

The Universal Print Client uses SSL/TLS to connect to the Universal Print Server.

Disabled.

The Universal Print Client uses SSL/TLS to connect to the Universal Print Server.

SSL FIPS mode

This setting specifies whether the SSL/TLS cryptographic module used by the Universal Print Client for print data stream (CGP) connections will run in FIPS mode.

Default value: Disabled

This setting has the following values:

Enabled.

FIPS mode is on.

Disabled.

FIPS mode is off.

SSL protocol version

This setting specifies the SSL/TLS protocol version used by the Universal Print Client.

Default value: ALL

This setting has the following values:

ALL.

Use TLS versions 1.0, 1.1 or 1.2.

TLSv1.

Use TLS version 1.0.

TLSv1.1.

Use TLS version 1.1.

TLSv1.2.

Use TLS version 1.2.

SSL Universal Print Server encrypted print data stream (CGP) port

This setting specifies the TCP port number of the Universal Print Server encrypted print data stream (CGP) port. This port receives data for print jobs.

Default value: 443

SSL Universal Print Server encrypted web service (HTTPS/SOAP) port

This setting specifies the TCP port number of the Universal Print Server encrypted web service (HTTP-S/SOAP) port. This port receives data for print commands.

Default value: 8443

Universal Print Server enable

This setting enables or disables the Universal Print Server feature on the virtual desktop or the server hosting applications. Apply this policy setting to Organizational Units (OUs) containing the virtual desktop or server hosting applications.

By default, the Universal Print Server is disabled.

When adding this setting to a policy, select one of the following options:

- **Enabled with fallback to Windows native remote printing**. Network printer connections are serviced by the Universal Print Server, if possible. If the Universal Print Server is not available, the Windows Print Provider is used. The Windows Print Provider continues to handle all printers previously created with the Windows Print Provider.
- **Enabled with no fallback to Windows native remote printing**. Network printer connections are serviced by the Universal Print Server exclusively. If the Universal Print Server is unavailable, the network printer connection fails. This setting effectively disables network printing through the Windows Print Provider. Printers previously created with the Windows Print Provider are not created while a policy containing this setting is active.
- **Disabled**. The Universal Print Server feature is disabled. No attempt is made to connect with the Universal Print Server when connecting to a network printer with a UNC name. Connections to remote printers continue to use the Windows native remote printing facility.

Universal Print Server print data stream (CGP) port

This setting specifies the TCP port number used by the Universal Print Server print data stream Common Gateway Protocol (CGP) listener. Apply this policy setting only to OUs containing the print server.

By default, the port number is set to 7229.

Valid port numbers must be in the range of 1 to 65535.

Universal Print Server print stream input bandwidth limit (kpbs)

This setting specifies the upper boundary (in kilobits per second) for the transfer rate of print data delivered from each print job to the Universal Print Server using CGP. Apply this policy setting to OUs containing the virtual desktop or server hosting applications.

By default, the value is 0, which specifies no upper boundary.

Universal Print Server web service (HTTP/SOAP) port

This setting specifies the TCP port number used by the Universal Print Server's web service (HTTP/-SOAP) listener. The Universal Print Server is an optional component that enables the use of Citrix universal print drivers for network printing scenarios. When the Universal Print Server is used, printing commands are sent from Citrix Virtual Apps and Desktops hosts to the Universal Print Server via SOAP over HTTP. This setting modifies the default TCP port on which the Universal Print Server listens for incoming HTTP/SOAP requests.

You must configure both host and print server HTTP port identically. If you do not configure the ports identically, the host software will not connect to the Universal Print Server. This setting changes the VDA on Citrix Virtual Apps and Desktops. In addition, you must change the default port on the Universal Print Server.

By default, the port number is set to 8080.

Valid port numbers must be in the range of 0 to 65535.

Universal Print Servers for load balancing

This setting lists the Universal Print Servers to be used to load balance printer connections established at session launch, after evaluating other Citrix printing policy settings. To optimize printer creation time, Citrix recommends that all print servers have the same set of shared printers. There is no upper limit to the number of print servers which can be added for load balancing.

This setting also implements print server failover detection and printer connections recovery. The print servers are checked periodically for availability. If a server failure is detected, that server is removed from the load balancing scheme, and printer connections on that server are redistributed among other available print servers. When the failed print server recovers, it is returned to the load balancing scheme.

Click **Validate Servers** to check that each server is a print server, that the server list doesn't contain duplicate server names, and that all servers have an identical set of shared printers installed. This operation may take some time.

Universal Print Servers out-of-service threshold

This setting specifies how long the load balancer should wait for an unavailable print server to recover before it determines that the server is permanently offline and redistributes its load to other available print servers.

By default, the threshold value is set to 180 (seconds).

Universal printing policy settings

February 6, 2020

The Universal Printing section contains policy settings for managing universal printing.

Universal printing EMF processing mode

This setting controls the method of processing the EMF spool file on the Windows user device.

By default, EMF records are spooled directly to the printer.

When adding this setting to a policy, select an option:

- Reprocess EMFs for printer forces the EMF spool file to be reprocessed and sent through the GDI subsystem on the user device. You can use this setting for drivers that require EMF reprocessing but that might not be selected automatically in a session.
- Spool directly to printer, when used with the Citrix Universal print driver, ensures the EMF records are spooled and delivered to the user device for processing. Typically, these EMF spool files are injected directly to the client's spool queue. For printers and drivers that are compatible with the EMF format, this is the fastest printing method.

Universal printing image compression limit

This setting specifies the maximum quality and the minimum compression level available for images printed with the Citrix Universal print driver.

By default, the image compression limit is set to Best quality (lossless compression).

If No Compression is selected, compression is disabled for EMF printing only.

When adding this setting to a policy, select an option:

- No compression
- Best quality (lossless compression)

- High quality
- Standard quality
- Reduced quality (maximum compression)

When adding this setting to a policy that includes the Universal printing optimization defaults setting, be aware of the following:

- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing optimization defaults

This setting specifies the default values for printing optimization when the universal print driver is created for a session.

- Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
- Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.
- Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached. Note that these settings apply only if the user device supports this behavior.
- Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.

Note: All of these options are supported for EMF printing. For XPS printing, only the Desired image quality option is supported.

When adding this setting to a policy that includes the Universal printing image compression limit setting, be aware of the following:

- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing preview preference

This setting specifies whether or not to use the print preview function for auto-created or generic universal printers.

By default, print preview is not used for auto-created or generic universal printers.

When adding this setting to a policy, select an option:

- Do not use print preview for auto-created or generic universal printers
- Use print preview for auto-created printers only
- Use print preview for generic universal printers only
- Use print preview for both auto-created and generic universal printers

Universal printing print quality limit

This setting specifies the maximum dots per inch (dpi) available for generating printed output in a session.

By default, No Limit is enabled, meaning users can select the maximum print quality allowed by the printer to which they connect.

If this setting is configured, it limits the maximum print quality available to users in terms of output resolution. Both the print quality itself and the print quality capabilities of the printer to which the user connects are restricted to the configured setting. For example, if configured to Medium Resolution (600 DPI), users are restricted to printing output with a maximum quality of 600 DPI and the Print Quality setting on the Advanced tab of the Universal Printer dialog box shows resolution settings only up to and including Medium Quality (600 DPI).

When adding this setting to a policy, select an option:

- Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)
- No Limit

Security policy settings

June 16, 2021

The Security section contains the policy setting for configuring session encryption and encryption of logon data.

SecureICA minimum encryption level

This setting specifies the minimum level at which to encrypt session data sent between the server and a user device.

Important: For the Virtual Delivery Agent 7.x, this policy setting can be used only to enable the encryption of the logon data with RC5 128-bit encryption. Other settings are provided only for backwards compatibility with legacy versions of Citrix Virtual Apps and Desktops.

For the VDA 7.x, encryption of session data is set using the basic settings of the VDA's Delivery Group. If Enable Secure ICA is selected for the Delivery Group, session data is encrypted using RC5 (128 bit) encryption. If Enable Secure ICA is not selected for the Delivery Group, session data is encrypted with Basic encryption.

When adding this setting to a policy, select an option:

- Basic encrypts the client connection using a non-RC5 algorithm. It protects the data stream from being read directly, but it can be decrypted. By default, the server uses Basic encryption for client-server traffic.
- RC5 (128 bit) logon only encrypts the logon data using RC5 128-bit encryption and the client connection using Basic encryption.
- RC5 (40 bit) encrypts the client connection using RC5 40-bit encryption.
- RC5 (56 bit) encrypts the client connection using RC5 56-bit encryption.
- RC5 (128 bit) encrypts the client connection using RC5 128-bit encryption.

The settings you specify for client-server encryption can interact with any other encryption settings in your environment and your Windows operating system. If a higher priority encryption level is set on either a server or user device, settings you specify for published resources can be overridden.

You can raise encryption levels to further secure communications and message integrity for certain users. If a policy requires a higher encryption level, Citrix Receivers using a lower encryption level are denied connection.

SecureICA does not perform authentication or check data integrity. To provide end-to-end encryption for your site, use SecureICA with TLS encryption.

SecureICA does not use FIPS-compliant algorithms. If this is an issue, configure the server and Citrix Receivers to avoid using SecureICA.

SecureICA uses the RC5 block cipher as described in RFC 2040 for confidentiality. The block size is 64 bits (a multiple of 32-bit word units). The key length is 128 bits. The number of rounds is 12.

Keys for the RC5 block cipher are negotiated when a session is created. Negotiation is performed using the Diffie-Hellman algorithm. This negotiation uses Diffie-Hellman public parameters, which are stored in the Windows registry when the Virtual Delivery Agent is installed. Public parameters are not secret. The result of the Diffie-Hellman negotiation is a secret key, from which session keys for

the RC5 block cipher are derived. Separate session keys are used for user logon, and for data transfer; and separate session keys are used for traffic to and from the Virtual Delivery Agent. Therefore there are four session keys for each session. The secret keys and session keys are not stored. Initialization vectors for the RC5 block cipher are also derived from the secret key.

Server limits policy settings

February 6, 2020

The Server Limits section contains the policy setting for controlling idle connections.

Server idle timer interval

This setting determines, in milliseconds, how long an uninterrupted user session is maintained if there is no input from the user.

By default, idle connections are not disconnected (server idle timer interval = 0). Citrix recommends setting this value to a minimum of 60000 milliseconds (60 seconds).

To display the policy, select **Multiple Versions**, clear the Single-session OS versions, and then select **Server Limits**.

> **Note**
>
> When this policy setting is used, an "Idle timer expired"dialog box might appear to users when the session has been idle for the specified time. Citrix policy settings don't control this Microsoft dialog box message. For more information, see http://support.citrix.com/article/CTX118618.

Session limits policy settings

February 6, 2020

The **Session Limits** section contains policy settings that control how long sessions remain connected before they are forced to log off.

> **Important:**
>
> The settings described in this article do not apply to Windows Server VDAs. For more information about configuring session time limits for Server VDAs, see Microsoft KB - Session Time Limits.

Disconnected session timer

This setting enables or disables a timer that specifies how long a disconnected, locked desktop remains locked before the session is logged off. If this timer is enabled, the disconnected session is logged off when the timer expires.

By default, disconnected sessions are not logged off.

Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop can remain locked before the session is logged off.

By default, the time period is 1,440 minutes (24 hours).

Session connection timer

This setting enables or disables a timer that specifies the maximum duration of an uninterrupted connection between a user device and a desktop. If this timer is enabled, the session is disconnected or logged off when the timer expires. The Microsoft **End session when time limits are reached** setting determines the next state for the session.

By default, this timer is disabled.

Session connection timer interval

This setting specifies the maximum number of minutes for an uninterrupted connection between a user device and a desktop.

By default, the maximum duration is 1,440 minutes (24 hours).

Session idle timer

This setting enables or disables a timer that specifies how long an uninterrupted user device connection to a desktop is maintained if the user supplies no input. When this timer expires, the session is placed in the disconnected state and the **Disconnected session timer** applies. If the **Disconnected session timer** is disabled, the session is not logged off.

By default, this timer is enabled.

Session idle timer interval

This setting specifies how many minutes an uninterrupted user device connection to a desktop is maintained if there is no input from the user.

By default, idle connections are maintained for 1,440 minutes (24 hours).

Session reliability policy settings

February 6, 2020

The session reliability section contains policy settings for managing session reliability connections.

Session reliability connections

This setting allows or prevents sessions to remain open during a loss of network connectivity. Session reliability, along with auto client reconnection, allows users to reconnect automatically to their Citrix Workspace app sessions after recovering from network disruptions. By default, session reliability is Allowed.

For Citrix Workspace app 1808 and later and Citrix Receiver for Windows 4.7 and later, the settings in Studio are enforced on the client. Citrix Receiver Group Policy Object on the clients are overridden by Studio policy. Updates to these policies in Studio synchronize session reliability from server to client.

> **Note:**
>
> - Citrix Receiver for Windows 4.7 and later and Citrix Workspace Apps for Windows - Set the policy in Studio.
> - Citrix Receivers for Windows earlier than 4.7 - Set policies in Studio and the Citrix Receiver Group Policy Object template on the client for consistent behavior.

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.

By using session reliability, the session remains active on the server. To indicate that connectivity is lost, the user display becomes opaque. The user might see a frozen session during the interruption and can resume interacting with the application when the network connection is restored. Session reliability reconnects users without reauthentication prompts.

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 specified in the session reliability timeout setting. After that, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session.

By default, session reliability is Allowed.

To disable session reliability:

1. Start Citrix Studio.
2. Open the **Session Reliability connections** policy.
3. Set the policy to **Prohibited**.

Session reliability port number

This setting specifies the TCP port number for incoming session reliability connections.

By default, the port number is set to 2598.

To change the session reliability port number:

1. Start Citrix Studio.
2. Open the **Session reliability port number** policy.
3. Edit the port number.
4. Click **OK**.

Session reliability timeout

This setting specifies the length of time, in seconds, the session reliability proxy waits for a user to reconnect before allowing the session to be disconnected.

Although you can extend the amount of time a session is kept open, this feature is a convenience and doesn't prompt the user for reauthentication. The longer a session open, chances increase that a user might leave the device unattended and potentially accessible to unauthorized users.

By default, the timeout is set to 180 seconds, or three minutes.

To change session reliability timeout:

1. Start Citrix Studio.
2. Open the **Session reliability timeout** policy.
3. Edit the timeout value.
4. Click **OK**.

Session watermark policy settings

February 6, 2020

The session watermark section contains policy settings to configure this feature.
Enabling this feature causes a significant rise in the network bandwidth and CPU usage by the VDA machine. We recommend that you configure session watermark for selected VDA machines based on your available hardware resources.

> **Important**
>
> Enable session watermark for the other watermark policy settings to be effective. To achieve a better user experience, don't enable more than two watermark text items.

Enable session watermark

When you enable this setting, the session display has an opaque textual watermark displaying session-specific information. The other watermark settings depend on this one being enabled.

By default, session watermark is disabled.

Include client IP address

When you enable this setting, the session displays the current client IP address as a watermark.

By default, Include client IP address is disabled.

Include connection time

When you enable this setting, the session watermark displays a connect time. The format is yyyy/mm/dd hh:mm. The time displayed is based on the system clock and time zone.

By default, Include connection time is disabled.

Include logon user name

When you enable this setting, the session displays the current logon user name as a watermark. The display format is USERNAME@DOMAINNAME. We recommend that the user name is a maximum of 20 characters. When a user name is more than 20 characters, excessively small character fonts or truncation might occur and lessen the watermark effectiveness.

By default, Include logon user name is enabled.

Include VDA host name

When you enable this setting, the session displays the VDA host name of the current ICA session as a watermark.

By default, Include VDA host name is enabled.

Include VDA IP address

When you enable this setting, the session displays the VDA IP address of the current ICA session as a watermark.

By default, VDA IP address is disabled.

Session watermark style

This setting controls whether you display a single watermark text label or multiple labels. Choose **Multiple** or **Single** from the **Value** drop-down menu.

Multiple displays five watermark labels in the session. One in the center and four in the corners.

Single displays a single watermark label in the center of the session.

By default, Session watermark style is Multiple.

Watermark custom text

This setting specifies a custom text string (for example, the corporate name) to display in the session watermark. When you configure a non-empty string, it displays the text in a new line appending other information enabled in the watermark.
The watermark custom text maximum is 25 Unicode characters. If you configure a longer string, it is truncated to 25 characters.

There is no default text.

Watermark transparency

You can specify watermark opacity from 0 through 100. The larger the value specified, the more opaque the watermark.

By default, the value is 17.

Time zone control policy settings

February 6, 2020

The Time Zone Control section contains policy settings related to using local time in sessions.

Estimate local time for legacy clients

This setting enables or disables estimating the local time zone of user devices that send inaccurate time zone information to the server.

By default, the server estimates the local time zone when necessary.

This setting is intended for use with legacy Citrix Receivers or ICA clients that do not send detailed time zone information to the server. When used with Citrix Receivers that send detailed time zone information to the server, such as supported versions of Citrix Receiver for Windows, this setting has no effect.

Restore desktop OS time zone on session disconnect or logoff

This setting determines whether or not the time zone setting for a Single-session OS VDA is restored to the machine's original time zone when the user disconnects or logs off. If you enable this setting, the VDA restores the machine's time zone to its original setting when the user disconnects or logs off. For this setting to take effect, set the **Use local time of client** to **Use client time zone**.

By default, this setting is enabled.

Use local time of client

This setting determines the time zone setting of the user session. The choices are the time zone of the user session (server time zone) or the time zone of the user device (client time zone).

By default, the time zone of the user session is used.

For this setting to take effect, enable the **Allow time zone redirection** setting in the Group Policy Editor. The setting is in **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Device and Resource Redirection**.

If the VDA is a Single-session OS VDA running on a Multi-session OS, configure the local user right **Change the time zone** to **Everyone**. This user right can be found in the **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.

> **Note:**
>
> In a Single-session OS, **Users** are included in the User Rights Assignment **Change the time zone**, though not in a Multi-session OS. In a Multi-session OS, the time zone synchronizes using the following group policy: Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Allow timezone redirection. This policy doesn't apply when the Server is not a Remote Desktop Session Host in the Multi-session OS VDA (installed with the `/ServerVDI` command). In a Multi-session OS, by default and by design, users don't have the local right to change the time zone.

TWAIN devices policy settings

February 6, 2020

The TWAIN devices section contains policy settings related to mapping client TWAIN devices, such as digital cameras or scanners, and optimizing image transfers from server to client.

> **Note**
>
> TWAIN 2.0 is supported with Citrix Receiver for Windows 4.5.

Client TWAIN device redirection

This setting allows or prevents users from accessing TWAIN devices on the user device from image processing applications hosted on servers. By default, TWAIN device redirection is allowed.

The following policy settings are related:

- TWAIN compression level
- TWAIN device redirection bandwidth limit
- TWAIN device redirection bandwidth limit percent

TWAIN compression level

This setting specifies the level of compression of image transfers from client to server. Use Low for best image quality, Medium for good image quality, or High for low image quality. By default, medium compression is applied.

USB devices policy settings

February 6, 2020

The **USB devices** section contains policy settings for managing file redirection for USB devices.

Client USB device optimization rules

Client USB device optimization rules can be applied to devices to disable optimization, or to change the optimization mode.

When a user plugs in a USB input device, the host checks if the **USB policy** settings allow the device. If the device is allowed, the host then checks the **Client USB device optimization rules** for the device. If no rule is specified, then the device is not optimized. Capture mode (04) is the recommended mode for signature devices. For other devices which have degraded performance over higher latency, administrators can enable Interactive mode (02). See descriptions of the available modes in the table in this article.

Good to know

- For the use of Wacom signature pads and tablets, we recommend that you disable the screen saver. Steps on how to disable the screen saver are at the end of this section.
- Support for the optimization of Wacom STU signature pads and tablets series of products has been preconfigured in the installation of Citrix Virtual Apps and Desktops policies.
- Signature devices work across Citrix Virtual Apps and Desktops and do not require a driver to be used as a signature device. Wacom has more software that can be installed to customize the device further. See http://www.wacom.com/.
- Drawing tablets. Certain drawing input devices might present as an HID device on PCI/ACPI buses and are not supported. Attach these devices on a USB host controller on the client to be redirected inside a Citrix Virtual Desktops session.

Policy rules take the format of tag=value expressions separated by whitespace. The following tags are supported:

Tag Name	Description
Mode	The optimization mode is supported for input devices for class=**03**. Supported modes are: No optimization - value **01**. Interactive mode - value **02**. Recommended for devices such as pen tablets and 3D Pro mice. Capture mode - value **04**. Preferred for devices such as signature pads.
VID	Vendor ID from the device descriptor, as a four digit hexadecimal number.
PID	Product ID from the device descriptor, as a four digit hexadecimal number.
REV	Revision ID from the device descriptor, as a four digit hexadecimal number.
Class	Class from either the device descriptor or an interface descriptor.
SubClass	Subclass from either the device descriptor or an interface descriptor.
Prot	Protocol from either the device descriptor or an interface descriptor.

Examples

Mode=00000004 VID=067B PID=1230 class=03 #Input device operating in capture mode

Mode=00000002 VID=067B PID=1230 class=03 #Input device operating in interactive mode (default)

Mode=00000001 VID=067B PID=1230 class=03 #Input device operating without any optimization

Mode=00000100 VID=067B PID=1230 # Device setup optimization disabled (default)

Mode=00000200 VID=067B PID=1230 # Device setup optimization enabled

Disabling the screen saver for Wacom signature pad devices

For the use of Wacom signature pads and tablets, Citrix recommends that you disable the screen saver as follows:

1. Install the **Wacom-STU-Driver** after redirecting the device.
2. Install **Wacom-STU-Display MSI** to gain access to the signature pad control panel.

3. Go to **Control Panel > Wacom STU Display > STU430** or **STU530**, and select the tab for your model.
4. Choose **Change**, then select **Yes** when the UAC security window pops up.
5. Select **Disable slideshow**, then **Apply**.

After the setting is set for one signature pad model, it is applied to all models.

Client USB device redirection

This setting allows or prevents redirection of USB devices to and from the user device.

By default, USB devices are not redirected.

Client USB device redirection rules

This setting specifies redirection rules for USB devices.

By default, no rules are specified.

When a user plugs in a USB device, the host device checks it against each policy rule in turn until a match is found. The first match for any device is considered definitive. If the first match is an Allow rule, the device is remoted to the virtual desktop. If the first match is a Deny rule, the device is available only to the local desktop. If no match is found, default rules are used.

Policy rules take the format {Allow: | Deny:} followed by a set of tag= value expressions separated by whitespace. The following tags are supported:

Tag Name	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
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, remember:

- Rules are case-insensitive.

- Rules can have an optional comment at the end, introduced by #.
- Blank and pure comment lines are ignored.
- Tags must use the matching operator = (for example, VID=067B_.
- Each rule must start on a new line or form part of a semicolon-separated list.
- See the USB class codes available from the USB Implementers Forum, Inc. website.

Examples of administrator-defined USB policy rules:

- Allow: VID=067B PID=0007 # Another Industries, Another Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- To create a rule that denies all USB devices, use "DENY:"without other tags.

Client USB plug and play device redirection

This setting allows or prevents plug-and-play devices such as cameras or point-of-sale (POS) devices to be used in a client session.

By default, plug-and-play device redirection is allowed. When set to Allowed, all plug-and-play devices for a specific user or group are redirected. When set to Prohibited, no devices are redirected.

Configure automatic redirection of USB devices

USB devices are automatically redirected when USB support is enabled, and the USB user preference settings are set to automatically connect USB devices.

> Note:
>
> In Receiver for Windows 4.2, USB devices are also automatically redirected when operating in Desktop Appliance mode, and the connection bar is not present. In earlier versions of Citrix Receiver for Windows, USB devices are also automatically redirected when operating in a desktop appliance mode or with virtual machine (VM) hosted applications.

It is not always best to redirect all USB devices. Users can explicitly redirect devices from the USB device list that is not automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules on either the client endpoint or the Virtual Desktop Agent (VDA). See Administration Guides for further details.

> Caution
>
> Using Registry Editor 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.

User preferences settings for auto redirection of USB devices

Policy:

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**.

Citrix Receiver:

1. Go to **Citrix Receiver Preferences > Connections**.
2. Ensure that the following options are selected:
   - When a session starts, connect devices automatically
   - When a new device is connected while a session is running, connect the device automatically.
3. Click **OK**.

All the registry keys and the policy changes are applied to the Windows client device.

Plain USB printers redirection

The best solution for plain USB printers is to use the dedicated Universal Printer Driver and virtual channel to perform printing. By default, plain USB printers are not automatically redirected.

Plain printers are detected using heuristics, and it is expected that advanced printers with scanning functions for example, might need to be redirected using USB support to work completely.

Use this registry to configure whether plain printers are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Type: DWORD

Data: 00000000

The default value is 0 (does not automatically redirect). Changing the value to any number greater than zero enables USB support to redirect plain USB printers.

You can also deploy Active Directory policies to this registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectAudio

Type: DWORD

Data: 00000000

Plain audio devices redirection

Like plain printers, the best user experience is achieved using the dedicated audio virtual channel of ICA to send audio data from plain audio devices. However, you might need to redirect some specialty devices using USB support. Heuristics are used to determine which devices are plain audio devices.

Use this registry to configure whether plain audio devices are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectAudio

Type: DWORD

Data: 00000000

The default is set to 0 (does not automatically redirect). Changing the value to non-zero, redirects plain USB audio devices with USB support.

You can use Active Directory policies to deploy this value to the registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectVideo

Type: DWORD

Data: 00000000

Plain storage devices (mass storage device) redirection

For plain storage devices, you achieve the best user experience using the dedicated virtual channel, such as client drive mapping that also performs optimization. In addition to simple reading or writing files, to perform certain special tasks like burning a CD/DVD or accessing encrypted file systems devices, the device might still need to be redirected using generic USB support.

Heuristics are used to determine which devices are plain storage devices. Use this registry key to configure whether plain storage devices are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectStorage

Type: DWORD

Data: 00000000

The default is set to 0 (does not automatically redirect). Changing the value to non-zero, redirects plain USB storage devices using generic USB support.

You can also use Active Directory policies to deploy this value to the following registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectStorage

Type: DWORD

Data: 00000000

> Note:
>
> Read only access to the plain storage device is not configurable if you are using generic USB support, while it is configurable if using CDM.

USB flash drives with hardware encryption redirection

USB flash drives with hardware encryption typically consist of an encrypted storage partition and a second *utility* partition that contains a utility for unlocking the encrypted partition. For USB Flash Drive devices, achieve the best user experience using the dedicated client drive mapping/dynamic thumbdrive mapping HDX virtual channel that also performs optimization.

Generic USB redirection is necessary for non-Windows clients (for example, Linux clients) and clients where the customer has restricted (locked down) user access to local functions on the client. Generic USB redirection can redirect any USB storage device without hardware encryption into both Single-session OS and Multi-session OS VDA sessions.

Before Citrix Virtual Apps and Desktop 7 1808, USB flash drives with hardware encryption could not be redirected in any useful way into Single-session OS or Multi-session OS VDA sessions. A new feature enhancement introduced in Citrix Virtual Apps and Desktop 7 1808 supports generic USB redirection of USB flash drives with hardware encryption into Single-session OS and Multi-session OS VDA sessions. After the device is redirected, none of its drives appear on the local client. So, if unlocking the drive is required, perform it in the session. This feature requires Windows update KB4074590.

Plain still image devices (scanners and digital cameras)

For plain still image devices, achieve the best user experience using the dedicated virtual channel (such as the TWAIN virtual channel) that also performs optimization. These devices must adhere to industry standards. If a device is non-compliant or if it is not used according to the original intentions, generic USB redirection might be the only way to use the device. Heuristics are used to determine which devices are plain still image devices.

Use this registry key to configure whether plain still image devices are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectImage

Type: DWORD

Data: 00000000

The default is set to 0 (does not automatically redirect). Changing the value to non-zero, redirects plain USB still image devices with generic USB.

You can also use Active Directory policies to deploy this value to this registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectImage

Type: DWORD

Data: 00000000

Device specific settings

The heuristics used to select Citrix optimizable devices (such as printers, audio, video, storage, and still image devices) do not always match what you want. You might want to control automatic redirection of devices that are not listed above. You can control automatic redirection on a device specific basis.

As an example, the DemoTech 2,000 bar code reader doesn't need to be redirected using USB support. It has a vendor identifier of 12AB and a product identifier of 5678. These hexadecimal numbers can be found in Device Manager.

To prevent this being automatically redirected, create this device specific registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Name: AutoRedirect

Type: DWORD

Data: 00000000

A value of 0 prevents the device from being automatically redirected. A non-zero value indicates that the device must be considered for automatic redirection (subject to user preferences). There is a single space character between the vendor and product identifiers.

You can also deploy this value using Active Directory policies to this registry key. It overrides the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Name: AutoRedirect

Type: DWORD

Data: 00000000

Device specific AutoRedirect settings take precedence over the more general AutoRedirectXXX values explained above. The default heuristics for Citrix optimized devices might misinterpret a device as generic. Therefore, set the device specific AutoRedirect value to 1 to redirect it automatically.

Visual display policy settings

February 6, 2020

The Visual Display section contains policy settings for controlling the quality of images sent from virtual desktops to the user device.

Preferred color depth for simple graphics

This policy setting is available in VDA versions 7.6 FP3 and later. The 8-bit option is available in VDA versions 7.12 and later.

This setting makes it possible to lower color depth at which simple graphics are sent over the network. Lowering to 8-bit or 16-bit per pixel potentially improves responsiveness over low bandwidth connections, at the cost of a slight degradation in image quality. The 8-bit color depth is not supported when the Use video codec for compression policy setting is set to For the entire screen.

The default preferred color depth is 24-bits per pixel.

VDAs fall back to 24-bit (default) color depth if the 8-bit setting is applied on VDA version 7.11 and earlier.

Target frame rate

This setting specifies the maximum number of frames per second sent from the virtual desktop to the user device.

By default, the maximum is 30 frames per second.

Setting a high number of frames per second (for example, 30) improves the user experience, but requires more bandwidth. Decreasing the number of frames per second (for example, 10) maximizes server scalability at the expense of user experience. For user devices with slower CPUs, specify a lower value to improve the user experience.

The maximum supported frame rate per second is 60.

Visual quality

This setting specifies the desired visual quality for images displayed on the user device.

By default, this setting is Medium.

To specify the quality of images, choose one of the following options:

- **Low** - Recommended for bandwidth-constrained networks where visual quality can be sacrificed for interactivity
- **Medium** - Offers the best performance and bandwidth efficiency in most use cases
- **High** - Recommended if you require visually lossless image quality
- **Build to lossless** - Sends lossy images to the user device during periods of high network activity and lossless images after network activity reduces. This setting improves performance over bandwidth-constrained network connections
- **Always lossless** - When preserving image data is vital, select Always lossless to ensure lossy data is never sent to the user device. For example, when displaying X-ray images where no loss of quality is acceptable.

Moving images policy settings

February 6, 2020

The Moving Images section contains settings that enable you to remove or alter compression for dynamic images.

Minimum image quality

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies the minimum acceptable image quality for Adaptive Display. The less compression used, the higher the quality of images displayed. Choose from Ultra High, Very High, High, Normal, or Low compression.

By default, this is set to Normal.

Moving image compression

This setting specifies whether or not Adaptive Display is enabled. Adaptive Display automatically adjusts the image quality of videos and transitional slides in slide shows based on available bandwidth. With Adaptive Display enabled, users should see smooth-running presentations with no reduction in quality.

By default, Adaptive Display is enabled.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1 and later, this setting applies when Legacy graphics mode is enabled, or when the legacy graphics mode is disabled and a video codec is not used to compress graphics.

When legacy graphics mode is enabled, the session must be restarted before policy changes take effect. Adaptive Display is mutually exclusive with Progressive Display; enabling Adaptive Display disables Progressive Display and vice versa. However, both Progressive Display and Adaptive Display can be disabled at the same time. Progressive Display, as a legacy feature, is not recommended for XenApp or XenDesktop. Setting Progressive threshold Level will disable Adaptive Display.

Progressive compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting provides a less detailed but faster initial display of images.

By default, no progressive compression is applied.

The more detailed image, defined by the normal lossy compression setting, appears when it becomes available. Use Very High or Ultra High compression for improved viewing of bandwidth-intensive graphics such as photographs.

For progressive compression to be effective, its compression level must be higher than the Lossy compression level setting.

Note: The increased level of compression associated with progressive compression also enhances the interactivity of dynamic images over client connections. The quality of a dynamic image, such as a rotating three-dimensional model, is temporarily decreased until the image stops moving, at which time the normal lossy compression setting is applied.

The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

Progressive compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection to which progressive compression is applied. This is applied only to client connections under this bandwidth.

By default, the threshold value is 2147483647 kilobits per second.

The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

Target minimum frame rate

This setting specifies the minimum frame rate per second the system attempts to maintain, for dynamic images, under low bandwidth conditions.

By default, this is set to 10fps.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1 and later, this setting applies when the Legacy graphics mode is disabled or enabled.

Still images policy settings

February 6, 2020

The Still Images section contains settings that enable you to remove or alter compression for static images.

Extra color compression

This setting enables or disables the use of extra color compression on images delivered over client connections that are limited in bandwidth, improving responsiveness by reducing the quality of displayed images.

By default, extra color compression is disabled.

When enabled, extra color compression is applied only when the client connection bandwidth is below the Extra color compression threshold value. When the client connection bandwidth is above the threshold value or Disabled is selected, extra color compression is not applied.

Extra color compression threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection below which extra color compression is applied. If the client connection bandwidth drops below the set value, extra color compression, if enabled, is applied.

By default, the threshold value is 8192 kilobits per second.

Heavyweight compression

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting enables or disables reducing bandwidth beyond progressive compression without losing image quality by using a more advanced, but more CPU-intensive, graphical algorithm.

By default, heavyweight compression is disabled.

If enabled, heavyweight compression applies to all lossy compression settings. It is supported on Citrix Workspace app but has no effect on other plug-ins.

The following policy settings are related:

- Progressive compression level
- Progressive compression threshold value

Lossy compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting controls the degree of lossy compression used on images delivered over client connections that are limited in bandwidth. In such cases, displaying images without compression can be slow.

By default, medium compression is selected.

For improved responsiveness with bandwidth-intensive images, use high compression. Where preserving image data is vital; for example, when displaying X-ray images where no loss of quality is acceptable, you may not want to use lossy compression.

Related policy setting: Lossy compression threshold value

Lossy compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection to which lossy compression is applied.

By default, the threshold value is 2147483647 kilobits per second.

Adding the Lossy compression level setting to a policy and including no specified threshold can improve the display speed of high-detail bitmaps, such as photographs, over a LAN.

Related policy setting: Lossy compression level

WebSockets policy settings

February 6, 2020

The WebSockets section contains policy settings for accessing virtual desktops and hosted applications using Citrix Workspace app for HTML5. The WebSockets feature increases security and reduces overhead by conducting two-way communication between browser-based applications and servers without opening multiple HTTP connections.

WebSockets connections

This setting allows or prohibits WebSockets connections.

By default, WebSocket connections are prohibited.

WebSockets port number

This setting identifies the port for incoming WebSocket connections.

By default, the value is 8008.

WebSockets trusted origin server list

This setting provides a comma-separated list of trusted origin servers, usually Citrix Workspace app for Web, expressed as URLs. The server accepts only WebSockets connections originating from one of these addresses.

By default, the wildcard * is used to trust all Citrix Workspace app for Web URLs.

If you choose to type an address in the list, use this syntax:

<protocol>://<Fully qualified domain name of host>:[port]

The protocol must be HTTP or HTTPS. If the port is not specified, port 80 is used for HTTP and port 443 is used for HTTPS.

The wildcard * can be used within the URL, except as part of an IP address (10.105..).

Load management policy settings

February 6, 2020

The Load Management section contains policy settings for enabling and configuring load management between servers delivering Windows Multi-session OS machines.

For information about calculating the load evaluator index, see CTX202150.

Concurrent logon tolerance

This setting specifies the maximum number of concurrent logons a server can accept.

By default, this is set to 2.

When this setting is enabled, load balancing tries to avoid having more than the specified number of logons active on a Server VDA at the same time. However, the limit is not strictly enforced. To enforce the limit (and cause concurrent logons that exceed the specified number to fail), create the following registry key:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> Type: DWORD
> Value: 1

CPU usage

This setting specifies the level of CPU usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and CPU usage is excluded from load calculations.

CPU usage excluded process priority

This setting specifies the priority level at which a process' CPU usage is excluded from the CPU Usage load index.

By default, this is set to Below Normal or Low.

Disk usage

This setting specifies the disk queue length at which the server reports a 75% full load. When enabled, the default value for disk queue length is 8.

By default, this setting is disabled and disk usage is excluded from load calculations.

Maximum number of sessions

This setting specifies the maximum number of sessions a server can host. When enabled, the default setting for maximum number of sessions a server can host is 250.

By default, this setting is enabled.

Memory usage

This setting specifies the level of memory usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and memory usage is excluded from load calculations.

Memory usage base load

This setting specifies an approximation of the base operating system's memory usage and defines, in MB, the memory usage below which a server is considered to have zero load.

By default, this is set to 768 MB.

Profile Management policy settings

November 3, 2020

This section contains policy settings for enabling Profile Management and specifying which groups to include in and exclude from Profile Management processing.

For other information, such as the names of the equivalent .ini file settings and which version of Profile Management is required for a policy setting, see Profile Management policies.

Advanced policy settings

November 3, 2020

Number of retries when accessing locked files

Sets the number of retries when accessing locked files.

If this policy is disabled, the default value of five retries is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Process Internet cookie files on logoff

Some deployments leave extra Internet cookies that are not referenced by the file Index.dat. The extra cookies left in the file system after sustained browsing can lead to profile bloat. Enable this policy to force processing of Index.dat and remove the extra cookies. The policy increases logoff times, so only enable it if you experience this issue.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no processing of Index.dat takes place.

Disable automatic configuration

Profile Management examines any Citrix Virtual Desktops environment, for example for the presence of personal vDisks, and configures Group Policy accordingly. Only Profile Management policies in the Not Configured state are adjusted, so any customizations you have made are preserved. This feature speeds up deployment and simplifies optimization. No configuration of the feature is necessary, but you can disable automatic configuration when upgrading (to retain settings from earlier versions) or when troubleshooting. Automatic configuration does not work in Citrix Virtual Apps or other environments.

You can regard automatic configuration as a dynamic configuration checker that automatically configures the default policy settings according to environments at runtime. It eliminates the need to configure the settings manually. Runtime environments include:

- Windows OS
- Windows OS versions
- Presence of Citrix Virtual Desktops
- Presence of personal vDisks

Automatic configuration might change the following policies if the environment changes:

- Active write back
- Always cache
- Delete locally cached profiles on logoff
- Delay before deleting cached profiles
- Profile streaming

See the following table for the default status of the policies on different OSs:

	Multi-session OS	Single-session OS
Active write back	Enabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.
Always cache	Disabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.
Delete locally cached profiles on logoff	Enabled	*Disabled* if Personal vDisk is in use or if Citrix Virtual Desktops is assigned or if Citrix Virtual Desktops is not installed; otherwise, enabled.

	Multi-session OS	Single-session OS
Delay before deleting cached profiles	0 seconds	60 seconds if user changes are not persistent; otherwise, 0 seconds.
Profile streaming	Enabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.

However, with automatic configuration disabled, all policies above default to **Disabled**.

Starting with Profile Management 1909, you can have an improved experience with the Start menu on Windows 10 (version 1607 and later) and Windows Server 2016 and later. This improvement is achieved through automatic configuration of the following policies:

- Add "Appdata\Local\Microsoft\Windows\Caches"and "Appdata\Local\Packages"to "Folders to Mirror"
- Add "Appdata\Local\Microsoft\Windows\UsrClass.Dat*"to "Files to synchronize"

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, automatic configuration is turned on so Profile Management settings might change if the environment changes.

Log off user if a problem is encountered

If this policy is disabled or not configured, users are given a temporary profile if a problem is encountered (for example, the user store is unavailable). If it is enabled, an error message is displayed and users are logged off. This setup can simplify troubleshooting of the problem.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, a temporary profile is provided.

Customer Experience Improvement Program

By default, the Customer Experience Improvement Program is enabled to help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

If this setting is not configured here, the value from the .ini file is used.

Enable search index roaming for Outlook

Allow user-based Outlook search experience by automatically roaming Outlook search data along with user profile. This requires extra spaces in the user store to store search index for Outlook.

You must log off and then log on again for this policy to take effect.

Outlook search index database –backup and restore

This setting configures what Profile Management does during logon when the Enable search index roaming for Outlook is enabled.

If this setting is enabled, Profile Management saves a backup of the search index database each time the database is mounted successfully on logon. Profile Management treats the backup as the good copy of the search index database. When an attempt to mount the search index database fails because the database becomes corrupted, Profile Management automatically reverts the search index database to the last known good copy.

Note: Profile Management deletes the previously saved backup after a new backup is saved successfully. The backup consumes the available storage space of the VHDX files.

Basic policy settings

November 3, 2020

This section contains policy settings relating to the basic configuration of Profile Management.

Enable Profile Management

By default, to facilitate deployment, Profile Management does not process logons or logoffs. Enable Profile Management only after carrying out all other setup tasks and testing how Citrix user profiles perform in your environment.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, Profile Management does not process Windows user profiles in any way.

Processed groups

Both computer local groups and domain groups (local, global, and universal) can be used. Domain groups must be specified in the format: DOMAIN NAME\GROUP NAME.

If this policy is configured here, Profile Management processes only members of these user groups. If this policy is disabled, Profile Management processes all users. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, members of all user groups are processed.

Excluded groups

You can use computer local groups and domain groups (local, global, and universal) to prevent particular user profiles from being processed. Specify domain groups in the form DOMAIN NAME\ GROUP NAME.

If this setting is configured here, Profile Management excludes members of these user groups. If this setting is disabled, Profile Management does not exclude any users. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no members of any groups are excluded.

Process logons of local administrators

Specifies whether logons of members of the BUILTIN\Administrators group are processed. If this policy is disabled or not configured on multi-session operating systems (such as Citrix Virtual Apps environments), Profile Management assumes that logons by domain users, but not local administrators, must be processed. On single-session operating systems (such as Citrix Virtual Desktops environments), local administrator logons are processed. This policy allows domain users with local administrator rights, typically Citrix Virtual Desktops users with assigned virtual desktops, to bypass any processing, log on, and troubleshoot the desktop experiencing problems with Profile Management.

Note: Domain users' logons might be subject to restrictions imposed by group membership, typically to ensure compliance with product licensing.
If this policy is disabled, Profile Management does not process logons by local administrators. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, administrators are not processed.

Path to user store

Sets the path to the directory (the user store) in which the user settings (registry changes and synchronized files) are saved.

The path can be:

- A relative path. It must be relative to the home directory (which is typically configured as the #homeDirectory# attribute for a user in Active Directory).

- A UNC path. It typically specifies a server share or a DFS namespace.
- Disabled or unconfigured. In this case, a value of #homeDirectory#\Windows is assumed.

The following types of variables can be used for this policy:

- System environment variables enclosed in percent signs (for example, %ProfVer%). System environment variables generally require extra setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile Management variables. For more information, see the Profile Management variables product document.

User environment variables cannot be used, except for `%username%` and `%userdomain%`. You can also create custom attributes to define organizational variables such as location or users fully. Attributes are case-sensitive.

Examples:

- \server\share#sAMAccountName# stores the user settings to the UNC path \server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user)
- \server\profiles$\%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! might expand to \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Important: Whichever attributes or variables you use, check that this policy expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in \server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile, set the path to the user store as \server\profiles$\JohnSmith.Finance\Win8x64 (not the \UPM_Profile subfolder).

For more information on using variables when specifying the path to the user store, see the following topics:

- Share Citrix user profiles on multiple file servers
- Administer profiles within and across OUs
- High availability and disaster recovery with Profile Management

If Path to user store is disabled, the user settings are saved in the Windows subdirectory of the home directory.

If this policy is disabled, the user settings are saved in the Windows subdirectory of the home directory. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the Windows directory on the home drive is used.

Migrate user store

Specifies the path to the folder where the user settings (registry changes and synchronized files) were previously saved (the user store path that you previously used).

If this setting is configured, the user settings stored in the previous user store are migrated to the current user store specified in the "Path to user store"policy.

The path can be an absolute UNC path or a path relative to the home directory.

In both cases, you can use the following types of variables: system environment variables enclosed in percent signs and attributes of the Active Directory user object enclosed in hash signs.

Examples:

- The folder `Windows\\%ProfileVer%` stores the user settings in a subfolder called `Windows\W2K3` of the user store (if %ProfileVer% is a system environment variable that resolves to W2K3).
- `\\server\share\\#SAMAccountName#` stores the user settings to the UNC path `\\server\share\<JohnSmith>` (if `#SAMAccountName#` resolves to JohnSmith for the current user).

In the path, you can use user environment variables except `%username%` and `%userdomain%`.

If this setting is disabled, the user settings are saved in the current user store.

If this setting is not configured here, the corresponding setting from the .ini file is used.

If this setting is not configured here or in the .ini file, the user settings are saved in the current user store.

Active write back

Files and folders (but not registry entries) that are modified can be synchronized to the user store in the middle of a session, before logoff.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, it is enabled.

Offline profile support

This policy allows profiles to synchronize with the user store at the earliest possible opportunity. It is aimed at laptop or mobile device users who roam. When a network disconnection occurs, profiles remain intact on the laptop or device even after rebooting or hibernating. As mobile users work, their profiles are updated locally and are eventually synchronized with the user store when the network connection is re-established.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, offline profiles are disabled.

Active write back registry

Use this policy along with "Active write back."Registry entries that are modified can be synchronized to the user store in the middle of a session.

If you do not configure this setting here, the value from the .ini file is used.

If you do not configure this setting here or in the .ini file, active write back registry is disabled.

Offline profile support

Enables the offline profiles feature. This feature is intended for computers that are commonly removed from networks, typically laptops or mobile devices not servers or desktops.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, offline profile support is disabled.

Cross-platform policy settings

November 3, 2020

This section contains policy settings relating to configuring the Profile Management cross-platform settings feature.

Enable cross-platform settings

By default, to facilitate deployment, cross-platform settings are disabled. Turn on processing by enabling this policy but only after thorough planning and testing of this feature.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no cross-platform settings are applied.

Cross-platform settings user groups

Enter one or more Windows user groups. For example, you might use this policy to process only the profiles from a test user group. If this policy is configured, the cross-platform settings feature of Pro-

file Management processes only members of these user groups. If this policy is disabled, the feature processes all users specified by the Processed groups policy.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all user groups are processed.

Path to cross-platform definitions

Identifies the network location of the definition files that you copied from the download package. This path must be a UNC path. Users must have read access to this location, and administrators must have write access to it. The location must be a Server Message Block (SMB) or Common Internet File System (CIFS) file share.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no cross-platform settings are applied.

Path to cross-platform settings store

Sets the path to the cross-platform settings store, the folder in which users'cross-platform settings are saved. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory.

This area is the common area of the user store where profile data shared by multiple platforms is located. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory. You can use the same variables as for Path to user store.

If this policy is disabled, the path Windows\PM_CP is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Source for creating cross-platform settings

Specifies a platform as the base platform if this policy is enabled in that platform's OU. This policy migrates data from the base platform's profiles to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. You must decide which platform's profile data to use to seed the cross-platform settings store. It is referred to as the base platform. If the cross-platform settings store contains a definition file with no data, or the cached data in a single-platform profile is newer than the definition's data in the store, Profile Management migrates the data from the single-platform profile to the store unless you disable this policy.

> **Important:**
>
> If this policy is enabled in multiple OUs, or multiple user or machine objects, the platform that the first user logs on to becomes the base profile.
> By default this policy is Enabled.

File system policy settings

November 3, 2020

This section contains policies that set which files and directories in a user profile are synchronized between the system where the profile is installed and the user store.

Exclusions policy settings

November 3, 2020

This section contains policy settings for configuring which files and directories in a users profile are excluded from the synchronization process.

Exclusion list - files

List of files that are ignored during synchronization. File names must be paths relative to the user profile (%USERPROFILE%). Wildcards are allowed and are applied recursively.

Examples:

- Desktop\Desktop.ini ignores the file Desktop.ini in the Desktop folder
- %USERPROFILE%*.tmp ignores all files with the extension .tmp in the entire profile
- AppData\Roaming\MyApp*.tmp ignores all files with the extension .tmp in one part of the profile

If this policy is disabled, no files are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no files are excluded.

Enable Default Exclusion List - directories

Default list of directories ignored during synchronization. Use this policy to specify GPO exclusion directories without having to fill them in manually.

If you disable this policy, Profile Management does not exclude any directories by default. If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not exclude any directories by default.

Exclusion list - directories

List of folders that are ignored during synchronization. Folder names must be specified as paths relative to the user profile (%USERPROFILE%).

Example:

- Desktop ignores the Desktop folder in the user profile

If this policy is disabled, no folders are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no folders are excluded.

Logon Exclusion Check

This setting configures what Profile Management does if a profile in the user store contains excluded files or folders.

If this setting is disabled or set to the default value **Synchronize excluded files or folders on logon**, Profile Management synchronizes these excluded files or folders from the user store to the local profile when a user logs on.

If this setting is set to **Ignore excluded files or folders on logon**, Profile Management ignores the excluded files or folders in the user store when a user logs on.

If this setting is set to **Delete excluded files or folder on logon**, Profile Management deletes the excluded files or folders in the user store when a user logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the excluded files or folders are synchronized from the user store to the local profile when a user logs on.

Large File Handling - Files to be created as symbolic links

To improve logon performance and to process large files, a symbolic link is created instead of copying files in this list.

You can use wildcards in policies that refer to files; for example, `!ctx_localappdata!\Microsoft\Outlook\*.OST`.

To process the offline folder file (`*.ost`) of Microsoft Outlook, make sure that the **Outlook** folder is not excluded for Profile Management.

Note: those files cannot be accessed in multiple sessions simultaneously.

Synchronization policy settings

November 3, 2020

This section contains policy settings for specifying which files and folders in a users profile are synchronized between the system on which the profile is installed and the user store.

Directories to synchronize

Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. It is not necessary to include subfolders of the user profile by adding them to this list.

Paths on this list must be relative to the user profile.

Example:

- Desktop\exclude\include ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not

Disabling this policy has the same effect as enabling it and configuring an empty list.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only non-excluded folders in the user profile are synchronized.

Files to synchronize

Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. It is not necessary to include files in the user profile by adding them to this list.

This policy can be used to include files under excluded folders. Paths on this list must be relative to the user profile. Wildcards can be used but are only allowed for file names. Wildcards cannot be nested and are applied recursively.

Examples:

- AppData\Local\Microsoft\Office\Access.qat specifies a file below a folder that is excluded in the default configuration

- AppData\Local\MyApp*.cfg specifies all files with the extension .cfg in the profile folder AppData\Local\MyApp and its subfolders

Disabling this policy has the same effect as enabling it and configuring an empty list.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only non-excluded files in the user profile are synchronized.

Folders to mirror

This policy can help solve issues involving any transactional folder (also known as a referential folder). That folder contains interdependent files, where one file references others. Mirroring folders allows Profile Management to process a transactional folder and its contents as a single entity, avoiding profile bloat. For example, you can mirror the Internet Explorer cookies folder so that Index.dat is synchronized with the cookies that it indexes. In these situations the "last write wins."So files in mirrored folders that have been modified in more than one session are overwritten by the last update, resulting in loss of profile changes.

For example, consider how Index.dat references cookies while a user browses the Internet. If a user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session, cookies from each site are added to the appropriate server. When the user logs off from the first session (or in the middle of a session, if the active write back feature is configured), the cookies from the second session must replace those cookies from the first session. However, instead they are merged, and the references to the cookies in Index.dat become out of date. Further browsing in new sessions results in repeated merging and a bloated cookie folder.

Mirroring the cookie folder solves the issue by overwriting the cookies with those cookies from the last session each time the user logs off. So Index.dat stays up-to-date.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no folders are mirrored.

Profile container

A profile container is a VHDX-based profile solution that lets you specify the folders to be contained in the profile disk. The profile container attaches the profile disk containing those folders, thus eliminating the need to save a copy of the folders to the local profile. Doing so decreases logon times.

To use a profile container, enable this policy and add the relative paths of the folders to the list. We recommend that you include the folders containing large cache files to the list. For example, add the **Citrix Files** content cache folder to the list: `AppData\Local\Citrix\Citrix Files\PartCache`.

There are two scenarios to be aware of:

- Profile container does not support simultaneous access by multiple sessions.
- Profile container does not support containing the entire profile.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, it is disabled.

Folder redirection policy settings

November 3, 2020

This section contains policy settings that specify whether to redirect folders that commonly appear in profiles to a shared network location.

Grant administrator access

This setting enables an administrator to access the contents of a user's redirected folders.

> **Note:**
>
> This setting grants permissions to administrators who have complete and unrestricted access to the domain.

By default, this setting is disabled and users are granted exclusive access to the contents of their redirected folders.

Include domain name

This setting enables the inclusion of the `%userdomain%` environment variable as part of the UNC path specified for redirected folders.

By default, this setting is disabled and the `%userdomain%` environment variable is not included as part of the UNC path specified for redirected folders.

AppData(Roaming) policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **AppData(Roaming)** folder to a shared network location.

AppData(Roaming) path

This setting specifies the network location to which the contents of the **AppData(Roaming)** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for AppData(Roaming)

This setting specifies how to redirect the contents of the **AppData(Roaming**) folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Contacts policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Contacts** folder to a shared network location.

Contacts path

This setting specifies the network location to which the contents of the **Contacts** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Contacts

This setting specifies how to redirect the contents of the **Contacts** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Desktop policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Desktop** folder to a shared network location.

Desktop path

This setting specifies the network location to which the contents of the **Desktop** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Desktop

This setting specifies how to redirect the contents of the **Desktop** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Documents policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Documents** folder to a shared network location.

Documents path

This setting specifies the network location to which files in the **Documents** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

The **Documents path** setting must be enabled not only to redirect files to the **Documents** folder, but also to redirect files to the Music, Pictures, and Videos folders.

Redirection settings for Documents

This setting specifies how to redirect the contents of the **Documents** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Documents** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Documents path policy setting.
- Redirect to the users home directory. Redirects content to the users home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Downloads policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Downloads** folder to a shared network location.

Downloads path

This setting specifies the network location to which files in the **Downloads** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Downloads

This setting specifies how to redirect the contents of the **Downloads** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Favorites policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Favorites** folder to a shared network location.

Favorites path

This setting specifies the network location to which the contents of the **Favorites** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Favorites

This setting specifies how to redirect the contents of the **Favorites** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Links policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Links** folder to a shared network location.

Links path

This setting specifies the network location to which the contents of the **Links** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Links

This setting specifies how to redirect the contents of the **Links** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Music policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Music** folder to a shared network location.

Music path

This setting specifies the network location to which the contents of the **Music** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Music

This setting specifies how to redirect the contents of the **Music** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Music** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Music path policy setting.
- Redirect relative to **Documents** folder. Redirects content to a folder relative to the **Documents** folder.

To redirect content to a folder relative to the **Documents** folder, the **Documents path** setting must be enabled.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Pictures policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Pictures** folder to a shared network location.

Pictures path

This setting specifies the network location to which the contents of the **Pictures** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Pictures

This setting specifies how to redirect the contents of the **Pictures** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Pictures** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Pictures path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the **Documents** folder, the **Documents path** setting must be enabled.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Saved Games policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Saved Games** folder to a shared network location.

Redirection settings for Saved Games

This setting specifies how to redirect the contents of the **Saved Games** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Saved Games path

This setting specifies the network location to which the contents of the **Saved Games** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Start menu policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Start Menu** folder to a shared network location.

Redirection settings for Start Menu

This setting specifies how to redirect the contents of the **Start Menu** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Start Menu path

This setting specifies the network location to which the contents of the **Start Menu** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Searches policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Searches** folder to a shared network location.

Redirection settings for Searches

This setting specifies how to redirect the contents of the **Searches** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Searches path

This setting specifies the network location to which the contents of the **Searches** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Video policy settings

November 3, 2020

This section contains policy settings for redirecting the contents of the **Video** folder to a shared network location.

Redirection settings for Video

This setting specifies how to redirect the contents of the **Video** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Video** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Video path policy setting.

- Redirect relative to **Documents** folder. Redirects content to a folder relative to the **Documents** folder.

To redirect content to a folder relative to the **Documents** folder, the **Documents path** setting must be enabled.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Video path

This setting specifies the network location to which the contents of the **Video** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Log policy settings

November 3, 2020

This section contains policy settings that configure Profile Management logging.

Active Directory actions

This setting enables or disables verbose logging of actions performed in Active Directory.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Common information

This setting enables or disables verbose logging of common information.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Common warnings

This setting enables or disables verbose logging of common warnings.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Enable logging

This setting enables or disables Profile Management logging in debug (verbose logging) mode. In debug mode, extensive status information is logged in the log files located in "%SystemRoot%\System32\Logfiles\UserProfileManager".

By default, this setting is disabled and only errors are logged.

Citrix recommends enabling this setting only if you are troubleshooting Profile Management.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only errors are logged.

File system actions

This setting enables or disables verbose logging of actions performed in the file system.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

File system notifications

This setting enables or disables verbose logging of file systems notifications.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Logoff

This setting enables or disables verbose logging of user logoffs.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Logon

This setting enables or disables verbose logging of user logons.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Maximum size of the log file

This setting specifies the maximum permitted size for the Profile Management log file, in bytes.

By default, this is set to 1048576 bytes (1 MB).

Citrix recommends increasing the size of this file to 5 MB or more, if you have sufficient disk space. If the log file grows beyond the maximum size, an existing backup of the file (.bak) is deleted, the log file is renamed to .bak, and a new log file is created.

The log file is created in %SystemRoot%\System32\Logfiles\UserProfileManager.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

Path to log file

This setting specifies an alternative path to save the Profile Management log file.

By default, this setting is disabled and log files are saved in the default location: %SystemRoot%\System32\Logfiles\UserProfileManager.

The path can point to a local drive or a remote network-based drive (UNC path). Remote paths can be useful in large distributed environments but they might create significant network traffic, which

might be inappropriate for log files. For provisioned, virtual machines with a persistent hard drive, set a local path to that drive. This ensures log files are preserved when the machine restarts. For virtual machines without a persistent hard drive, setting a UNC path allows you to retain the log files, but the system account for the machines must have write access to the UNC share. Use a local path for any laptops managed by the offline profiles feature.

If a UNC path is used for log files, Citrix recommends that an appropriate access control list is applied to the log file folder to ensure that only authorized user or computer accounts can access the stored files.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default location %SystemRoot%\System32\Logfiles\UserPr
is used.

Personalized user information

This setting enables or disables verbose logging of personalized user information.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Policy values at logon and logoff

This setting enables or disables verbose logging of policy values when a user logs on and off.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Registry actions

This setting enables or disables verbose logging of actions performed in the registry.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Registry differences at logoff

This setting enables or disables verbose logging of any differences in the registry when a user logs off.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Profile handling policy settings

November 3, 2020

This section contains policy settings that specify how Profile Management handles user profiles.

Delay before deleting cached profiles

This setting specifies an optional extension to the delay, in minutes, before Profile Management deletes locally cached profiles at logoff.

A value of 0 deletes the profiles immediately at the end of the logoff process. Profile Management checks for logoffs every minute, so a value of 60 ensures that profiles are deleted between one and two minutes after users log off (depending on when the last check occurred). Extending the delay is useful if you know that a process keeps files or the user registry hive open during logoff. With large profiles, this can also speed up logoff.

By default, this is set to 0 and Profile Management deletes locally cached profiles immediately.

When enabling this setting, ensure the Delete locally cached profiles on logoff is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, profiles are deleted immediately.

Delete locally cached profiles on logoff

This setting specifies whether locally cached profiles are deleted after a user logs off.

When this setting is enabled, a user's local profile cache is deleted after they have logged off. Citrix recommends enabling this setting for terminal servers.

By default, this setting is disabled and a users local profile cache is retained after they log off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, cached profiles are not deleted.

Local profile conflict handling

This setting configures how Profile Management behaves if a user profile exists both in the user store and as a local Windows user profile (not a Citrix user profile).

By default, Profile Management uses the local Windows profile, but does not change it in any way.

To control how Profile Management behaves, choose one of the following options:

- Use local profile. Profile Management uses the local profile, but does not change it in any way.
- Delete local profile. Profile Management deletes the local Windows user profile, and then imports the Citrix user profile from the user store.
- Rename local profile. Profile Management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local profiles are used.

Migration of existing profiles

This setting specifies the types of profile migrated to the user store during logon if a user has no current profile in the user store.

Profile Management can migrate existing profiles "on the fly"during logon if a user has no profile in the user store. After this, the user store profile is used by Profile Management in both the current session and any other session configured with the path to the same user store.

By default, both local and roaming profiles are migrated to the user store during logon.

To specifies the types of profile migrated to the user store during logon, choose one of the following options:

- Local and roaming profiles
- Local
- Roaming
- None (Disabled)

If you select **None**, the system uses the existing Windows mechanism to create profiles, as if in an environment where Profile Management is not installed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local and roaming profiles are migrated.

Automatic migration of existing application profiles

This setting enables or disables the automatic migration of existing application profiles across different operating systems. The application profiles include both the application data in the **AppData** folder and the registry entries under `HKEY_CURRENT_USER\SOFTWARE`. This setting can be useful in cases where you want to migrate your application profiles across different operating systems.

For example, suppose you upgrade your operating system (OS) from Windows 10 version 1803 to Windows 10 version 1809. If this setting is enabled, Profile Management automatically migrates the existing application settings to Windows 10 version 1809 the first time each user logs on. As a result, the application data in the **AppData** folder and the registry entries under HKEY_CURRENT_USER\SOFTWARE are migrated.

If there are multiple existing application profiles, Profile Management performs the migration in the following order of priority:

1. Profiles of the same OS type (single-session OS to single-session OS and multi-session OS to multi-session OS).
2. Profiles of the same Windows OS family; for example, Windows 10 to Windows 10, or Windows Server 2016 to Windows Server 2016).
3. Profiles of an earlier version of the OS; for example, Windows 7 to Windows 10, or Windows Server 2012 to Windows 2016.
4. Profiles of the closest OS.

Note: You must specify the short name of the OS by including the variable "!CTX_OSNAME!"in the user store path. Doing so lets Profile Management locate the existing application profiles.

If this setting is not configured here, the setting from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled by default.

Path to the template profile

This setting specifies the path to the profile you want Profile Management to use as a template to create user profiles.

The specified path must be the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template profile.

Note: Do not include NTUSER.DAT in the path. For example, with the file \\myservername\myprofiles\template\ntu
set the location as \\myservername\myprofiles\template.

Use absolute paths, which can be either UNC paths or paths on the local machine. Use the latter, for example, to specify a template profile permanently on a Citrix Provisioning Services image. Relative paths are not supported.

Note: This setting does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile overrides local profile

This setting enables the template profile to override the local profile when creating user profiles.

If a user has no Citrix user profile, but a local Windows user profile exists, by default the local profile is used (and migrated to the user store, if this is not disabled). Enabling this policy setting allows the template profile to override the local profile used when creating user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile overrides roaming profile

This setting enables the template profile to override a roaming profile when creating user profiles.

If a user has no Citrix user profile, but a roaming Windows user profile exists, by default the roaming profile is used (and migrated to the user store, if this is not disabled). Enabling this policy setting allows the template profile to override the roaming profile used when creating user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile used as a Citrix mandatory profile for all logons

This setting enables Profile Management to use the template profile as the default profile for creating all user profiles.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Registry policy settings

November 3, 2020

This section contains policy settings that specify which registry keys are included or excluded from Profile Management processing.

Exclusion list

List of registry keys in the HKCU hive which are ignored during logoff.

Example: Software\Policies

If this policy is disabled, no registry keys are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no registry keys are excluded.

Inclusion list

List of registry keys in the HKCU hive that are processed during logoff.

Example: Software\Adobe.

If this policy is enabled, only keys on this list are processed. If this policy is disabled, the complete HKCU hive is processed. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all of HKCU is processed.

Enable Default Exclusion List - Profile Management 5.5

Default list of registry keys in the HKCU hive that are not synchronized to the user's profile. Use this policy to specify GPO exclusion files without having to fill them in manually.

If you disable this policy, Profile Management does not exclude any registry keys by default. If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not exclude any registry keys by default.

NTUSER.DAT backup

Enables a backup of the last known good copy of NTUSER.DAT and rollback in case of corruption.

If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not back up NTUSER.DAT.

Streamed user profiles policy settings

November 3, 2020

This section contains policy settings that specify how Profile Management processes streamed user profiles.

Always cache

This setting specifies whether Profile Management caches streamed files as soon as possible after a user logs on. Caching files after a user logs on saves network bandwidth, enhancing the user experience.

Use this setting with the **Profile streaming** setting.

By default, this setting is disabled and streamed files are not cached as soon as possible after a user logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

Always cache size

This setting specifies a lower limit, in MB, on the size of files that are streamed. Profile Management caches any files this size or larger as soon as possible after a user logs on.

By default, this is set to 0 (zero) and the cache entire profile feature is used. When the cache entire profile feature is enabled, Profile Management fetches all profile contents in the user store, after a user logs on, as a background task.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

Profile streaming

This setting enables and disables the Citrix streamed user profiles feature. When enabled, files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and files in the pending area are fetched immediately.

By default, profile streaming is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

Streamed user profile groups

This setting specifies which user profiles within an OU are streamed, based on Windows user groups.

When enabled, only user profiles within the specified user groups are streamed. All other user profiles are processed normally.

By default, this setting is disabled and all user profiles within an OU are processed normally.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all user profiles are processed.

To enable profile streaming exclusion

When profile streaming exclusion is enabled, Profile Management does not stream folders in the exclusion list, and all the folders are fetched immediately from the user store to the local computer when a user logs on.

For more information, see Stream user profiles.

Timeout for pending area lock files

This setting specifies the number of days after which users' files are written back to the user store from the pending area, in the event that the user store remains locked when a server becomes unresponsive. This prevents bloat in the pending area and ensures the user store always contains the most up-to-date files.

By default, this is set to 1 (one) day.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

User personalization policy settings

February 6, 2020

To enable mounting of user layers within the Virtual Delivery Agents, use configuration parameters to specify:

- Where on the network to access the user layers.
- How large any new user layer disks can grow.

To do so, these two policies appear in the list of available policies:

- User Layer Repository Path - Enter a path in the format '\server name or address\folder name' in the Value field.
- User Layer Size GB - Change the default value of 0 to the maximum size (in GB) that the user layer can grow. If you keep the default value, the maximum user layer size is 10 GB.

> Note:
>
> Changing the User Layer Size in the policy does not change the size of existing layers.

Default layer size is 0.

For more information, see User personalization layer.

Virtual Delivery Agent policy settings

February 6, 2020

The Virtual Delivery Agent (VDA) section contains policy settings that control communication between the VDA and controllers for a site.

Important: The VDA requires information provided by these settings to register with a Delivery Controller, if you are not using the auto-update feature. Because this information is required for registration, you must configure the following settings using the Group Policy Editor, unless you provide this information during the VDA installation:

- Controller registration IPv6 netmask
- Controller registration port
- Controller SIDs
- Controllers
- Only use IPv6 controller registration
- Site GUID

Controller registration IPv6 netmask

This policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the IPv6 address and network where the VDA will register. The VDA will register only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 controller registration policy setting is enabled.

By default this setting is blank.

Controller registration port

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies the TCP/IP port number the VDA uses to register with a Controller when using registry-based registration.

By default, the port number is set to 80.

Controller SIDs

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies a space-separated list of controller Security Identifiers (SIDs) the VDA uses to register with a Controller when using registry-based registration. This is an optional setting which may be used with the Controllers setting to restrict the list of Controllers used for registration.

By default, this setting is blank.

Controllers

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies a space-separated list of controller Fully Qualified Domain Names (FQDNs) the VDA uses to register with a Controller when using registry-based registration. This is an optional setting that may be used with the Controller SIDs setting.

By default, this setting is blank.

Enable auto update of controllers

This setting enables the VDA to register with a Controller automatically after installation.

After the VDA registers, the Controller with which it registered sends a list of the current controller FQDNs and SIDs to the VDA. The VDA writes this list to persistent storage. Each Controller also checks

the Site database every 90 minutes for Controller information; if a Controller has been added or removed since the last check, or if a policy change has occurred, the Controller sends updated lists to its registered VDAs. The VDA will accept connections from all the Controllers in the most recent list it received.

By default, this setting is enabled.

Only use IPv6 controller registration

This setting controls which form of address the VDA uses to register with the Controller:

- When enabled, the VDA registers with the Controller using the machine's IPv6 address. When the VDA communicates with the Controller, it uses the following address order: global IP address, Unique Local Address (ULA), link-local address (if no other IPv6 addresses are available).
- When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.

By default, this is setting is disabled.

Site GUID

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies the Globally Unique Identifier (GUID) of the site the VDA uses to register with a Controller when using Active Directory-based registration.

By default, this setting is blank.

HDX 3D Pro policy settings

February 6, 2020

The HDX 3D Pro section contains policy settings for enabling and configuring the image quality configuration tool for users. The tool enables users to optimize use of available bandwidth by adjusting in real time the balance between image quality and responsiveness.

Enable lossless

This setting specifies whether or not users can enable and disable lossless compression using the image quality configuration tool. By default, users are not given the option to enable lossless compression.

When a user enables lossless compression, the image quality is automatically set to the maximum value available in the image configuration tool. By default, either GPU or CPU-based compression can be used, according to the capabilities of the user device and the host computer.

HDX 3D Pro quality settings

This setting specifies the minimum and maximum values that define the range of image quality adjustment available to users in the image quality configuration tool.

Specify image quality values of between 0 and 100, inclusive. The maximum value must be greater than or equal to the minimum value.

Monitoring policy settings

May 6, 2020

The Monitoring section contains policy settings for process, resource monitoring, and application failure monitoring.

The scope of these policies can be defined based on the Site, Delivery Group, type of Delivery Group, organizational unit, and tags.

Policies for process and resource monitoring

Each data point for CPU, memory, and processes is collected from the VDA and stored on the Monitoring database. Sending the data points from the VDA consumes network bandwidth and storing them consumes considerable space on the monitoring database. If you do not want to monitor either resource data or process data or both for a specific scope (for example, a specific delivery group or organizational unit), it is recommended to disable the policy.

Enable process monitoring

Enable this setting to allow monitoring of processes running on machines with VDAs. Statistics such as CPU and memory use are sent to the Monitoring Service. The statistics are used for real-time notifications and historical reporting in Director.

The default for this setting is Disabled.

Enable resource monitoring

Enable this setting to allow monitoring of critical performance counters on machines with VDAs. Statistics (such as CPU and memory use, IOPS and disk latency data) are sent to the Monitoring Service. The statistics are used for real-time notification and historical reporting in Director.

The default for this setting is Enabled.

Scalability

The CPU and memory data is pushed to the database from each VDA at 5-minute intervals; process data (if enabled) is pushed to the database at 10-minute intervals. IOPS and disk latency data is pushed to the database at 1-hour intervals.

CPU and memory data

CPU and memory data is **enabled** by default. The data retention values are as follows (Platinum license):

Data granularity	Number of Days
5 Minute Data	1 Day
10 Minute Data	7 Days
Hourly Data	30 Days
Daily Data	90 Days

IOPS and disk latency data

IOPS and disk latency data is **enabled** by default. The data retention values are as follows (Platinum license):

Data granularity	Number of Days
Hourly Data	3 Days
Daily Data	90 Days

With the data retention settings as above, approximately 276 KB of disk space is required to store the CPU, memory, IOPS and disk latency data for one VDA over a period of one year.

Number of machines	Approximate storage required
1	276 KB
1K	270 MB
40K	10.6 GB

Process data

Process data is **disabled** by default. It is recommended to enable process data on a subset of machines on a need basis. The default data retention settings for the process data is as follows:

Data granularity	Number of Days
10-minute Data	1 Day
Hourly Data	7 Days

If process data is enabled, with the default retention settings, process data would consume approximately 1.5 MB per VDA and 3 MB per Terminal Services VDA (TS VDA) over a period of one year.

Number of machines	Approximate storage required VDA	Approximate storage required TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

> **Note**
>
> The above numbers do not include the Index space. And all the above calculations are approximate and may vary depending on the deployment.

Optional Configurations

You can modify the default retention settings to suit your needs. However, this consumes extra storage. By enabling the settings below you can gain more accuracy in the process utilization data. The configurations which can be enabled are:

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

These Configurations can be enabled from the Monitoring PowerShell cmdlet: Set-MonitorConfiguration

Policies for application failure monitoring

The **Application Failure** tab, by default, displays only application faults from Multi-session OS VDAs. Settings of Application failure monitoring can be modified with the following Monitoring policies:

Enable monitoring of application failures

Use this setting to configure application failure monitoring to monitor either application errors or faults (crashes and unhandled exceptions), or both. Disable application failure monitoring by setting the **Value** to **None**. The default for this setting is Application faults only.

Enable monitoring of application failures on Single-session OS VDAs

By default, failures only from applications hosted on the Multi-session OS VDAs are monitored. To monitor Single-session OS VDAs, set the policy to **Allowed**. The default for this setting is **Prohibited**.

List of applications excluded from failure monitoring

Specify a list of applications that are not to be monitored for failure.
By default this list is empty.

Storage planning tips

Group policy. If you are not interested in monitoring the Resource Data or Process Data, either or both can be turned off using the group policy. For more information, see the Group Policy section of Create policies.

Data grooming. The default data retention settings can be modified to groom the data early and free up storage space. For more information on grooming settings, see Data granularity and retention in Accessing data using the API.

Virtual IP policy settings

February 6, 2020

> **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.

The Virtual IP section contains policy settings that control whether sessions have their own virtual loopback address.

Virtual IP loopback support

When this setting is enabled, each session has its own virtual loopback address. When disabled, sessions do not have individual loopback addresses.

By default, this setting is disabled.

Virtual IP virtual loopback programs list

This setting specifies the application executables that can use virtual loopback addresses. When adding programs to the list, specify only the executable name; you do not need to specify the entire path.

By default, no executables are specified.

Configure COM Port and LPT Port Redirection settings using the registry

February 6, 2020

In VDA versions 7.0 through 7.8, COM Port and LPT Port settings are only configurable using the registry. For VDA versions earlier than 7.0 and for VDA versions 7.9 and later, these settings are configurable in Studio. For more information, see Port redirection policy settings and Bandwidth policy settings.

Policy settings for COM Port and LPT Port Redirection are located under HKLM\Software\Citrix\GroupPolicy\Default on the VDA image or machine.

To enable COM port and LPT port redirection, add new registry keys of type REG_DWORD, as follows:

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.

Registry key	Description	Permitted values
AllowComPortRedirection	Allow or prohibit COM port redirection	1 (Allow) or 0 (Prohibit)
LimitComBw	Bandwidth limit for COM port redirection channel	Numeric value
LimitComBWPercent	Bandwidth limit for COM port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientComPorts	Automatically connect COM ports from the user device	1 (Allow) or 0 (Prohibit)
AllowLptPortRedirection	Allow or prohibit LPT port redirection	1 (Allow) or 0 (Prohibit)
LimitLptBw	Bandwidth limit for LPT port redirection channel	Numeric value
LimitLptBwPercent	Bandwidth limit for LPT port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientLptPorts	Automatically connect LPT ports from the user device	1 (Allow) or 0 (Prohibit)

After configuring these settings, change your machine catalogs to use the new master image or updated physical machine. Desktops are updated with the new settings the next time users log off.

Connector for Configuration Manager 2012 policy settings

February 6, 2020

The Connector for Configuration Manager 2012 section contains policy settings for configuring the Citrix Connector 7.5 agent.

Important: Warning, logoff, and reboot message policies apply only to deployments to Multi-session OS machine catalogs that are managed manually or by Provisioning Services. For those machine catalogs, the Connector service alerts users when there are pending application installs or software updates.

For catalogs managed by MCS, use Studio to notify users. For manually managed Single-session OS catalogs, use Configuration Manager to notify users. For Single-session OS catalogs managed by Provisioning Services, use Provisioning Services to notify users.

Advance warning frequency interval

This setting defines the interval between appearances of the advance warning message to users.

Intervals are set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the interval setting is 1 hour (01:00:00).

Advance warning message box body text

This setting contains the editable text of the message to users notifying them of upcoming software updates or maintenance that requires them to log off.

By default, the message is: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}

Advance warning message box title

This setting contains the editable text of the title bar of the advance warning message to users.

By default, the title is: Upcoming Maintenance

Advance warning time period

This setting defines how far before maintenance the advance warning message first appears.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the setting is 16 hours (16:00:00), indicating that the first advance warning message appears approximately 16 hours before maintenance.

Final force logoff message box body text

This setting contains the editable text of the message alerting users that a forced logoff has begun.

By default, the message is: The server is currently going offline for maintenance

Final force logoff message box title

This setting contains the editable text of the title bar of the final force logoff message.

By default, the title is: Notification From IT Staff

Force logoff grace period

This setting defines the period of time between notifying users to log off and the implementation of the forced logoff to process the pending maintenance.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the force logoff grace period setting is 5 minutes (00:05:00).

Force logoff message box body text

This setting contains the editable text of the message telling users to save their work and log off prior to the start of a forced logoff.

By default, the message contains the following: {TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}

Force logoff message box title

This setting contains the editable text of the title bar of the force logoff message.

By default, the title is: Notification From IT Staff

Image-managed mode

The Connector agent automatically detects if it is running on a machine clone managed by Provisioning Services or MCS. The agent blocks Configuration Manager updates on image-managed clones and automatically installs the updates on the master image of the catalog.

After a master image is updated, use Studio to orchestrate the reboot of MCS catalog clones. The Connector Agent automatically orchestrates the reboot of PVS catalog clones during Configuration Manager maintenance windows. To override this behavior so that software is installed on catalog clones by Configuration Manager, change Image-managed mode to Disabled.

Reboot message box body text

This setting contains the editable text of the message notifying users when the server is about to be restarted.

By default, the message is: The server is currently going offline for maintenance

Regular time interval at which the agent task is to run

This setting determines how frequently the Citrix Connector agent task runs.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the regular time interval setting is 5 minutes (00:05:00).

Manage

February 12, 2021

Managing a Citrix Virtual Apps and Desktops site covers a variety of items and tasks.

Licensing

A valid connection to the Citrix License Server is required when you create a site. Later, you can complete several licensing tasks from Studio, including adding licenses, changing license types or models,

and managing license administrators. You can also access the License Administration Console from Studio.

Applications

Manage applications in Delivery Groups and optionally, Application Groups.

Zones

In a geographically disperse deployment, you can use zones to keep applications and desktops closer to end users, which can improve performance. When you install and configure a site, all Controllers, Machine Catalogs, and host connections are in one primary zone. Later, you can use Studio to create satellite zones containing those items. After your site has more than one zone, you will be able to indicate in which zone any newly-created Machine Catalogs, host connections, or added Controllers will be placed. You can also move items between zones.

Connections and resources

If you are using a hypervisor or cloud service to host machines that will deliver applications and desktops to users, you create your first connection to that hypervisor or cloud service when you create a site. The storage and network details for that connection form its *resources*. Later, you can change that connection and its resources, and create new connections. You can also manage the machines that use a configured connection.

Local Host Cache

Local Host Cache allows connection brokering operations in a site to continue when the connection between a Delivery Controller and the site database fails.

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. 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.*).

Delivery Controllers

This article details considerations and procedures when adding and removing Controllers from a site. It also describes how to move Controllers to another zone or site, and how to move a VDA to another site.

VDA registration with Controllers

Before a VDA can facilitate delivery of applications and desktops, it must register (establish communication) with a Controller. Controller addresses can be specified in several ways, which are described in this article. It is critical that VDAs have current information as Controllers are added, moved, and removed in the site.

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.

- Session reliability
- Auto Client Reconnect
- ICA Keep-Alive
- Workspace control
- Session roaming

Using search in Studio

When you want to view information about machines, sessions, Machine Catalogs, applications, or Delivery Groups in Studio, use the flexible search feature.

Tags

Use tags to identify items such as machines, applications, groups, and policies. You can then tailor certain operations to apply on to items with a specific tag.

IPv4/IPv6

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.

User profiles

By default, Citrix Profile management is installed automatically when you install a VDA. If you use this profile solution, review this article for general information and see the Profile management documentation for full details.

Citrix Insight Services

Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation.

Licensing

August 4, 2022

> **Note:**
>
> Studio and Director do not support Citrix License Server VPX.

From Studio, you can manage and track licensing, if the license server is in the same domain as Studio or in a trusted domain. For information about other licensing tasks, see the licensing documentation and Multi-type licensing.

You must be a full license administrator to complete the tasks described in this article, except for viewing license information. To view license information in Studio, an administrator must have at least the Read Licensing Delegated Administration permission; the built-in Full Administrator and Read-Only Administrator roles have that permission.

The following table lists the supported editions and license models:

Products	Editions	License models
Citrix Virtual Apps	Premium, Advanced, Standard	Concurrent
Citrix Virtual Desktops	Premium, Advanced, Standard	User/Device and Concurrent

For more information about license sharing, see Concurrent licenses.

> **Important:**
>
> The License Server VPX is deprecated and won't receive any further maintenance or security fixes. Customers using 11.16.6 or previous versions of License Server VPX are advised to migrate to the latest version of License Server for Windows as soon as possible.

Supported Current Release (CRs) and Long Term Service Release (LTSRs) version

For information about supported Current Release (CRs), Long Term Service Release (LTSRs), and minimum compatible LS versions, see the Citrix Virtual Apps and Desktops current release documentation.

View license information

Select **Configuration > Licensing** in the Studio navigation pane. A summary of license usage and settings for the Site is displayed with a list of all the licenses currently installed on the specified license server.

Ensure that the licensing settings for the site, which include the product type, license edition, and licensing model, match the licenses your configured License Server uses. If not, you might have to download or allocate your exiting licenses to match the site's license settings.

To download a license from Citrix:

1. Select **Configuration > Licensing** in the Studio navigation pane.

2. Select **Allocate Licenses** in the Actions pane.
3. Type the License Access Code, which is supplied in an email from Citrix.
4. Select a product and choose **Allocate Licenses**. All the licenses available for that product are allocated and downloaded. After you allocate and download all the licenses for a specific License Access Code, you cannot use that License Access Code again. To perform other transactions with that code, log on to My Account.

To add licenses that are stored on your local computer or on the network:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select **Add Licenses** in the Actions pane.
3. Browse to a license file and add it to the license server.

To change the license server:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select **Change License Server** in the Actions pane.
3. Type the address of the license server in the form *name:port*, where the name is a DNS, NetBIOS, or IP address. If you do not specify a port number, the default port (27000) is used.

To select the type of license to use:

- When configuring the Site, after you specify the license server, you are prompted to select the type of license to use. If there are no licenses on the server, the option to use the product for a 30-day trial period without a license is automatically selected.
- If there are licenses on the server, their details are displayed and you can select one of them. Or, you can add a license file to the server and then select that one.

To change the product edition and licensing model:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select **Edit Product Edition** in the Actions pane.
3. Update the appropriate options.

To access the License Administration Console, in the Actions pane, select **License Administration Console**. The console either appears immediately, or if the dashboard is configured as password-protected, you are prompted for License Administration Console credentials. For details about how to use the console, see the licensing documentation.

To add a licensing administrator:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane.
3. Select **Add licensing administrator** in the Actions pane.
4. Browse to the user you want to add as an administrator and choose permissions.

To change a licensing administrator's permissions or delete a licensing administrator:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane and then select the administrator.
3. Select either **Edit licensing administrator** or **Delete licensing administrator** in the Actions pane.

To add a licensing administrator group:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane.
3. Select **Add licensing administrator group** in the Actions pane.
4. Browse to the group you want to act as licensing administrators and choose permissions. Adding an Active Directory Group gives licensing administrator permissions to the users within that group.

To change a licensing administrator group's permissions or delete a licensing administrator group:

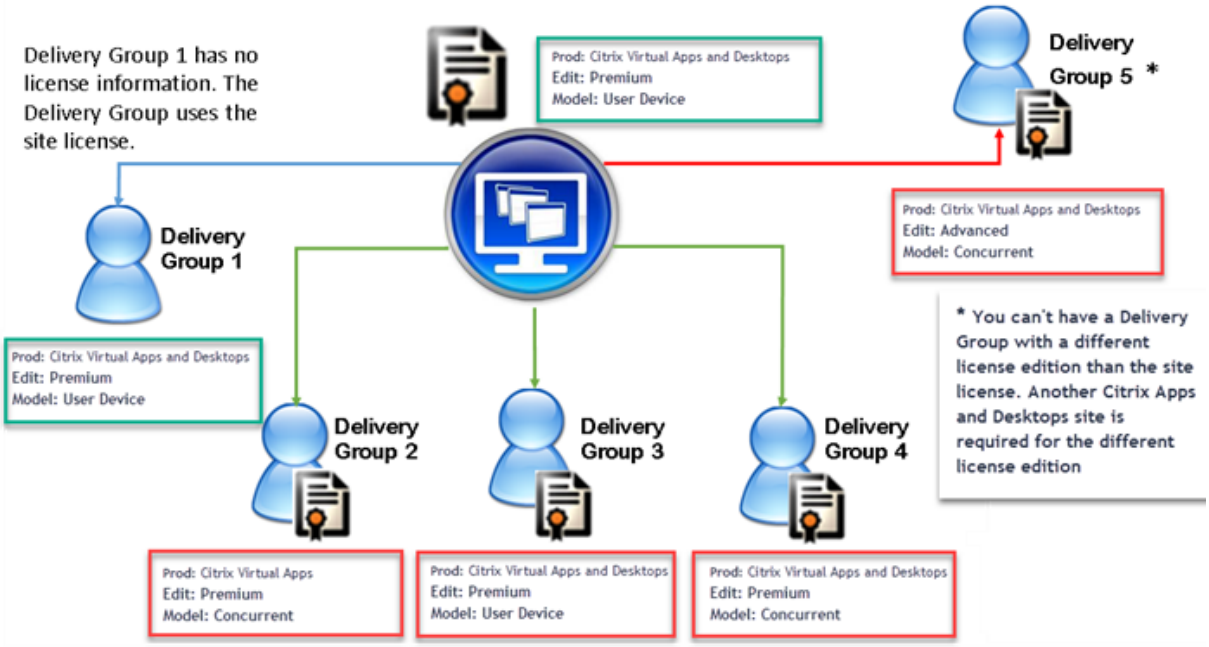
1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane and then select the administrator group.
3. Select either **Edit licensing administrator group** or **Delete licensing administrator group** in the Actions pane.

Multi-type licensing

March 7, 2022

Multi-type licensing supports consumption of different license types for delivery groups on a single Citrix Virtual Apps and Desktops site. **Type** is a single combination of Product ID (XDT or MPS) and Model (UserDevice or Concurrent). The delivery groups must use the same Product Edition (PLT/Premium or ENT/Advanced) as configured at the site level. Be aware of the special considerations at the end of this article when looking to configure multi-type licensing for your Citrix Virtual Apps and Desktops deployments.

If multi-type licensing is not configured, different license types can be used only when configured for separate sites. The delivery groups use the site license. For important notification limitations when multi-type licensing is configured, see Special considerations.



To determine the Delivery Groups that consume the different types of licenses, use these Broker PowerShell cmdlets:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

To install licenses, use:

- Citrix Studio
- Citrix Licensing Manager
- License Administration Console
- citrix.com

Subscription Advantage dates are specific to each license file and to each product and model. Delivery Groups set differently might have different Subscription Advantage dates than each other.

License compatibility matrix

This table details old product names, new product names, and the associated feature names. The four compatibility columns specify which product and license model combinations are compatible for multi-type licensing. For example, all types with an **X** under column **1** are compatible. CCU and CCS stand for concurrent licenses and UD is user/device licenses.

Old Name	New Name	Feature	Multi-type licensing compatibility 1	2	3	4
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
CSP - Citrix XenApp Base	Citrix Virtual Apps Base	XDT_ADV_UD		X		
CSP Premium	Citrix Virtual Apps and Desktops Premium	XDT_PLT_UD				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops - Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

Broker PowerShell SDK

The **DesktopGroup** object has these two properties you can manipulate using the associated New-BrokerDesktopGroup and Set-BrokerDesktopGroup cmdlets.

Name	Value	Restriction
LicenseModel	A parameter (Concurrent or UserDevice) specifying the licensing model for the group. If none is specified, the site-wide license model is used.	If the feature toggle is disabled, attempting to set a property fails.
ProductCode	A text string of XDT (for Citrix Virtual Desktops) or MPS (for Citrix Virtual Apps) specifying the licensing Product ID for the group. If none is specified, the site-wide product code is used.	If the feature toggle is disabled, attempting to set a property fails.

For more information about the **LicenseModel** and **ProductCode**, see about_Broker_Licensing.

New-BrokerDesktopGroup

Creates a desktop group for managing the brokering of groups of desktops. For more information on this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

Set-BrokerDesktopGroup

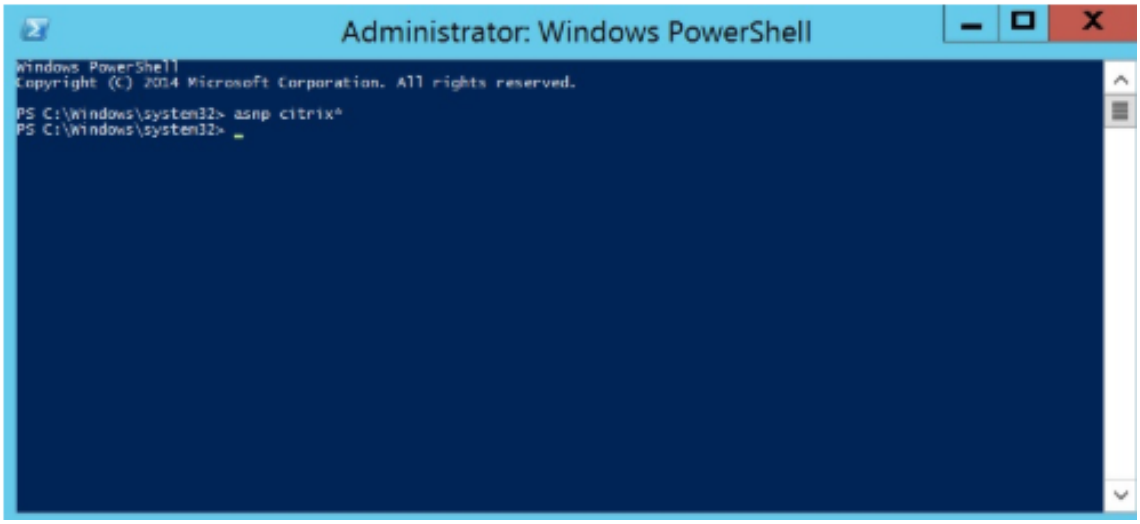
Disables or enables an existing broker desktop group or alters its settings. For more information on this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

Get-BrokerDesktopGroup

Retrieves desktop groups matching the specified criteria. The output of the Get-BrokerDesktopGroup cmdlet includes the **ProductCode** and **LicenseModel** properties of the group. If the properties have not been set using New- BrokerDesktopGroup or Set-BrokerDesktopGroup, null values are returned. If null, the site-wide license model and product code are used. For more information on this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

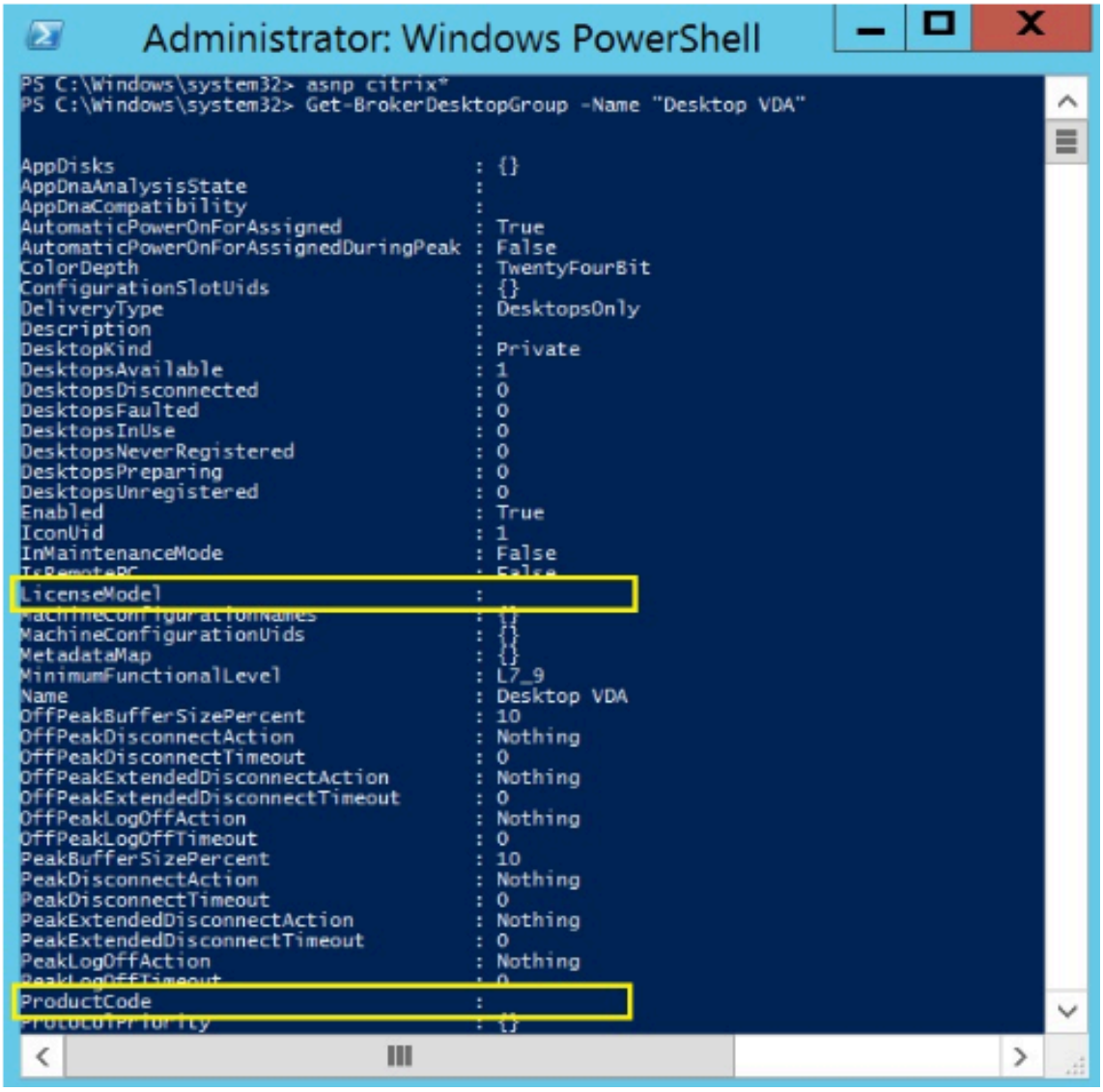
Configure different license products and models per delivery group

1. Open PowerShell with Administrative rights and add the Citrix snapin.

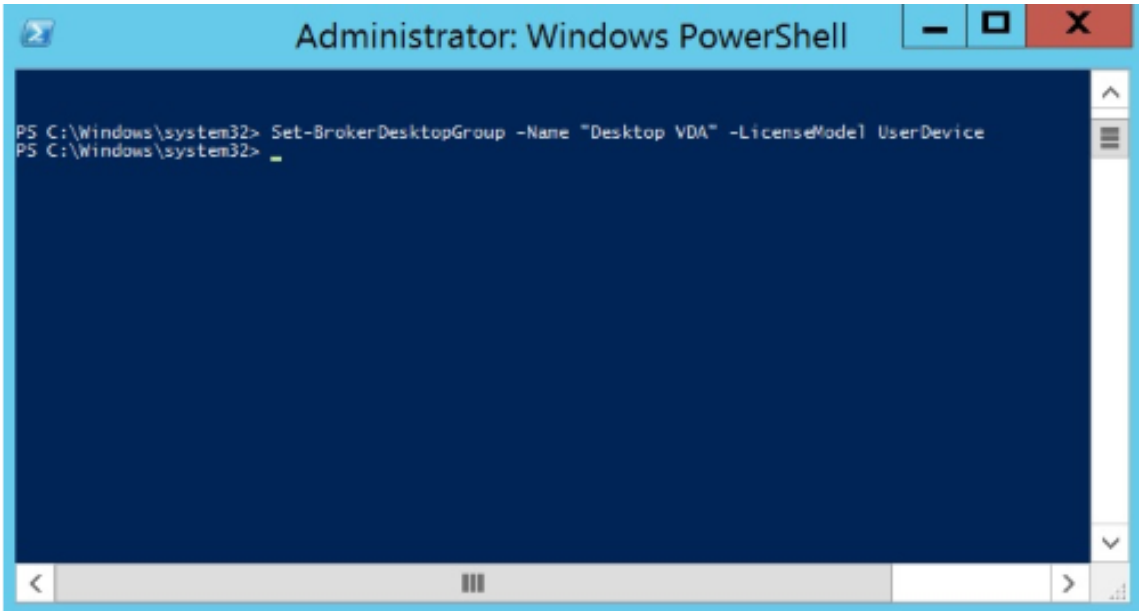


2. Run the command **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** to view the current license configuration. Find the parameters **LicenseModel** and **ProductCode**. If you haven't configured these parameters before, they might be blank.

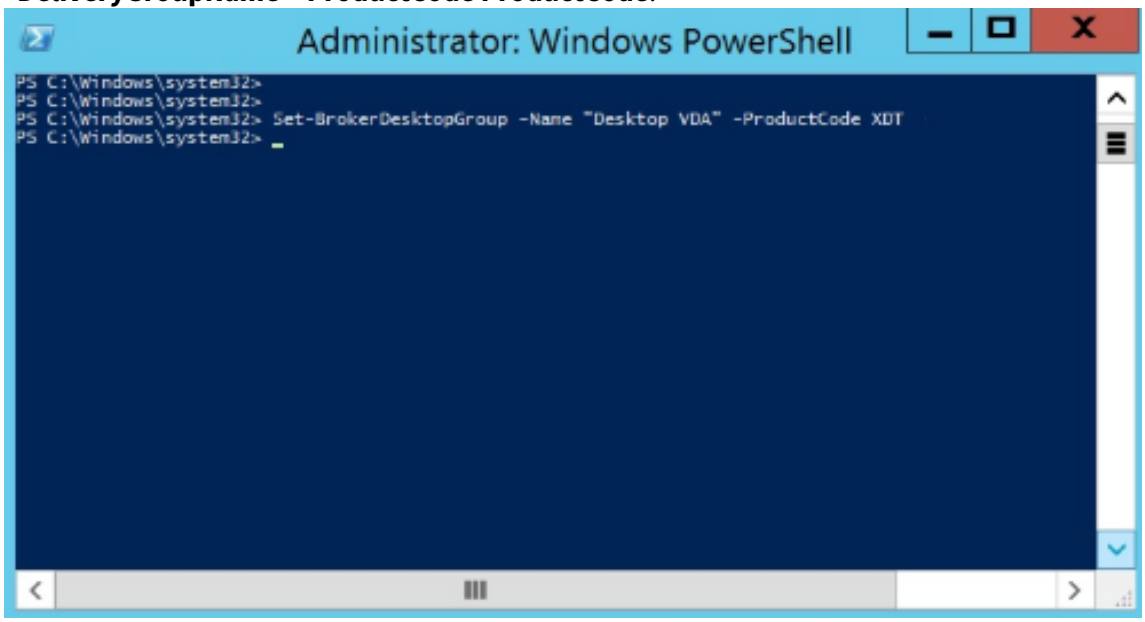
> Note:
>
> If a delivery group does not have license information set, it defaults to **Site level Site license**.



3. Change the license model by running the command: **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–LicenseModel LicenseModel**.

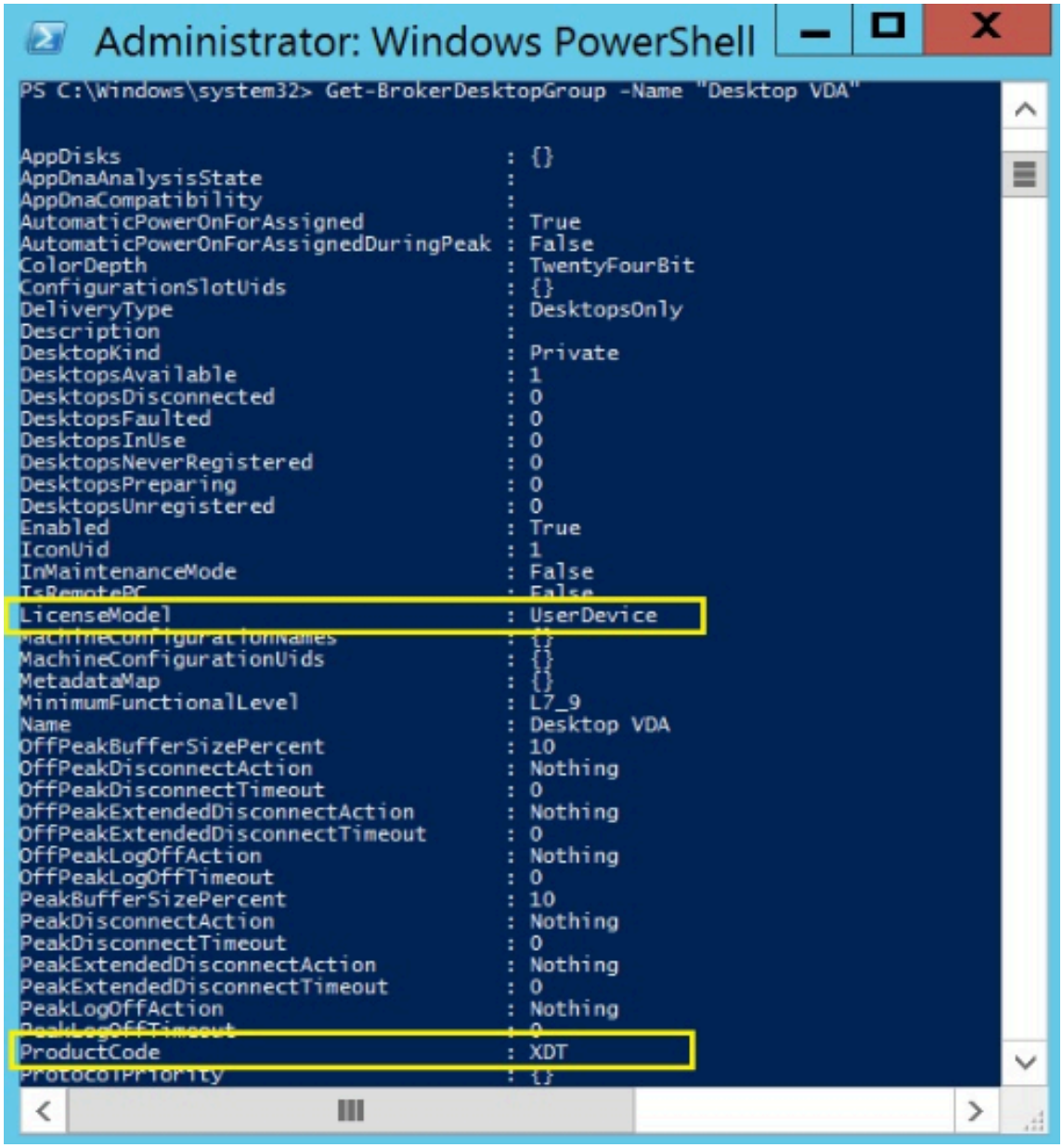


4. Change the license product by running the command: **Set-BrokerDesktopGroup** –**Name "DeliveryGroupName"**–**ProductCode ProductCode**.



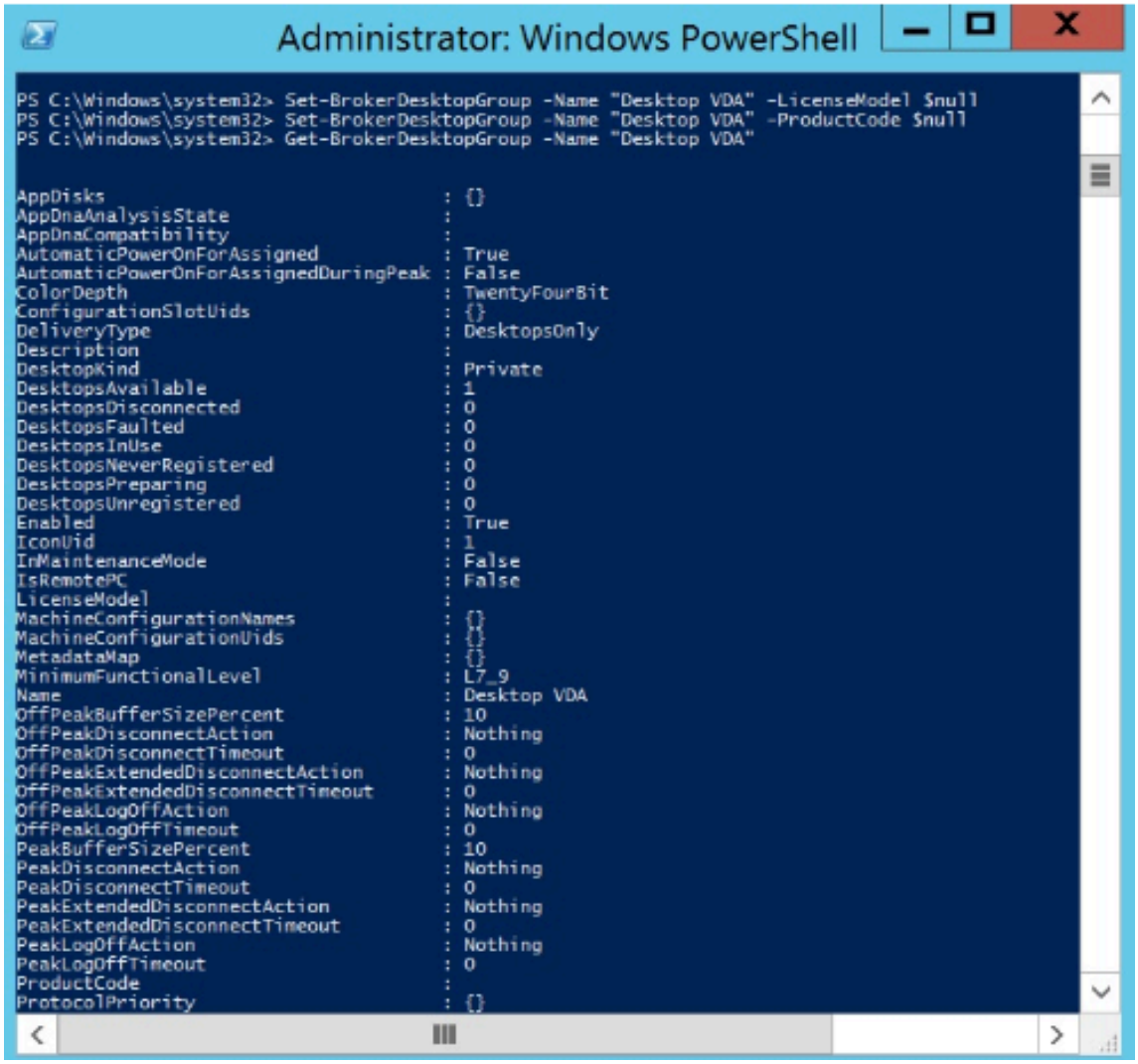
5. Enter the command **Get-BrokerDesktopGroup** –**Name "DeliveryGroupName"** to validate the changes.

> Note:
>
> You cannot mix and match editions in the same site. For example, Premium and Advanced licenses. Multiple sites are required if you have licenses with different editions.



6. Remove the license configuration by running the same **Set-BrokerDesktopGroup** commands as described above, and set the value to **$null**.

> Note:
>
> Studio doesn't display the license configuration for each delivery group. Use PowerShell to view the current configuration.



Example

This PowerShell cmdlet example illustrates setting multi-type licensing for two existing Delivery Groups and creates and sets a third delivery group.

To see the license product and license model associated with a delivery group, use the **Get-BrokerDesktopGroup** PowerShell cmdlet.

1. We set the first delivery group for XenApp and Concurrent.

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Apps Premium Concurrent”-ProductCode MPS -LicenseModel Concurrent

2. We set the second delivery group for XenDesktop and Concurrent.

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent”-ProductCode XDT -LicenseModel Concurrent

3. We create and set the third delivery group for XenDesktop and UserDevice.

   New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Special considerations

Multi-type licensing has different functionality than regular Citrix Virtual Apps and Desktops licensing.

There are no alerts and notifications from Director or Studio for delivery groups configured to use a type that differs from the site configuration:

- No information when nearing license limits or the trigger or expiry of the supplemental grace period.
- No notification when a specific group has a problem.

Delivery groups configured for multi-type licenses consume ONLY that license type and don’t fall back to the site configuration when fully consumed.

Though Citrix Virtual Apps Standard and Citrix Virtual Desktops Standard license edition names indicate that they are both Standard, they are not the same edition. Multi-type licensing does not work with Citrix Virtual Apps Standard and Citrix Virtual Desktop Standard licenses.

FAQ for licensing

October 27, 2022

> **Note:**
>
> - For business continuity resources related to the COVID-19 pandemic, see CTX27055.
> - For general information about maintaining business continuity, see Business continuity — on demand.
> - For more information about the current Citrix License Server, see Licensing.

How is Citrix Virtual Apps and Desktops licensed?

The Citrix Virtual Apps and Desktops licensing offers user/device and concurrent license models.

User/device:

The flexible user/device model aligns with:

- Enterprise-wide desktop usage.
- Underlying Microsoft desktop virtualization licensing.
- Concurrent licensing for customers with users needing only occasional access to their virtual desktops and apps.

User/device licensing gives users access to their virtual desktops and apps from an unlimited number of devices. Device licenses give an unlimited number of user's access to their virtual desktops and apps from a single device. This approach provides you with maximum flexibility and improves alignment with Microsoft desktop virtualization licensing.

> **Important:**
>
> You can't manually assign licenses to a user or device. The License Server or cloud service assigns licenses. With user/device licensing, once a license is assigned it can't be assigned to another user until after 90 days of inactivity.

Concurrent:

Concurrent licenses allow one connection to an unlimited number of virtual apps and desktops for any user and any device. A license is consumed only during an active session. If the session disconnects or is terminated, the license is checked back into the pool.

For more information about user/device licensing, see User/device licenses and concurrent licenses see, Concurrent licenses.

Is it possible to try Citrix Virtual Apps and Desktops before purchasing licenses?

Yes. You can download the Citrix Virtual Apps and Desktops software and run it in trial mode. Trial mode lets you use Citrix Virtual Apps and Desktops on-premises for 30 days, for 10 connections, without a license.

Citrix Virtual Apps and Desktops Services for Citrix Cloud is available for trial service based on approval. Check with your Citrix representative for further details.

How does Citrix define concurrency for Citrix Virtual Apps and Desktops?

The Citrix Virtual Apps and Desktops concurrent model allows one connection to an unlimited number of virtual apps and desktops for any user and any device. A license is consumed only during an active session. If the session disconnects or is terminated, the license is checked back into the pool for reissue.

How does Citrix assign licenses to users in the user/device licensing model?

With the user/device license model, the License Server assigns the license to a unique user ID. It allows that single user unlimited connections from unlimited devices. If a user connects to a desktop or device, the user requires one license assigned to that user to access a virtual desktop or application. The License Server or cloud service assigns the license. You can't assign these licenses manually. The license is assigned to the user, not the shared device. Once a license is assigned, it can't be assigned to another user until after 90 days of inactivity.

How does Citrix define a licensed device in the user/device licensing model?

A licensed device requires a unique endpoint device ID. Under the user/device model, a device is any piece of equipment that you authorized for use by any individuals to access instances of Citrix Virtual Apps and Desktops. For a shared device, a single Citrix Virtual Apps and Desktops user/device license can support multiple users that share the device. For example, a shared device can be a classroom workstation or a clinical workstation in a hospital.

Can I convert my Citrix Virtual Desktops Standard Edition concurrent licenses to the user/device model?

You cannot convert Citrix Virtual Desktops Standard Edition concurrent licenses to Citrix Virtual Desktops Standard Edition user/device licenses. Similarly, you cannot convert Citrix Virtual Desktops Standard Edition user/device licenses to Citrix Virtual Desktops Standard Edition concurrent licenses.

If you have Citrix Virtual Desktops Standard Edition concurrent licenses and you want the user/device license model, upgrade to either Citrix Virtual Apps and Desktops Advanced or Premium Edition.

From	To Standard concurrent	To Standard user/device	To Advanced user/device	To Premium user/device
Citrix Virtual Desktops Standard Edition concurrent licenses	N/A	Concurrent to user/device conversion NOT allowed	You cannot convert license models, but you can upgrade to Citrix Virtual Apps and Desktops Advanced or Premium Edition.	You cannot convert license models, but you can upgrade to Citrix Virtual Apps and Desktops Advanced or Premium Edition.

From	To Standard concurrent	To Standard user/device	To Advanced user/device	To Premium user/device
Citrix Virtual Desktops Standard Edition user/device licenses	User/device to concurrent conversion NOT allowed	N/A	N/A	N/A

How does concurrent licensing work differently from user/device licensing?

We base concurrent licensing on concurrent device connections. A concurrent license is in use only when a device has established an active connection. Once the connection ends, the concurrent license returns to the license pool for immediate use. We recommend this licensing model for occasional usage. User/device licenses are leased for a period and are not available for other users until the lease expires.

Under the user/device model, can we assign licenses to both users and devices in the same enterprise?

Yes. Both types can be present in the same enterprise. The License Server optimally assigns licenses to users or devices based on usage. You can't assign these licenses manually.

How do I decide how many users or devices to license?

Assess the use case requirements to determine the appropriate number of licenses. User/device licensing enables unlimited access to unlimited virtual desktops and virtual apps from an unlimited number of devices. Concurrent licensing enables unlimited access to unlimited virtual desktops and virtual apps from a single device that an unlimited number of users can use. Consider the following formula:

```
(Number of total users) – (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 – 700 + 300 = 600 licenses.
<!--NeedCopy-->
```


Under the user/device model, what is the maximum number of devices a licensed user can use to connect to my environment?

Each licensed user is entitled to use an unlimited number of connected or offline devices.

Under the user/device model, what is the maximum number of users who can access a licensed device?

Each licensed device can service an unlimited number of users within an organization.

Under the user/device model, what is the maximum number of virtual desktops or Remote Browser Isolation (RBI) web applications a licensed user can consume at any given time?

Each licensed user can connect to an unlimited number of virtual desktops or web applications.

What is the maximum number of virtual applications a licensed user can consume at any given time?

Each licensed user can connect to an unlimited number of virtual applications.

What happens if a licensed user leaves my organization?

When an existing licensed user leaves your organization, you can release the departing user's license without notifying Citrix. Use the `udadmin` utility to release the license. If you don't release the license, the License Server automatically releases any license after 90 days of inactivity. This information is subject to terms specified in the EULA.

What happens if a licensed user is absent for a protracted period?

If an existing licensed user is absent for a protracted period, you can release the license without notifying Citrix, so that it becomes available for reassignment. Use the `udadmin` utility to release the license.

What happens if we replace a licensed device in my organization?

If you replace an existing licensed device, you can release the license without notifying Citrix so that it becomes available for reassignment. Use the `udadmin` utility to release the license.

What happens if a licensed device is out of service for an extended period?

When an existing licensed device is out of service for an extended period, you can release the license without notifying Citrix, so that it becomes available for reassignment. Use the `udadmin` utility to release the licenses. If you don't release the license, the License Server automatically releases any license after 90 days of inactivity. This information is subject to terms specified in the EULA.

Can I switch user licenses to device licenses and conversely after I've assigned the licenses to a device or user?

Yes. This change happens automatically. The License Server assigns licenses to either users or devices based on usage patterns. If usage patterns change, the License Server might switch the assignment based on the new usage. The License Server always assigns licenses in the most economical fashion for the customer. Also, the License Server monitors licenses to identify **unused** licenses after their 90-day assignment period. You can reassign licenses identified as unused after the 90-day assignment period to other users or devices.

Under the concurrent model, what is the maximum number of virtual desktops a Citrix Virtual Apps and Desktops licensed user can consume at any given time?

An endpoint can service many users and allows for unlimited connections.

Can I purchase Citrix Virtual Apps and Desktops licenses to increase the number of licensed users/devices in my existing Citrix Virtual Apps and Desktop environment?

Yes. You can purchase Citrix Virtual Apps and Desktop licenses to increase the number of licensed users/devices in your existing Citrix Virtual Apps and Desktop environment.

Can I deploy concurrent licenses from a previous version of Citrix Virtual Apps and Desktops and new user/device or concurrent licenses to a single License Server?

Yes. You can continue to use the same License Server to support user/device or concurrent licensed deployments.

Can I deploy concurrent licenses and user/device or concurrent licenses to a single License Server?

Yes. You can continue to use the same License Server to support concurrent and user/device or concurrent licensed deployments.

Can I deploy multiple editions of Citrix Virtual Apps and Desktops licenses on a common License Server?

Yes. The License Server manages licenses for both Citrix Virtual Apps and Desktops simultaneously. We recommend that you install the latest License Server version. If you are unsure if your License Server version is current, verify it by comparing your version with the number on the Citrix downloads site.

Can a single site use both Citrix Virtual Apps and Citrix Virtual Apps and Desktops licenses?

Depending on the version, a single Citrix Virtual Apps or Citrix Virtual Apps and Desktops site can support both licensing models - user/device or concurrent. A single Citrix Virtual Apps or Citrix Virtual Apps and Desktops site can support only one edition. For more information, see Multi-type licensing.

The minimum versions that support multi-type licensing are XenApp and XenDesktop 7.15 Long Term Service Release (LTSR) and Citrix Virtual Apps and Desktops 7 1808.

Can I select Citrix Virtual Apps concurrent as a product model if I have Citrix Virtual Apps and Desktops user/device or Citrix Virtual Apps and Desktops concurrent licenses installed on the License Server?

If you use Citrix Virtual Apps as a feature of Citrix Virtual Apps and Desktops Advanced or Premium Edition, your Citrix Virtual Apps license model is the same as your Advanced or Premium Edition of Citrix Virtual Apps and Desktops. If you have purchased Citrix Virtual Apps and Desktops, configure your licensing as Citrix Virtual Apps and Desktops even if you plan to use only the Citrix Virtual Apps functionality. Select Citrix Virtual Apps as a product model only if you have Citrix Virtual Apps concurrent standalone licenses installed on the License Server.

Overdraft licenses

This section answers your questions about overdraft licenses.

How do I get overdraft licenses? License overdraft is included in all user/device licenses. When you purchase user/device licenses, you receive a 10% overdraft. The overdraft becomes available after you allocate all your purchased and evaluation licenses. We offer the overdraft feature as a convenience, not as a license entitlement. If you use the overdraft licenses often, we suggest you purchase more licenses.

How can I identify a license overdraft? You can view usage information, including the number of licenses in overdraft in the Citrix Licensing Manager. Studio also contains overdraft usage information.

What happens when an overdraft license is consumed?
A license is assigned from your installed licenses to enable access to your Citrix Virtual Apps and Desktops environment. This overdraft license provides as much access and functionality as your other licenses.

Can I get an alert when my overdraft licenses are consumed?
Currently, there are no specific alerts provided when overdraft licenses are consumed.

How long can an overdraft license be consumed?
You must purchase any overdraft licenses used within 30 days of the first use.

What product components are included with each Citrix Virtual Apps and Citrix Virtual Apps and Desktops edition?

For a full feature matrix by edition, see Citrix Virtual Apps and Desktops features.

How do I license Citrix Virtual Desktops environments in compliance with the Citrix Virtual Apps and Desktops EULA?

To deploy Citrix Virtual Apps and Desktops under the user/device or the concurrent license model in compliance with the Citrix Virtual Apps and Desktops EULA, apply the license files to your License Server. The License Server then controls and monitors license compliance. We recommend that you configure your product based on what you purchased. For example, if you purchase Citrix Virtual Apps and Desktops Premium but only want to use the Citrix Virtual Apps feature, configure the product to Citrix Virtual Apps and Desktops to meet compliance. For more information, see the Product License Compliance Center.

How do I license Citrix Virtual Apps environments in compliance with the Citrix Virtual Apps EULA?

To deploy Citrix Virtual Apps under the concurrent license model in compliance with the Citrix Virtual Apps EULA, apply the license files to your License Server. The License Server then controls and monitors license compliance.

Do Citrix Virtual Apps and Desktops Advanced and Premium editions include Citrix Virtual Apps concurrent licenses?

Citrix Virtual Apps and Desktops Advanced and Premium user/device licenses include concurrent Citrix Virtual Apps licenses for compatibility only. These concurrent licenses are for use only with earlier product versions that are incompatible with user/device licenses. Use of the concurrent compatibility licenses included with user/device licenses is permissible only with these versions - XenApp versions earlier than 6.5 and XenDesktop versions earlier than 5.0 Service Pack 1.

How can I get my license file?

We send the license access code in email. There are three ways to generate license files using the license access code:

- The Manage Licenses toolbox from your My Account page on citrix.com
- Citrix Studio to allocate your purchase and the license file automatically installs on your Citrix License Server.
- Citrix Licensing Manager within the Citrix License Server to allocate your purchase and install your license file.

For more information, see Licensing in the Citrix Licensing documentation and Licensing in the Citrix Virtual Apps and Desktop documentation.

What TCP ports does Citrix licensing use?

- License Server port number is 27000
- Vendor daemon port number is 7279
- Management console web port is 8082
- Web Services for Licensing port is 8083

What is the Citrix License Server?

The Citrix License Server is a system that allows licenses to be shared across the network. For more information, see Licensing operations overview.

Can I virtualize or cluster the Citrix License Server?

Yes. You can virtualize or cluster the Citrix License Server. For more information, see Clustered License Servers.

What benefits are available to me if I virtualize the Citrix License Server?

Virtualizing the Citrix License Server provides a redundant solution. That solution allows for mobility between multiple physical servers without the need for downtime.

Are there any limitations to consider if I virtualize the Citrix License Server?

No.

Does the Citrix License Server manage all the licenses for my Citrix Virtual Apps and Desktop deployment?

The Citrix License Server manages all licenses you receive for Citrix Virtual Apps and Desktop, except licenses in the Premium Edition used with Citrix Gateway. License servers built in to the network appliances as required for those security-oriented network devices manage those licenses.

What is the Citrix Licensing Manager?

The Citrix Licensing Manager enables downloading and allocation of license files from the License Server on which you installed the Citrix Licensing Manager. The Citrix Licensing Manager is the recommended License Server management method, which enables the following:

- Short code registration of the License Server to Citrix Cloud and easy removal of registration.
- Configure user and group accounts.
- Use the dashboard to display installed, in-use, expired and available licenses, and Customer Success Services dates.
- Export license use data for use in reporting.
- Configure the historical use data retention period. Default data retention period is 180 days.
- Simplified installation of license files on the License Server using a license access code or downloaded file.
- Enable and disable the supplemental grace period.
- Configure Customer Experience Improvement Program (CEIP) and Call Home.
- Automatically or manually checks for Customer Success Services renewal licenses and notifies you or installs the licenses if found.
- Notifies you of the License Server state - Missing startup license, time issues, uploader failures.
- Modify these ports:
  - License Server (default 27000)
  - Vendor Daemon (default 7279)
  - Web Services for Licensing (default 8083)

For more information, see Citrix Licensing Manager.

What is the Citrix License Administration Console?

The License Administration Console is an interface that enables you to manage the licenses for Citrix infrastructure. The console also enables you to configure License Server settings and view current license use.

You can use Studio to manage and track licensing, provided the License Server is in the same domain as Studio, or in a trusted domain.

For more information, see License Administration Console.

What is the license assignment period?

The license assignment period is the term that a Citrix Virtual Apps and Desktops license is assigned to a user or device. The default license assignment period is 90 days.

How do I release an authorized user/device license?

To release the assignment of an authorized user/device, use the `udadmin` utility in accordance with the EULA terms. The License Server then assigns the license to the next appropriate user/device.

How do I know how many licenses my organization has purchased?

All purchased licenses are available to review and access at any time (24x7) from your secure **Manage Licenses** toolbox on your **My Account** page on https://www.citrix.com.

How do I know how many licenses are in use at any time?

The Citrix Licensing Manager, the License Administration Console, and Studio provide details on real time license use.

What happens if I exceed my purchased user/device license count?

User/device licenses include a 10% overdraft, which is included when licenses are generated. The overdraft is also included in the installed license count. If the usage spike exceeds the installed count including overdraft, access for more users is denied. You must purchase and deploy a new license to enable access for more users.

If all licenses are in use, including the license overdraft, the supplemental grace period enables unlimited connections to a product. The supplemental grace period gives you time to determine why you exceeded the maximum license count and to purchase more licenses without disrupting your users. This period lasts until 15 days elapses or you install more retail licenses, whichever comes first. For more information, see Supplemental grace period.

Director displays the grace period states. For more information, see Panels on the Director Dashboard.

What happens if I exceed my purchased concurrent license count?

If all licenses are in use, the supplemental grace period enables unlimited connections to a product. The supplemental grace period gives you time to determine why you exceeded the maximum license count and to purchase more licenses without disrupting your users. This period lasts until 15 days elapses or you install more retail licenses, whichever comes first. For more information, see Supplemental grace period.

Director displays the grace period states. For more information, see Panels on the Director Dashboard.

Is there a licensing requirement for Citrix Virtual Apps and Desktops Servicing Options: Long Term Service Release (LTSR) or Current Release (CR)?

Citrix Virtual Apps and Desktops Servicing Options, such as Long-Term Service Release, are a benefit of the Customer Success Services program. You must have active Customer Success Services to qualify for the benefits of LTSR. For more information, see [Citrix Virtual Apps, Citrix Virtual Apps and Desktops, and Citrix Hypervisor Servicing Options.

How do the RBI Service pooled hours work?

When you purchase a minimum of 25 users of the service, you receive 5000 of hours of rights to use the service, pooled across all users. Subsequent purchases of user rights don't increase the pooled hours entitlement. To increase the entitlement of service hours, buy add-on packs.

License Server disaster recovery and maintenance

For information about disaster recovery and maintenance of your License Server, see Disaster recovery and maintenance in the Citrix Licensing documentation.

Can I use Remote PC Access with CCU licenses?

Yes.

For information about Remote PC Access, see Remote PC Access.

Product-specific licensing FAQs and information

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor

Applications

October 21, 2020

Introduction

If your deployment uses only Delivery Groups (and not Application Groups), you add applications to the Delivery Groups. If you also have Application Groups, generally you should add applications to the Application Groups. This guidance provides easier administration. An application must always belong to at least one Delivery Group or Application Group.

In the Add Applications wizard, you can select one or more Delivery Groups, or one or more Application Groups, but not both. Although you can later change an application's group association (for example, moving an application from an Application Group to a Delivery Group), best practice discourages adding that complexity. Keep your applications in one type of group.

When you associate an application with more than one Delivery Group or 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 is associated.

If you publish two applications with the same name (perhaps from different groups) to the same users, change the Application name (for user) property in Studio; otherwise, users will see duplicate names in Citrix Workspace app.

You can change an application's properties (settings) when you add it, or later. You can also change the application folder where the application is placed, either when you add the application, or later.

For details, see:

- Create Delivery Groups
- Create Application Groups
- Tags

Add applications

You can add applications when you create a Delivery Group or Application Group; those procedures are detailed in the Create Delivery Groups and Create Application Groups articles. The following procedure describes how to add applications after you create a group.

Good to know:

- You cannot add applications to Remote PC Access Delivery Groups.
- You cannot use the Add Application wizard to remove applications from Delivery Groups or Application Groups. That is a separate operation.

To add one or more applications:

1. Select **Applications** in the Studio navigation pane and then select **Add Applications** in the Actions pane.
2. The Add Applications wizard launches with an **Introduction** page, which you can remove from future launches of this wizard.
3. The wizard guides you through the Groups, Applications, and Summary pages described below. When you are done with each page, click **Next** until you reach the Summary page.

Alternatives to step 1 if you want to add applications to a single Delivery Group or Application Group:

- To add applications to only one Delivery Group, in step 1, select **Delivery Groups** in the Studio navigation pane, then select a Delivery Group in the middle pane, and then select **Add Applications** in the Actions pane. The wizard will not display the **Groups** page.
- To add applications to only one Application Group, in step 1, select **Applications** in the Studio navigation pane, then select an **Application Group** in the middle pane, and then select the **Add Applications** entry under the Application Group's name in the Actions pane. The wizard will not display the **Groups** page.

Groups

This page lists all the Delivery Groups in the Site. If you have also created Application Groups, the page lists the Application Groups and Delivery Groups. You can choose from either group, but not from both groups. In other words, you cannot add applications to an Application Group and a Delivery Group

at the same time. Generally, if you are using Application Groups, applications should be added to Application Groups rather than Delivery Groups.

When adding an application, you must select the check box next to at least one Delivery Group (or Application Group, if available) because every application must always be associated with at least one group

Applications

Click 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 click **OK**.

  This source cannot be selected if you (1) selected Application Groups that have no associated Delivery Groups, (2) selected Application Groups with associated Delivery Groups that contain no machines, or (3) selected a Delivery Group containing no machines.

- **Manually defined:** 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, click 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 click **OK**.

  This source cannot be selected If the Site has no applications.

- **App-V:** Applications in App-V packages. When you select this source, a new page launches where you select the App-V server or the Application Library. From the resulting display, select the checkboxes of applications to add, and then click **OK**. For more information, see the App-V article.

  This source cannot be selected if App-V is not configured for the Site.

- **Application Group**: Application Groups. When you select this source, a new page launches with a list of Application Groups. (Although the display also lists the applications in each group, you can select only the group, not individual applications.) All current and future applications in the selected groups will be added. Select the check boxes of Application Groups to add, and then click **OK**.

  This source cannot be selected if (1) there are no Application Groups, or (2) if the selected Delivery Groups do not support Application Groups (for example, Delivery Groups with statically assigned machines).

As noted in the table, some sources in the Add dropdown cannot be selected if there is no valid source of that type. Sources that are incompatible (for example, you cannot add Application Groups to Application Groups) are not included in the dropdown. Applications that have already been added to the groups you chose cannot be selected.

To add an application from an assigned AppDisk, select **From Start menu**. If the application is not available there, select **Manually defined** and provide the details. If a folder access error occurs, configure the folder as **shared** and try to add the application through **Manually defined** again.

You can change an application's properties (settings) from this page, or later.

By default, applications you add are placed in the application folder named `Applications`. You can change the application from this page, or later. If you try to add an application and one with the same name already exists in the same folder, you are prompted to rename the application you're adding. You can accept the new name offered, or decline and then rename the application or select a different folder. For example, if `app` already exists in the `Application`s folder, and you attempt to add another application named `app` to that folder, the new name `app_1` will be offered.

Summary

If you are adding 10 or fewer applications, their names are listed in **Applications to add**. If you are adding more than 10 applications, the total number is specified.

Review the summary information and then click **Finish**.

Change an application's group association

After adding an application, you can change the Delivery Groups and Application Groups with which the application is associated.

You can use drag-and-drop to associate an application with an additional group. This is an alternative to using commands in the Actions pane.

If an application is associated with more than one Delivery Group or more than one Application Group, group priority can used to specify the order in which multiple groups are checked to find applications. By default, all groups are priority 0 (the highest). Groups at the same priority are load balanced.

An application 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 desktops only, if (1) the Delivery Group contains shared machines and was created with a XenDesktop 7.x version earlier than 7.9, and (2) you have Edit Delivery Group permission. The Delivery Group type is automatically converted to "desktops and applications" when the properties dialog is committed.

1. Select **Applications** in the Studio navigation pane and then select the application in the middle pane.
2. Select **Properties** in the Actions pane.
3. Select the **Groups** page.
4. To add a group, click the **Add** dropdown and select **Application Groups** or **Delivery Groups**. (If you have not created any Application Groups, the only entry will be Delivery Groups.) Then select one or more available groups. Groups that are incompatible with the application, or that are already associated with the application, cannot be selected.
5. To remove a group, select one or more groups and then click **Remove**. If removing group association would result in the application no longer being associated with any Application Group or Delivery Group, you will be alerted that the application will be deleted.
6. To change the priority of a group, select the group and then click **Edit Priority**. Select a priority value and then click **OK**.
7. When you are finished, click **Apply** to apply the changes and leave the window open, or click **OK** to apply the changes and close the window.

Duplicate, enable or disable, rename, or delete an application

The following actions are available:

- **Duplicate:** You might want to duplicate an application to create a different version with different parameters or properties. When you duplicate an application, it is automatically renamed with a unique suffix and placed adjacent to the original. You might also want to duplicate an application and then add it to a different group. (After duplicating, the easiest way to move an application is using drag-and-drop.)
- **Enable or disable:** Enabling and disabling an application is a different action than enabling and disabling a Delivery Group or Application Group.
- **Rename:** You can rename only one application at a time. If you try to rename an application and one with the same name already exists in the same folder or group, you are prompted to specify a different name.
- **Delete:** Deleting an application removes it from the Delivery Groups and Application Groups with which it was associated, but not from the source that was used to add the application originally. Deleting an application is a different action than removing it from a Delivery Group or Application Group.

To duplicate, enable or disable, rename, or delete an application:

1. Select **Applications** in the Studio navigation pane.
2. Select one or more applications in the middle pane and then select the appropriate task in the Actions pane.
3. Confirm the action, when prompted.

Remove applications from a Delivery Group

An application must be associated (belong) with at least one Delivery Group or Application Group. If you attempt to remove an application from a Delivery Group that would remove that application's association with any Delivery Group or Application Group, you are notified that the application will be deleted if you continue. When that happens, if you want to deliver that application, you must add it again from a valid source.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a Delivery Group. In the lower middle pane, select the **Applications** tab and then the application you want to remove.
3. Select **Remove Application** from the Actions pane.
4. Confirm the removal.

Remove applications from an Application Group

An application must belong to at least one Delivery Group or Application Group. If you attempt to remove an application from an Application Group that will result in that application no longer belonging to any Delivery Group or Application Group, you are notified that the application will be deleted if you continue. When that happens, if you want to deliver that application, you must add it again from a valid source.

1. Select **Applications** in the Studio navigation pane.
2. Select the Application Group in the middle pane, and then select one or more applications in the middle pane.
3. Select **Remove from Application Group** in the Actions pane.
4. Confirm the removal.

Change application properties

You can change the properties of only one application at a time.

To change the properties of an application:

1. Select **Applications** in the Studio navigation pane.
2. Select an application and then select **Edit Application Properties** in the Actions pane.
3. Select the page containing the property you want to change.
4. When you are finished, click **Apply** to apply any hanges you made and keep the window open, or click **OK** to apply changes tand close the window.

In the following list, the page is shown in parentheses.

Property	Page
Category/folder where application appears in Citrix Workspace app	Delivery
Command line arguments; see Pass parameters to published applications	Location
Delivery Groups and Application Groups where the application is available	Groups
Description	Identification
File extensions and file type association: which extensions the application opens automatically	File Type Association
Icon	Delivery
Keywords for StoreFront	Identification
Limits; see Configure application limits	Delivery
Name: the names seen by the user and by the administrator	Identification
Path to executable; see Pass parameters to published applications	Location
Shortcut on user's desktop: enable or disable	Delivery
Visibility: limits which users can see the application in Citrix Workspace app; an invisible application can still be started; to make it unavailable as well as invisible, add it to a different group	Limit Visibility
Working directory	Location

Application changes may not take effect for current application users until they log off their sessions.

Configure application limits

Configure application limits to help manage application use. For example, you can use application limits to manage the number of users accessing an application simultaneously. Similarly, application limits can be used to manage the number of simultaneous instances of resource-intensive applications, this can help maintain server performance and prevent deterioration in service.

This feature limits the number of application launches that are brokered by the Controller (for example, from Citrix Workspace app and StoreFront), and not the number of running applications that

could be launched by other methods. This means that application limits assist administrators when managing concurrent usage, but do not provide enforcement in all scenarios. For example, application limits cannot be applied when the Controller is in leased connection mode.

By default, there is no limit on how many application instances can run at the same time. There are several application limit settings; you can configure any or all:

- The maximum number of concurrent instances of the application by all users in the Delivery Group.
- One instance of the application per user in the Delivery Group.
- The maximum number of concurrent instances of the application per machine (PowerShell only).

If a limit is configured, an error message is generated when a user attempts to launch an instance of the application that will exceed the configured limit. If more than one limit is configured, an error is reported when the first limit is reached.

Examples using application limits:

- **Maximum number of simultaneous instances limit:** In a Delivery Group, you configure the maximum number of simultaneous instances of application Alpha to 15. Later, users in that Delivery Group have 15 instances of that application running at the same time. If any user in that Delivery Group now attempts to launch Alpha, an error message is generated, and Alpha is not launched because it would exceed the configured simultaneous application instance limit (15).
- **One-instance-per-user application limit:** In another Delivery Group, you enable the one-instance-per-user option for application Beta. User Tony launches application Beta successfully. Later in the day, while that application is still running in Tony's session, he attempts to launch another instance of Beta. An error message is generated and Beta is not launched because it would exceed the one-instance-per-user limit.
- **Maximum number of simultaneous instances and one-instance-per-user limits:** In another Delivery Group, you configure a maximum number of simultaneous instances of 10 and enable the one-instance-per-user option for application Delta. Later, when ten users in that Delivery Group each have an instance of Delta running, any other user in that Delivery Group who tries to launch Delta will receive an error message, and Delta will not be launched. If any of the ten current Delta users attempt to launch a second instance of that application, they will receive an error message and second instance will not be launched.
- **Maximum number of simultaneous instances per machine, and using tag restrictions:** Application Charlie has licensing and performance requirements that dictatehow many instances can be running at the same time on a specific server, as well as howmany instances can be running simultaneously across all servers in the Site.

The application instances per machine limit affects any server in the Site (not just machines in a particular Delivery Group). Let's say your Site has three servers. For application Charlie, you configure the app instances per machine limit to 2. So, no more than six instances of application Charlie will be allowed to launch site-wide. (That's a limit of two instances of Charlie on each of the three servers.)

To restrict an application's usage to only certain machines within a Delivery Group (inaddition to limiting the instances on all machines Site-wide), use the tagging functionality for those machines, and configure the maximum number of instances per machine limitfor that application.

If application instances are also launched by methods other than Controller brokering (for example, while a Controller is in outage mode) and configured limits are exceeded, users will not be able to launch additional instances until they close sufficient instances to no longer exceed the limits. The instances that exceeded the limit will not be forcibly shut down; they will be allowed to continue until their users close them.

If you disable session roaming, then disable the one-instance-per-user application limit. If you enable the one-instance-per-user application limit, do not configure either of the two values that allow new sessions on new devices. For information about roaming, see the Sessions article.

To configure the maximum instances per Delivery Group limit, and the one-instance-per-user limit:

1. Select **Applications** in the Studio navigation pane and then select an application.
2. Select the **Edit Application Properties** in the Actions pane.
3. On the **Delivery** page, choose one of the following options.
    - Allow unlimited use of the application. There is no limit to the number of instances running at the same time. This is the default.
    - Set limits for the application. There are two limit types; specify either or both.
        - Specify the maximum number of instances that can run concurrently
        - Limit to one instance of the application per user
4. Click **OK** to apply the change and close the dialog box, or **Apply** to apply the change and leavee the dialog box open.

To configure the maximum instances per machine limit (PowerShell only):

- In PowerShell (using the Remote PowerShell SDK for Citrix Cloud deployments, or the PowerShell SDK for on-premises deployments), enter the appropriate `BrokerApplication` cmdlet with the `MaxPerMachineInstances` parameter.
- For guidance, use the `Get-Help` cmdlet. For example:

```
Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
```


Pass parameters to published applications

Use the **Location** page of an application's properties to enter the command line and pass parameters to published applications.

When you associate a published application with file types, the symbols "%*"(percent and star symbols enclosed in double quotation marks) are appended to the end of the command line for the application. 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. To do this, add double quotation marks around the path, and another set of double quotation marks around the %* symbols. Be sure to include a space between the closing quotation mark for the path and the opening quotation mark for the %* symbols.

For example, the command line for the published application Windows Media Player is:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

Manage application folders

By default, new applications you add to Delivery Groups are placed in a folder named **Applications**. You can specify a different folder when you create the Delivery Group, when you add an application, or later.

Good to know:

- You cannot rename or delete the Applications folder, but you can move all the applications it contains to other folders you create.
- A folder name can contain 1-64 characters. Spaces are permitted.
- Folders can be nested up to five levels.
- Folders do not have to contain applications; empty folders are allowed.
- Folders are listed alphabetically in Studio unless you move them or specify a different location when you create them.
- You can have more than one folder with the same name, as long as each has a different parent folder. Similarly, you can have more than one application with the same name, as long as each is in a different folder.

- You must have View Applications permission to see the applications in folders, and you must have Edit Application Properties permission for all applications in the folder to remove, rename, or delete a folder that contains applications.
- Most of the following procedures request actions using the Actions pane in Studio. Alternatively, you can use right-click menus or drag and drop. For example, if you create or move a folder in a location you did not intend, you can drag/drop it to the correct location.

To manage application folders, select **Applications** in the Studio navigation pane. Use the following list for guidance.

- **To view all folders (excluding nested folders):** Click **Show all** above the folder list.
- **To create a folder at the highest level (not nested):** Select the Applications folder. To place the new folder under an existing folder other than Applications, select that folder. Then, select **Create Folder** in the Actions pane. Enter a name.
- **To move a folder:** Select the folder and then select **Move Folder** in the Actions pane. You can move only one folder at a time unless the folder contains nested folders. (The easiest way to move a folder is to use drag and drop.)
- **To rename a folder:** Select the folder, and then select **Rename Folder** in the Actions pane. Enter a name.
- **To delete a folder:** Select the folder, and then select **Delete Folder** in the Actions pane. When you delete a folder that contains applications and other folders, those objects are also deleted. Deleting an application removes the application assignment from the Delivery Group; it does not remove it from the machine.
- **To move applications into a folder:** Select one or more applications. Then, select **Move Application** in the Actions pane. Select the folder.

You can also place applications you are adding in a specific folder (even a new one) on the **Application** page of the Create Delivery Group and Create Application Group wizards. By default, added applications go in the **Applications** folder; click **Change** to select or create a folder.

Control local launch of applications on published desktops

When users launch a published application from within a published desktop, you can control whether the application is launched in that desktop session or as a published application. Citrix Workspace app searches for the installation path of the application in the Windows registry on the VDA and, if present, launches the local instance of the application. Otherwise, a hosted instance of the application is launched. If you launch an application that is not installed on the VDA, the hosted application is launched. For more information, see vPrefer launch.

In PowerShell (using the Remote PowerShell SDK in Citrix Cloud deployments or the PowerShell SDK in on-premises deployments), you can change this action.

In the `New-Broker Application` or `Set-BrokerApplication` cmdlet, use the `LocalLaunchDisable` option. For example:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

By default, this option's value is false (`-LocalLaunchDisabled $false`). When launching a published application from within a published desktop, the application is launched in that desktop session.

If you set the option's value to true (`-LocalLaunchDisabled $true`), the published application is launched. This creates a separate, additional session from the published desktop (using Citrix Workspace app for Windows) to the published application.

Requirements and limits:

- The application's `ApplicationType` value must be `HostedOnDesktop`.
- This option is available only through the appropriate PowerShell SDK. It is not currently available in the Studio graphical interface.
- This option requires minimum: StoreFront 3.14, Citrix Receiver for Windows 4.11, and Delivery Controller 7.17.

Universal Windows Platform Apps

January 4, 2023

For information about Universal Windows Platform (UWP) apps, see the following Microsoft documentation:

- What's a Universal Windows Platform (UWP) app?
- Windows Package Manager

Requirements and limitations

Citrix Virtual Apps and Desktops supports the use of UWP apps with VDAs on the following Windows machines:

- Windows 10 and later versions
- Windows Server 2016 and later versions

VDAs must be minimum version 7.11.

The following Citrix Virtual Apps and Desktops features are either not supported or limited when using UWP apps:

- File type association is not supported.
- Local App Access is not supported.
- Dynamic preview: If apps running in the session overlap, the preview shows the default icon. The Win32 APIs used for Dynamic Preview are not supported in UWP apps.
- Action Center remoting: UWP apps can use the Action Center for displaying the messages in the session. These messages are currently not redirected to the endpoint to be displayed to the user.

Launching UWP apps and non-UWP apps from the same server is not supported. Instead, place UWP apps and non-UWP apps in separate delivery groups or application groups.

Because all UWP apps installed on the machine are enumerated, Citrix recommends disabling user access to the Windows Store. This precludes the UWP apps installed by one user from being accessed by a different user.

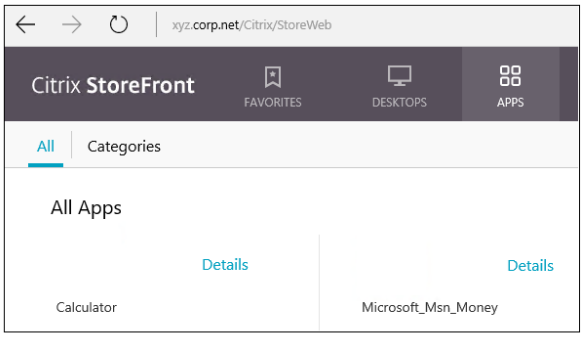
During sideloading, the UWP app is installed on the machine and is available for use by other users. When another user launches the app, then it is installed, and the OS updates its AppX database to indicate "as installed"by that user.

A graceful logoff started from a published UWP app that was launched in a fixed or seamless window might prevent the VDA session from closing, and forcibly log off the user. When this occurs, several processes remaining in the VDA session prevent it from properly closing. To resolve this, determine which process is preventing the VDA session from closing, and then add it to the "LogoffCheckSysModules"registry key value, following the guidance in CTX891671.

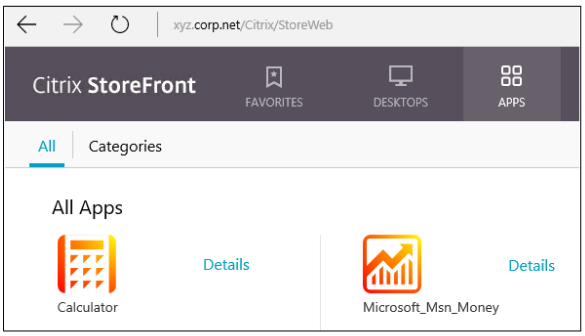
Application Display Names and Descriptions for UWP apps might not have correct names. Edit and correct these properties when adding the applications to the Delivery Group.

Check Known issues for any additional issues.

Currently, several UWP apps have white icons with transparency enabled, which results in the icon not being visible against the white background of the StoreFront display. To avoid this issue, you can change the background. For example, on the StoreFront machine, edit the file C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css. At the end of the file, add `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow , red ); }`. The graphic below illustrates the before-and-after for this example.



Before



After

On Windows Server 2016 and later versions, the Server Manager might also launch when a Univeral App is launched. To prevent this from occurring, disable Server Manager from auto-starting during logon with the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon registry key. For details, see https://blog.rmilne.ca/2014/05/30/how-to-hide-server-manager-at-logon/.

Install and publish UWP apps

Support for UWP apps is enabled by default.

To install one or more UWP apps on VDAs (or a master image), use one of the following methods:

- Complete an offline install from the Windows Store for Business, using a tool such as Deployment Image Servicing and Management (DISM) to deploy the apps to the desktop image. For more information, see Windows Package Manager.
- Sideload the apps. For more information, see Sideload line of business (LOB) apps in Windows client devices.
- Install the UWP apps for each intended user directly from the Windows Store for Business.

To add (publish) one or more UWP apps in Citrix Virtual Apps or Citrix Virtual Desktops:

1. After the UWP apps are installed on the machine, add the UWP apps to a delivery group or application group. You can do this when you create a group, or later. On the **Applications** page, in the **Add** menu, select **From Start menu**.
2. When the applications list appears, select the UWP apps you want to publish.
3. Continue with the wizard or close the edit dialog.

For information about additional configuration requirements when using User Profile Manager (UPM), see
Windows Apps - Microsoft Store.

To disable the use of UWP apps on a VDA, add the registry setting **EnableUWASeamlessSupport** in `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` and set to **0**.

Uninstall UWP apps

When you uninstall a UWP app with a command such as `Remove-AppXPackage`, the item is uninstalled only for administrators. To remove the app from the machines of users who may have launched and used the app, you must run the removal command on each machine. You cannot uninstall the AppX package from all users' machines with one command.

Zones

August 21, 2020

Deployments that span widely-dispersed locations connected by a WAN can face challenges due to network latency and reliability. There are two options that mitigate those challenges:

- Deploy multiple Sites, each with their own SQL Server Site database.

  This option is recommended for large enterprise deployments. Multiple Sites are managed separately, and each requires its own SQL Server Site database. Each Site is a separate Citrix Virtual Apps deployment.

- Configure multiple zones within a single Site.

  Configuring zones can help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of the WAN. Using zones allows effective Site management from a single Citrix Studio console, Citrix Director, and the Site database. This saves the costs of deploying, staffing, licensing, and operating additional Sites containing separate databases in remote locations.

  Zones can be helpful in deployments of all sizes. You can use zones to keep applications and desktops closer to end users, which improves performance. A zone can have one or more Controllers installed locally for redundancy and resiliency, but it is not required.

  The number of Controllers configured in the Site can affect the performance of some operations, such as adding new Controllers to the Site itself. To avoid this, we recommend that you limit the number of zones in your Citrix Virtual Apps or Citrix Virtual Desktops Site to no more than 50.

  When the network latency of your zones is more than 250 ms RTT, we recommend that you deploy multiple Sites instead of zones.

Throughout this article the term local refers to the zone being discussed. For example, "A VDA registers with a local Controller"means that a VDA registers with a Controller in the zone where the VDA is located.

Zones in this release are similar, but not identical to zones in XenApp version 6.5 and earlier. For example, in this implementation of zones, there are no data collectors. All Controllers in the Site communicate with one Site database in the primary zone. Also, failover and preferred zones work differently in this release.

Zone types

A Site always has one primary zone. It can also optionally have one or more satellite zones. Satellite zones can be used for disaster recovery, geographically-distant datacenters, branch offices, a cloud, or an availability zone in a cloud.

Primary zone:

The primary zone has the default name "Primary,"which contains the SQL Server Site database (and high availability SQL servers, if used), Studio, Director, Citrix StoreFront, Citrix License Server, and Citrix Gateway. The Site database should always be in the primary zone.

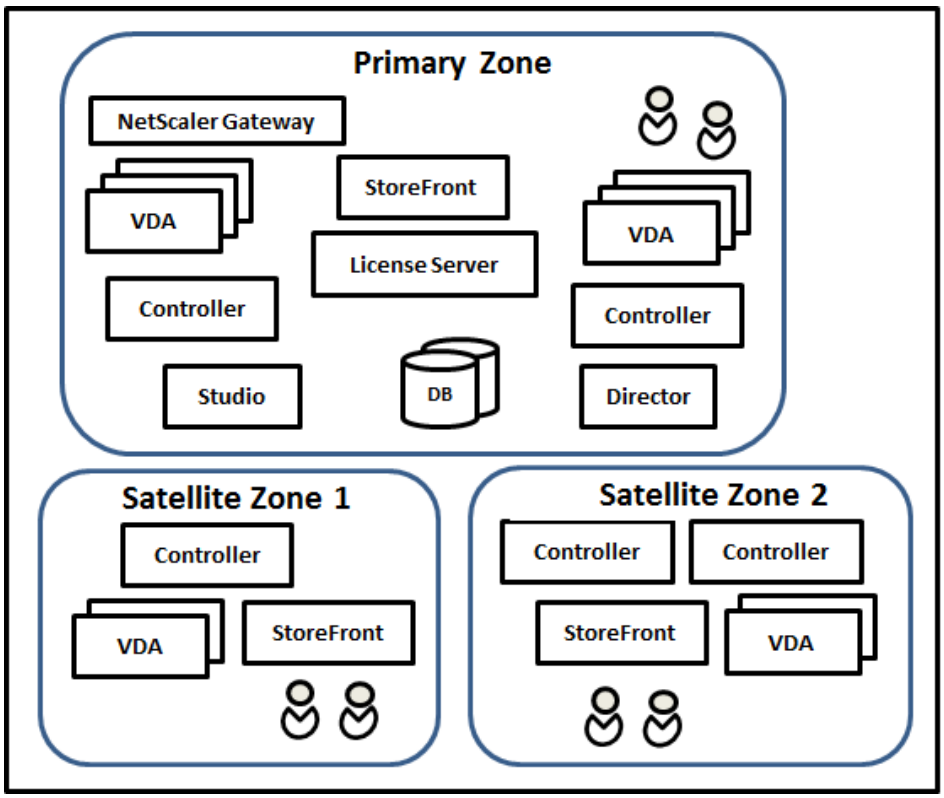
The primary zone should also have at least two Controllers for redundancy, and may have one or more VDAs with applications that are tightly-coupled with the database and infrastructure.

Satellite zone:

A satellite zone contains one or more VDAs, Controllers, StoreFront servers, and Citrix Gateway servers. Under normal operations, Controllers in a satellite zone communicate directly with the database in the primary zone.

A satellite zone, particularly a large one, might also contain a hypervisor that is used to provision and/or store machines for that zone. When you configure a satellite zone, you can associate a hypervisor or cloud service connection with it. (Be sure any Machine Catalogs that use that connection are in the same zone.)

A Site can have satellite zones of different configurations, based on your unique needs and environment. The following figure illustrates a primary zone and examples of satellite zones.



In the illustration:

- **Primary zone:** Contains two Controllers, Studio, Director, StoreFront, License Server, and the Site database (plus high availability SQL Server deployments). The Primary zone also contains several VDAs and a Citrix Gateway.
- **Satellite zone 1: VDAs with Controller:** Satellite zone 1 contains a Controller, VDAs, and a StoreFront server. VDAs in this satellite zone register with the local Controller. The local Controller communicates with the Site database and license server in the primary zone.

  If the WAN fails, the Local Host Cache feature allows the Controller in the satellite zone to continue brokering connections to VDAs in that zone. Such a deployment can be effective in an office where workers use a local StoreFront site and the local Controller to access their local resources, even if the WAN link connecting their office to the corporate network fails.
- **Satellite zone 2: VDAs with redundant Controllers:** Satellite zone 2 contains two Controllers, VDAs, and a StoreFront server. This is the most resilient zone type, offering protection against a simultaneous failure of the WAN and one of the local Controllers.

Where VDAs register and where Controllers fail over

In a Site containing primary and satellite zones, with VDAs at minimum version 7.7:

- A VDA in the primary zone registers with a Controller in the primary zone. A VDA in the primary zone will never attempt to register with a Controller in a satellite zone.
- A VDA in a satellite zone registers with a local Controller, if possible. (This is considered the preferred Controller.) If no local Controllers are available (for example, because the local Controllers cannot accept more VDA registrations or the local Controllers have failed), the VDA will attempt to register with a Controller in the primary zone. In this case, the VDA stays registered in the primary zone, even if a Controller in satellite zone becomes available again. A VDA in a satellite zone will never attempt to register with a Controller in another satellite zone.
- When auto-update is enabled for VDA discovery of Controllers, and you specify a list of Controller addresses during VDA installation, a Controller is randomly selected from that list for initial registration (regardless of which zone the Controller resides in). After the machine with that VDA is restarted, the VDA will start to prefer registering with a Controller in its local zone.
- If a Controller in a satellite zone fails, it fails over to another local Controller, if possible. If no local Controllers are available, it fails over to a Controller in the primary zone.
- If you move a Controller in or out of a zone, and auto-update is enabled, VDAs in both zones receive updated lists indicating which Controllers are local and which are in the primary zone, so they know with whom they can register and accept connections from.
- If you move a Machine Catalog to another zone, the VDAs in that catalog will re-register with Controllers in the zone where you moved the catalog. (When you move a catalog to another zone, make sure this zone and the zone with the associated host connection are well connected. If there is limited bandwidth or high-latency, move the host connection to the same zone containing the associated machine catalog.)

If all Controllers in the primary zone fail:

- Studio cannot connect to the Site.
- Connections to VDAs in the primary zone cannot be made.
- Site performance will increasingly degrade until the Controllers in the primary zone become available.

For Sites containing VDA versions earlier than 7.7:

- A VDA in a satellite zone will accept requests from Controllers in their local zone and the primary zone. (VDAs at minimum version 7.7 can accept Controller requests from other satellite zones.)
- A VDA in a satellite zone will register with a Controller in the primary zone or the local zone at random. (VDAs at minimum version 7.7 prefer the local zone.)

Zone preference

To use the zone preference feature, you must be using minimum StoreFront 3.7 and Citrix Gateway 11.0-65.x.

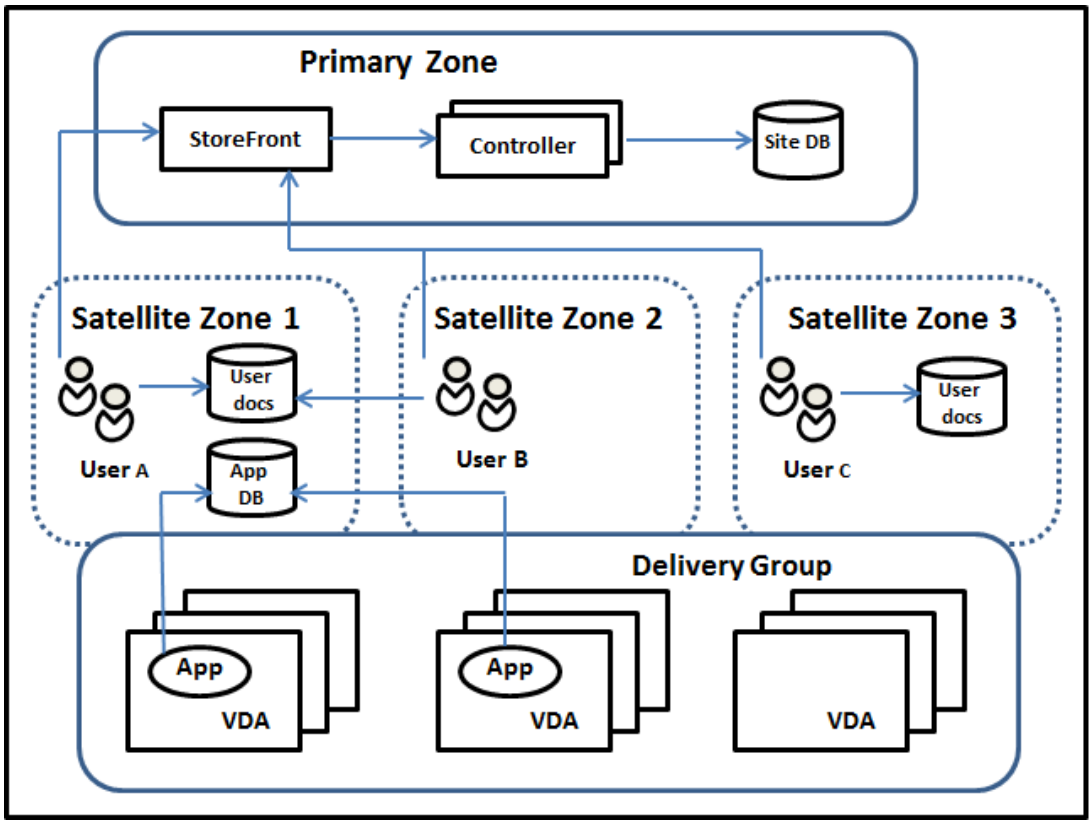
In a multi-zone Site, the zone preference feature offers the administrator more flexibility to control which VDA is used to launch an application or desktop.

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.

The following graphic shows an example multi-zone configuration.



In this example, VDAs are spread among three satellite zones, but they are all in the same Delivery Group. Therefore, the broker might have a choice which VDA to use for a user launch request. This example indicates there are a number of locations where users can be running their Citrix Workspace app endpoints: User A is using a device with Citrix Workspace app in satellite zone 1; User B is using a device in satellite zone 2. A user's documents could be stored in a number of locations: Users A

and B use a share based in satellite zone 1; User C uses a share from satellite zone C. Also, one of the published applications uses a database located in satellite zone 1.

You associate a user or application with a zone by configuring a home zone for the user or application. The broker in the Delivery Controller then uses those associations to help select the zone where a session will be launched, if resources are available. You can:

- 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 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; see the "Other considerations" section. 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. You can restrict the sequence; see Tailoring zone preference. 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 has a configured zone association (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 will (or will not) be used.

- **Mandatory user home zone use:** In a Delivery Group, you can specify that a session should be launched 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 when you need to avoid the risk of copying large profiles or data files between zones. In other words, you would rather deny a session launch than to launch the session in a different zone.
- **Mandatory application home zone use:** Similarly, when you configure a home zone for an application, you can indicate that the application should be launched 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 indicate that any configured user zones should not be considered when launching that application. For example, you might prefer that users run a specific application on a VDA close to the machine they are using (where Citrix Workspace app is running), using the user location zone preference, 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, that can use session sharing for an application, or a session that is already running the resource being launched), but that session is running on a VDA in a zone other than the preferred zone for the user/application, then the system may create a new session. This 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 zone other than the preferred zone.
3. Start a new session in the preferred zone.
4. Reconnect to a connected existing session in a zone other than the preferred zone.
5. Start a new session in a zone other than the 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 could 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. Once 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 Gateway must be configured to associate ranges of IP addresses with particular zones, and discovered zone identity must be passed through StoreFront to the Controller.

For more information about zone preference, see Zone preference internals.

Considerations, requirements, and best practice

- You can place the following items in a zone: Controllers, Machine Catalogs, host connections, users, and applications. If a Machine Catalog uses a host connection, both the catalog and the connection should be in the same zone. (However, with a low-latency high-bandwidth connection available, they can be in different zones.)
- When you place items in a satellite zone it affects how the Site interacts with them and with other objects related to them.
  - When Controller machines are placed into a satellite zone, it is assumed that those machines have good (local) connectivity to hypervisors and VDA machines in the same satellite zone. Controllers in that satellite zone are then used in preference to Controllers in the primary zone for handling those hypervisors and VDA machines.
  - When a hypervisor connection is placed into a satellite zone, it is assumed that all the hypervisors managed via that hypervisor connection also reside in that satellite zone. Controllers in that satellite zone are then used in preference to Controllers in the primary zone when communicating with that hypervisor connection.
  - When a machine catalog is placed into a satellite zone, it is assumed that all the VDA machines in that catalog are in the satellite zone. Local Controllers are used in preference to Controllers in the primary zone when attempting to register with the Site, after the Controller list auto-update mechanism has activated after the first registration of each VDA.
  - Citrix Gateway instances can also be associated with zones. This is done as part of the StoreFront Optimal HDX Routing configuration rather than, as for the other elements described here, as part of the Site configuration. When a Citrix Gateway is associated with a zone, it is preferred to be used when HDX connections to VDA machines in that zone are used.
- When you create a production Site and then create the first Machine Catalog and Delivery Group, all items are in the primary zone –you cannot create satellite zones until after you complete that

initial setup. (If you create an empty Site, the primary zone will initially contain only a Controller. You can create satellite zones before or after creating a Machine Catalog and Delivery Group.)

- When you create the first satellite zone containing one or more items, all other items in your Site remain in the primary zone.
- The primary zone is named 'Primary' by default; you can change that name. Although the Studio display indicates which zone is the primary zone, it is best practice to use an easily-identifiable name for the primary zone. You can reassign the primary zone (that is, make another zone the primary zone), but it should always contain the Site database and any high availability servers.
- The Site database should always be in the primary zone.
- After you create a zone, you can later move items from one zone to another. Note that this flexibility allows you to potentially separate items that work best in close proximity - for example, moving a Machine Catalog to a different zone than the connection (host) that creates the machines in the catalog, may 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, or in zones which are well connected (for example, via a low-latency and high-bandwidth network).
- For optimal performance, install Studio and Director only in the primary zone. If you want another Studio instance in a satellite zone (for example, if a satellite zone containing Controllers is being used as failover in the event the primary zone becomes inaccessible), run Studio as a locally-published application. You can also access Director from a satellite zone because it is a web application.
- Ideally, Citrix Gateway in a satellite zone should be used for user connections coming into that zone from other zones or external locations, although you can use it for connections within the zone.
- Remember: To use the zone preference feature, you must be using minimum StoreFront 3.7 and Citrix Gateway 11.0-65.x.

Connection quality limits

The Controllers in the satellite zone perform SQL interactions directly with the Site database. This imposes some limits on the quality of the link between the satellite zone and the primary zone containing the Site database. The specific limits are relative to the number of VDAs and user sessions on those VDAs that are deployed in the satellite zone. So satellite zones with only a few VDAs and sessions can function with a poorer-quality connection to the database than satellite zones with large numbers of VDAs and sessions.

For more information, see Latency and SQL Blocking Query Improvements.

The impact of latency on brokering performance

Although zones allow users to be on higher-latency links, providing that there is a local broker, the additional latency inevitably impacts end-user experience. For most work that users do, they experience slowness caused by round trips between Controllers in the satellite zone and the Site database.

For launching applications, extra delays occur while the session brokering process identifies suitable VDAs to send session launch requests to.

Create and manage zones

A Full Administrator can perform all zone creation and management tasks. However, you can also create a custom role that allows you to create, edit, or delete a zone. 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 Machine Catalog. For more information, see the Delegated Administration article.

If you use Citrix Provisioning: The Citrix Provisioning console provided with this release is not aware of zones, so Citrix recommends using Studio to create Machine Catalogs that you want to place in satellite zones. Use the Studio wizard to create the catalog, specifying the correct satellite zone. Then, use the Citrix Provisioning console to provision machines in that catalog. (If you create the catalog using the Citrix Provisioning wizard, it will be placed in the primary zone, and you will need to use Studio to move it to the satellite zone later.)

Create a zone

1. Select **Configuration > Zones** in the Studio navigation pane.
2. Select **Create Zone** in the Actions pane.
3. Enter a name for the zone, and a description (optional). The name must be unique within the Site.
4. Select the items to place in the new zone. You can filter or search the list of items from which you can select. You can also create an empty zone; simply do not select any items.
5. Click **Save**.

As an alternative to this method, you can select one or more items in Studio and then select **Create Zone** in the Actions pane.

Change a zone name or description

1. Select **Configuration > Zones** in the Studio navigation pane.

2. Select a zone in the middle pane and then select **Edit Zone** in the Actions pane.
3. Change the zone name and/or description. If you change the name of the primary zone, make sure the zone remains easily identifiable as the primary zone.
4. Click **OK** or **Apply**.

Move items from one zone to another zone

1. Select **Configuration > Zones** in the Studio navigation 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 Actions pane and then specify which zone to move them to.

A confirmation message lists the items you selected and asks if you are sure you want to move all of them.

Remember: When a Machine Catalog uses a host connection to a hypervisor or cloud service, both the catalog and the connection should be in the same zone. Otherwise, performance can be affected. If you move one, move the other, too.

Delete a zone

A zone must be empty before it can be deleted. You cannot delete the primary zone.

1. Select **Configuration > Zones** in the Studio navigation pane.
2. Select a zone in the middle pane.
3. Select **Delete Zone** from the Actions pane. If the zone is not empty (it contains items), you are asked to choose the zone where those items will be moved.
4. Confirm the deletion.

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. Select **Configuration > Zones** in the Studio navigation pane and then select a zone in the middle pane.
2. Select **Add Users to Zone** in the Actions pane.
3. In the **Add Users to Zone** dialog box, click **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. Click **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. Select **Configuration > Zones** in the Studio navigation pane and then select a zone in the middle pane.
2. Select **Remove Users from Zone** in the Actions pane.
3. In the **Add Users to Zone** dialog box, click **Remove** and then select the users and groups to remove from the zone. Note that this action removes the users only from the zone; those users remain in the Delivery Groups and Application 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, by selecting the application in Studio and editing its properties.

- When creating a Delivery Group, creating an Application 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 **Applications** in the Studio navigation pane. Select an application and then select **Edit Application Properties** in the Actions pane.

On the **Zones** page of the application's properties/settings:

- If you want the application to have a home zone:
  - Select **Use the selected zone to decide** radio button and then select the zone from the dropdown.

  - 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 or user home zones will be used to determine where to launch this application.

Other actions that include specifying zones

When you add a host connection or create a Machine Catalog (other than during Site creation), you can specify a zone where the item will be assigned, if you have already created at least one satellite zone.

In most cases, the primary zone is the default. When using Machine Creation Services to create a Machine Catalog, the zone that is configured for the host connection is automatically selected.

If the Site contains no satellite zones, the primary zone is assumed and the zone selection box does not appear.

Connections and resources

May 4, 2020

Introduction

You can optionally create your first connection to hosting resources when you create a Site. Later, you can change that connection and create other connections. Configuring a connection includes selecting the connection type from among the supported hypervisors and cloud services. The storage and network you select from the resources for that connection.

Read Only Administrators can view connection and resource details; you must be a Full Administrator to perform connection and resource management tasks. For details, see Delegated Administration.

Where to find information about connection types

You can use the supported virtualization platforms to host and manage machines in your Citrix Virtual Apps or Citrix Virtual Desktops environment. The System requirements article lists the supported

types. You can use the supported cloud deployment solutions to host product components and provision virtual machines. These solutions pool computing resources to build public, private, and hybrid Infrastructure as a Service (IaaS) clouds.

For details, see the following information sources.

- **Microsoft Azure Resource Manager:**
  - Microsoft Azure Resource Manager virtualization environments article.
  - Microsoft documentation.
- **Amazon Web Services (AWS):**
  - Citrix and AWS.
  - AWS documentation.
  - When you create a connection in Studio, 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. Include the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials.
  - Configure an AWS Hosting Connection to use IAM roles by entering **role_based_auth** as the value for the Access Key and Secret Key fields. An IAM Role defining the policy and permissions required by Citrix is required when attaching to AWS hosted Delivery Controllers or Cloud Connectors instances.
  - 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, Studio cannot use the file to populate the **API** key and secret key fields. Ensure that you are using AWS IAM credentials files.
- **Citrix Hypervisor (formerly XenServer):**
  - Citrix Hypervisor virtualization environments.
  - Citrix Hypervisor documentation.
- **Nutanix Acropolis:**
  - Nutanix virtualization environments.
  - Nutanix documentation.
- **VMware:**
  - VMware virtualization environments.
  - VMware product documentation.
- **Microsoft Hyper-V:**
  - Microsoft System Center Virtual Machine Manager virtualization environments article.

  - Microsoft documentation.

- **Microsoft Azure (Classic):**

  - This host type is deprecated.
  - Microsoft Azure virtualization environments article.
  - Microsoft documentation.

- **CloudPlatform:**

  - This host type is deprecated.
  - CloudPlatform documentation.
  - When you create a connection in Studio, you must provide the **API** key and secret key values. You can export the key file containing those values from CloudPlatform and then import those values into Studio.

Host storage

A storage product is supported if it is managed by a supported hypervisor. Citrix Support assists those storage product vendors in troubleshooting and resolving issues, and document those issues in the knowledge center, as needed.

When provisioning machines, data is classified by type:

- Operating system (OS) data, which includes master images.
- Temporary data, which includes all non-persistent data written to MCS-provisioned machines, Windows page files, user profile data, and any data that is synchronized with ShareFile. This data is discarded each time a machine restarts.
- Personal data stored on personal vDisks.

Providing separate storage for each data type can reduce load and improve IOPS performance on each storage device, making best use of the host's available resources. It also enables appropriate storage to be used for the different data types –persistence and resilience is more important for some data than others.

Storage can be shared (located centrally, separate from any host, used by all hosts) or local to a hypervisor. For example, central shared storage could be one or more Windows Server 2012 clustered storage volumes (with or without attached storage), or an appliance from a storage vendor. The central storage might also provide its own optimizations such as hypervisor storage control paths and direct access through partner plugins.

Storing temporary data locally avoids having to traverse the network to access shared storage. Storing data also reduces load (IOPS) on the shared storage device. Shared storage can be more costly, so

storing data locally can lower expenses. These benefits must be weighed against the availability of sufficient storage on the hypervisor servers.

When you create a connection, you choose one of two storage management methods: storage shared by hypervisors, or storage local to the hypervisor.

When using local storage on one or more Citrix Hypervisor 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.)

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 and the personal vDisk 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 method 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.

When you create a connection, if you enable the option to store temporary data locally, you can then enable and configure nondefault values for each VM's cache disk size and memory size when you create a Machine Catalog that uses that connection. However, the default values are tailored to the connection type, and are sufficient for most cases. For details, see Create Machine Catalogs.

The hypervisor can also provide optimization technologies through read caching of the disk images locally. For example, Citrix Hypervisor 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, master images and other OS data are transferred to all of 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.

When you select this method, you can choose whether to use shared storage for personal vDisks, to provide resilience and support for backup and disaster recovery systems.

Create a connection and resources

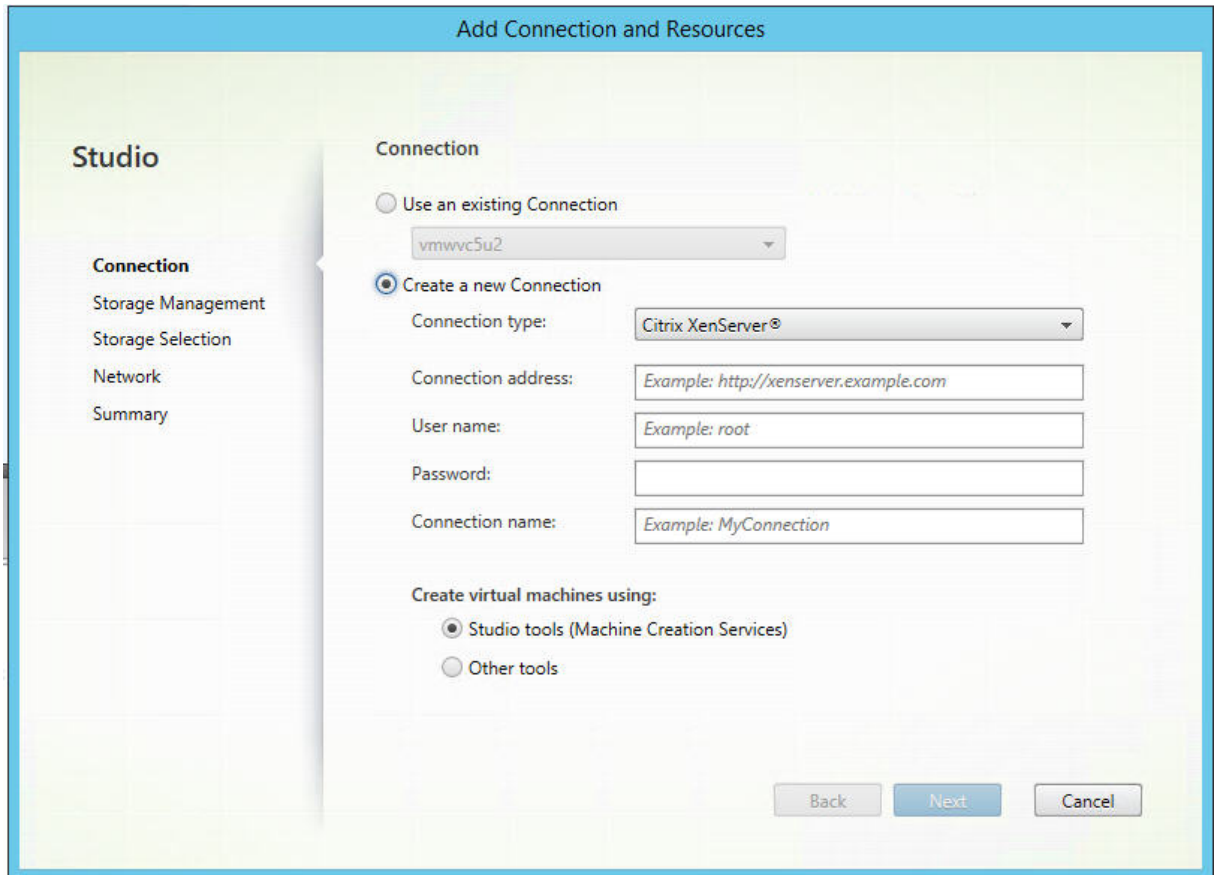
You can optionally create the first connection when you create the Site. The Site creation wizard contains the connection-related pages described below: Connection, Storage Management, Storage Selection, and Network.

If you are creating a connection after you create the Site, start with step 1 below.

> **Important:**
> The host resources (storage and network) must be available before you create a connection.

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select **Add Connections and Resources** in the **Actions** pane.
3. The wizard guides you through the following pages (specific page content depends on the selected connection type). After completing each page, click **Next** until you reach the **Summary** page.

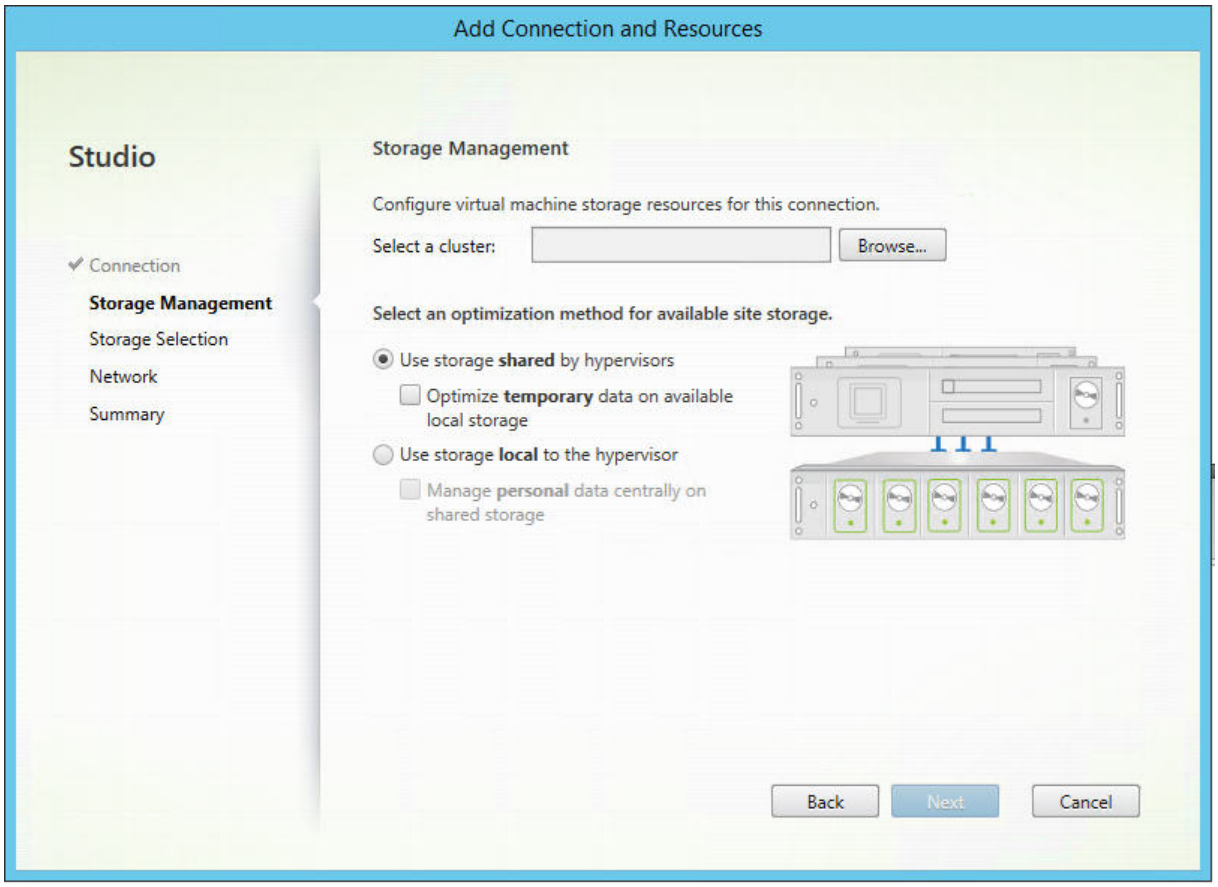
Connection



On the **Connection** page:

- To create a 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 the hypervisor or cloud service you are using in the **Connection type** field.
- The connection address and credentials fields differ, depending on the selected connection type. Enter the requested information.
- Enter a connection name. This name appears in Studio.
- Choose the tool you use to create virtual machines: Studio tools (such as Machine Creation Services or Citrix Provisioning) or other tools.

Storage management



For information about storage management types and methods, see Host storage.

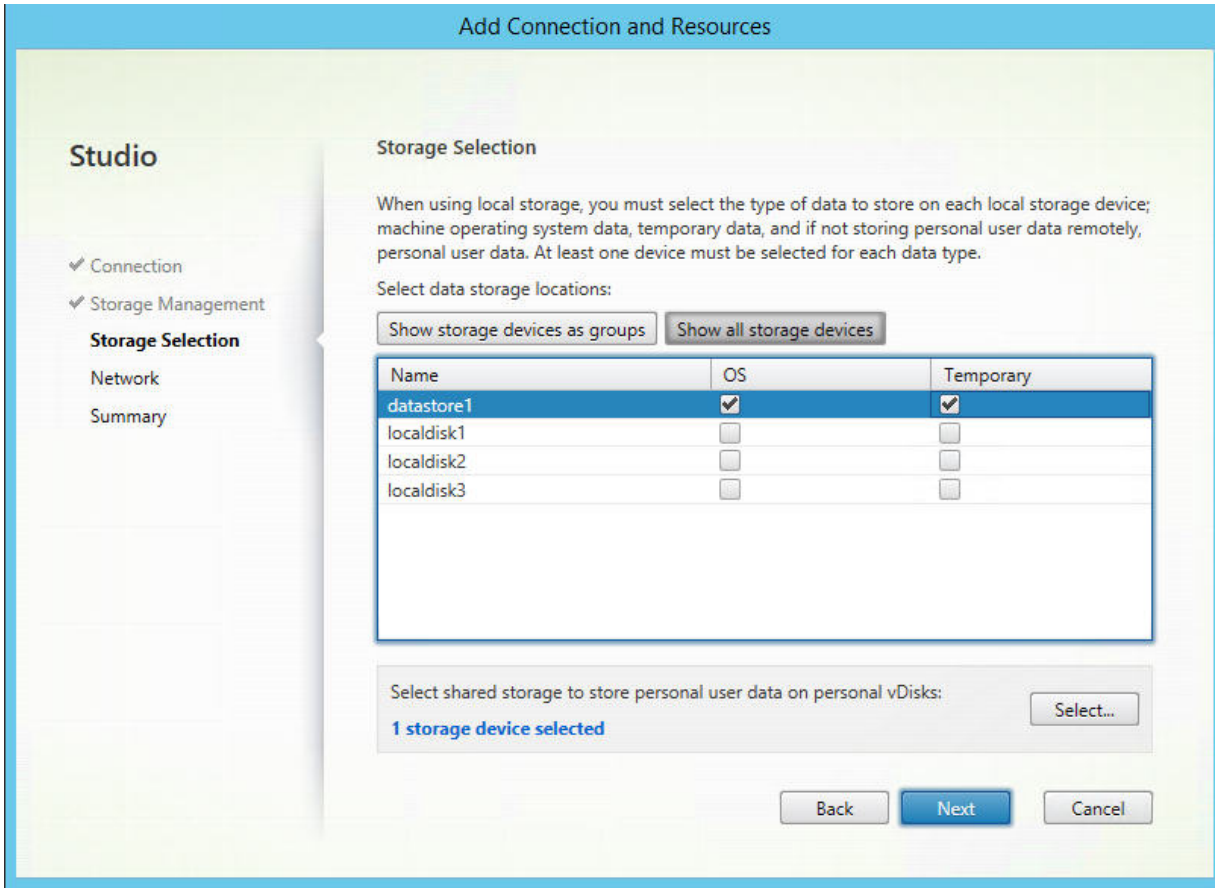
If you are configuring a connection to a Hyper-V or VMware host, browse to and then select a cluster name. Other connection types do not request a cluster name.

Select a storage management method: storage shared by hypervisors or storage local to the hypervisor.

- If you choose storage shared by hypervisors, indicate if you want to keep temporary data on available local storage. (You can specify nondefault temporary storage sizes in the Machine Catalogs that use this connection.) **Exception:** When using Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks to be created on local storage, so configuring that storage management setup in Studio fails.
- If you choose storage local to the hypervisor, indicate if you want to manage personal data (personal vDisks) on shared storage.

If you use shared storage in a Citrix Hypervisor pool, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Use IntelliCache for Citrix Hypervisor connections.

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 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.

The lower portion of the **Storage Selection** page contains more configuration options if you selected either of the following on the previous page.

- If you chose storage shared by hypervisors, and enabled the **Optimize temporary data on available local storage** check box, you can select which local storage devices (in the same hypervisor pool) to use for temporary data.
- If you chose storage local to the hypervisor, and enabled the **Manage personal data centrally on shared storage** check box, you can select which shared devices to use for personal (PvD) data.

The number of currently selected storage devices is shown (in the graphic above, "1 storage device selected"). When you hover over that entry, the selected device names appear (unless there are no

devices configured).

1. Click **Select** to change the storage devices to use.
2. In the **Select Storage** dialog box, select or clear the storage device check boxes, and then click **OK**.

Network

On the **Network** page, enter a name for the resources. This name appears in Studio to identify the storage and network combination associated with the connection.

Select one or more networks that the VMs use.

Summary

On the **Summary** page, review your selections. When you're done, click **Finish**.

Remember: If you chose to store temporary data locally, you can configure nondefault values for temporary data storage when you create the Machine Catalog containing machines that use this connection. See Create Machine Catalogs.

Edit connection settings

Do not use this procedure to rename a connection or to create a connection. Those are different operations. 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.

You cannot change the **GPU** settings for a connection, because Machine Catalogs accessing this resource must use an appropriate GPU-specific master image. Create a connection.

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the connection and then select **Edit Connection** in the **Actions** pane.
3. Follow the guidance below for the settings available when you edit a connection.
4. When you are finished, click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

Connection Properties page:

- To change the connection address and credentials, select **Edit settings** and then enter the new information.
- To specify the high-availability servers for a Citrix Hypervisor connection, select **Edit HA servers**. Citrix recommends that you select all servers in the pool to allow communication with Citrix Hypervisor if the pool master fails.

Advanced page:

- For a Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN connection type, which is used with Remote PC Access, enter **ConfMgr Wake Proxy**, magic packets, and packet transmission information.
- The throttling threshold settings enable you to specify a maximum number of power actions allowed on a 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 and should not 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 the **Connection options** field only under the guidance of a Citrix Support representative or explicit documentation instructions.

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. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the connection. To turn maintenance mode on, select **Turn On Maintenance Mode** in the **Actions** pane. To turn maintenance mode off, select **Turn Off Maintenance Mode**.

You can also turn maintenance mode on or off for individual machines. Also, you can turn maintenance mode on or off for machines in Machine Catalogs or Delivery Groups.

Delete a connection

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 is referenced by that catalog. If this connection is referenced by a catalog, you have the option to delete the catalog. Before you delete a catalog, make sure it is not used by other connections.

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the connection and then select **Delete Connection** in the **Actions** pane.
3. If this connection has machines stored on it, you are asked whether the machines should be deleted. If they are to be deleted, specify what should be done with the associated Active Directory computer accounts.

Rename or test a connection

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the connection and then select **Rename Connection** or **Test Connection** in the **Actions** pane.

View machine details on a connection

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the connection and then select **View Machines** in the **Actions** pane.

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 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, click **Unfold**, and then select from the lists of properties and operators.

Manage machines on a connection

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select a connection and then select **View Machines** in the **Action** pane.
3. Select one of the following in the **Actions** pane. Some actions are not available, depending on the machine state and the connection host type.

Action	Description
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 above.)
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

is powered off before the updates are complete.

Edit storage

You can display the status of servers that are used to store 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. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the connection and then select **Edit Storage** in the **Actions** pane.
3. In the left pane, select the data type: operating system, personal vDisk, or temporary.
4. Select or clear the checkboxes for one or more storage devices for the selected data type.
5. Click **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 in this storage.
- **Not in use:** The storage is not being used for creating machines.

If you clear the check box 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 it is possible for that location to become full even after it stops being used for creating machines.

Delete, rename, or test resources

1. Select **Configuration > Hosting** in the **Studio** navigation pane.
2. Select the resource and then select the appropriate entry in the **Actions** pane: **Delete Resources**, **Rename Resources**, or **Test Resources**.

Connection timers

You can use 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.

Troubleshoot

Use the information in this section to troubleshoot issues related to host connections.

Access key error when adding AWS EC2 URL on the hosting resource

In the Citrix Studio **Hosting node** screen, adding AWS EC2 as the hosting connection and specifying the **API** key, secret key, and connection name generates an SSL error. A message appears, indicating "An error occurred with your **API** key and secret key combination. Ensure that you enter them correctly."

This issue occurs as a result of:

- using the proxy server to connect to the external network.
- using another EC2 connection that has a different URL connection from the Amazon AWS server.

In the Studio **Hosting node** screen, the default address string for an EC2 connection is hard coded as `https://ec2.amazonaws.com`, which is a global endpoint URL. If the AWS service is not able to route the endpoint URL to the one you specify, access keys, including the access key ID and the secret access key, cannot be verified.

To resolve this issue, add the EC connection using a different URL, or use connect to the Internet using a proxy server. In addition, create an EC2 hosting connection manually using PowerShell rather than Citrix Studio:

1. Launch PowerShell from the DDC host and load all Citrix modules using the command `asnp Citrix`.
2. Configure environment variables for the proxy server and the port:

```
$server = "<PROXY_SERVER>"
$port = "<PROXY_SERVER_PORT>"
$options = "ProxyHost=$server,ProxyPort=$port"
<!--NeedCopy-->
```

Run the following commands to add the EC2 hosting connection:


```
$hyp= New-Item -Path xdhyp:\Connections -AdminAddress "localhost" -Name
     " AWSEC2 "  -ConnectionType "AWS" -HypervisorAddress @[AWS URL](
    https://<AWS_URL>) -UserName "APIkey" -Password "Secret key" -
    Metadata @{
  "Citrix_MachineManagement_Options" = $options  }
  -Persist
<!--NeedCopy-->
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $hyp.
    HypervisorConnectionUid
<!--NeedCopy-->
```

Launch Citrix Studio and check the host connection to verify the generation of the AWS EC2 site.

Local Host Cache

April 1, 2024

To ensure that the Citrix Virtual Apps and Desktops Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment, by following high availability best practices from Microsoft. (For supported SQL Server high availability features, see Databases.) However, network issues and interruptions may result in users not being able to connect to their applications or desktops.

The Local Host Cache (LHC) feature allows connection brokering operations in a Site to continue when an outage occurs. An outage occurs when the connection between a Delivery Controller and the Site database fails in an on-premises Citrix environment. Local Host Cache engages when the site database is inaccessible for 90 seconds.

As of XenApp and XenDesktop 7.16, the connection leasing feature (a predecessor high availability feature in earlier releases) was removed from the product, and is no longer available.

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 specifically 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.

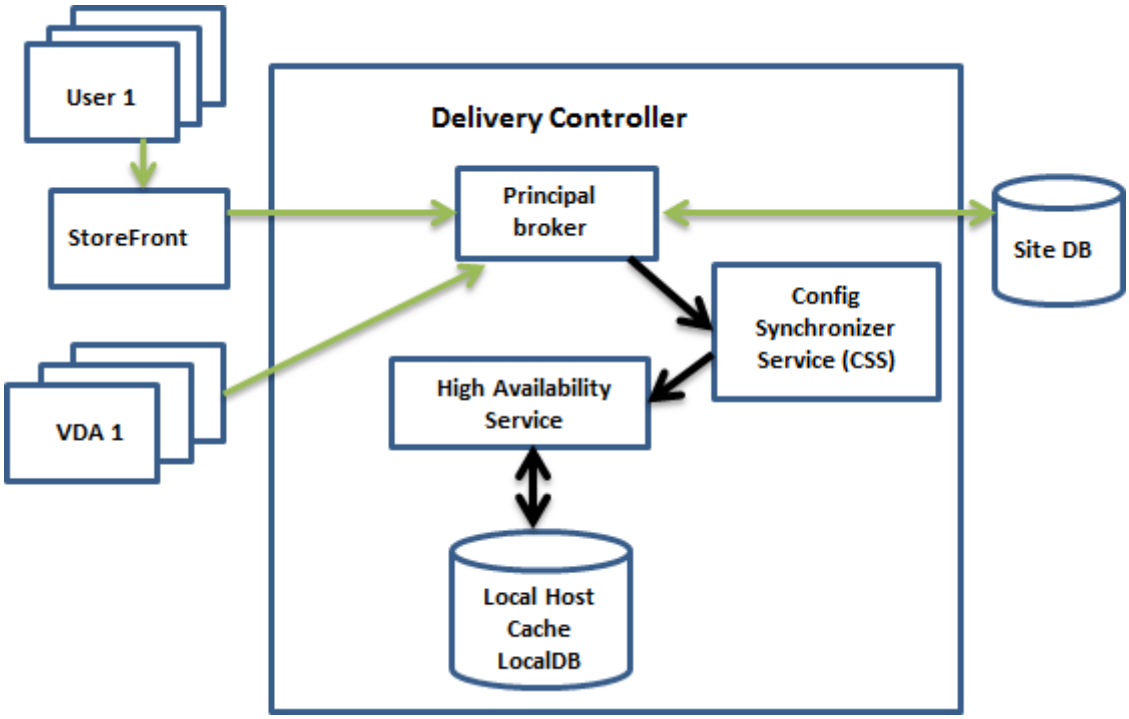
- Identities (names and IP addresses) of client Citrix Receiver machines being actively used to connect to published resources.

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 Receiver.
- Identities of infrastructure machines (such as NetScaler Gateway and StoreFront servers) involved with the Site.
- Dates and times and types of recent activity by users.

How it works

The following graphic illustrates the Local Host Cache components and communication paths during normal operations.

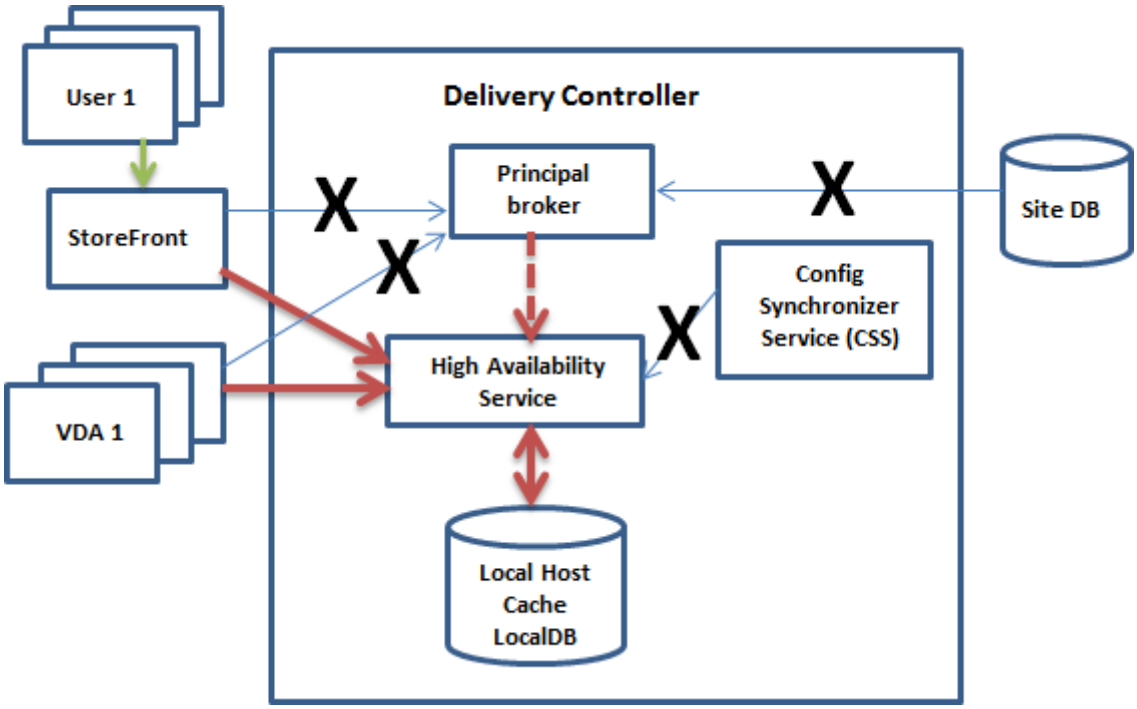


During normal operations:

- The *principal broker* (Citrix Broker Service) on a Controller accepts connection requests from StoreFront, and communicates with the Site database to connect users with VDAs that are registered with the Controller.
- A check is made periodically (one minute after the previous check finished) to determine whether changes have been made to the principal broker's configuration. Those changes could have been initiated by PowerShell/Studio actions (such as changing a Delivery Group property) or system actions (such as machine assignments).

- If a change has been made since the last check, the Citrix Config Synchronizer Service (CSS) synchronizes (copies) information to the Citrix High Availability Service on the Controller. (In some documentation, the High Availability Service is referred to as the secondary broker.) All broker configuration data is copied, not just items that have changed since the previous check. The High Availability Service imports the data into a Microsoft SQL Server Express LocalDB database on the Controller. The CSS ensures that the information in the LocalDB database matches the information in the Site database. The LocalDB database is re-created each time synchronization occurs.
- If no changes have occurred since the last check, no data is copied.

The following graphic illustrates the changes in communications paths if the principal broker loses contact with the Site database (an outage begins).



When an outage begins:

- The principal broker can no longer communicate with the Site database, and stops listening for StoreFront and VDA information (marked X in the graphic). The principal broker then instructs the High Availability Service to start listening for and processing connection requests (marked with a red dashed line in the graphic). The High Availability Service disards all calls from the CSS.
- When the outage begins, the High Availability Service has no current VDA registration data, but as soon as a VDA communicates with it, a re-registration process is triggered. During that process, the High Availability Service also gets current session information about that VDA.
- While the High Availability Service is handling connections, the principal broker continues to monitor the connection to the Site database. When the connection is restored, the principal

broker instructs the High Availability Service to stop listening for connection information, and the principal broker resumes brokering operations. The next time a VDA communicates with the principal broker, a re-registration process is triggered. The High Availability Service removes any remaining VDA registrations from the previous outage, and resumes updating the LocalDB database with configuration changes received from the CSS.

The transition between normal and outage mode does not affect existing sessions; it affects only the launching of new sessions.

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 provides information about synchronizations and outages. See the "Monitor"section below for details.

You can also intentionally trigger an outage; see the "Force an outage"section below for details about why and how to do this.

Sites with multiple Controllers

Among its other tasks, the CSS routinely provides the High Availability Service with information about all Controllers in the zone. (If your deployment does not contain multiple zones, this action affects all Controllers in the Site.) Having that information, each High Availability Service knows about all peer High Availability Services.

The High Availability Services communicate with each other on a separate channel. They use an alphabetical list of FQDN names of the machines they're running on to determine (elect) which High Availability Service will be in charge of brokering operations in the zone if an outage occurs. During the outage, all VDAs re-register with the elected High Availability Service. The non-elected High Availability Services in the zone will actively reject incoming connection and VDA registration requests.

If an elected High Availability Service fails during an outage, another High Availability Service is elected to take over, and VDAs will re-register with the newly-elected High Availability Service.

During an outage, if a Controller is restarted:

- If that Controller is not the elected primary broker, the restart has no impact.
- If that Controller is the elected primary broker, a different Controller is elected, causing VDAs to re-register. After the restarted Controller powers on, it automatically takes over brokering, which causes VDAs to re-register again. In this scenario, performance may be affected during the re-registrations.

If you power off a Controller during normal operations and then power it on during an outage, Local Host Cache cannot be used on that Controller if it is elected as the primary broker.

The event log provides information about elections. See the "Monitor"section below.

Design considerations and requirements

There is no time limit imposed for operating in outage mode. However, restore the site to normal operation as quickly as possible.

What is unavailable during an outage, and other differences

- You cannot use Studio or run PowerShell cmdlets.
- 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 may use more sessions than their configured session limits, if the resources are in different zones.
- Users can launch applications and desktops only from registered VDAs in the zone containing the currently active/elected High Availability Service. Launches across zones (from a High Availability Service in one zone to a VDA in a different zone) are not supported during an outage.
- 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 can have unintended results. For more information, see Scheduled restarts delayed due to database outage.
- Tag restrictions where tags are used to designate zones 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.

Local Host Cache is supported for server-hosted applications and desktops, and static (assigned) desktops.

By default, power-managed desktop VDAs in pooled delivery groups (created by MCS or Citrix Provisioning) that have the `ShutdownDesktopsAfterUse` property enabled are not available for new connections during a Local Host Cache event. You can change this default, to allow those desktops to be used during Local Host Cache. However, you cannot rely on the power management during the outage. (Power management resumes after normal operations resume.) Also, those desktops might contain data from the previous user, because they have not been restarted.

To override the default behavior, you must enable it site-wide and for each affected Delivery Group. Run the following PowerShell cmdlets.

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true Set
-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
```



```
$true
```

Enabling this feature in the Site and the Delivery Groups does not affect how the configured "ShutdownDesktopsAfterUse"property works during normal operations. When this feature is enabled, VDAs do not automatically reboot after the LHC event is complete. Power-managed desktop VDAs in pooled delivery groups can retain data from previous sessions until the VDA is rebooted. This can occur when a user logs off of the VDA during non-LHC operations or the reboot can be triggered manually.

> **Important:**
>
> Without enabling ReuseMachinesWithoutShutdownInOutageAllowed at the Site level and ReuseMachinesWithoutShutdownInOutage at the delivery group level, all session launch attempts to power-managed desktop VDAs in pooled delivery groups will fail during a Local Host Cache event.

RAM size considerations

The LocalDB service can use approximately 1.2 GB of RAM (up to 1 GB for the database cache, plus 200 MB for running SQL Server Express LocalDB). The High Availability Service can use up to 1 GB of RAM if an outage lasts for an extended interval with many logons occurring (for example, 12 hours with 10K users). These memory requirements are in addition to the normal RAM requirements for the Controller, so you might need to increase the total amount of RAM capacity.

Note that if you use a SQL Server Express installation for the Site database, the server will have two sqlserver.exe processes.

CPU core and socket configuration considerations

A Controller's CPU configuration, particularly the number of cores available to the SQL Server Express LocalDB, directly affects Local Host Cache performance, even more than memory allocation. This CPU overhead is observed only during the outage period when the database is unreachable and the High Availability service is active.

While LocalDB can use multiple cores (up to 4), it's limited to only a single socket. Adding more sockets will not improve the performance (for example, having 4 sockets with 1 core each). Instead, Citrix recommends using multiple sockets with multiple cores. In Citrix testing, a 2x3 (2 sockets, 3 cores) configuration provided better performance than 4x1 and 6x1 configurations.

Storage considerations

As users access resources during an outage, the LocalDB grows. For example, during a logon/logoff test running at 10 logons per second, the database grew by one MB every 2-3 minutes. When normal

operation resumes, the local database is recreated and the space is returned. However, sufficient space must be available on the drive where the LocalDB is installed to allow for the database growth during an outage. Local Host Cache also incurs additional I/O during an outage: approximately 3 MB of writes per second, with several hundred thousand reads.

Performance considerations

During an outage, one High Availability Service handles all the connections, so in Sites (or zones) that load balance among multiple Controllers during normal operations, the elected High Availability Service might need to handle many more requests than normal during an outage. Therefore, CPU demands will be higher. Every High Availability Service in the Site (zone) must be able to handle the additional load imposed by LocalDB and all of the affected VDAs, because the High Availability Service elected during an outage could change.

VDI limits:

- In a single-zone VDI deployment, up to 10,000 VDAs can be handled effectively during an outage.
- In a multi-zone VDI deployment, up to 10,000 VDAs in each zone can be handled effectively during an outage, to a maximum of 40,000 VDAs in the site. For example, each of the following sites can be handled effectively during an outage:
  - A site with four zones, each containing 10,000 VDAs.
  - A site with seven zones, one containing 10,000 VDAs, and six containing 5,000 VDAs each.

During an outage, load management within the Site may be affected. Load evaluators (and especially, session count rules) may be exceeded.

During the time it takes all VDAs to re-register with a High Availability Service, that service might not have complete information about current sessions. So, a user connection request during that interval could result in a new session being launched, even though reconnection to an existing session was possible. This interval (while the "new"High Availability Service acquires session information from all VDAs during re-registration) is unavoidable. Note that sessions that are connected when an outage starts are not impacted during the transition interval, but new sessions and session reconnections could be.

This interval occurs whenever VDAs must re-register:

- An outage starts: When migrating from a principal broker to a High Availability Service.
- High Availability Service failure during an outage: When migrating from a High Availability Service that failed to a newly-elected High Availability Service.
- Recovery from an outage: When normal operations resume, and the principal broker resumes control.

You can decrease the interval by lowering the Citrix Broker Protocol's HeartbeatPeriodMs registry value (default = 600000 ms, which is 10 minutes). This heartbeat value is double the interval the VDA uses for pings, so the default value results in a ping every 5 minutes.

For example, the following command changes the heartbeat to five minutes (300000 milliseconds), which results in a ping every 2.5 minutes:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Use caution when changing the heartbeat value. Increasing the frequency results in greater load on the Controllers during both normal and outage modes.

The interval cannot be eliminated entirely, no matter how quickly the VDAs register.

The time it takes to synchronize between High Availability Services increases with the number of objects (such as VDAs, applications, groups). For example, synchronizing 5000 VDAs might take ten minutes of more to complete. See Monitor for information about synchronization entries in the event log.

Differences from XenApp 6.x releases

Although this Local Host Cache implementation shares the name of the Local Host Cache feature in XenApp 6.x and earlier XenApp releases, there are significant improvements. This implementation is more robust and immune to corruption. Maintenance requirements are minimized, such as eliminating the need for periodic dsmaint commands. This Local Host Cache is an entirely different implementation technically.

Manage Local Host Cache

For Local Host Cache to work correctly, the PowerShell execution policy on each Controller must be set to RemoteSigned, Unrestricted, or Bypass.

SQL Server Express LocalDB

The Microsoft SQL Server Express LocalDB that Local Host Cache uses is installed automatically when you install a Controller or upgrade a Controller from a version earlier than 7.9. There is no administrator maintenance needed for the LocalDB. Only the High Availability Service communicates with this database. You cannot use PowerShell cmdlets to change anything about this database. The LocalDB cannot be shared across Controllers.

The SQL Server Express LocalDB database software is installed regardless of whether Local Host Cache is enabled.

To prevent its installation, install or upgrade the Controller using the XenDesktopServerSetup.exe command, and include the `/exclude "Local Host Cache Storage (LocalDB)"` option. However, keep in mind that the Local Host Cache feature will not work without the database, and you cannot use a different database with the High Availability Service.

Installation of this LocalDB database has no effect on whether or not you install SQL Server Express for use as the site database.

For information about replacing an earlier SQL Server Express LocalDB version with a newer version, see Replace SQL Server Express LocalDB.

Default settings after product installation and upgrade

During a new installation of Citrix Virtual Apps and Desktops (minimum version 7.16), Local Host Cache is enabled. After an upgrade (to version 7.16 or later), Local Host Cache is enabled if there are fewer than 10,000 VDAs in the entire deployment.

Enable and disable Local Host Cache

- To enable Local Host Cache, enter:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  To determine whether Local Host Cache is enabled, enter:

  ```
  Get-BrokerSite
  ```

  Check that the LocalHostCacheEnabled property is True.

- To disable Local Host Cache, enter:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Remember: As of XenApp and XenDesktop 7.16, connection leasing (the feature that preceded Local Host Cache beginning with version 7.6) was removed from the product, and is no longer available.

Verify that Local Host Cache is working

To verify that Local Host Cache is set up and working correctly:

- Ensure that synchronization imports complete successfully. Check the event logs.
- Ensure that the SQL Server Express LocalDB database was created on each Delivery Controller. This confirms that the High Availability Service can take over, if needed.
- On the Delivery Controller server, browse to C:\Windows\ServiceProfiles\NetworkService.
- Verify that HaDatabaseName.mdf and HaDatabaseName_log.ldf are created.

- Force an outage on the Delivery Controllers. After you've verified that Local Host Cache works, remember to place all of the Controllers back into normal mode. This can take approximately 15 minutes, to avoid VDA registration storms.

Force an outage

You might want to deliberately force a database outage.

- If your network is going up and down repeatedly. Forcing an outage until the network issues resolve prevents continuous transition between normal and outage modes.
- To test a disaster recovery plan.
- While replacing or servicing the site database server.

To force an outage, edit the registry of each server containing a Delivery Controller. In `HKLM\Software\Citrix\DesktopServer\LHC`, set `OutageModeForced` as `REG_DWORD` to 1. This instructs the broker to enter outage mode, regardless of the state of the database. Setting the value to 0 takes the server out of outage mode.

Monitor

Event logs indicate when synchronizations and outages occur.

Config Synchronizer Service:

During normal operations, the following events can occur when the CSS copies and exports the broker configuration and imports it to the LocalDB using the High Availability Service.

- 503: A change was found in the principal broker configuration, and an import is starting.
- 504: The broker configuration was copied, exported, and then imported successfully to the LocalDB.
- 505: An import to the LocalDB failed; see below for more information.
- 507: An import was abandoned due to a pending outage. When an outage begins during a synchronization, the current import is discarded and the last known configuration is used.
- 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:

- 3502: An outage occurred and the High Availability Service is performing brokering operations.
- 3503: An outage has been resolved and normal operations have resumed.
- 3504: Indicates which High Availability Service is elected, plus others involved in the election.

Troubleshoot

Several troubleshooting tools are available when an synchronization import to the LocalDB fails and a 505 event is posted.

CDF tracing: Contains options for the ConfigSyncServer and BrokerLHC modules. Those options, along with other broker modules, will likely identify the problem.

Report: You can generate and provide a report that details the failure point. This report feature affects synchronization speed, so Citrix recommends disabling it when not in use.

To enable and produce a CSS trace report, enter:

```
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\CitrixBrokerConfi

After the report is generated, disable the reporting feature:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Export the broker configuration: Provides the exact configuration for debugging purposes.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

For example, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

Manage security keys

June 13, 2024

> **Note:**
>
> You must use this feature in combination with StoreFront 1912 LTSR CU2 or 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. Enable Studio to show the feature settings.
2. Configure settings for your site (Use the Studio console or PowerShell).

3. Configure settings in StoreFront (Use PowerShell).
4. Configure settings in Citrix ADC (Use PowerShell).

Enable Studio to show the feature settings

By default, settings for security keys are hidden from Studio. To enable Studio to show them, use the PowerShell SDK as follows:

To enable the feature, perform these steps:

1. Run the Citrix Virtual Apps and Desktops 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"`

For more information about the Remote PowerShell SDK, see SDKs and APIs.

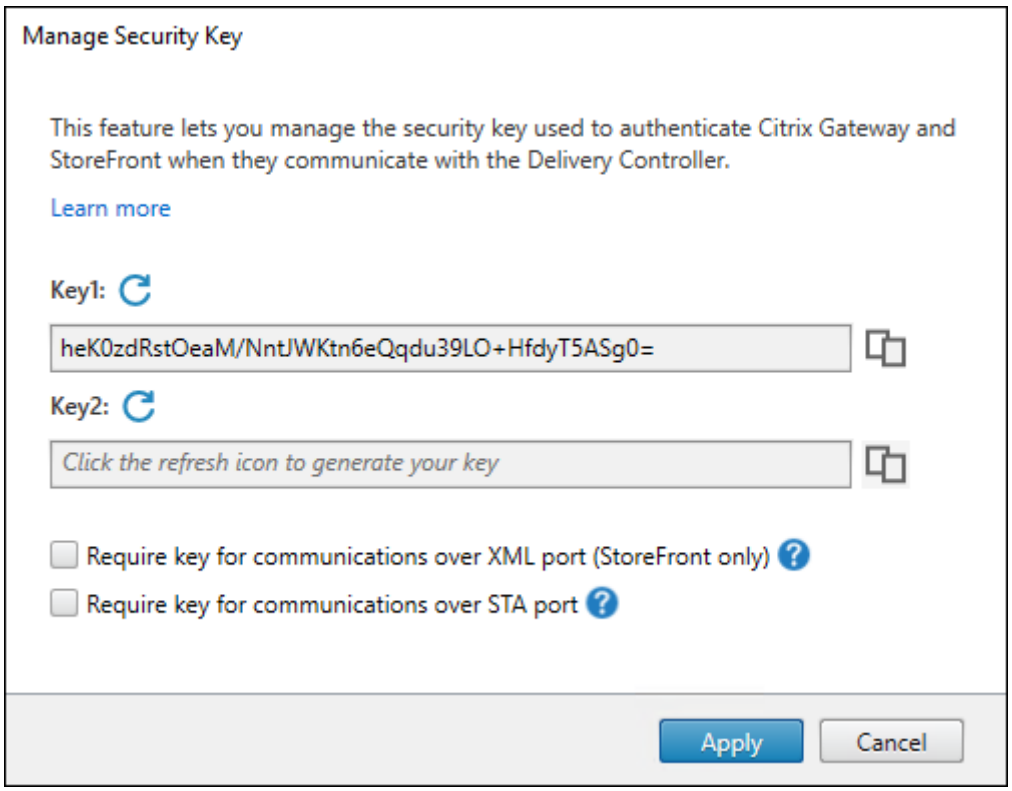
Configure settings for your site

You can configure settings in Studio by using the Studio console or PowerShell.

Use the Studio console

After you enable Studio to show the feature settings, go to **Studio > Configuration > Manage Security Key**. You might need to click **Refresh** for the **Manage Security Key** option to appear.

The **Manage Security Key** window appears after you click **Manage Security Key**.



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** window.

Use PowerShell

The following are PowerShell steps equivalent to Studio operations.

1. Run the Citrix Virtual Apps and Desktops 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 configuration in Studio, 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	https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html]. For example

```
$store = Get-STFStoreService -VirtualPath [Path to store]
$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed name]
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -XMLValidationSecret [secret]
<!--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:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]
$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
    $sta1,$sta2
<!--NeedCopy-->
```

Enter the appropriate values for the following parameters:

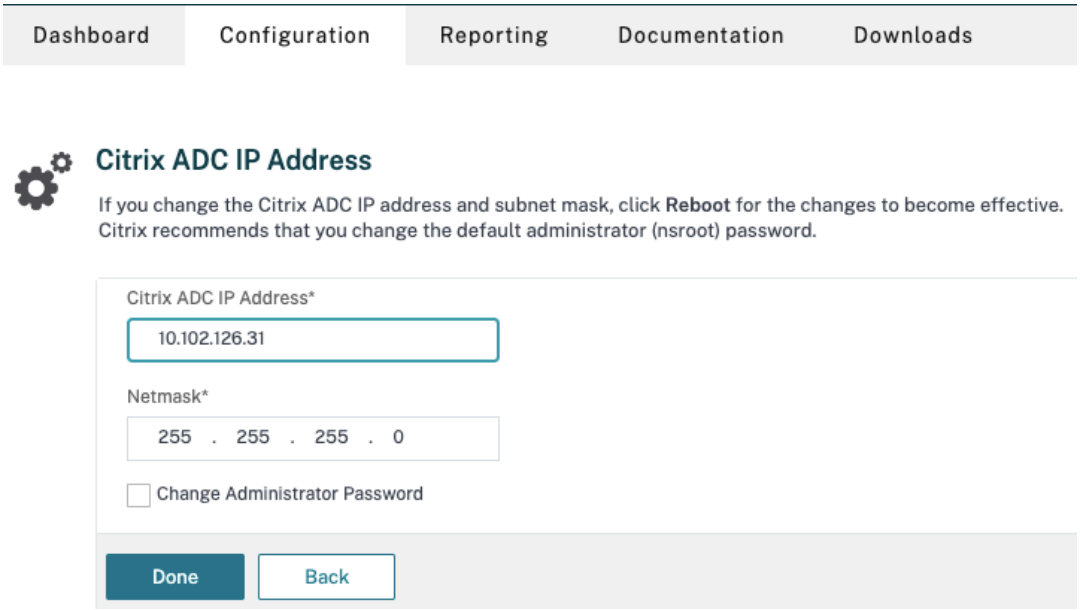
- Gateway name
- STA URL
- Secret

See the PowerShell command help for guidance and syntax.

Configure settings in Citrix ADC

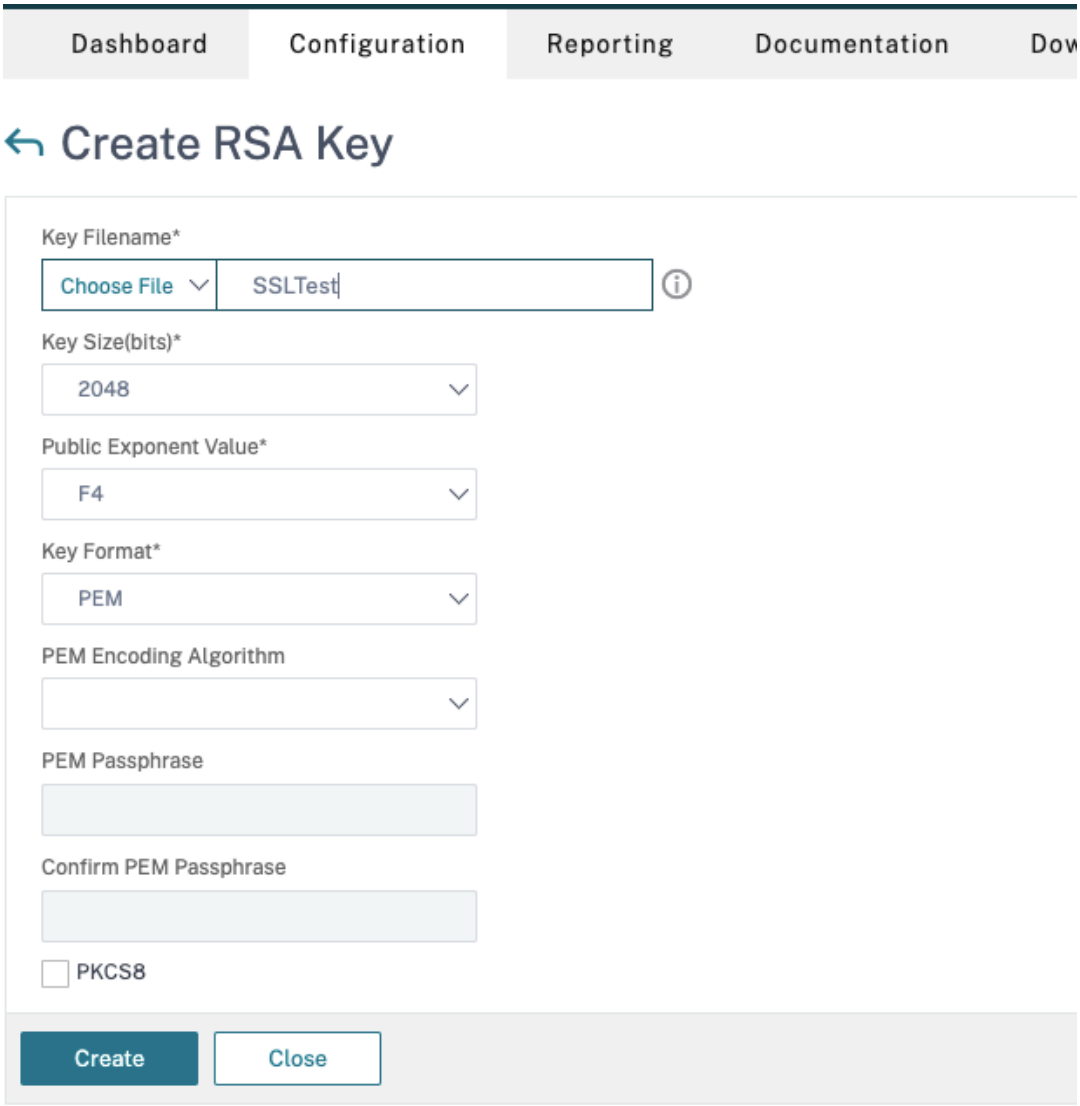
> **Note:**
>
> Configuring this feature in Citrix ADC is not required unless you use Citrix ADC as your gateway. If you use Citrix ADC, follow the steps below.

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.

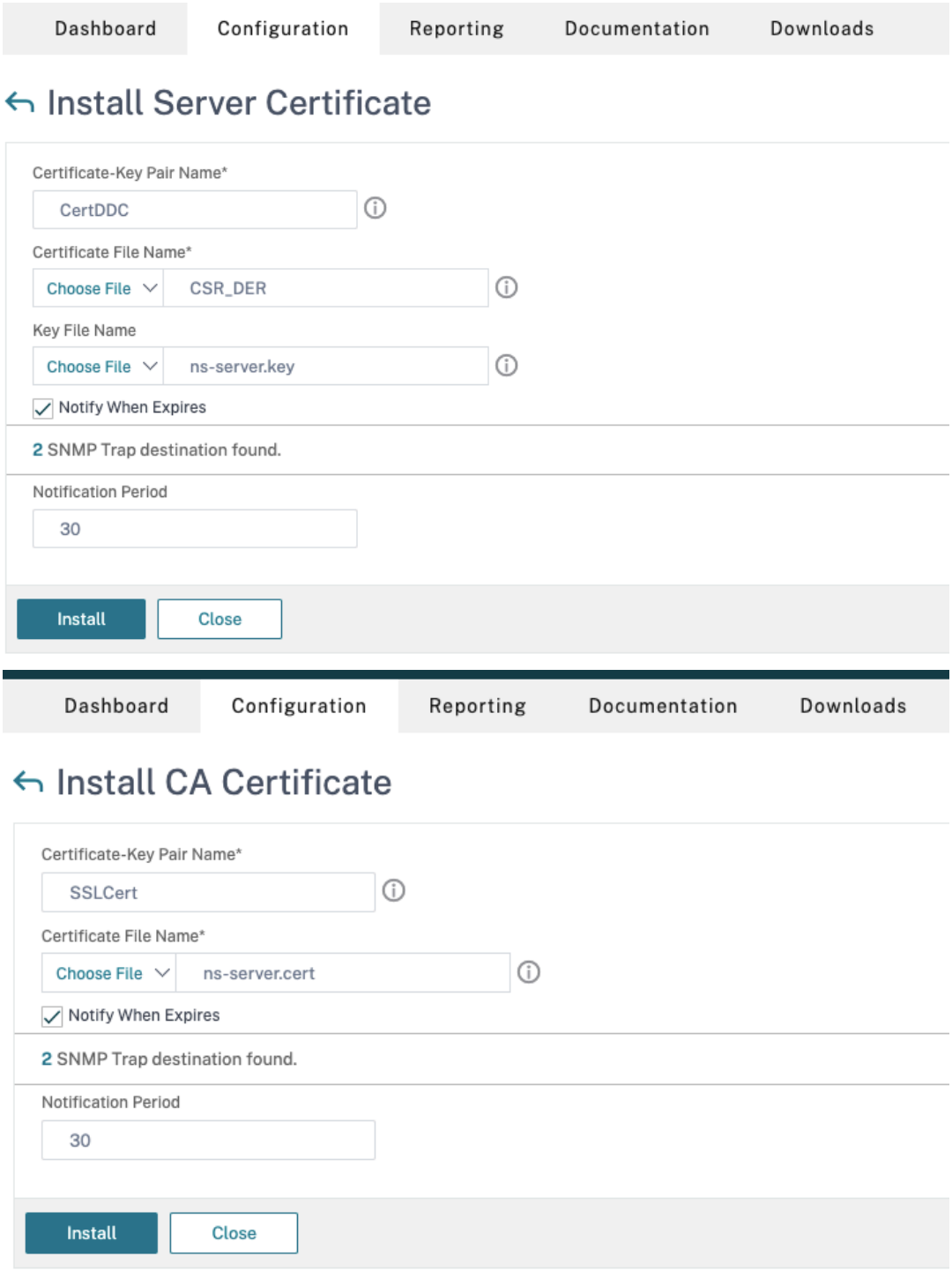


- Subnet IP (SNIP) address for enabling communication between the Citrix ADC appliance and the back-end servers. For details, see Configuring Subnet IP Addresses.
- Citrix Gateway virtual IP address and load balancer virtual IP address to log in to the ADC appliance for session launch. For details, see Create a virtual server.

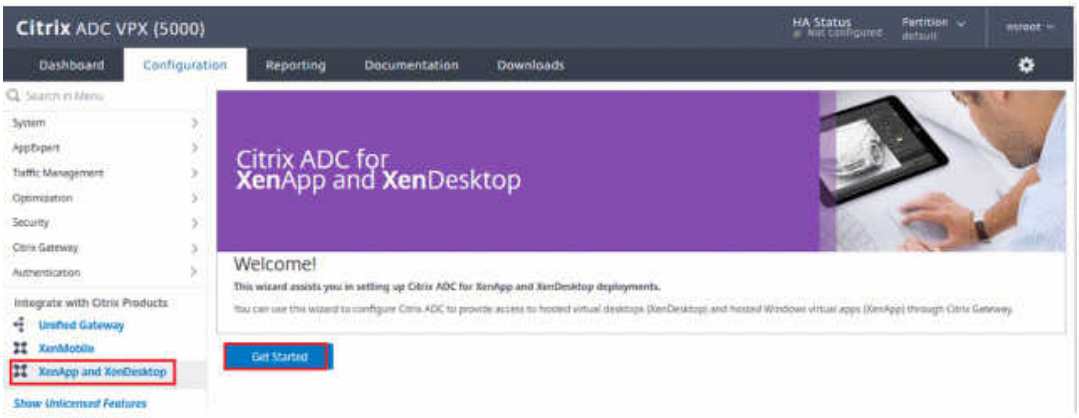
- The required modes and features in the Citrix ADC appliance are enabled.
  - To enable the modes, in the Citrix ADC GUI go to **System > Settings > Configure Mode**.
  - To enable the features, in the Citrix ADC GUI go to **System > Settings > Configure Basic Features**.
- Certificates related configurations 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.

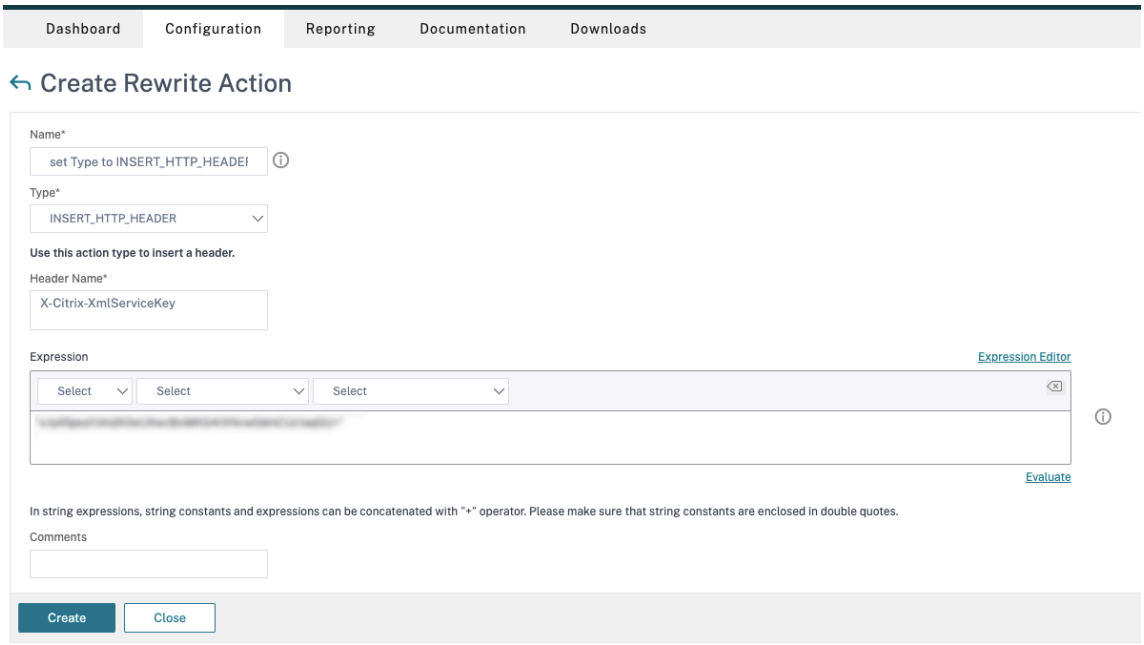


- A Citrix Gateway has been created for Citrix Virtual Desktops. Test the connectivity by clicking the **Test STA Connectivity** button to confirm that the virtual servers are online. For details, see Setting up Citrix ADC for Citrix Virtual Apps and Desktops.

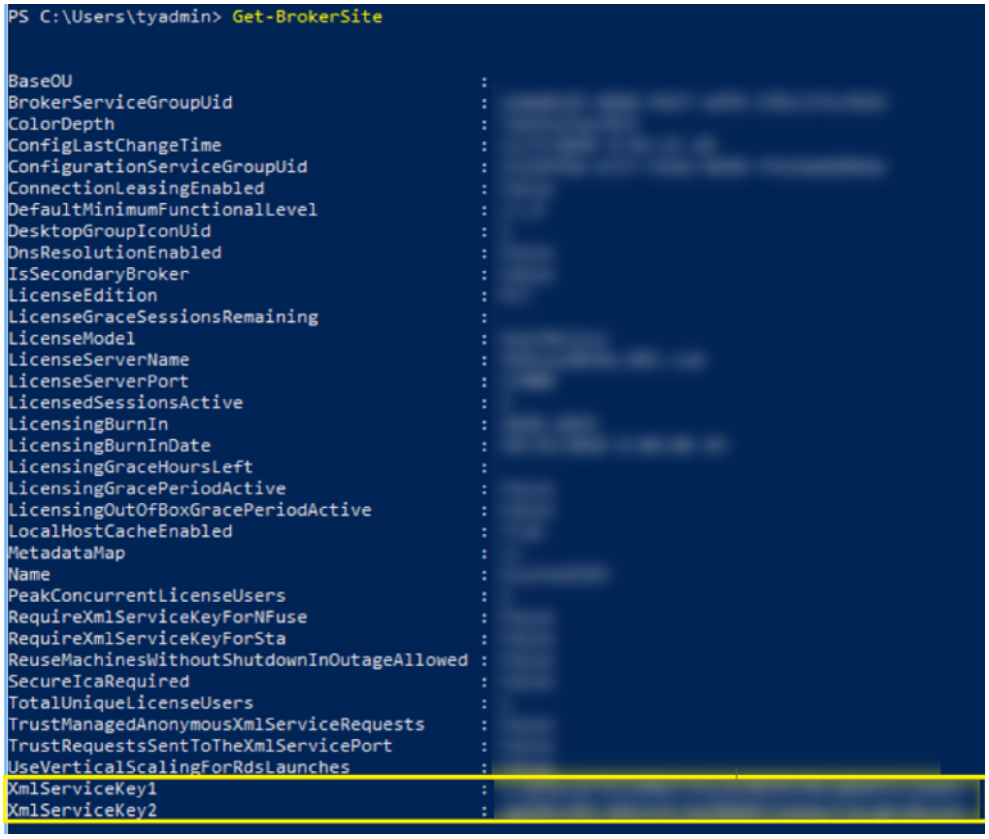


2. Add a rewrite action. For details, see Configuring a Rewrite Action.

   a) Go to **AppExpert > Rewrite > Actions**.
   b) Click **Add** to add a rewrite action. You can name the action as "set Type to INSERT_HTTP_HEADER".



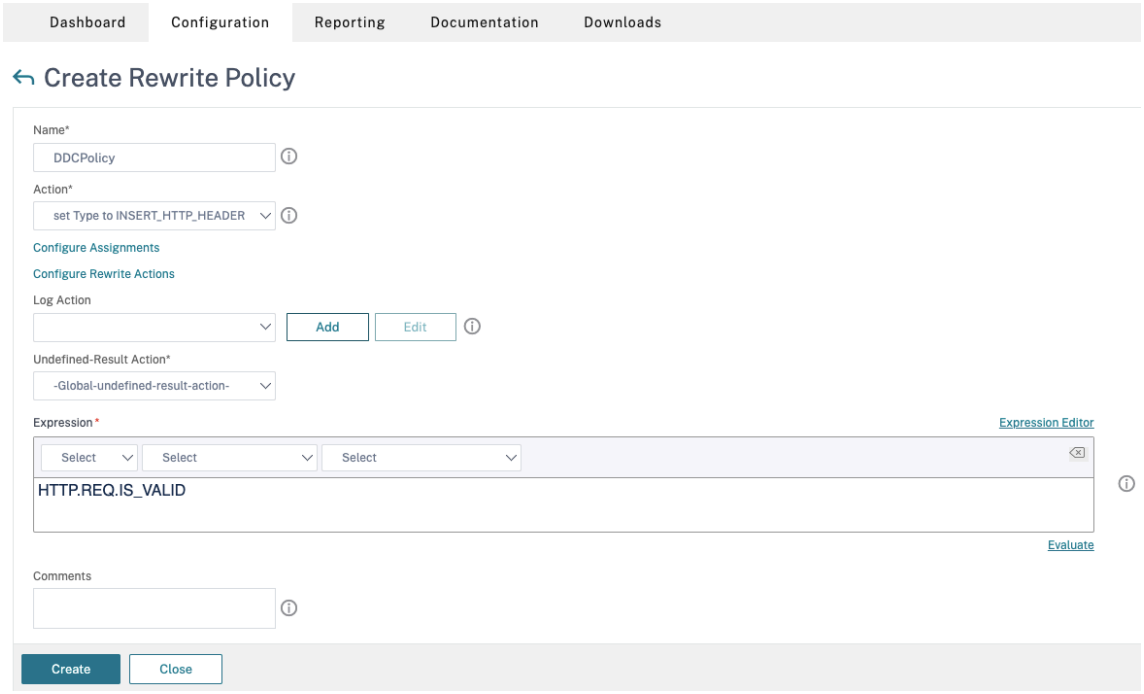
   a) In **Type**, select **INSERT_HTTP_HEADER**.
   b) In **Header Name**, enter X-Citrix-XmlServiceKey.
   c) In **Expression**, add <XmlServiceKey1 value> with the quotes. You can copy the XmlServiceKey1 value from your Desktop Delivery Controller configuration.



3. Add a rewrite policy. For details, see Configuring a Rewrite Policy.

   a) Go to **AppExpert > Rewrite > Policies**.

   b) Click **Add** to add a policy.



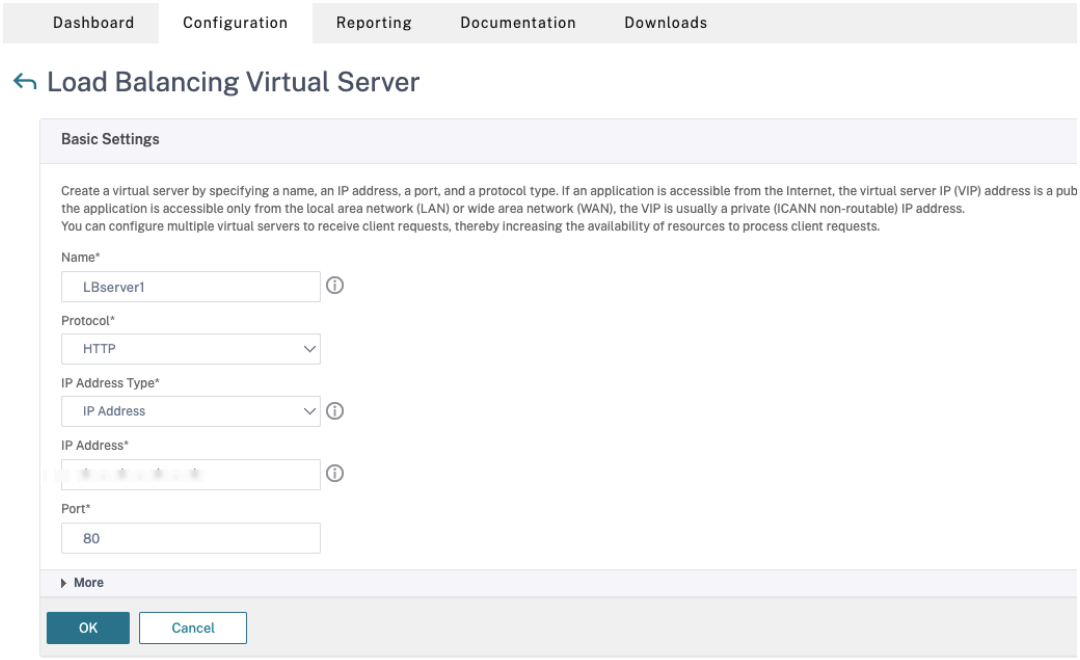
a) In **Action**, select the action created in the earlier step.
b) In **Expression**, add HTTP.REQ.IS_VALID.
c) Click **OK**.

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.

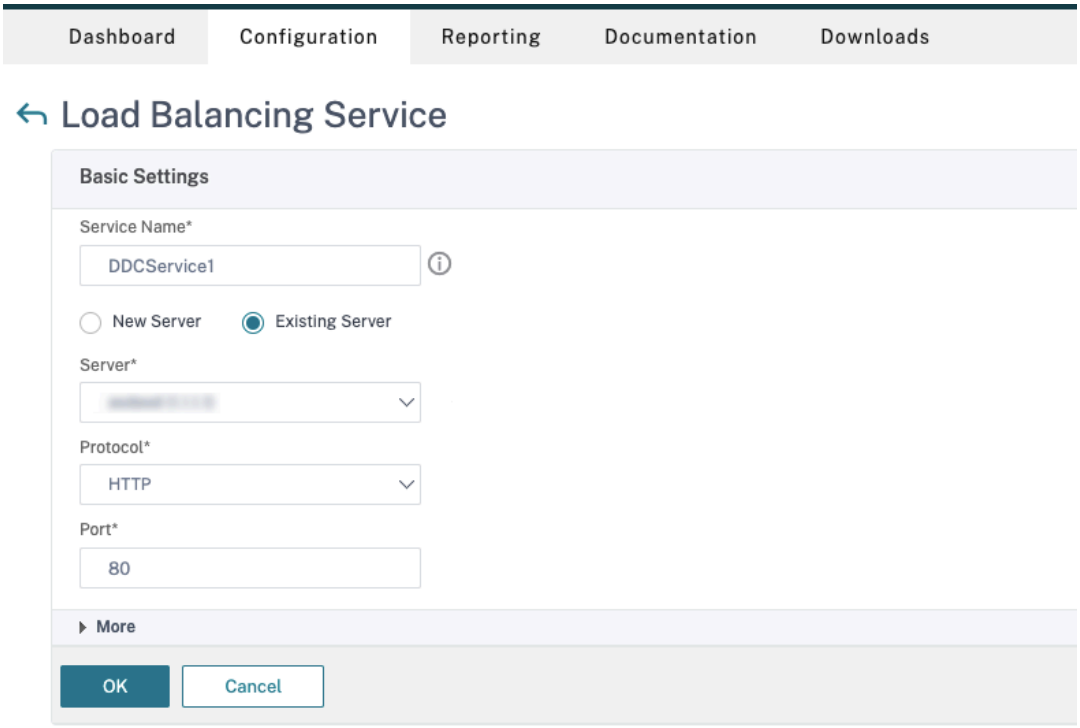
      - Go to **Traffic Management > Load Balancing > Servers**.
      - On **Virtual Servers** page, click **Add**.



- In **Protocol**, select **HTTP**.
- Add the load balancing virtual IP address and in **Port** select **80**.
- Click **OK**.

b) Create a load balancing service.

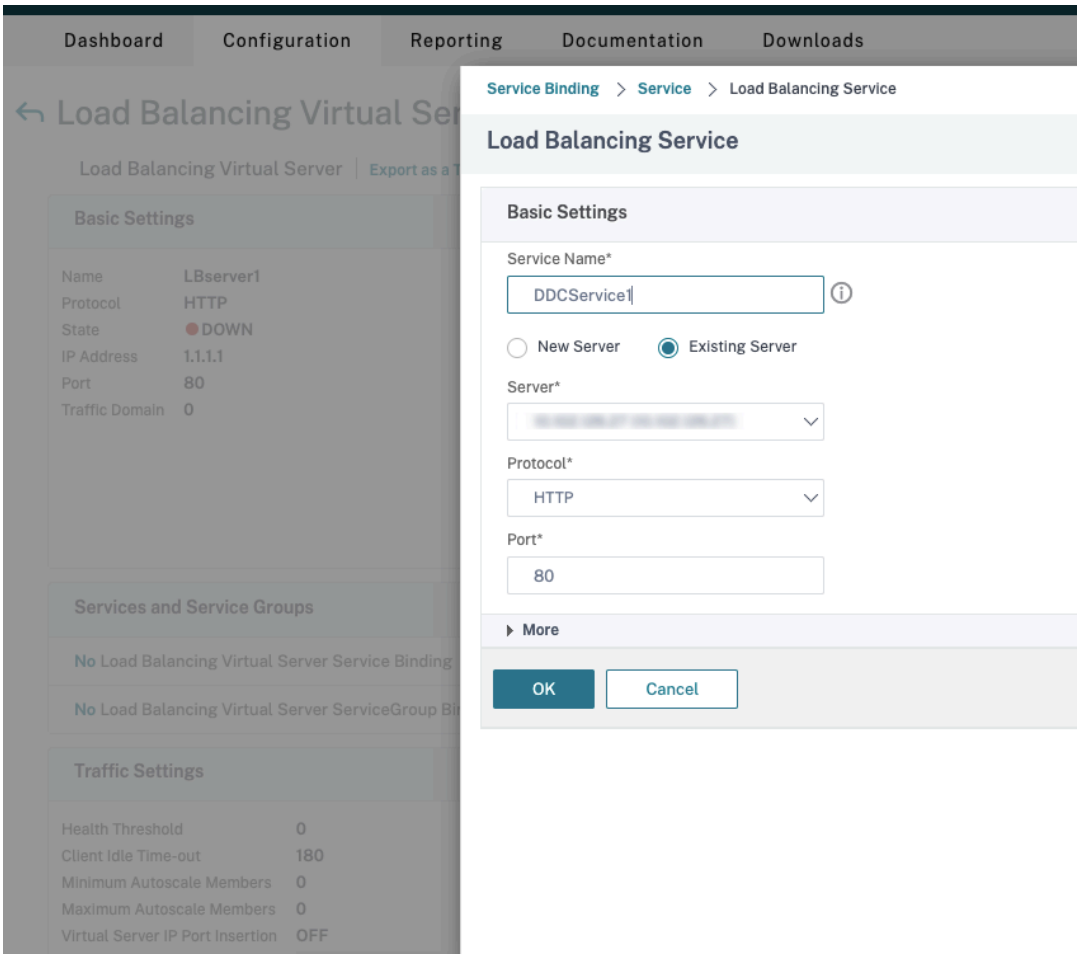
- Go to **Traffic Management > Load Balancing > Services**.



- 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.

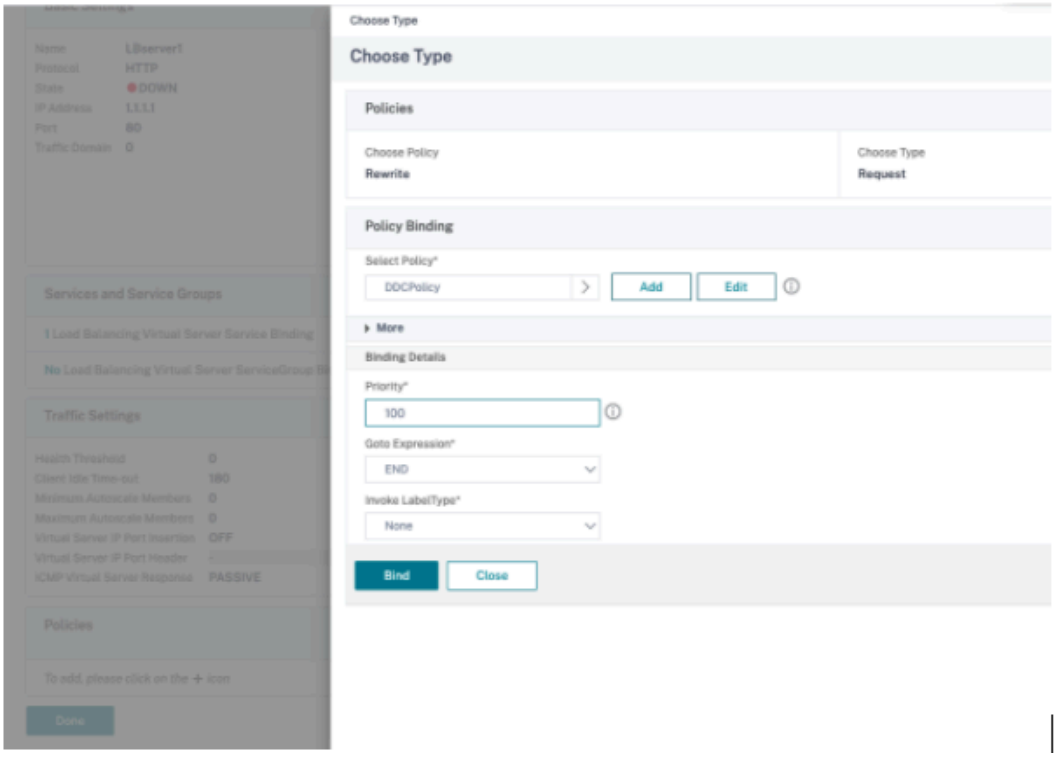
- Select the virtual server created earlier and click **Edit**.
- In **Services and Service Groups**, click **No Load Balancing Virtual Server Service Binding**.



- In **Service Binding**, select the service created earlier.
- Click **Bind**.

d) Bind the rewrite policy created earlier to the virtual server.

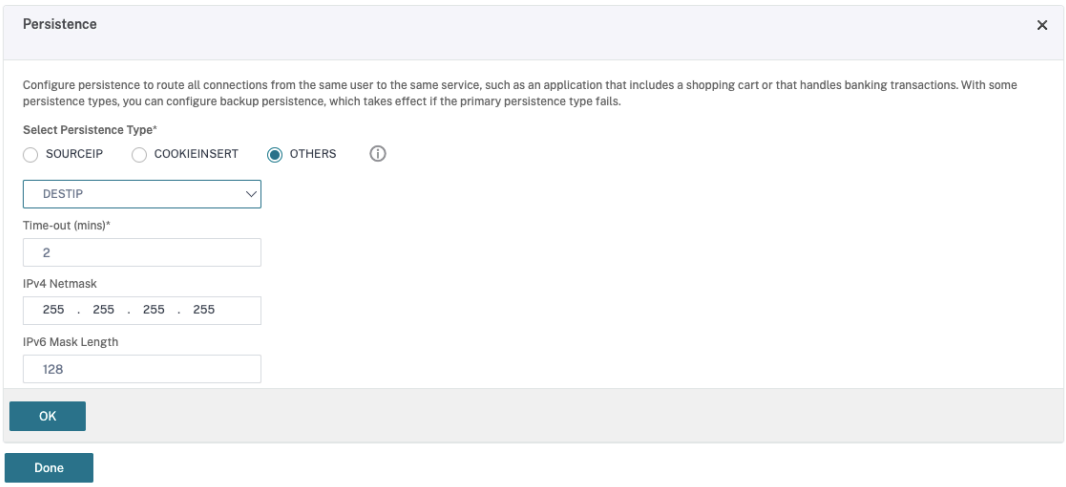
- Select the virtual server created earlier and click **Edit**.
- In **Advanced Settings**, click **Policies,** and then in **Policies** section click **+**.



- 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**.

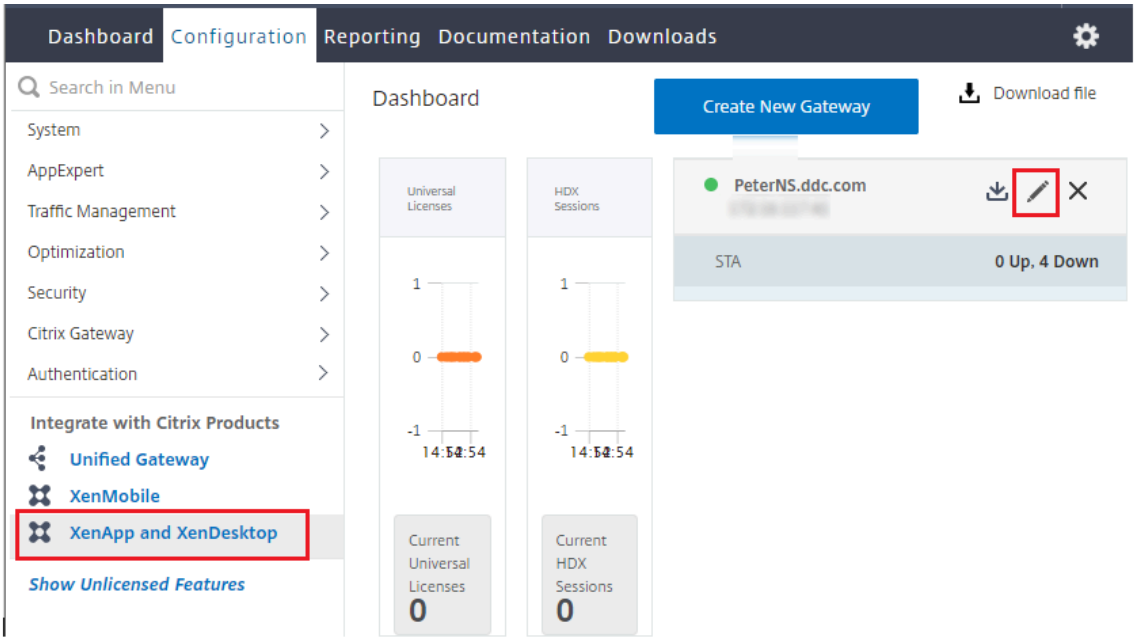
f) Repeat these steps for the other virtual server as well.

Configuration changes if the Citrix ADC appliance is already configured with Citrix Virtual Desktops

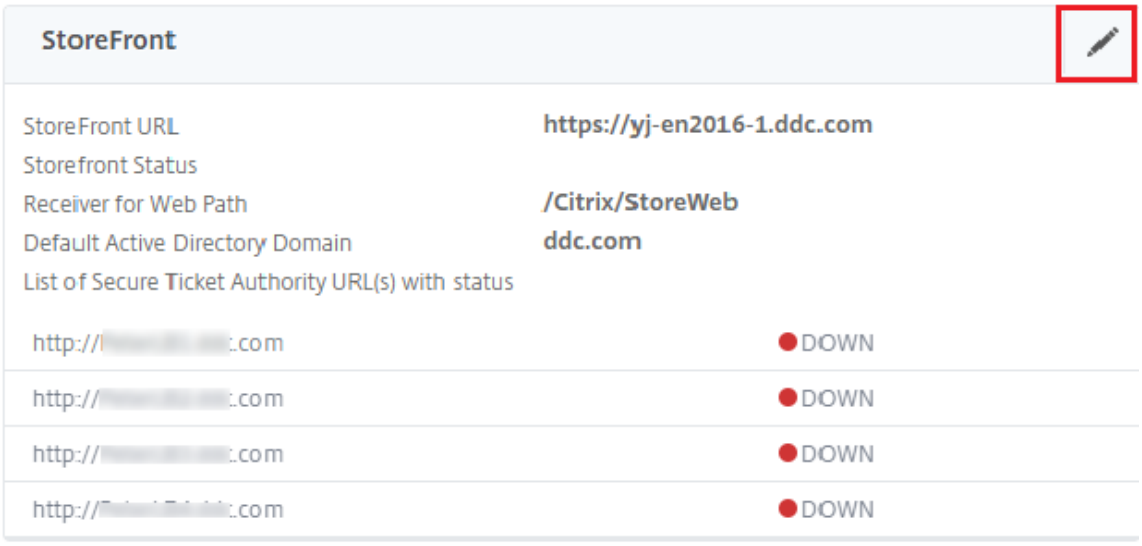
If you have already configured the Citrix ADC appliance with Citrix Virtual Desktops, then to use the Secure XML feature, you must make the following configuration changes.

- 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 Virtual Desktops, 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.

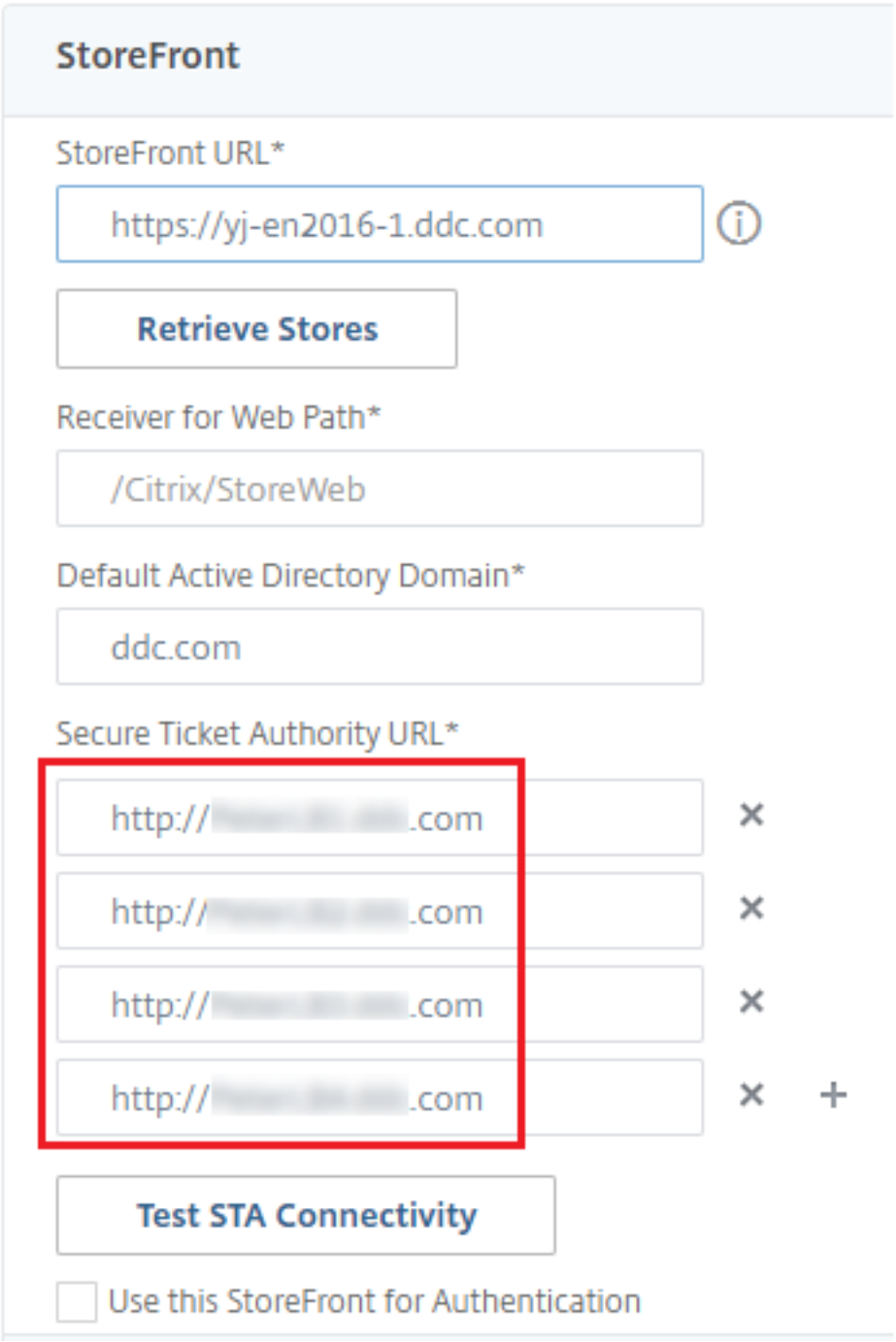


3. In the StoreFront pane, click the edit icon.



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.



Virtual IP and virtual loopback

February 9, 2021

> **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 Reg-

istry 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>

Delivery Controllers

December 1, 2020

The Delivery Controller is the server-side component that is responsible for managing user access, plus brokering and optimizing connections. Controllers also provide the Machine Creation Services that create desktop and server images.

A Site must have at least one Controller. After you install the initial Controller, you can add more Controllers when you create a Site, or later. There are two primary benefits from having more than one Controller in a Site.

- **Redundancy:** As best practice, a production Site always has at least two Controllers on different physical servers. If one Controller fails, the others can manage connections and administer the Site.
- **Scalability:** As Site activity grows, so does CPU utilization on the Controller and database activity. More Controllers provide the ability to handle more users and more applications and desktop requests, and can improve overall responsiveness.

Each Controller communicates directly with the Site database. In a Site with more than one zone, the Controllers in every zone communicate with the Site database in the primary zone.

> **Important:**
>
> Do not change the computer name or the domain membership of a Controller after the site is configured.

How VDAs register with Controllers

Before a VDA can be used, it must register (establish communication) with a Delivery Controller in the Site. For information about VDA registration, see VDA registration with Controllers.

Add, remove, or move Controllers

To add, remove, or move a Controller, you must have the server role and database role permissions listed in the Databases article.

Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

If your deployment uses database mirroring:

- Before adding, removing, or moving a Controller, ensure that the principal and mirrored databases are both running. In addition, if you are using scripts with SQL Server Management Studio, enable SQLCMD mode before running the scripts.
- To verify mirroring after adding, removing, or moving a Controller, run the PowerShell `Get-configdbconnection` cmdlet to ensure that the Failover Partner has been set in the connection string to the mirror.

After you add, remove, or move a Controller:

- If auto-update is enabled, the VDAs receive an updated list of Controllers within 90 minutes.
- If auto-update is not enabled, ensure that the Controller policy setting or ListOfDDCs registry key are updated for all VDAs. After moving a Controller to another Site, update the policy setting or registry key on both Sites.

Add a Controller

You can add Controllers when you create a Site and later. You cannot add Controllers installed with an earlier version of this software to a Site that was created with this version.

1. Run the installer on a server containing a supported operating system. Install the Delivery Controller component and any other core components you want. Complete the installation wizard.
2. If you have not yet created a Site, launch Studio. You are prompted to create a Site. On the Databases page in the Site creation wizard, click the Select button and then add the address of the server where you installed the additional Controller.

   If you plan to generate scripts that initialize the databases, add the Controllers before you generate the scripts.
3. If you have already created a Site, point Studio to the server where you installed the additional Controller. Click **Scale your deployment** and enter the Site address.

Remove a Controller

Removing a Controller from a Site does not uninstall the Citrix software or any other component. The action removes the Controller from the database so that it can no longer be used to broker connec-

tions and perform other tasks. If you remove a Controller, you can later add it back to the same Site or to another Site. A Site requires at least one Controller, so you cannot remove the last one listed in Studio.

When you remove a Controller from a Site, the Controller logon to the database server is not removed. This avoids potentially removing a logon that is used by other products' services on the same machine. The logon must be removed manually if it is no longer required. The `securityadmin` server role permission is needed to remove the logon.

> **Important:**
>
> Do not remove the Controller from Active Directory until after you remove it from the Site.

1. Make sure the Controller is powered on so that Studio loads in less than one hour. Once Studio loads the Controller you want to remove, power off the Controller when prompted to do so.
2. Select **Configuration > Controllers** in the Studio navigation pane and then select the Controller you want to remove.
3. Select **Remove Controller** in the Actions pane. If you do not have the correct database roles and permissions, you can generate a script that allows your database administrator to remove the Controller for you.
4. You might need to remove the Controller's machine account from the database server. Before doing this, check that another service is not using the account.

After using Studio to remove a Controller, traffic to that Controller might linger for a short amount of time to ensure proper completion of current tasks. If you want to force the removal of a Controller in a short time, Citrix recommends you shut down the server where it was installed, or remove that server from Active Directory. Then, restart the other Controllers on the Site to ensure no further communication with the removed Controller.

Move a Controller to another zone

If your Site contains more than one zone, you can move a Controller to a different zone. See the *Zones* article for information about how this can affect VDA registration and other operations.

1. Select **Configuration > Controllers** in the Studio navigation pane and then select the Controller you want to move.
2. Select **Move** in the Actions pane.
3. Specify the zone where you want to move the Controller.

Move a Controller to another Site

You cannot move a Controller to a Site that was created with an earlier version of this software.

1. On the Site where the Controller is located (the old Site), select **Configuration > Controllers** in the Studio navigation pane and then select the Controller you want to move.
2. Select **Remove Controller** in the Actions pane. If you do not have the correct database roles and permissions, you can generate a script that allows someone with those permissions (such as a database administrator) to remove the Controller for you. A Site requires at least one Controller, so you cannot remove the last one listed in Studio.
3. On the Controller you are moving, open Studio, reset the services when prompted, select **Join existing site**, and enter the address of the new Site.

Move a VDA to another Site

If a VDA was provisioned using Citrix Provisioning or is an existing image, you can move a VDA to another Site (from Site 1 to Site 2) when upgrading. You can also move a VDA image that was created in a test Site to a production Site. VDAs provisioned using Machine Creation Services (MCS) cannot be moved from one Site to another because MCS does not support changing the ListOfDDCs a VDA checks to register with a Controller. VDAs provisioned using MCS always check the ListOfDDCs associated with the Site in which they were created.

There are two ways to move a VDA to another Site: using the installer or Citrix policies.

Installer Run the installer and add a Controller, specifying the FQDN (DNS entry) of a Controller in Site 2.

Specify Controllers in the installer only when the Controllers policy setting is not used.

Group Policy Editor The following example moves multiple VDAs between Sites.

1. Create a policy in Site 1 that contains the following settings, then filter the policy to the Delivery Group level to initiate a staged VDA migration between the Sites.
    - Controllers: Containing FQDNs (DNS entries) of one or more Controllers in Site 2.
    - Enable auto update of Controllers: set to disabled.
2. Each VDA in the Delivery Group is alerted within 90 minutes of the new policy. The VDA ignores the list of Controllers it receives (because auto-update is disabled). The VDA selects one of the Controllers specified in the policy, which lists the Controllers in Site 2.
3. When the VDA successfully registers with a Controller in Site 2, it receives the Site 2 ListOfDDCs and policy information, which has auto-update enabled by default. Since the Controller with which the VDA was registered in Site 1 is not on the list sent by the Controller in Site 2, the VDA re-registers, choosing among the Controllers in the Site 2 list. From then on, the VDA is automatically updated with information from Site 2.

VDA registration

February 5, 2024

Introduction

Before a VDA can be used, it must register (establish communication) with one or more Controllers or Cloud Connectors on the Site. (In an on-premises Citrix Virtual Apps and Desktops deployment, VDAs register with Controllers. In a Citrix Virtual Apps and Desktops service deployment, VDAs register with Cloud Connectors.) The VDA finds a Controller or Connector by checking a list called the `ListofDDCs`. The `ListOfDDCs` on a VDA contains DNS entries that point that VDA to Controllers or Cloud Connectors on the site. For load balancing, the VDA automatically distributes connections across all Controllers or Cloud Connectors in the list.

Why is VDA registration so important?

- From a security perspective, registration is a sensitive operation. You're establishing a connection between the Controller or Cloud Connector and the VDA. For such a sensitive operation, the expected behavior is to reject the connection if everything is not in perfect shape. You are effectively establishing two separate communication channels: VDA to Controller or Cloud Connector, and Controller or Cloud Connector to VDA. The connection uses Kerberos, so time synchronization and domain membership issues are unforgiving. Kerberos uses Service Principal Names (SPNs), so you cannot use load balanced IP\hostname.
- If a VDA does not have accurate and current Controller (or Cloud Connector) information as you add and remove Controllers, the VDA might reject session launches that were brokered by an unlisted Controller. Invalid entries can delay the startup of the virtual desktop system software. A VDA won't accept a connection from an unknown and untrusted Controller or Cloud Connector.

In addition to the `ListOfDDCs`, the `ListOfSIDs` (Security IDs) indicates which machines in the `ListOfDDCs` are trusted. The `ListOfSIDs` can be used to decrease the load on Active Directory or to avoid possible security threats from a compromised DNS server. For more information, see ListOfSIDs.

If a `ListOfDDCs` specifies more than one Controller or Cloud Connector, the VDA attempts to connect to them in random order. In an on-premises deployment, the `ListOfDDCs` can also contain Controller groups. The VDA attempts to connect to each Controller in a group before moving to other entries in the `ListOfDDCs`.

Citrix Virtual Apps and Desktops automatically tests the connectivity to configured Controllers or Cloud Connectors during VDA installation. Errors are displayed if a Controller or Cloud Connector cannot be reached. If you ignore a warning that a Controller cannot be contacted (or when you do not

specify Controller or Cloud Connector addresses during VDA installation), several messages remind you.

Methods for configuring Controller or Cloud Connector addresses

The administrator chooses the configuration method to use when the VDA registers for the first time. (This is called the initial registration.) During the initial registration, a persistent cache is created on the VDA. During subsequent registrations, the VDA retrieves the list of Controllers or Cloud Connectors from this local cache, unless a configuration change is detected.

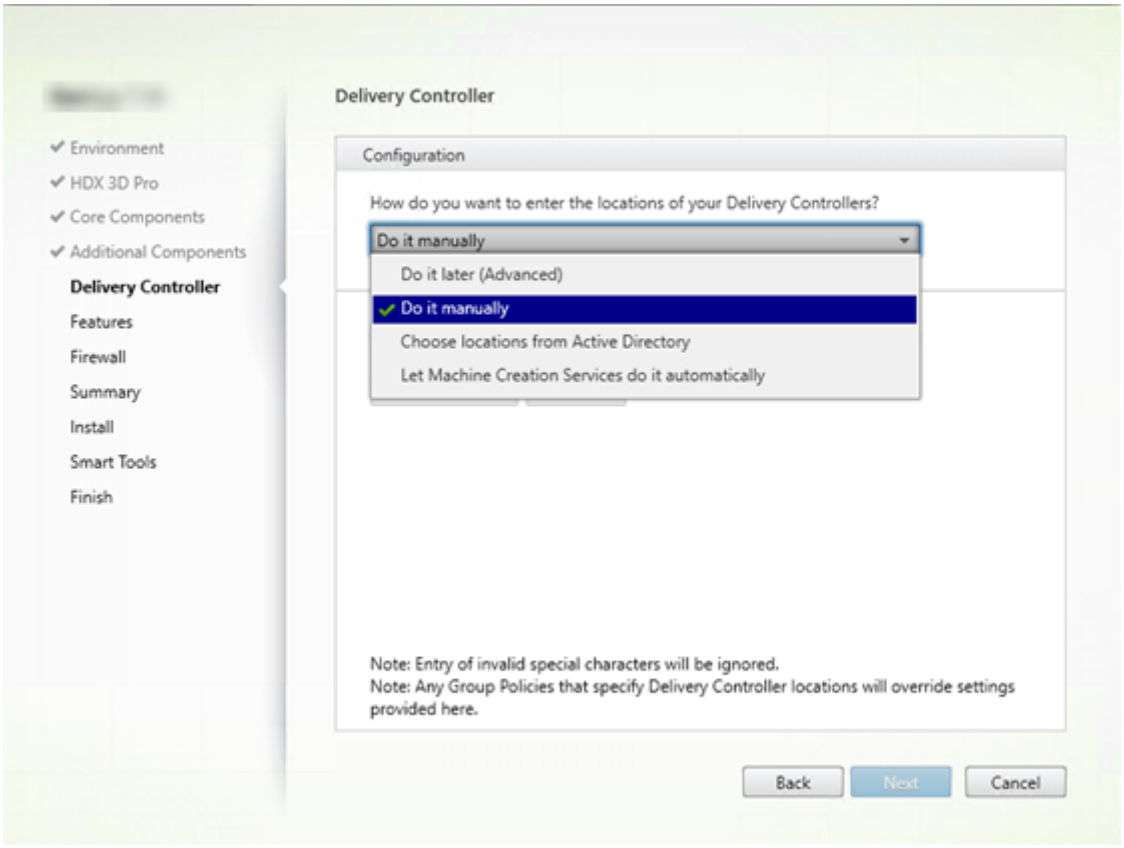
The easiest way to retrieve that list during subsequent registrations is by using the auto-update feature. Auto-update is enabled by default. For more information, see Auto-update.

There are several methods for configuring Controller or Cloud Connector addresses on a VDA.

- Policy-based (LGPO or GPO)
- Registry-based (manual, GPP, specified during VDA installation)
- Active Directory OU-based (legacy OU discovery)
- MCS-based (personality.ini)

You specify the initial registration method when you install a VDA. (If you disable auto-update, the method you select during VDA installation will also be used for subsequent registrations.)

The following graphic shows the **Delivery Controller** page of the VDA installation wizard.



Policy-based (LGPO\GPO)

Citrix recommends using GPO for initial VDA registration. It has the highest priority. (Auto-update is listed earlier as the highest priority, but auto-update is used only after the initial registration.) Policy-based registration offers the centralizing advantages of using Group Policy for configuration.

To specify this method, complete both of the following steps:

- On the **Delivery Controller** page in the VDA installation wizard, select **Do it later (advanced)**. The wizard reminds you several times to specify Controller addresses, even though you're not specifying them during VDA installation. (Because VDA registration is that important!)
- Enable or disable policy-based VDA registration through Citrix policy with the `Virtual Delivery Agent Settings > Controllers` setting. (If security is your top priority, use the `Virtual Delivery Agent Settings > Controller SIDs` setting.)

This setting is stored under `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

Registry-based

To specify this method, complete one of the following steps:

- On the **Delivery Controller** page in the VDA installation wizard, select **Do it manually**. Then, enter the FQDN of an installed Controller and then click **Add**. If you've installed other Controllers, add their addresses.
- For a command-line VDA installation, use the `/controllers` option and specify the FQDNs of the installed Controllers or Cloud Connectors.

This information is usually stored in registry value `ListOfDDCs` under registry key `HKLM\Software\Citrix\VirtualDesktopAgent` or `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

You can also configure this registry key manually or use Group Policy Preferences (GPP). This method might be preferable to the policy-based method (for example, if you want conditional processing of different Controllers or Cloud Connectors, such as: use XDC-001 for computer names that begin with XDW-001-).

Update the `ListOfDDCs` registry key, which lists the FQDNs of all the Controllers or Cloud Connectors in the Site. (This key is the equivalent of the Active Directory Site OU.)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs` (`REG_SZ`)

If the `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` registry location contains both the `ListOfDDCs` and `FarmGUID` keys, `ListOfDDCs` is used for Controller or Cloud Connector discovery. `FarmGUID` is present if a site OU was specified during VDA installation. (This might be used in legacy deployments.)

Optionally, update the `ListOfSIDs` registry key (for more information, see ListOfSIDs:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` (`REG_SZ`)

Remember: If you also enable policy-based VDA registration through Citrix policy, that configuration overrides settings you specify during VDA installation, because it is a higher-priority method.

Active Directory OU-based (legacy)

This method is supported primarily for backward compatibility and is not recommended. If you're still using it, Citrix suggests changing to another method.

To specify this method, complete both of the following steps:

- On the **Delivery Controller** page in the VDA installation wizard, select **Choose locations from Active Directory.**

- Use the `Set-ADControllerDiscovery.ps1` script (available on every Controller). Also, configure the `FarmGuid‘` registry entry on each VDA to point to the right OU. This setting can be configured using Group Policy.

For details, see Active Directory OU-based discovery.

MCS-based

If you use MCS to provision VMs, MCS sets up the list of Controllers or Cloud Connectors. This feature works with auto-update. When creating the catalog, MCS injects the list of Controllers or Cloud Connectors into the `Personality.ini` file during initial provisioning. Auto-update keeps the list current.

To specify this method, on the **Delivery Controller** page in the VDA installation wizard, select **Let Machine Creation Services do it**.

Recommendations

As best practice:

- Use the Group Policy registration method for initial registration.
- Use auto-update (enabled by default) to keep your list of Controllers up-to-date.
- In a multi-zone deployment, use Group Policy for initial configuration (with at least two Controllers or Cloud Connectors). Point VDAs to Controllers or Cloud Connectors local to (in) their zone. Use auto-update to keep them up-to-date. Auto-update automatically optimizes the ListOfDDCs for VDAs in satellite zones.
- List more than one controller on ListOfDDCs registry key separated by a space to prevent registration issues if a controller is not available.

  Example:

  `DDC7x.xd.local DDC7xHA.xd.local`

  32-bit: `HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs`

  `HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`
- Ensure all values listed under `ListOfDDCs` map to a valid fully qualified domain name to prevent startup registration delays.

Auto-update

Auto-update (introduced in XenApp and XenDesktop 7.6) is enabled by default. It is the most efficient method for keeping your VDA registrations up-to-date. Although auto-update is not used for initial registration, the auto-update software downloads and stores the `ListOfDDCs` in a persistent cache on the VDA when initial registration occurs. This is done for each VDA. (The cache also holds machine policy information, which ensures that policy settings are retained across restarts.)

Auto-update is supported when using MCS or Citrix Provisioning to provision machines, except for Citrix Provisioning server-side cache (which is not a common scenario because there is no persistent storage for auto-update cache).

To specify this method:

- Enable or disable auto-update through a Citrix policy containing the setting: `Virtual Delivery Agent Settings` > `Enable auto update of Controllers`. This setting is enabled by default.

How it works:

- Each time a VDA re-registers (for example, after a machine restart), the cache is updated. Each Controller (or Cloud Connector) also checks the site database every 90 minutes. If a Controller was added or removed since the last check, or if a policy change occurred that affects VDA registration, the Controller sends an updated list to its registered VDAs and the cache is updated. The VDA accepts connections from all the Controllers in its most recently cached list.
- If a VDA receives a list that does not include the Controller (or Cloud Connector) it is registered with (in other words, that Controller was removed from the site), the VDA re-registers, choosing among the Controllers in the ListOfDDCs.

Example:

- A deployment has three Controllers: A, B, and C. A VDA registers with Controller B (which was specified during VDA installation).
- Later, two Controllers (D and E) are added to the Site. Within 90 minutes, VDAs receive updated lists and then accept connections from Controllers A, B, C, D, and E. (The load is not spread equally to all Controllers until the VDAs are restarted.)
- Later still, Controller B is moved to another Site. Within 90 minutes, VDAs in the original Site receive updated lists because there has been a Controller change since the last check. The VDA that originally registered with Controller B (which is no longer on the list) re-registers, choosing among Controllers in the current list (A, C, D, and E).

In a multi-zone deployment, auto-update in a satellite zone automatically caches all local Controllers first. All Controllers in the primary zone are cached in a backup group. If no local Controllers in the satellite zone are available, registration is attempted with Controllers in the primary zone.

As shown in the following example, the cache file contains host names and a list of Security IDs (ListOfSIDs). The VDA does not query SIDs, which reduces the Active Directory load.

You can retrieve the cache file with a WMI call. However, it is stored in a location that's readable only by the SYSTEM account.

> **Important:**
>
> This information is provided only for information purposes. DO NOT MODIFY THIS FILE. Any modifications to this file or folder results in an unsupported configuration.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

If you need to manually configure the `ListOfSIDs` for security reasons (as distinct from reducing Active Directory load), you cannot use the auto-update feature. For details, see ListOfSIDs.

Exception to auto-update priority

Although auto-update usually has the highest priority of all VDA registration methods and overrides settings for other methods, there is an exception. The `NonAutoListOfDDCs` elements in the cache specify the initial VDA configuration method. Auto-update monitors this information. If the initial registration method changes, the registration process skips auto-update, and uses the next-highest configured priority method. This can be helpful when you move a VDA to another site (for example, during disaster recovery).

Configuration considerations

Consider the following when configuring items that can affect VDA registration.

Controller or Cloud Connector addresses

Regardless of which method you use to specify Controllers or Cloud Connectors, Citrix recommends using an FQDN address. An IP address is not considered a trusted configuration, because it's easier to compromise an IP than a DNS record. If you populate the `ListOfSIDs` manually, you can use an IP in a `ListOfDDCs`. However, FQDN is still recommended.

Load balancing

As noted earlier, the VDA automatically distributes connections across all Controllers or Cloud Connectors in the `ListOfDDCs`. Failover and load balancing functionality is built into the Citrix Brokering Protocol (CBP). If you specify multiple Controllers or Cloud Connectors in your configuration, registration automatically fails over between them, if needed. With auto-update, automatic failover occurs automatically for all VDAs.

For security reasons, you cannot use a network load balancer, such as Citrix ADC. VDA registration uses Kerberos mutual authentication, where the client (VDA) must prove its identity to the service (Controller). However, the Controller or Cloud Connector must prove its identity to the VDA. This means that the VDA and the Controller or Cloud Connector are acting as server and client at the same time. As noted at the beginning of this article, there are two communications channels: VDA to Controller or Cloud Connector, and Controller or Cloud Connector to VDA.

A component in this process is called Service Principal Name (SPN), which stored as a property in an Active Directory computer object. When your VDA connects to a Controller or Cloud Connector, it must specify "who"it wants to communicate with. This address is an SPN. If you use a load-balanced IP, mutual Kerberos authentication correctly recognizes that the IP does not belong to the expected Controller or Cloud Connector.

For more information, see:

- Introduction to Kerberos
- Mutual authentication using Kerberos

Auto-update replaces CNAME

The auto-update feature replaces the CNAME (DNS alias) function from XenApp and XenDesktop versions earlier than 7.x. CNAME functionality is disabled, beginning with XenApp and XenDesktop 7. Use auto-update instead of CNAME. (If you must use CNAME, see CTX137960. For DNS aliasing to work consistently, do not use both auto-update and CNAME at the same time.)

Controller/Cloud Connector groups

Sometimes, you might want to process Controllers or Cloud Connectors in groups, with one group being preferred and the other group used for a failover if all Controllers/Cloud Connectors fail. Remember that Controllers or Cloud Connectors are randomly selected from the list, so grouping can help enforce preferential use.

These groups are intended for use within a single Site (not multiple Sites).

Use parentheses to specify groups of Controllers/Cloud Connectors. For example, with four Controllers (two primary and two backup), a grouping might be:

```
(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)
```

In this example, the Controllers in the first group (001 and 002) are processed first. If they both fail, Controllers in the second group (003 and 004) are processed.

For XenDesktop 7.0 or higher, there is one more step you need to perform to use **Registration Groups** feature. You need to Prohibit **Enable Auto Update of Controller** policy from Citrix Studio.

ListOfSIDs

The list of Controllers that a VDA can contact for registration is the `ListOfDDCs`. A VDA must also know which Controllers to trust. VDAs do not automatically trust the Controllers in the `ListOfDDCs`. The `ListOfSIDs` (Security IDs) identifies the trusted Controllers. VDAs attempt to register only with trusted Controllers.

In most environments, the `ListOfSIDs` is generated automatically from the `ListOfDDCs`. You can use a CDF trace to read the `ListOfSIDs`.

Generally, there is no need to manually modify the `ListOfSIDs`. There are several exceptions. The first two exceptions are no longer valid because newer technologies are available.

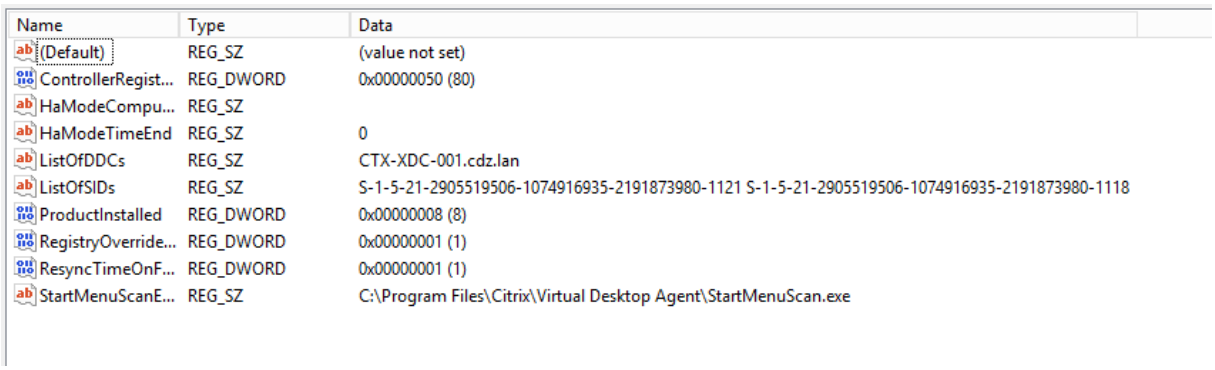
- **Separate roles for Controllers:** Before zones were introduced in XenApp and XenDesktop 7.7, the `ListOfSIDs` was manually configured when only a subset of Controllers was used for registration. For example, if you were using XDC-001 and XDC-002 as XML brokers, and XDC-003 and XDC-004 for VDA registration, you specified all Controllers in the ListOfSIDs, and XDC-003 and XDC-004 in the ListOfDDCs. This is not a typical or recommended configuration in newer environments. Instead, use zones.
- **Reducing Active Directory load:** Before the auto-update feature was introduced in XenApp and XenDesktop 7.6, the `ListOfSIDs` was used to reduce the load on domain controllers. By pre-populating the `ListOfSIDs`, the resolution from DNS names to SIDs can be skipped. However, the auto-update feature removes the need for this work, because this persistent cache contains SIDs. Citrix recommends keeping the auto-update feature enabled.

- **Security:** In some highly secured environments, the SIDs of trusted Controllers were manually configured to avoid possible security threats from a compromised DNS server. However, if you do this, you must also disable the auto-update feature. Otherwise, the configuration from persistent cache is used.

So, unless you have a specific reason, do not modify the `ListOfSIDs`.

If you must modify the `ListOfSIDs`, create a registry key named `ListOfSIDs (REG_SZ)` under `HKLM\Software\Citrix\VirtualDesktopAgent`. The value is a list of trusted SIDs, separated by spaces if you have more than one.

In the following example, one Controller is used for VDA registration (`ListOfDDCs`), but two Controllers are used for brokering (`List OfSIDs`).



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

Controller search during VDA registration

When a VDA tries to register, the Broker Agent first performs a DNS lookup in the local domain to ensure that the specified Controller can be reached.

If that initial lookup doesn't find the Controller, the Broker Agent can start a fallback top-down query in AD. That query searches all domains, and repeats frequently. If the Controller address is invalid (for example, the administrator entered an incorrect FQDN when installing the VDA), that query's activity can potentially lead to a distributed denial of service (DDoS) condition on the domain controller.

The following registry key controls whether the Broker Agent uses the fallback top-down query when it cannot locate a Controller during the initial search.

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- Name: `DisableDdcWildcardNameLookup`
- Type: `DWORD`
- Value: `1` (default) or `0`

When set to `1`, the fallback search is disabled. If the initial search for the Controller fails, the Broker Agent stops looking. This is the default setting.

When set to `0`, the fallback search is enabled. If the initial search for the Controller fails, the fallback top-down search is started.

Troubleshoot VDA registration issues

As noted previously, a VDA must be registered with a Delivery Controller to be considered when launching brokered sessions. Unregistered VDAs can result in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which an administrator can troubleshoot. Studio provides troubleshooting information in the catalog creation wizard, and after you create a Delivery Group.

- **Identifying issues during machine catalog creation:** 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 was not obtained about a machine (perhaps because it had never registered with a Delivery Controller), you might choose to add the machine anyway.

  A catalog's functional level controls which product features are available to machines in the catalog. Using features introduced in new product versions may require a new VDA. Setting a functional level makes all features introduced in that version (and later, if the functional level does not change) available to machines in the catalog. However, machines in that catalog with an earlier VDA version will not be able to register.

- **Identifying issues after creating Delivery Groups:** After you create a Delivery Group, Studio displays details about machines associated with that group. The details pane for a Delivery Group indicates the number of machines that are expected to be registered but are not. In other words, there might be one or more machines that are powered on and not in maintenance mode, but are not currently registered with a Controller. When viewing a "not registered, but expected to be" machine, review the Troubleshoot tab in the details pane for possible causes and recommended corrective actions.

More information about troubleshooting VDA registration

- For more information about functional levels, see VDA versions and functional levels.
- For more information about VDA registration troubleshooting, see CTX136668.
- You can also use the Citrix Health Assistant to troubleshoot VDA registration and session launch. For details, see CTX207624.

Sessions

March 7, 2023

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 health-care 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.

You can also log a user off of a session, disconnect a session, and configure session prelaunch and linger; see Manage Delivery Groups.

Session reliability

Session Reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application 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, 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 period of time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period of time is five minutes. To change this period of time, 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 Reconnect 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 new 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 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 health-care 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, as well as 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 need to keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applica-

tions 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 only for Citrix Workspace app users who access desktops and applications through a Citrix StoreFront connection. 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 currently logged on to the session. For example, if a health care 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

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 available on both devices. The applications follow, regardless of the device or whether current sessions exist. In many cases, 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 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 will be 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 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 0-3600.

If you change a master image, update the catalog.

This setting applies only to VMs with desktop (workstation) VDAs. Microsoft controls the logon timeout on machines with server VDAs.

Use Search in Studio

February 6, 2020

Use the Search feature to view information about specific machines, sessions, machine catalogs, applications, or Delivery Groups.

1. Select **Search** in the Studio navigation pane.

   You cannot search within the machine catalogs or Delivery Groups tabs using the Search box. Use the Search node in the navigation pane.

   To display additional search criteria in the display, click the plus sign next to the Search drop-down fields. Remove search criteria by clicking the minus button.

2. Enter the name or use the drop-down list to select another search option for the item you want to find.
3. Optionally, save your search by selecting **Save as**. The search appears in the **Saved searches** list.

Alternatively, click the **Expand Search** icon (dual downward angle brackets) to display a menu of search properties. You can perform an advanced search by building an expression from the properties in the menu.

Tips to enhance a search:

- To display additional characteristics to include in the display on which you can search and sort, right click any column and select **Select columns**.
- 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 of the machines in a Delivery Group, select **Delivery Groups** in the navigation pane, then select the group, and then select **View Machines** in the Actions pane.

Tags

November 30, 2020

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 to only items that have a specified tag.

- Tailor search displays in Studio.

  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 Studio 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 or can be helpful when isolating and troubleshooting a subset of machines in a Delivery Group.

- 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 do not 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, 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 (PowerShell only; see Tags on machine catalogs)
- Delivery Groups
- Application Groups

You can configure a tag restriction can be configured when creating or editing the following in Studio:

- 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:

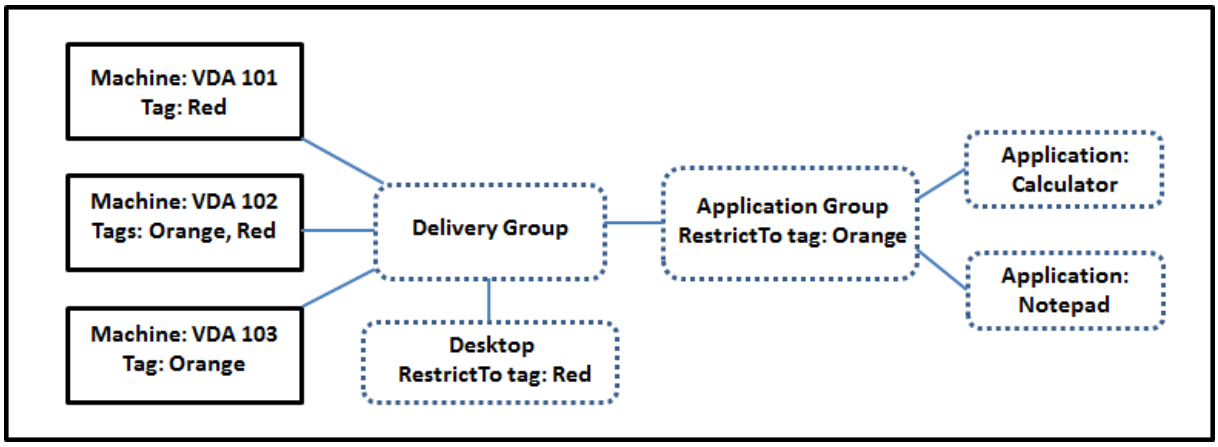
- Create the tag and then add (apply) it to machines.
- Create or edit a group with the tag restriction (in other words, "restrict launches to machines with tag x").

A tag restriction extends the broker's machine selection process. The broker 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 broker 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. The site has one shared Delivery Group, one published desktop, and one Application Group configured with two applications.



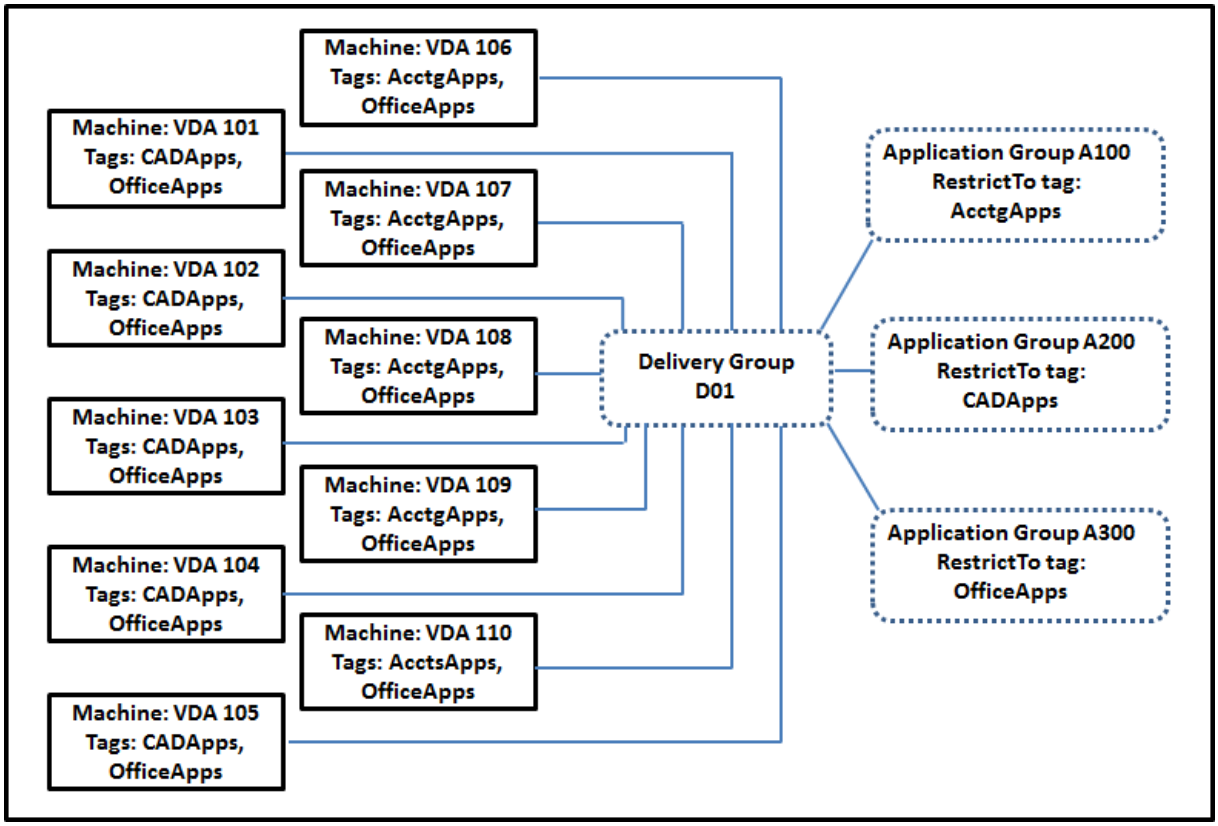
- Tags have been added to each of the three machines (VDA 101-103).
- The desktop in the shared Delivery Group was created with a tag restriction named `Red`, so that desktop can be launched only on machines in that Delivery Group that have the tag `Red`: VDA 101 and 102.
- The Application Group was 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 Studio.

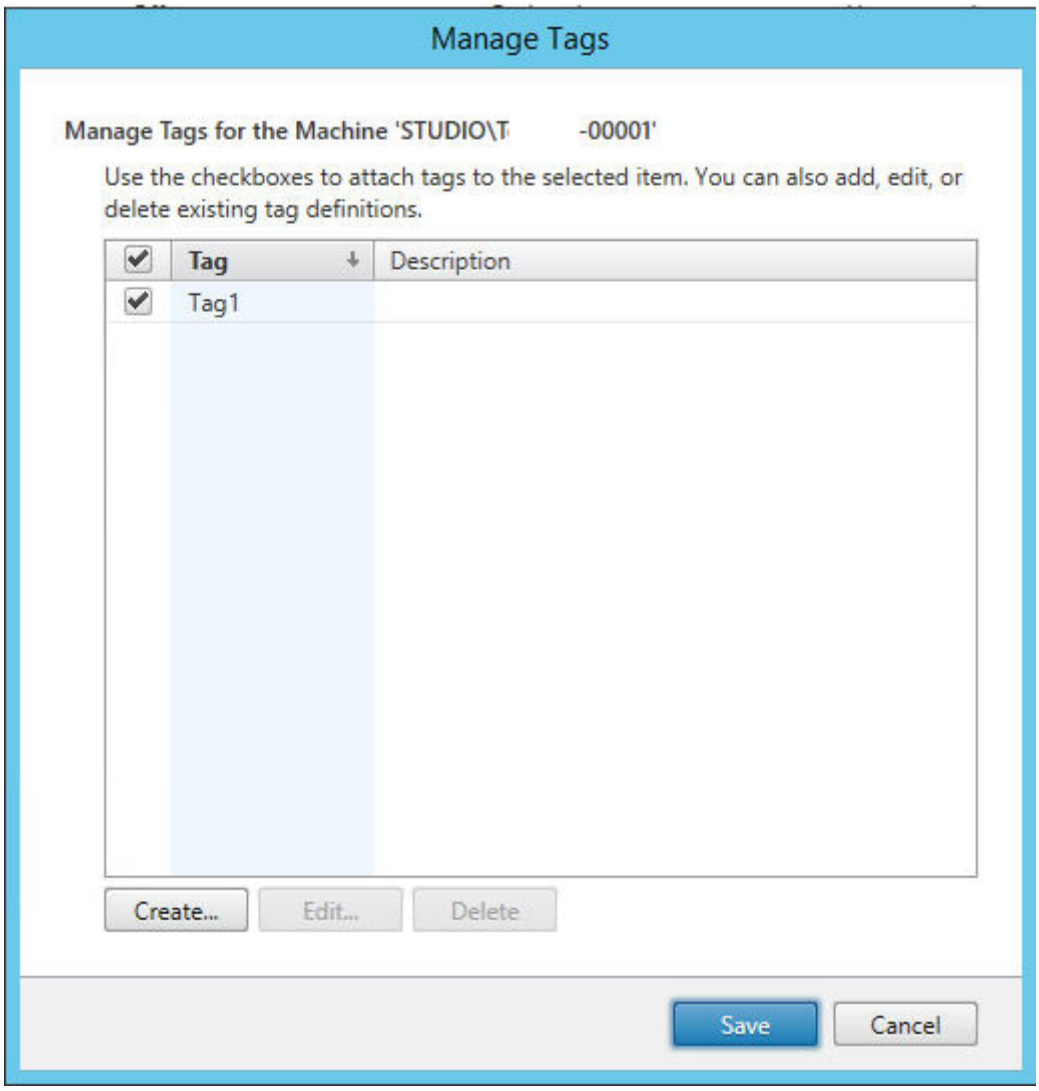
(Exception: Tags used for policy assignments are created, edited, and deleted through the **Manage Tags** action in Studio. However, tags are applied (assigned) when you create the policy. See Create policies for details.)

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 dialogs in Studio

In Studio, select the items you want to apply a tag to (machines, applications, a desktop, a Delivery Group, or an Application Group) and then select **Manage Tags** in the Actions pane. The **Manage Tags** dialog box lists all the tags that have been created in the Site, not just for the items you selected.

- A check box containing a check mark indicates that tag has already been added to the selected items. (In the screen capture below, the selected machine has the tag named `Tag1` applied.)
- If you selected 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:**

  Click **Create.** Enter a name and description. Tag names must be unique and are not case-sensitive. Then click **OK**. (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. If you selected multiple items and the check box next to a tag contains a hyphen (indicating that some, but not all selected items already have the tag applied), changing it to a check mark affects all of the selected machines.

  If you try to add a tag to machines, and that tag is used as a restriction in an Application Group, Studio warns that might result in making 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 hyphen in the check box indicates that some, but not all selected items have the tag applied. If you selected multiple items and the check box next to a tag contains a hyphen, clearing the check box removes the tag from all selected machines.

  If you attempt to remove a tag from a machine that is using that tag as a restriction, Studio warns that action might affect which machines are considered for launch. If that's what you intend, proceed.

- **To edit a tag:**

  Select a tag and then click **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 click **Delete**. The **Delete Tag** dialog box indicates how many items currently use the selected tags (for example "2 machines"). Click an item to display more information. For example, clicking a "2 machines"item displays the names of the two machines that have that tag applied. Confirm whether you want to delete the tags.

  You cannot use Studio to 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, click **Save**.

To see if a machine has any tags applied: Select **Delivery Groups** in the navigation pane. Select a Delivery Group in the middle pane and then select **View Machines** in the Actions pane. Select a machine in the middle pane and then select the Tags tab on the Details pane.

Manage tag restrictions

Configuring a tag restriction is a multi-step process: First create the tag and add/apply it to machines. Then, 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 to be affected by the tag restriction, using the **Manage Tags** actions described earlier.

- **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 by clearing **Restrict launches to machines with the tag**.

- **To add a tag restriction to a desktop:**

  Create or edit a Delivery Group. Click **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, click **Edit**. In the dialog box, either select a different tag from the list or remove the tag restriction 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, so keep in mind that adding, removing, and deleting a tag can have unintended effects. You can use a tag to sort machine displays in the Studio search field. You can use the same tag as a restriction in an Application Group or a desktop. That limits launch consideration to only machines in specified Delivery Groups that have that tag.

If you attempt to add a tag to machines when that tag is used as a tag restriction for a desktop or an Application Group, Studio displays a warning. Adding that tag might make the machines available for launching additional applications or desktops. If that is 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 attempt to add the Red tag to those machines, Studio displays 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, if a tag is being used in an Application Group to restrict launches, Studio warns that you cannot delete the tag until you edit the group and remove it as a restriction. (If you were allowed to delete a tag used as a restriction in an Application Group, that 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 are 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 are 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 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. In Studio, select Delivery Group `D01` and then select **View Machines** in the Action pane.
2. Select machines VDA 101-105 and then select **Manage Tags** in the Actions pane.

3. In the **Manage Tags** dialog box, click **Create**. Create a tag named `CADApps`. Click **OK**.
4. Click **Create** again and create a tag named `OfficeApps`. Click **OK**.
5. While still in the **Manage Tags** dialog box, add (apply) the newly created tags to the selected machines by enabling the check boxes next to each tag's name (`CADApps` and `OfficeApps`). Close the dialog box.
6. Select Delivery Group `D01`, select **View Machines** in the Action pane.
7. Select machines VDA 106-110 and then select **Manage Tags** in the Actions pane.
8. In the **Manage Tags** dialog box, click **Create**. Create a tag named `AcctgApps`. Click **OK**.
9. Apply the newly created `AcctgApps` tag and the `OfficeApps` tag to the selected machines by clicking the check boxes next to each tag's name. Close the dialog box.

Create the Application Groups with tag restrictions.

1. In Studio, select **Applications** in the navigation pane and then select **Create Application Group** in the Actions pane.
2. On the **Delivery Groups** page, select Delivery Group `D01`. Select **Restrict launches to machines with tag**. Then select the `AcctgApps` tag from the list.
3. 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` .
4. Repeat the preceding steps to create Application Group `A200`, specifying machines that have the `CADApps` tag, plus the appropriate users and applications.
5. Repeat steps to create Application Group `A300`, specifying machines that have the `OfficeApps` tag, plus the appropriate users and applications.

Tags on machine catalogs

You can use tags on machine catalogs. The overall sequence of creating a tag and then applying it to a catalog is the same as described previously. However, applying tags to catalogs is supported only through the PowerShell interface. You cannot use Studio to apply a tag to a catalog or remove a tag from a catalog. Catalog displays in Studio do not indicate if a tag is applied.

Summary: You can use Studio or PowerShell to create or delete a tag for use on a catalog. Use PowerShell to apply the tag to the catalog.

Here are some examples of using tags with catalogs:

- A Delivery Group has 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.

- In an Application Group, you want to limit application sessions to machines in a specific catalog. Applying a tag to that catalog accomplishes that.

Affected PowerShell cmdlets:

- 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 tag named `fy2018` to the catalog named `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (The tag was previously created using either Studio or PowerShell.)

See the PowerShell cmdlet help for guidance and syntax.

More information

Blog post: How to assign desktops to specific servers.

IPv4/IPv6 support

February 7, 2020

This release supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks.

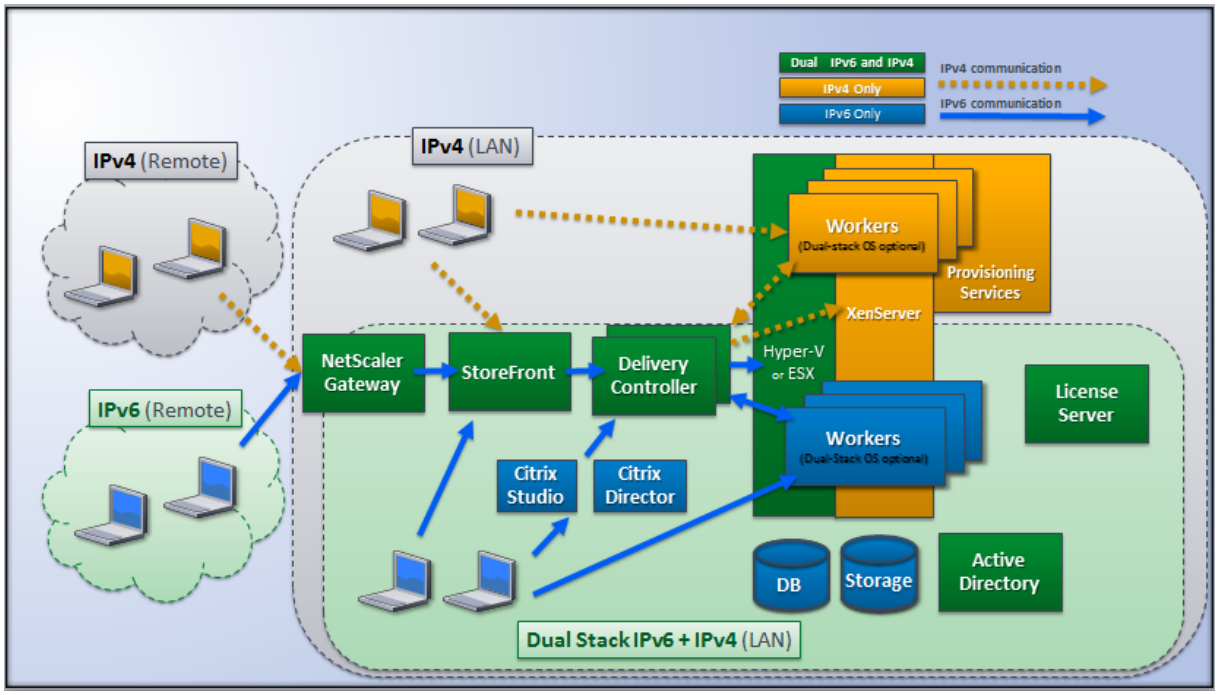
IPv6 communications are controlled with two Virtual Delivery Agent (VDA) connection-related Citrix policy settings:

- A primary setting that enforces the use of IPv6: Only use IPv6 Controller registration.
- A dependent setting that defines an IPv6 netmask: Controller registration IPv6 netmask.

When the Only use IPv6 Controller registration policy setting is enabled, VDAs register with a Delivery Controller for incoming connections using an IPv6 address.

Dual-stack IPv4/IPv6 deployment

The following figure illustrates a dual-stack IPv4/IPv6 deployment. In this scenario, a worker is a VDA installed on a hypervisor or on a physical system, and is used primarily to enable connections for applications and desktops. Components that support dual IPv6 and IPv4 are running on operating systems that use tunneling or dual protocol software.



These Citrix products, components, and features support only IPv4:

- Citrix Provisioning
- XenServer
- VDAs not controlled by the **Only use IPv6 Controller registration** policy setting
- XenApp versions earlier than 7.5, XenDesktop versions earlier than 7, and Director

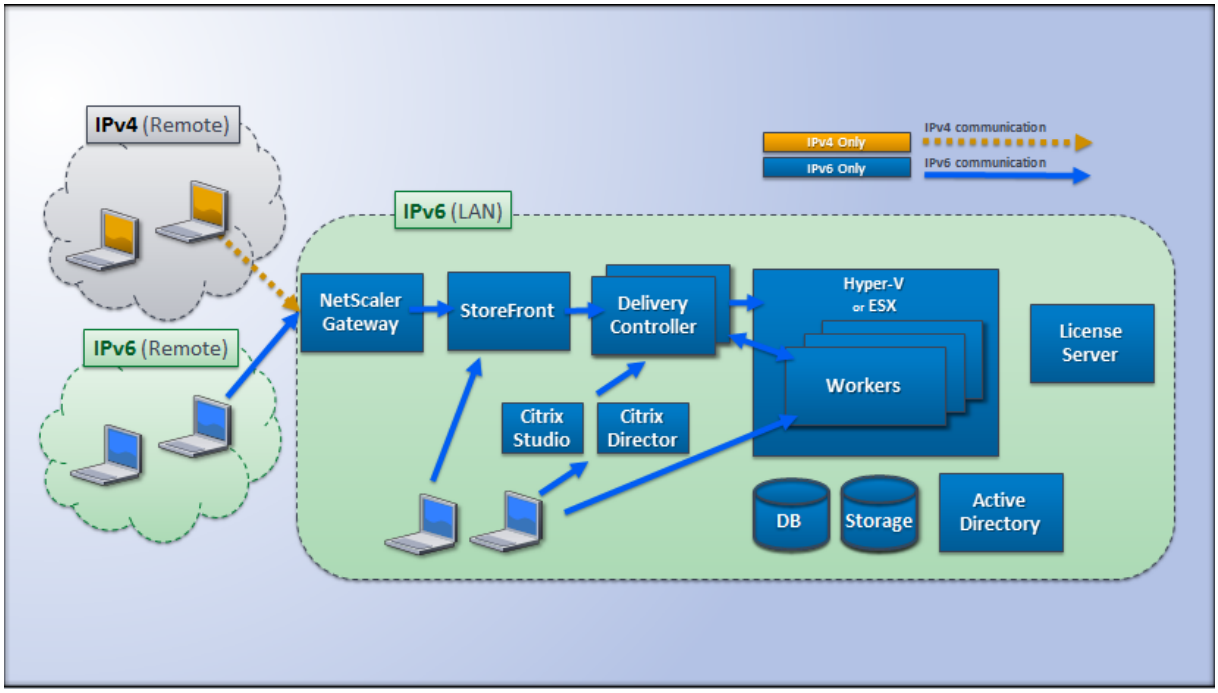
In this deployment:

- If a team frequently uses an IPv6 network and the administrator wants them to use IPv6 traffic, the administrator will publish IPv6 desktops and applications for those users based on a worker image or Organizational Unit (OU) that has the primary IPv6 policy setting turned on (that is, Only use IPv6 Controller registration is enabled).
- If a team frequently uses an IPv4 network, the administrator will publish IPv4 desktops and applications for those users based on a worker image or OU that has the primary IPv6 policy setting turned off (that is, Only use IPv6 Controller registration is disabled), which is the default.

Pure IPv6 deployment

The following figure illustrates a pure IPv6 deployment. In this scenario:

- The components are running on operating systems configured to support an IPv6 network.
- The primary Citrix policy setting (Only use IPv6 Controller registration) is enabled for all VDAs; they must register with the Controller using an IPv6 address.



Policy settings for IPv6

Two Citrix policy settings affect support for a pure IPv6 or dual stack IPv4/IPv6 implementation. Configure the following connection-related policy settings:

- **Only use IPv6 Controller registration:** Controls which form of address the Virtual Delivery Agent (VDA) uses to register with the Delivery Controller. Default = Disabled
  - When the VDA communicates with the Controller, it uses a single IPv6 address chosen in the following precedence: global IP address, Unique Local Address (ULA), link-local address (only if no other IPv6 addresses are available).
  - When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.
- **Controller registration IPv6 netmask:** A machine can have multiple IPv6 addresses; this policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the network where the VDA will register: the VDA registers only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 Controller registration policy setting is enabled. Default = Empty string

Use of IPv4 or IPv6 by a VDA is determined solely by these policy settings. In other words, to use IPv6 addressing, the VDA must be controlled by a Citrix policy with the **Only use IPv6 Controller registration** setting enabled.

Deployment considerations

If your environment contains both IPv4 and IPv6 networks, you will need separate Delivery Group configurations for the IPv4-only clients and for the clients who can access the IPv6 network. Consider using naming, manual Active Directory group assignment, or Smart Access filters to differentiate users.

Reconnection to a session may fail if the connection is initiated on an IPv6 network, and then attempts are made to connect again from an internal client that has only IPv4 access.

User profiles

April 12, 2022

By default, Citrix Profile management is installed silently on master images when you install the Virtual Delivery Agent, but you do not have to use Profile management as a profile solution.

To suit your users' varying needs, you can use Citrix Virtual Apps and Desktops policies to apply different profile behavior to the machines in each Delivery Group. For example, one Delivery Group might require Citrix mandatory profiles, whose template is stored in one network location, while another Delivery Group requires Citrix roaming profiles stored in another location with several redirected folders.

- If other administrators in your organization are responsible for Citrix Virtual Apps and Desktops policies, work with them to ensure that they set any profile-related policies across your Delivery Groups.
- Profile management policies can also be set in Group Policy, in the Profile management .ini file, and locally on individual virtual machines. These multiple ways of defining profile behavior are read in the following order:

  1. Group Policy (.adm or .admx files)
  2. Citrix Virtual Apps and Desktops policies in the Policy node
  3. Local policies on the virtual machine that the user connects to
  4. Profile management .ini file

  For example, if you configure the same policy in both Group Policy and the Policy node, the system reads the policy setting in Group Policy and ignores the Citrix Virtual Apps and Desktops policy setting.

Whichever profile solution you choose, Director administrators can access diagnostic information and troubleshoot user profiles. For more information, see the Director documentation.

If you use the Personal vDisk feature, Citrix user profiles are stored on virtual desktops' Personal vDisks by default. Do not delete the copy of a profile in the user store while a copy remains on the Personal vDisk. Doing so creates a Profile management error, and causes a temporary profile to be used for logons to the virtual desktop.

Automatic configuration

The desktop type is automatically detected, based on the Virtual Delivery Agent installation and, in addition to the configuration choices you make in Studio, sets Profile management defaults accordingly.

The policies that Profile management adjusts are shown in the table below. Any non-default policy settings are preserved and are not overwritten by this feature. Consult the Profile management documentation for information about each policy. The types of machines that create profiles affect the policies that are adjusted. The primary factors are whether machines are persistent or provisioned, and whether they are shared by multiple users or dedicated to just one user.

Persistent systems have some type of local storage, the contents of which can be expected to persist when the system turns off. Persistent systems may employ storage technology such as storage area networks (SANs) to provide local disk mimicking. In contrast, provisioned systems are created "on the fly" from a base disk and some type of identity disk. Local storage is usually mimicked by a RAM disk or network disk, the latter often provided by a SAN with a high speed link. The provisioning technology is generally Citrix Provisioning or Machine Creation Services (or a third-party equivalent). Sometimes provisioned systems have persistent local storage, which may be provided by Personal vDisks; these are classed as persistent.

Together, these two factors define the following machine types:

- **Both persistent and dedicated** –Examples are Single-session OS machines with a static assignment and a Personal vDisk that are created with Machine Creation Services, desktops with Personal vDisks that are created with VDI-in-a-Box, physical workstations, and laptops
- **Both persistent and shared** –Examples are Multi-session OS machines that are created with Machine Creation Services
- **Both provisioned and dedicated** –Examples are Single-session OS machines with a static assignment but without a Personal vDisk that are created with Citrix Provisioning
- **Both provisioned and shared** –Examples are Single-session OS machines with a random assignment that are created with Citrix Provisioning and desktops without Personal vDisks that are created with VDI-in-a-Box

The following Profile management policy settings are suggested guidelines for the different machine types. They work well in most cases, but you may want to deviate from these as your deployment requires.

> **Important:**
>
> Delete locally cached profiles on logoff, Profile streaming, and Always cache are enforced by the auto-configuration feature. Adjust the other policies manually.

Persistent machines

Policy	Both persistent and dedicated	Both persistent and shared
Delete locally cached profiles on logoff	Disabled	Enabled
Profile streaming	Disabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)
Active write back	Disabled	Disabled (note 3)
Process logons of local administrators	Enabled	Disabled (note 4)

Provisioned machines

Policy	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled (note 5)	Enabled
Profile streaming	Enabled	Enabled
Always cache	Disabled (note 6)	Disabled
Active write back	Enabled	Enabled
Process logons of local administrators	Enabled	Enabled (note 7)

1. Because Profile streaming is disabled for this machine type, the Always cache setting is always ignored.
2. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
3. Disable Active write back except to save changes in profiles of users who roam between Citrix Virtual Apps servers. In this case, enable this policy.

4. Disable Process logons of local administrators except for Hosted Shared Desktops. In this case, enable this policy.
5. Disable Delete locally cached profiles on logoff. This retains locally cached profiles. Because the machines are reset at logoff but are assigned to individual users, logons are faster if their profiles are cached.
6. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
7. Enable Process logons of local administrators except for profiles of users who roam between Citrix Virtual Apps and Desktops servers. In this case, disable this policy.

Folder redirection

Folder redirection lets you store user data on network shares other than the location where the profiles are stored. This reduces profile size and load time but it might impact network bandwidth. Folder redirection does not require that Citrix user profiles are employed. You can choose to manage user profiles on your own, and still redirect folders.

Configure folder redirection using Citrix policies in Studio.

- Ensure that the network locations used to store the contents of redirected folders are available and have the correct permissions. The location properties are validated.
- Redirected folders are set up on the network and their contents populated from users' virtual desktops at logon.

Configure folder redirection using only Citrix Policies or Active Directory Group Policy Objects, not both. Configuring folder redirection using both policy engines may result in unpredictable behavior.

Advanced folder redirection

In deployments with multiple operating systems (OSs), you might want some of a user's profile to be shared by each OS. The rest of the profile is not shared and is used only by one OS. To ensure a consistent user experience across the OSs, you need a different configuration for each OS. This is advanced folder redirection. For example, different versions of an application running on two OSs might need to read or edit a shared file, so you decide to redirect it to a single network location where both versions can access it. Alternatively, because the Start Menu folder contents are structured differently in two OSs, you decide to redirect only one folder, not both. This separates the Start Menu folder and its contents on each OS, ensuring a consistent experience for users.

If your deployment requires advanced folder redirection, you must understand the structure of your users' profile data and determine which parts of it can be shared between OSs. This is important because unpredictable behavior can result unless folder redirection is used correctly.

To redirect folders in advanced deployments:

- Use a separate Delivery Group for each OS.
- Understand where your virtual applications, including those on virtual desktops, store user data and settings, and understand how the data is structured.
- For shared profile data that can safely roam (because it is structured identically in each OS), redirect the containing folders in each Delivery Group.
- For non-shared profile data that cannot roam, redirect the containing folder in only one of the Desktop Groups, typically the one with the most used OS or the one where the data is most relevant. Alternatively, for non-shared data that cannot roam between OSs, redirect the containing folders on both systems to separate network locations.

Example advanced deployment

This deployment has applications, including versions of Microsoft Outlook and Internet Explorer, running on Windows 8 desktops and applications, including other versions of Outlook and Internet Explorer, delivered by Windows Server 2008. To achieve this, you have already set up two Delivery Groups for the two OSs. Users want to access the same set of Contacts and Favorites in both versions of those two applications.

Important: The following decisions and advice are valid for the OSs and deployment described. In your organization, the folders you choose to redirect and whether your decide to share them depend on a number of factors that are unique to your specific deployment.

- Using policies applied to the Delivery Groups, you choose the following folders to redirect.

Folder	Redirected in Windows 8?	Redirected in Windows Server 2008?
My Documents	Yes	Yes
Application Data	No	No
Contacts	Yes	Yes
Desktop	Yes	No
Downloads	No	No
Favorites	Yes	Yes
Links	Yes	No

Folder	Redirected in Windows 8?	Redirected in Windows Server 2008?
My Music	Yes	Yes
My Pictures	Yes	Yes
My Videos	Yes	Yes
Searches	Yes	No
Saved Games	No	No
Start Menu	Yes	No

- For the shared, redirected folders:
  - After analyzing the structure of the data saved by the different versions of Outlook and Internet Explorer, you decide it is safe to share the Contacts and Favorites folders
  - You know the structure of the My Documents, My Music, My Pictures, and My Videos folders is standard across OSs, so it is safe to store these in the same network location for each Delivery Group
- For the non-shared, redirected folders:
  - You do not redirect the Desktop, Links, Searches, or Start Menu folders folder in the Windows Server Delivery Group because data in these folders is organized differently in the two OSs. It therefore cannot be shared.
  - To ensure predictable behavior of this non-shared data, you redirect it only in the Windows 8 Delivery Group. You choose this, rather than the Windows Server Delivery Group, because Windows 8 will be used more often by users in their day-to-day work; they will only occasionally access the applications delivered by the server. Also, in this case the non-shared data is more relevant to a desktop environment rather than an application environment. For example, desktop shortcuts are stored in the Desktop folder and might be useful if they originate from a Windows 8 machine but not from a Windows Server machine.
- For the non-redirected folders:
  - You do not want to clutter your servers with users'downloaded files, so you choose not to redirect the Downloads folder
  - Data from individual applications can cause compatibility and performance issues, so you decide not to redirect the Application Data folder

For more information on folder redirection, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766489(v=ws.10)?redirectedfrom=MSDN.

Folder redirection and exclusions

In Citrix Profile management (but not in Studio), a performance enhancement allows you to prevent folders from being processed using exclusions. If you use this feature, do not exclude any redirected folders. The folder redirection and exclusion features work together, so ensuring no redirected folders are excluded allows Profile management to move them back into the profile folder structure again, while preserving data integrity, if you later decide not to redirect them. For more information on exclusions, see To include and exclude items.

Collect a Citrix Diagnostic Facility (CDF) trace at system startup

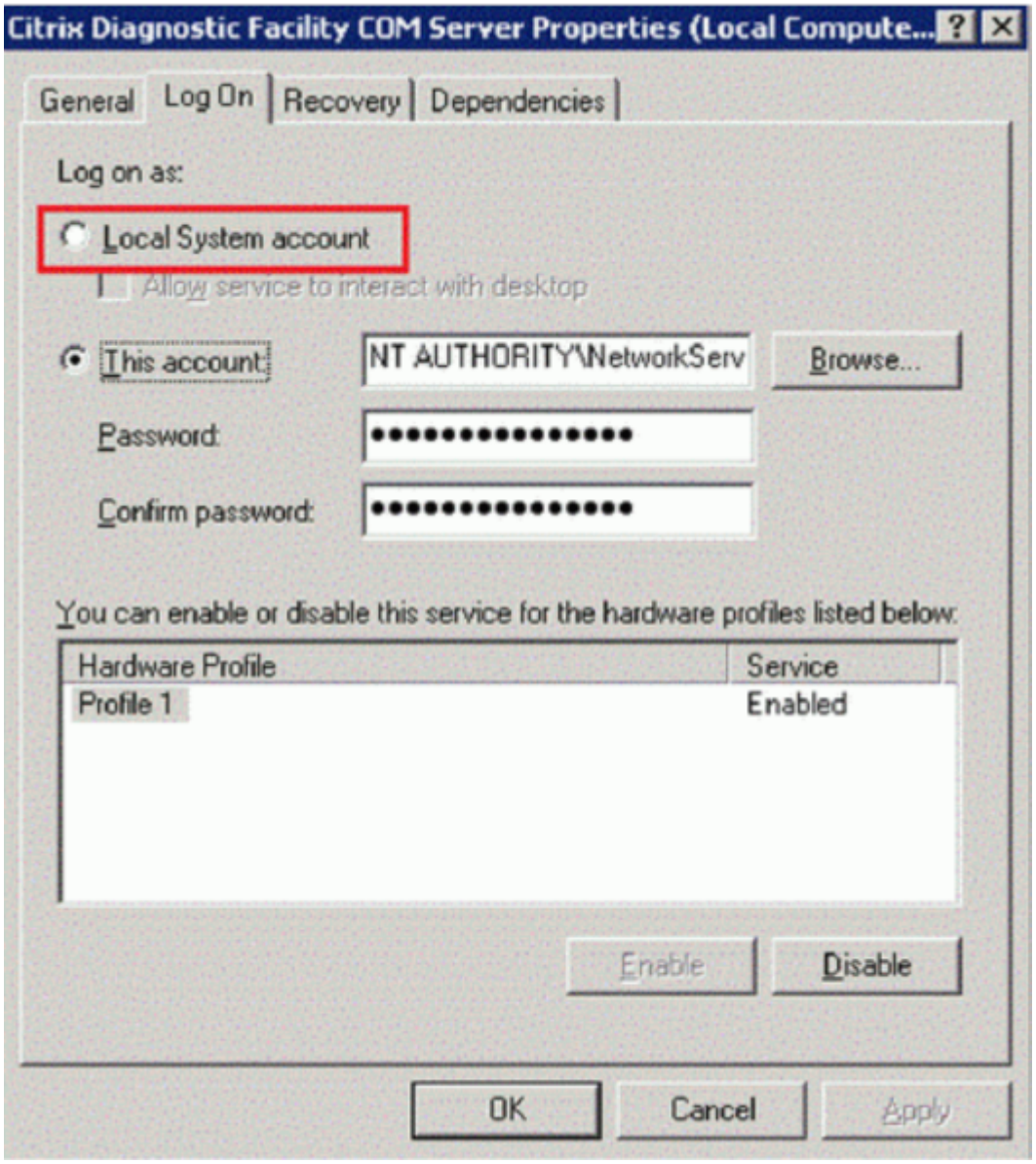
February 7, 2020

The CDFControl utility is an event tracing controller or consumer for capturing Citrix Diagnostic Facility (CDF) trace messages displayed from various Citrix tracing providers. It is made to troubleshoot complex Citrix related issues, parse filter support, and collect performance data. To download the CDFControl utility, see CTX111961.

Use the Local System account

To use the Local System account for the CDF COM server service, complete the following steps:

1. Click **Run** from the **Start** menu.
2. Type `services.msc` in the dialog box and click **OK**.
3. Select the **Citrix Diagnostics Facility COM Server** service and choose **Properties**.
4. Click the **Log On** tab and enable the **Local System** account. Then click **OK**.

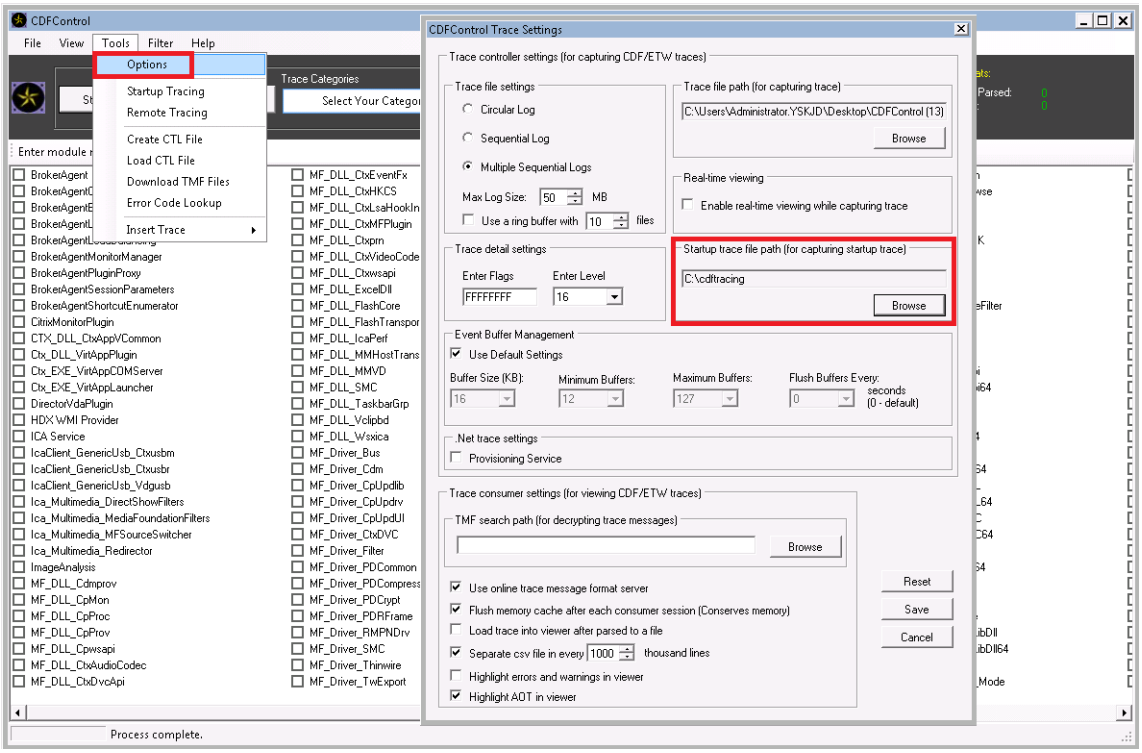


5. Restart the service.

Collect a trace at system startup

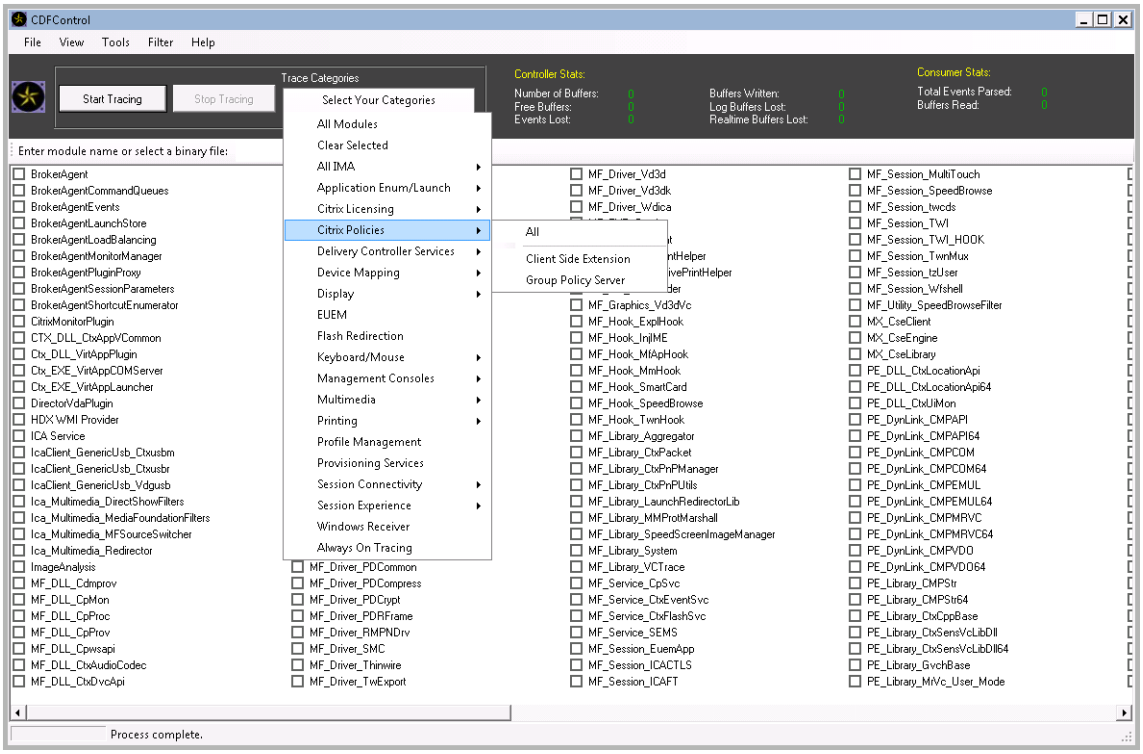
To collect a CDF trace at system startup, refer to the procedure:

1. Start **CDFControl** and select **Options** from the **Tools** menu.
2. Specify the trace file path in the **Startup trace file path for capturing startup trace** section. Then click **Save**.



3. Select the **Trace Categories** as recommended by Citrix Technical Support. In this example, **Citrix Policies** is selected.

   The **Citrix Policies** selection below is shown only as an example of startup tracing. We recommend that you enable the providers for the specific issue you are troubleshooting.



4. With administrator privileges, select **Startup Tracing** and click **Enable** from the **Tools** menu.

   After selecting **Enable**, the animated bar starts scrolling. This does not affect the procedure. Continue to Step 5.

5. Close the **CDFControl utility** and restart the system after the **Startup Tracing** is enabled.
6. Start the **CDFControl** utility. After the system restarts and the error appears, disable the **Startup Tracing** option by selecting **Disable**.

   Disable the **Startup Tracing** option by selecting Startup Tracing from the **Tools** menu and clicking **Disable** as described in Steps 4 and 5.

7. Stop the **Citrix Diagnostics Facility COM** server service.
8. Collect the trace log file (.etl) for analysis in the specified file path by following the Steps 1 and 2.
9. Start the **Citrix Diagnostics Facility COM** server service.

Citrix Insight Services

April 19, 2024

Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation. Its instrumentation and telemetry capabilities enable technical users (customers, partners, and engineers) to self-diagnose and fix problems and optimize their environments. For details and the latest information about CIS and how it works, see https://cis.citrix.com (Citrix account credentials required).

All information uploaded to Citrix is used for troubleshooting and diagnostic purposes, and improving the quality, reliability, and performance of products, subject to:

- Citrix Insight Services Policy at https://cis.citrix.com/legal
- Citrix Privacy Policy at https://www.cloud.com/privacy-policy

This Citrix Virtual Apps and Desktops release supports the following technologies.

- Citrix Virtual Apps and Desktops install and upgrade analytics
- Citrix Customer Experience Improvement Program (CEIP)
- Citrix Call Home
- Citrix Scout

In addition to (and separate from) CIS and Citrix Analytics: Google Analytics are collected (and later uploaded) automatically when you install (or upgrade) Studio. After installing Studio, you can change

this setting with the registry key HKLM\Software\Citrix\DesktopStudio\GAEnabled. A value of 1 enables collection and upload, 0 disables collection and upload.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade Citrix Virtual Apps and Desktops components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers'installation experiences.

The information is stored locally under %ProgramData%\Citrix\CTQs.

Automatic upload of this data is enabled by default in both the graphical and command line interfaces of the full-product installer.

- You can change the default value in a registry setting. If you change the registry setting before installing/upgrading, that value is used when you use the full-product installer.
- You can override the default setting if you install/upgrade with the command line interface by specifying an option with the command.

Control automatic uploads:

- Registry setting that controls automatic upload of install/upgrade analytics (default = 1):
  - Location: HKLM:\Software\Citrix\MetaInstall
  - Name: SendExperienceMetrics
  - Value: 0 = disabled, 1 = enabled
- Using PowerShell, the following cmdlet disables automatic upload of install/upgrade analytics:

```
1  New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
       SendExperienceMetrics -PropertyType DWORD -Value 0
2  <!--NeedCopy-->
```

- To disable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the `/disableexperiencemetrics` option.

  To enable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the `/sendexperiencemetrics` option.

Citrix Customer Experience Improvement Program

When you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous statistics and usage information are sent to Citrix to help Citrix improve the quality and performance of Citrix products. For more information, see https://more.citrix.com/XD-CEIP.

Enrollment during Site creation or upgrade

You are automatically enrolled in CEIP when you create a Site (after you install the first Delivery Controller). The first upload of data occurs approximately seven days after you create the Site. You can stop your participation at any time after creating the Site. Select the **Configuration** node in the Studio navigation pane (**Product Support** tab) and follow the guidance.

When you upgrade a Citrix Virtual Apps and Desktops deployment:

- If you upgrade from a version that did not support CEIP, you are asked if you want to participate.
- If you upgrade from a version that supported CEIP, and participation was enabled, CEIP is enabled in the upgraded Site.
- If you upgrade from a version that supported CEIP, and participation was disabled, CEIP is disabled in the upgraded Site.
- If you upgrade from a version that supported CEIP, and participation is unknown, you are asked if you want to participate.

The collected information is anonymous, so it cannot be viewed after it is uploaded to Citrix Insight Services.

Enrollment when installing a VDA

By default, you are automatically enrolled in CEIP when you install a Windows VDA. You can change this default in a registry setting. If you change the registry setting before installing the VDA, that value is used.

Registry setting that controls automatic enrolment in CEIP (default = 1):

Location: HKLM: \Software\Citrix\Telemetry\CEIP
Name: Enabled
Value: 0 = disabled, 1 = enabled

By default, the `Enabled` property is hidden in the registry. When it remains unspecified, the automatic upload feature is enabled.

Using PowerShell, the following cmdlet disables enrollment in CEIP:

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

The collected runtime datapoints are periodically written as files to an output folder (default %programdata%/Citrix/VdaCeip).

The first upload of data occurs approximately seven days after you install the VDA.

Enrollment when installing other products and components

You can also participate in CEIP when you install related Citrix products, components, and technologies, such as Citrix Provisioning, AppDNA, Citrix License Server, Citrix Workspace app for Windows, Universal Print Server, and Session Recording. See their documentation for details about installation and participation default values.

Citrix Call Home

When you install certain components and features in Citrix Virtual Apps and Desktops, you are offered the opportunity to participate in Citrix Call Home. Call Home collects diagnostic data and then periodically uploads telemetry packages containing that data directly to Citrix Insight Services (via HTTPS on default port 443) for analysis and troubleshooting.

In Citrix Virtual Apps and Desktops, Call Home runs as a background service under the name Citrix Telemetry Service. For more information, see https://more.citrix.com/XD-CALLHOME.

The Call Home scheduling functionality is also available in Citrix Scout. For details, see Citrix Scout.

What is collected

Citrix Diagnostic Facility (CDF) tracing logs information that can be useful for troubleshooting. Call Home collects a subset of CDF traces that can be helpful when troubleshooting common failures, for example, VDA registrations and application/desktop launches. This technology is known as always-on tracing (AOT). AOT logs are saved to disk at C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT.

Call Home does not collect any other Event Tracing for Windows (ETW) information, nor can it be configured to do so.

Call Home also collects other information, such as:

- Registries created by Citrix Virtual Apps and Desktops under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Windows Management Instrumentation (WMI) information under the Citrix namespace.
- List of processes running.
- Crash dumps of Citrix processes that are stored in %PROGRAM DATA%\Citrix\CDF.
- Installation and upgrade information. This can include the full product metainstaller log, failing MSI logs, output from the MSI log analyzer, StoreFront logs, Licensing compatibility check logs, and results from preliminary site upgrade tests.

The trace information is compressed as it is collected. The Citrix Telemetry Service retains a maximum of 10 MB of compressed recent trace information, with a maximum time limit of eight days.

- Compressing data allows Call Home to maintain a small footprint on the VDA.
- Traces are held in memory to avoid IOPs on provisioned machines.
- The trace buffer uses a circular mechanism to retain traces in memory.

Call Home collects the key datapoints listed in Call Home key datapoints.

Configure and manage summary

You can enroll in Call Home when using the full-product installation wizard or later, using PowerShell cmdlets. When you enroll, by default, diagnostics are collected and uploaded to Citrix every Sunday at approximately 3:00 AM, local time. The upload is randomized with a two hour interval from the specified time. This means an upload using the default schedule occurs between 3:00 AM and 5:00 AM.

If you do not want to upload diagnostic information on a scheduled basis (or if you want to change a schedule), you can use PowerShell cmdlets to manually collect and upload diagnostics or store them locally.

When you enroll in scheduled Call Home uploads and when you manually upload diagnostic information to Citrix, you provide Citrix account or Citrix Cloud credentials. Citrix exchanges the credentials for an upload token that is used to identify the customer and upload the data. The credentials are not saved.

When an upload occurs, a notification is emailed to the address associated with the Citrix account.

If you enable Call Home when you install a component, you can disable it later.

Prerequisites

- The machine must be running PowerShell 3.0 or later.
- The Citrix Telemetry Service must be running on the machine.
- The system variable `PSModulePath` must be set to Telemetry's install path, for example, C:\Program Files\Citrix\Telemetry Service\.

Enable Call Home during component installation

During VDA installation or upgrade: When you install or upgrade a Virtual Delivery Agent using the graphical interface in the full-product installer, you are asked if you want to participate in Call Home. There are two options:

- Participate in Call Home.
- Do not participate in Call Home.

If you're upgrading a VDA and previously enrolled in Call Home, that wizard page does not appear.

During Controller installation or upgrade: When you install or upgrade a Delivery Controller using the graphical interface, you are asked if you want to participate in Call Home. There are three options:

When you're installing a Controller, you cannot configure information on the Call Home page in the installation wizard if that server has an Active Directory GPO with the policy setting "Log on as a service" applied. For details, see CTX218094.

If you're upgrading a Controller and previously enrolled in Call Home, you're not asked about participating.

PowerShell cmdlets

The PowerShell help provides comprehensive syntax, including descriptions of cmdlets and parameters that are not used in these common use cases.

To use a proxy server for uploads, see Configure a proxy server.

- **Enable scheduled uploads:** Diagnostic collections are automatically uploaded to Citrix. If you do not enter additional cmdlets for a custom schedule, the default schedule is used.

  ```
  $cred = Get-Credential
  Enable-CitrixCallHome -Credential $cred
  <!--NeedCopy-->
  ```

  To confirm that scheduled uploads are enabled, enter `Get-CitrixCallHomeGet-CitrixCallHome`. If enabled, the return is `IsEnabled=True` and `IsMasterImage=False`.

- **Enable scheduled uploads for machines created from a master image:** Enabling scheduled uploads in a master image eliminates having to configure each machine that is created in the machine catalog.

  ```
  Enable-CitrixCallHome -Credential $cred -MasterImage
  ```

  To confirm that scheduled uploads are enabled, enter **Get-CitrixCallHome**. If enabled, the return is `IsEnabled=True` and `IsMasterImage=True`.

- **Create a custom schedule:** Create a daily or weekly schedule for diagnostic collections and uploads.

  ```
  $timespan = New-TimeSpan –Hours hours -Minutes minutes
  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
     -UploadFrequency {
  Daily|Weekly }

  <!--NeedCopy-->
  ```


Examples:

The following cmdlet creates a schedule to bundle and upload data at 10:20 every evening. The Hours parameter uses a 24-hour clock. When the `UploadFrequency` parameter value is Daily, the `DayOfWeek` parameter is ignored, if specified.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
<!--NeedCopy-->
```

To confirm the schedule, enter `Get-CitrixCallHomeSchedule`. In the preceding example, it returns `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency =Daily`.

The following cmdlet creates a schedule to bundle and upload data at 10:20 every Wednesday evening.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -
    UploadFrequency Weekly
<!--NeedCopy-->
```

To confirm the schedule, enter `Get-CitrixCallHomeSchedule`. In the preceding example, it returns `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly` .

Disable Call Home

You can disable Call Home using a PowerShell cmdlet or through Citrix Scout.

AOT logs are collected and saved to disk, even when Call Home scheduled uploads are disabled. (When scheduled uploads are disabled, AOT logs are not automatically uploaded to Citrix.) You can disable the collection and local storage of AOT logs.

Disable Call Home with PowerShell After running the following cmdlet, diagnostic data will not be uploaded to Citrix automatically. (You can still upload diagnostic data using Citrix Scout or telemetry PowerShell cmdlets.)

```
Disable-CitrixCallHome
```

To confirm that Call Home is disabled, enter `Get-CitrixCallHome`. If disabled, the return is `IsEnabled=False` and `IsMasterImage=False`.

Disable a collection schedule using Citrix Scout To disable a diagnostic collection schedule using Citrix Scout, follow the guidance in Schedule collections. In step 3, click **Off** to cancel the schedule for the selected machines.

Disable collection of AOT logs After running the following cmdlet (with the `Enabled` field set to **`false`**), AOT logs will not be collected.

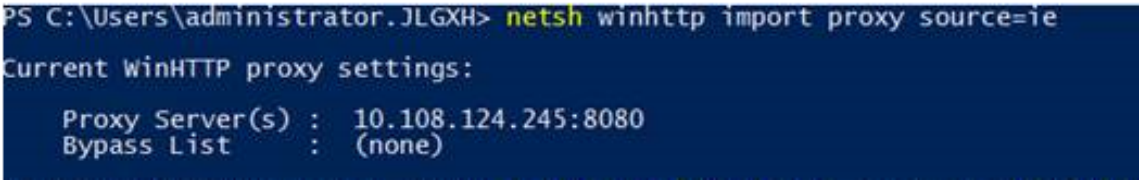
```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300
} } '
```

The `Listen` parameter contains arguments in JSON format.

Configure a proxy server for Call Home uploads

Complete the following tasks on the machine where Call Home is enabled. Example diagrams in the following procedure contain server address and port 10.158.139.37:3128. Your information will differ.

1. Add proxy server information in your browser. In Internet Explorer, select **Internet Options > Connections > LAN settings**. Select **Use a proxy server for your LAN**"and enter the proxy server address and port number.
2. In PowerShell, run `netsh winhttp import proxy source=ie`.



3. Using a text editor, edit the TelemetryService.exe config file, which is located in C:\Program Files\Citrix\Telemetry Service. Add the information shown in the red box.

4. Restart the Telemetry Service.

Run the Call Home cmdlets in PowerShell.

Manually collect and upload diagnostic information

You can use the CIS website to upload a diagnostic information bundle to CIS. You can also use PowerShell cmdlets to collect and upload diagnostic information to CIS.

To upload a bundle using the CIS website:

1. Log on to Citrix Insight Services using your Citrix account credentials.
2. Select **My Workspace**.
3. Select **Healthcheck** and then navigate to the location of your data.

CIS supports several PowerShell cmdlets that manage data uploads. This documentation covers the cmdlets for two common cases:

- Use the `Start-CitrixCallHomeUpload` cmdlet to manually collect and upload a diagnostic information bundle to CIS. (The bundle is not saved locally.)
- Use the `Start-CitrixCallHomeUpload` cmdlet to manually collect data and store a diagnostic information bundle locally. This allows you to preview the data. Later, use the `Send-CitrixCallHomeBundle` cmdlet to manually upload a copy of that bundle to CIS. (The data you originally saved remains locally.)

The PowerShell help provides comprehensive syntax, including descriptions of cmdlets and parameters that are not used in these common use cases.

When you enter a cmdlet to upload data to CIS, you are prompted to confirm the upload. If the cmdlet times out before the upload completes, check the status of the upload in the system event log. The upload request might be rejected if the service is already performing an upload.

Collect data and upload bundle to CIS:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
<!--NeedCopy-->
```

Collect data and save it locally:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
<!--NeedCopy-->
```

The following parameters are valid:

- **Credential:** Directs the upload to CIS.
- **InputPath:** Location of zip file to include in the bundle. This might be an additional file that Citrix Support requests. Be sure to include the .zip extension.
- **OutputPath:** Location where the diagnostic information is saved. This parameter is required when saving Call Home data locally.
- **Description and Incident Time:** Free form information about the upload.
- **SRNumber:** Citrix Technical Support incident number.
- **Name:** Name that identifies the bundle.
- **UploadHeader:** JSON-formatted string specifying the upload headers uploaded to CIS.
- **AppendHeaders:** JSON-formatted string specifying the appended headers uploaded to CIS.
- **Collect:** JSON-formatted string specifying which data to collect or omit, in the form {'collector' :{'enabled':Boolean}}, where Boolean is true or false.
  Valid collector values are:
  - 'wmi'
  - 'process'
  - 'registry
  - 'crashreport'
  - 'trace'
  - 'file'
  - 'msi'
  - 'localdata'
  - 'sitedata'
  - 'sfb'

  By default, all collectors except 'sfb'are enabled.

  The 'sfb'collector is designed to be used on demand to diagnose Skype for Business issues. In addition to the 'enabled'parameter, the 'sfb'collector supports the 'account'and 'accounts' parameters to specify target users. Use one of the forms:
  - "-Collect "{'sfb':{'account':'domain\\user1'}}"
  - "-Collect "{'sfb':{'accounts':['domain\\user1', 'domain\\user2']}}"
- **Common Parameters:** See the PowerShell help.

Upload data that was previously saved locally:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```


The Path parameter specifies the location of the previously saved bundle.

Examples:

The following cmdlet requests an upload of Call Home data (excluding data from the WMI collector) to CIS. This data relates to registration failures of Citrix Provisioning VDAs, which were noted at 2:30 PM for Citrix Support case 123456. In addition to the Call Home data, the file "c:\Diagnostics\ExtraData.zip"is incorporated into the uploaded bundle.

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
    zip" -Description "Registration failures with Citrix Provisioning
    VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
    RegistrationFailure-021812016" -Collect "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
<!--NeedCopy-->
```

The following cmdlet saves Call Home data related to Citrix Support case 223344, noted at 8:15 AM. The data saved in the file mydata.zip on a network share. In addition to the Call Home data, the file "c:\Diagnostics\ExtraData.zip"will be incorporated into the saved bundle.

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\
    mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
<!--NeedCopy-->
```

The following cmdlet uploads the data bundle you saved earlier.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  – Credential $cred -Path \\mynetwork\
    myshare\mydata.zip
<!--NeedCopy-->
```

Citrix Scout

January 9, 2023

Introduction

Citrix Scout collects diagnostics and runs health checks. You can use the results for proactive maintenance in your Citrix Virtual Apps and Desktops deployment. Citrix offers comprehensive, automated analysis of diagnostics collections through Citrix Insight Services. You can also use Scout to troubleshoot issues, on your own or with Citrix Support guidance.

You can upload collection files to Citrix for analysis and guidance from Citrix Support. Or, you can save a collection locally for your own review, and then later upload the collection file to Citrix for analysis.

Scout offers the following procedures:

- **Collect:** Runs a one-time diagnostics collection on machines you select in a site. You can then either upload the file to Citrix or save it locally.
- **Trace & Reproduce:** Starts a manual trace on machines you select. Then you re-create issues on those machines. After re-creating the issue, the trace is stopped. Scout then collects other diagnostics and uploads the file to Citrix, or saves the file locally.
- **Schedule:** Schedules diagnostics collections to occur daily or weekly at a specified time on machines you select. The file is automatically uploaded to Citrix.
- **Health Check:** Runs checks that gauge the health and availability of the site and its components. You can run health checks for Delivery Controllers, VDAs, StoreFront servers, and Citrix License Servers. If issues are found during the checks, Scout provides a detailed report. Each time Scout starts, it checks for updated health check scripts. If new versions are available, Scout downloads them automatically, for use the next time health checks are run.

The graphical interface described in this article is the primary way to use Scout. Alternatively, you can use PowerShell to configure one-time or scheduled diagnostic collections and uploads. See Call Home.

Where to run Scout:

- In an on-premises deployment, run Scout from a Delivery Controller to capture diagnostics or run checks on one or more Virtual Delivery Agents (VDAs), Delivery Controllers, StoreFront servers, and License Servers. You can also run Scout from a VDA to collect local diagnostics.
- In a Citrix Cloud environment that uses the Citrix Virtual Apps and Desktops service, run Scout from a VDA to collect local diagnostics.

The log for the Scout application is stored in `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. This file can be used for troubleshooting.

What is collected

The diagnostics collected by Scout include Citrix Diagnostic Facility (CDF) trace log files. A subset of CDF traces called Always-on Tracing (AOT) is also included. AOT information can be helpful when trou-

bleshooting common issues such as VDA registrations and application/desktop launches. No other Event Tracing for Windows (ETW) information is collected.

The collection includes:

- Registry entries created by Citrix Virtual Apps and Desktops under `HKEY\\_LOCAL\\_MACHINE\\SOFTWARE\\CITRIX`.
- Windows Management Instrumentation (WMI) information under the **Citrix namespace**.
- Processes that are running.
- Crash dumps of Citrix processes that are stored in %PROGRAM DATA%\Citrix\CDF.
- Citrix policy information, in CSV format.
- Installation and upgrade information. The collection can include the full product metainstaller log, failing MSI logs, output from the MSI log analyzer, StoreFront logs, Licensing compatibility check logs, and results from preliminary site upgrade tests.

About trace information:

- The trace information is compressed as it is collected, keeping a small footprint on the machine.
- On each machine, the Citrix Telemetry Service keeps compressed recent trace information for a maximum of eight days.
- Beginning with Citrix Virtual Apps and Desktops 7 1808, AOT traces are saved to the local disk by default. (In earlier versions, traces were held in memory.) Default path = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- Beginning with Citrix Virtual Apps and Desktops 7 1811, AOT traces saved to network shares are collected with other diagnostics.
- You can modify the maximum size (default = 10 MB) and slice duration, using the `Enable-CitrixTrace` cmdlet or the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` registry string.
- Traces append to the file until the file reaches 10% of `MaxSize`.

For a list of the datapoints that Scout collects, see Call Home key datapoints.

About health checks

Health check data is stored in folders under `C:\ProgramData\Citrix\TelemetryService\` .

Site health checks

Site health checks are included in the Environment Test Service, which provides a comprehensive evaluation of the FlexCast Management Architecture (FMA) services. In addition to checking for service availability, these checks look for other health indicators such as database connections.

Site health checks run on Delivery Controllers. Depending on your site's size, these checks can take up to an hour to complete.

Delivery Controller configuration checks As part of the site health checks. Delivery Controller configuration checks verify whether the following issues exist, based on Citrix recommendations for Virtual Apps and Desktops sites:

- One or more Delivery Controllers are in a failed state.
- There is only one Delivery Controller in the site.
- Delivery Controllers are of different versions.

In addition to meeting the permissions and requirements for health checks, Delivery Controller configuration checks require:

- At least one Controller powered on.
- The Broker Service running on a Controller.
- A working connection from the Controller to the site database.

VDA health checks

VDA health checks identify possible causes for common VDA registration, session launch, and time zone redirection issues.

For registration on the VDA, Scout 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 launch on VDAs, Scout 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

For time zone redirection on VDAs, Scout checks:

- Windows hotfix installation
- Citrix hotfix installation
- Microsoft group policy settings
- Citrix group policy settings

StoreFront health checks

StoreFront checks verify:

- Citrix Default Domain service is running
- Citrix Credential Wallet service is running
- Connection from the StoreFront server to Active Directory port 88
- Connection from the StoreFront server to Active Directory port 389
- Base URL has a valid FQDN
- Correct IP address from the base URL can be retrieved
- IIS application pool is using .NET 4.0
- Whether the certificate is bound to the SSL port for the host URL
- Whether the certificate chain is complete
- Whether certificates have expired
- Whether a certificate is expiring soon (within 30 days)

License Server checks

License Server checks verify:

- License Server connection from the Delivery Controller
- License Server firewall remote access status
- Citrix Licensing service status
- License Server grace period state
- License Server ports connection
- Whether the Citrix vendor daemon (CITRIX) is running
- Whether system clocks are synchronized
- Whether the Citrix Licensing service is running under the Local Service account
- Presence of the `CITRIX.opt` file
- Customer Success Services eligibility date
- Citrix License Server Update
- Whether the License Server certificate is in the Delivery Controller's trusted root store

In addition to meeting the permissions and requirements for health checks, the License Server must be joined to a domain. Otherwise, the License Server won't be discovered.

Permissions and requirements

Permissions:

- To collect diagnostics:
  - You must be a local administrator and domain user for each machine from which you're collecting diagnostics.
  - You must have permission to write to the LocalAppData directory on each machine.
- To run health checks:
  - You must be a member of the domain users group.
  - You must be either a full administrator or have a custom role with read-only and **Run Environment Tests** permissions for the site.
- Use **Run as administrator** when launching Scout.

For each machine from which you collect diagnostics or run health checks:

- Scout 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.
- The Citrix Telemetry Service must be running on the machine.
- Windows Management Infrastructure (WMI) access must be enabled on the machine.
- To set a schedule for diagnostic collection, the machine must be running a compatible Scout version.

Do not use the dollar sign ($) in user names specified in pathnames. It prevents the collection of diagnostic information.

Scout runs verification tests on the machines you select, to make sure these requirements are met.

Verification tests

Before a diagnostic collection or health check starts, verification tests run automatically for each selected machine. These tests make sure that the requirements are met. If a test fails for a machine, Scout displays a message, with suggested corrective actions.

- **Scout 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 at the same time. Using **Run as administrator**, run the `Enable-PSRemoting` cmdlet. For details, see the Microsoft help for the cmdlet.
- **Scout requires PowerShell 3.0 (minimum):** Install PowerShell 3.0 (or later) on the machine, and then enable PowerShell remoting.
- **Unable to access LocalAppData directory on this machine:** Ensure that account has permission to write to the LocalAppData directory on the machine.
- **Cannot locate Citrix Telemetry Service:** Ensure that the Citrix Telemetry Service is installed and started on the machine.
- **Cannot get schedule:** Upgrade the machine to (minimum) XenApp and XenDesktop 7.14.
- **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.
- **Newer version of Citrix Telemetry Service required:** (Version is checked only for Collect and Trace & Reproduce.) Upgrade the Telemetry Service version on the machine (see Install and upgrade). If you do not upgrade the service, that machine won't be included in the **Collect** or **Trace & Reproduce** actions.

Version compatibility

This version of Scout (3.x) is intended to be run on Citrix Virtual Apps and Desktops (or minimum XenApp and XenDesktop 7.14) Controllers and VDAs.

An earlier version of Scout is provided with XenApp and XenDesktop versions earlier than 7.14. For information about that earlier version, see CTX130147.

If you upgrade a Controller or VDA earlier than 7.14 to version 7.14 (or a later supported version), the earlier version of Scout is replaced with the current version.

Feature	Scout 2.23	Scout 3.0
Support Citrix Virtual Apps and Desktops (plus XenApp and XenDesktop 7.14 through 7.18)	Yes	Yes
Support XenDesktop 5.x, 7.1 to 7.13	Yes	No
Support XenApp 6.x, 7.5 to 7.13	Yes	No

Feature	Scout 2.23	Scout 3.0
Delivered with product	7.1 to 7.13	Beginning with 7.14
Can be downloaded from CTX article	Yes	No
Capture CDF traces	Yes	Yes
Capture Always-on-Traces (AOT)	No	Yes
Allow collection of diagnostic data	Up to 10 machines at once (by default)	Unlimited (subject to resource availability)
Allow diagnostic data to be sent to Citrix	Yes	Yes
Allow diagnostic data to be saved locally	Yes	Yes
Support Citrix Cloud credentials	No	Yes
Support Citrix credentials	Yes	Yes
Support proxy server for uploads	Yes	Yes
Adjust schedules	N/A	Yes
Script support	Command line (local Controller only)	PowerShell using Call Home cmdlets (any machine with the Telemetry Service installed)
Health checks	No	Yes
Data Masking	No	Beginning with 3.17

Install and upgrade

By default, Scout is installed or upgraded automatically as part of the Citrix Telemetry Service when you install or upgrade a VDA or a Controller.

If you omit the Citrix Telemetry Service when you install a VDA, or remove the service later, run `TelemetryServiceInstaller_xx.msi` from the `x64\Virtual Desktop Components` or `x86\Virtual Desktop Components` folder on the Citrix Virtual Apps and Desktops installation media.

When you select the **Collect** or **Trace & Reproduce** action, you're notified if a machine is running an older version of the Citrix Telemetry Service. Citrix recommends using the latest supported version. If

you don't upgrade the Telemetry Service on that machine, it won't participate in the **Collect** or **Trace & Reproduce** actions. To upgrade the Telemetry Service, use the same procedure as installing it.

Upload authorization

If you plan to upload diagnostic collections to Citrix, you must have a Citrix or Citrix Cloud account. (These are the credentials you use to access Citrix downloads or access the Citrix Cloud Control Center.) After your account credentials are validated, a token is issued.

- If you authenticate with a Citrix account, the token-issuing process isn't visible. You simply enter your account credentials. After Citrix validates the credentials, you can then continue in the Scout wizard.
- If you authenticate with a Citrix Cloud account, you click a link to access Citrix Cloud using HTTPS with your default browser. After you enter your Citrix Cloud credentials, the token is displayed. Copy the token and then paste it into Scout. You can then continue in the Scout wizard.

The token is stored locally on the machine where you're running Scout. To enable use of that token the next time you run **Collect** or **Trace & Reproduce**, select the **Store token and skip this step in the future** check box.

You must reauthorize each time you select **Schedule** on the Scout opening page. You cannot use a stored token when creating or changing a schedule.

Use a proxy for uploads

If you want to use a proxy server to upload collections to Citrix, you can instruct Scout to use the proxy settings configured for your browser's Internet Properties. Alternatively, you can specify the proxy server's IP address and port number.

Add machines manually

After Scout lists the Controllers and VDAs it discovers, you can manually add other machines in the deployment, such as StoreFront servers, License Servers, and Citrix Provisioning servers.

When running health checks:

- Citrix License Servers in the domain are discovered automatically. You cannot add License Servers manually.
- Health checks do not currently support Citrix Provisioning servers.

On any Scout page that lists the discovered machines, click **+ Add machine**. Type the FQDN of the machine you want to add, and then click **Continue**. Repeat to add other machines, as needed. (Although entering a DNS alias instead of an FQDN can appear valid, the health checks might fail.)

Manually added machines always appear at the top of the machines list, above the discovered machines.

An easy way to identify a manually added machine is the red delete button on the right end of the row. Only manually added machines have that button. Discovered machines don't.

To remove a manually added machine, click the red button on the right end of the row. Confirm the deletion. Repeat to delete other manually added machines.

Scout remembers manually added machines until you remove them. When you close and then reopen Scout, the manually added machines are still listed at the top of the list.

CDF traces are not collected when using **Trace & Reproduce** on StoreFront servers. However, all other trace information is collected.

Collect diagnostics

The **Collect** procedure comprises selecting machines, starting the diagnostics collection, and then uploading the file containing the collection to Citrix or saving it locally.

1. Launch Scout. From the machine's **Start** menu, select **Citrix > Citrix Scout**. On the opening page, click **Collect**.
2. Select machines. The **Select machines** page lists all the VDAs and Controllers in the site. You can filter the display by machine name. Select the check box next to each machine you want to collect diagnostics from, and then click **Continue**.

   To add other machines manually (such as StoreFront or Citrix Provisioning servers), see Add machines manually.

   Scout automatically launches verification tests on each selected machine, ensuring it meets the criteria listed in Verification tests. If verification fails, a message is posted in the **Status** column, and that machine's check box is unselected. You can either:

   - Resolve the issue and then select the machine's check box again. This triggers a retry of the verification tests.
   - Skip that machine (leave its check box unselected). Diagnostics won't be collected from that machine.

   When the verification tests complete, click **Continue**.
3. Collect diagnostics. The summary lists all the machines from which diagnostics will be collected (the machines you selected that passed the verification tests). Click **Start Collecting**.

During collection:

- The **Status** column indicates the current collection state for a machine.
- To stop an in-progress collection on a single machine, click **Cancel** in the **Action** column for that machine.
- To stop all in-progress collections, click **Stop Collection** in the lower right corner of the page. Diagnostics from machines that have completed collection are kept. To resume the collection, click **Retry** in the **Action** column for each machine.
- When the collection completes for all selected machines, the **Stop Collection** button in the lower right corner changes to **Continue**.
- To collect diagnostics again, click **Collect Again** in that machine's **Action** column. The newer collection overwrites the earlier.
- If a collection fails, you can click **Retry** in the **Action** column. Only successful collections are uploaded or saved.
- After the collection completes for all selected machines, don't click **Back**. (If you click it, the collection is lost.)

When the collection completes, click **Continue**.

4. Save or upload the collection. Choose whether to upload the file to Citrix, or save it on the local machine.

   If you choose to upload the file now, continue with Step 5.

   If you choose to save the file locally:

   - A Windows **Save** dialog box appears. Navigate to the desired location.
   - When the local save completes, the pathname of the file is displayed and linked. You can view the file. You can upload the file later to Citrix. See CTX136396.

   Click **Done** to return to the Scout opening page. You don't need to complete any further steps in this procedure.

5. Authenticate for uploads and optionally specify a proxy. For details, see Upload authorization.

   - If you haven't authenticated through Scout, continue with this step.
   - If you have authenticated through Scout, the stored authorization token is used by default. If this is what you want to do, select this option and click **Continue**. You aren't prompted for credentials for this collection. Continue with Step 6.
   - If you authenticated previously, but want to reauthorize and get a new token, click **Change/Reauthorize** and continue with this step.

   Choose whether you want to use Citrix credentials or Citrix Cloud credentials to authenticate the upload. Click **Continue**. The credentials page appears only if you're not using a stored token.

On the credentials page:

- If you want to use a proxy server for the file upload, click **Configure proxy**. You can instruct Scout to use the proxy settings configured for your browser's internet properties. Or, you can enter the proxy server's IP address and port number. Close the proxy dialog box.
- For a Citrix Cloud account, click **Generate token**. Your default browser launches to a Citrix Cloud page where a token is displayed. Copy the token, and then paste it on the Scout page.
- For a Citrix account, enter your credentials.

When you're done, click **Continue**.

6. Enter information about the upload.

   - The name field contains the default name for the file for the collected diagnostics. This suffices for most collections, although you can change the name. (If you delete the default name and leave the name field empty, the default name is used.)
   - Optionally, specify an 8-digit Citrix Support case number.
   - In the optional **Description** field, describe the issue and indicate when the issue occurred, if applicable.

   When you're done, click **Start Upload**.

   During the upload, the lower left portion of the page approximates the percentage of the upload that has completed. To cancel an in-progress upload, click **Stop Upload**.

   When the upload completes, the URL of its location is displayed and linked. You can follow the link to the Citrix location to view the analysis of the upload, or you can copy the link.

   Click **Done** to return to the Scout opening page.

Trace and reproduce

The **Trace and Reproduce** procedure comprises selecting machines, starting a trace, reproducing issues, completing the diagnostics collection, and then uploading the file to Citrix, or saving it locally.

This procedure is similar to the standard **Collect** procedure. However, it allows you to start a trace on machines and then re-create issues on those machines. All diagnostics collections include AOT trace information. This procedure adds CDF traces to help troubleshooting.

1. Launch Scout. From the machine's **Start** menu, select **Citrix > Citrix Scout**. On the opening page, click **Trace & Reproduce**.
2. Select machines. The **Select machines** page lists all the VDAs and Controllers in the site. You can filter the display by machine name. Select the check box next to each machine you want to collect traces and diagnostics from. Then click **Continue**.

To add other machines manually (such as StoreFront or Citrix Provisioning servers), see Add machines manually.

Scout automatically launches verification tests on each selected machine, making sure it meets the criteria listed in Verification tests. If verification fails for a machine, a message is posted in the **Status** column, and that machine's check box is unselected. You can either:

- Resolve the issue and then select the machine's check box again. This triggers a retry of the verification tests.
- Skip that machine (leave its check box unselected). Diagnostics and traces won't be collected from that machine.

When the verification tests complete, click **Continue**.

3. Start the trace. The summary lists all the machines from which traces will be collected. Click **Start Tracing**.

   On one or more of the selected machines, reproduce the issues you experienced. Trace collection continues while you're doing that. When you're done reproducing the issue, click **Continue** in Scout. That stops the trace.

   After you stop the trace, indicate whether you reproduced the issue during the trace.

4. Collect diagnostics from machines. Click **Start Collecting**. During collection:

   - The **Status** column indicates the current collection state for a machine.
   - To stop an in-progress collection on a single machine, click **Cancel** in the **Action** column for that machine.
   - To stop all in-progress collections, click **Stop Collection** in the lower right corner of the page. Diagnostics from machines that have completed collection are kept. To resume the collection, click **Retry** in the **Action** column for each machine.
   - When the collection completes for all selected machines, the **Stop Collection** button in the lower right corner changes to **Continue**.
   - To collect diagnostics again from a machine, click **Collect Again** in that machine's **Action** column. The newer collection overwrites the earlier.
   - If a collection fails, you can click **Retry** in the **Action** column. Only successful collections are uploaded or saved.
   - After the collection completes for all selected machines, don't click **Back**. (If you do, the collection is lost.)

   When the collection completes, click **Continue**.

5. Save or upload the collection. Choose whether to upload the file to Citrix or save it locally.

   If you choose to upload the file now, continue with Step 6.

   If you choose to save the file locally:

- A Windows Save dialog box appears. Select the desired location.
- When the local save completes, the pathname of the file is displayed and linked. You can view the file. Remember: You can upload the file later from Citrix; see CTX136396 for Citrix Insight Services.

Click **Done** to return to the Scout opening page. You don't need to complete any further steps in this procedure.

6. Authenticate for uploads and optionally specify proxy. Review Upload authorization for details of this process.

   - If you haven't authenticated through Scout, continue with this step.
   - If you authenticated through Scout, the stored authorization token is used by default. If this what you want to do, choose this option and click **Continue**. You aren't prompted for credentials for this collection. Continue with Step 7.
   - If you previously authenticated, but want to reauthorize and get a new token, click **Change/Reauthorize** and continue with this step.

   Choose whether you want to use Citrix credentials or Citrix Cloud credentials to authenticate the upload. Click **Continue**. The credentials page appears only if you're not using a stored token.

   On the credentials page:

   - If you want to use a proxy server for the file upload, click **Configure proxy**. You can instruct Scout to use the proxy settings configured for your browser's Internet Properties. Or, you can enter the proxy server's IP address and port number. Close the proxy dialog box.
   - For a Citrix Cloud account, click **Generate token**. Your default browser launch to a Citrix Cloud page where a token is displayed. Copy the token, and then paste it on the Scout page.
   - For a Citrix account, enter your credentials.

   When you're done, click **Continue**.

7. Provide information about the upload.

   Enter upload details:

   - The name field contains the default name for the file for the collected diagnostics. This suffices for most collections, although you can change the name. (If you delete the default name and leave the name field empty, the default name is used.)
   - Optionally, specify an 8-digit Citrix Support case number.
   - In the optional Description field, describe the issue and indicate when the issue occurred, if applicable.

When you're done, click **Start Upload**.

During the upload, the lower left portion of the page approximates what percentage of the upload has completed. To cancel an in-progress upload, click **Stop Upload**.

When the upload completes, the URL of its location is displayed and linked. You can follow the link to the Citrix location to view the analysis of the upload, or you can copy the link.

Click **Done** to return to the Scout opening page.

Schedule collections

> Note:
>
> You can currently schedule collections, but not health checks.

The Schedule procedure comprises selecting machines and then setting or canceling the schedule. Scheduled collections are automatically uploaded to Citrix. (You can save scheduled collections locally using the PowerShell interface. See Citrix Call Home.)

1. Launch Scout. From the machine's Start menu, select **Citrix > Citrix Scout**. On the opening page, click **Schedule**.
2. Select machines. All the VDAs and Controllers in the site are listed. You can filter the display by machine name.

   When you installed VDAs and Controllers using the graphical interface, if you set a Call Home schedule (see Citrix Call Home), Scout displays those settings, by default. You can use this version of Scout to start scheduled collections for the first time, or change a previously configured schedule.

   Although you enabled/disabled Call Home on a per-machine basis during component installation, a schedule configured in Scout affects all the machines you select.

   Select the check box next to each machine you want to collect diagnostics from, and then click **Continue**.

   To add other machines manually (such as StoreFront or Citrix Provisioning servers), see Add machines manually.

   Scout automatically launches verification tests on each of the selected machines, making sure it meets the criteria in Verification tests. If verification fails for a machine, a message is posted in the **Status** column, and that machine's check box is unselected. You can either:

   - Resolve the issue and then select the machine's check box again. This triggers a retry of the verification tests.
   - Skip that machine (leave its check box unselected). Diagnostics (or traces) won't be collected from that machine.

When the verification tests complete, click **Continue**.

The summary page lists the machines to which schedules will be applied. Click **Continue**.

3. Set the schedule. Indicate when you want diagnostics to be collected. Remember: The schedule affects all selected machines.

   - To configure a weekly schedule for the selected machines, click **Weekly**. Choose the day of the week. Enter the time of day (24-hour clock) for the collection to begin.
   - To configure a daily schedule for the selected machines, click **Daily**. Enter the time of day (24-hour clock) for the collection to begin.
   - To cancel an existing schedule for the selected machines (and not replace it with another), click **Off**. This cancels any schedule that was previously configured for those machines.

   Click **Continue**.

4. Authenticate for uploads and optionally specify a proxy. Review Upload authorization for details of this process. Remember: You cannot use a stored token to authenticate when working with a Scout schedule.

   Choose whether you want to use Citrix credentials or Citrix Cloud credentials to authenticate the upload. Click **Continue**.

   On the credentials page:

   - If you want to use a proxy server for the file upload, click **Configure proxy**. You can instruct Scout to use the proxy settings configured for your browser's Internet Properties. Or, you can enter the proxy server's IP address and port number. Close the proxy dialog box.
   - For a Citrix Cloud account, click **Generate token**. Your default browser launches to a Citrix Cloud page where a token is displayed. Copy the token, and then paste it on the Scout page.
   - For a Citrix account, enter your credentials.

   When you're done, click **Continue**.

   Review the configured schedule. Click **Done** to return to the Scout opening page.

   During a collection, each selected machine's Windows application log contains entries about the collection and upload.

Run health checks

The Health Check procedure comprises selecting machines, starting the checking, and then reviewing the results report.

1. Launch Scout. From the machine's **Start** menu, select **Citrix > Citrix Scout**. On the opening page, click **Health Check**.

2. Select machines. The **Select machines** page lists all the VDAs, Delivery Controllers, and License Servers discovered in the site. You can filter the display by machine name. Select the check box next to each machine you want to collect diagnostics from, and then click **Continue**.

   To add other component types (such as StoreFront servers), see Add machines manually. You cannot manually add Citrix Provisioning Servers or License Servers.

   Scout automatically launches verification tests on each selected machine, making sure it meets the criteria listed in Verification tests. If verification fails, a message is posted in the **Status** column, and that machine's check box is cleared. You can either:

   - Resolve the issue and then select the machine's check box again. This triggers a retry of the verification tests.
   - Skip that machine (leave its check box unselected). Health checks won't be run for that machine.

   When the verification tests complete, click **Continue**.

3. Run the health checks on the selected machines. The summary lists the machines where the tests will run (the machines you selected that passed the verification tests). Click **Start Checking**.

   During and after checking:

   - The **Status** column indicates the current checking state for a machine.
   - 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, only all selected machines. Information from machines that have completed the checks is kept.
   - When the checks 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 show the results.
   - After the check completes for all selected machines, don't click **Back**. (If you do, the check results are lost.)

4. When the checks complete, click **Done** to return to the Scout opening page.

Heath check results

For report-generating Citrix checks, the reports contain:

- Time and date when the results report was generated
- Machines that were checked
- Conditions that the check looked for on the targeted machines

Monitor

February 6, 2020

Administrators and help desk personnel can monitor Citrix Virtual Apps and Desktops Sites using a variety of features and tools. Using these tools, you can monitor:

- User sessions and session use
- Logon performance
- Connections and machines, including failures
- Load evaluation
- Historical trends
- Infrastructure

Citrix Director

Director is a real-time web tool that you can use to monitor and troubleshoot, and to perform support tasks for end users.

For details, see the Director articles.

Configuration Logging

Configuration Logging allows administrators to keep track of administrative changes to a Site. Configuration Logging can help administrators diagnose and troubleshoot problems after configuration changes are made, assist change management and track configurations, and report administration activity.

You can view and generate reports about logged information from Studio. You can also view logged items in Director with the Trend View to provide notifications of configuration changes. This feature is useful for administrators who do not have access to Studio.

The Trends View gives historical data of configuration changes over a period of time so administrators can assess what changes were made to the Site, when they were made, and who made them to find the cause of an issue. This view sorts configuration information into three categories:

- Connection Failures
- Failed Single-session Machines
- Failed Multi-session Machines

For details about how to enable and configure Configuration Logging, see Configuration Logging. The Director articles describe how to view logged information from that tool.

Event logs

Services within Citrix Virtual Apps and Desktops log events that occur. Event logs can be used to monitor and troubleshoot operations.

For details, see Event logs. Individual feature articles might also contain event information.

Configuration Logging

February 6, 2020

Configuration Logging captures Site configuration changes and administrative activities to the database. 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 administration activity

You set Configuration Logging preferences, display configuration logs, and generate HTML and CSV reports from Citrix Studio. You can filter configuration log displays by date ranges and full text search results. Mandatory logging, when enabled, prevents configuration changes from being made unless they can be logged. With appropriate permission, you can delete entries from the configuration log. You cannot use the Configuration Logging feature to edit log content.

Configuration Logging uses a PowerShell SDK and the Configuration Logging Service. The Configuration Logging Service runs on every Controller in the Site. If one Controller fails, the service on another Controller automatically handles logging requests.

By default, the Configuration Logging feature is enabled, and uses the database that is created when you create the Site (the Site Configuration database). You can specify a different location for the database. The Configuration Logging Database supports the same high availability features as the Site Configuration Database.

Access to Configuration Logging is controlled through Delegated Administration, with the Edit Logging Preferences and View Configuration Logs permissions.

Configuration logs are localized when they are created. For example, a log created in English is read in English, regardless of the locale of the reader.

What is logged

Configuration changes and administrative activities initiated from Studio, Director, and PowerShell scripts are logged. 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 Studio

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Studio or Director sending a message to a user

The following operations are not logged:

- Autonomic 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, direct access of the database, or from sources other than Studio, Director, or PowerShell.
- When the deployment is initialized, Configuration Logging becomes available when the first Configuration Logging Service instance registers with the Configuration Service. Therefore, the very early stages of configuration are not logged (for example, when the database schema is obtained and applied, when a hypervisor is initialized).

Manage Configuration Logging

By default, Configuration Logging uses the database that is created when you create a Site (also known as the Site Configuration database). Citrix recommends that you use a separate location for the Configuration Logging database (and the Monitoring database) for the following reasons:

- The backup strategy for the Configuration Logging database is likely to differ from the backup strategy for the Site Configuration database.
- The volume of data collected for Configuration Logging (and the Monitoring Service) might adversely affect the space available to the Site Configuration database.
- It splits the single point of failure for the three databases.

Product editions that do not support Configuration Logging do not have a Logging node in Studio.

Enable and disable Configuration Logging and mandatory logging

By default, Configuration Logging is enabled, and mandatory logging is disabled.

1. Select **Logging** in the Studio navigation pane.
2. Select **Preferences** in the Actions pane. The Configuration Logging dialog box contains database information and indicates whether Configuration Logging and mandatory logging are enabled or disabled.
3. Select the desired action:

   To enable Configuration Logging, select **Enable**. This is the default setting. If the database cannot be written to, the logging information is discarded, but the operation continues.

   To disable Configuration Logging, select **Disable**. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.

   To enable mandatory logging, select **Prevent changes to the site configuration when the database is not available**. No configuration change or administrative activity that is normally logged is allowed unless it can be written in the Configuration Logging database. You can enable mandatory logging only when Configuration Logging is enabled (when **Enable** is selected). If the Configuration Logging Service fails, and high availability is not in use, mandatory logging is assumed. In such cases, operations that would normally be logged are not performed.

   To disable mandatory logging, select **Allow changes when to the site configuration when the database is not available**. Configuration changes and administrative activities are allowed, even if the Configuration Logging database cannot be accessed. This is the default setting.

Change the Configuration Logging database location

You cannot change the database location when mandatory logging is enabled, because the location change includes a brief disconnect interval that cannot be logged.

1. Create a database server, using a supported SQL Server version.
2. Select **Logging** in the Studio navigation pane.
3. Select **Preferences** in the Actions pane.
4. In the Logging Preferences dialog box, select **Change logging database**.
5. In the Change Logging Database dialog box, specify the location of the server containing the new database server. See Database address formats for valid formats.
6. To allow Studio to create the database, click **OK**. When prompted, click **OK**, and the database is created automatically. Studio attempts to access the database using the current Studio user's credentials. If that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. (The credentials are retained only during database creation.)

7. To create the database manually, click **Generate database script**. The generated script includes instructions for manually creating the database. Ensure that the database is empty and that at least one user has permission to access and change the database before uploading the schema.

The Configuration Logging data in the previous database is not imported to the new database. Logs cannot be aggregated from both databases when retrieving logs. The first log entry in the new Configuration Logging database indicates that a database change occurred, but it does not identify the previous database.

Display configuration log content

When initiating configuration changes and administrative activities, the high level operations created by Studio and Director are listed in the upper middle pane in Studio. A high level operation results in one or more service and SDK calls, which are low level operations. When you select a high level operation in the upper pane, the lower pane displays the low level operations.

If an operation fails before completion, the log operation might not be completed in the database. For example, a start record will have 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 all logs for the last five days are requested and a log exists with a start time in the last five days but has no end time, it is included.

When using a script that calls PowerShell cmdlets, if you create a low level operation without specifying a parent high level operation, Configuration Logging creates a surrogate high level operation.

To display configuration log content, select **Logging** in the Studio navigation pane. By default, the center pane lists the log content chronologically (newest entries first), separated by date. You can:

- Sort the display by column heading.
- Filter the display by specifying a day interval, or entering text in the **Search** box. To return to the standard display after using search, clear the text in the **Search** box.

Generate reports

You can generate CSV and HTML reports containing configuration log data.

- The CSV report contains all the logging data from a specified time interval. The hierarchical data in the database is flattened into a single CSV table. No aspect of the data has precedence in the file. No formatting is used and no human readability is assumed. The file (named MyReport) contains the data in a universally consumable format. CSV files are often used for archiving data or as a data source for a reporting or data manipulation tool such as Microsoft Excel.

- The HTML report provides a human-readable form of the logging data for a specified time interval. It provides a structured, navigable view for reviewing changes. An HTML report comprises two files, named Summary and Details. Summary lists high level operations: when each operation occurred, by whom, and the outcome. Clicking a Details link next to each operation takes you to the low level operations in the Details file, which provides additional information.

To generate a configuration log report, select **Logging** in the Studio navigation pane, and then select **Create custom report** in the Actions pane.

- Select the date range for the report.
- Select the report format: CSV, HTML, or both.
- Browse to the location where the report should be saved.

Delete configuration log content

To delete the configuration log, you must have certain Delegated Administration and SQL Server database permissions.

- **Delegated Administration:** You must have a Delegated Administration role that allows the deployment configuration to be read. The Full administrator role has this permission. A custom role must have Read Only or Manage selected in the Other permissions category.

  To create a backup of the configuration logging data before deleting it, the custom role must also have Read Only or Manage selected in the Logging Permissions category.

- **SQL Server database:** You must have a SQL server login with permission to delete records from the database. There are two ways to do this:

  - Use a SQL Server database login with a sysadmin server role, which allows you to perform any activity on the database server. Alternatively, the serveradmin or setupadmin server roles allow you to perform deletion operations.
  - If your deployment requires additional security, use a non-sysadmin database login mapped to a database user who has permission to delete records from the database.

    1. In SQL Server Management Studio, create a SQL Server login with a server role other than 'sysadmin.'
    2. Map the login to a user in the database. SQL Server automatically creates a user in the database with the same name as the login.
    3. In Database role membership, specify at least one of the role members for the database user: ConfigurationLoggingSchema_ROLE or dbowner.

    For more information, see the SQL Server Management Studio documentation.

To delete the configuration logs:

1. Select **Logging** in the Studio navigation pane.
2. Select **Delete logs** in the Actions pane.
3. You are asked if you want to create a backup of the logs before they are deleted. If you choose to create a backup, browse to the location where the backup archive is saved. The backup is created as a CSV file.

After the configuration logs are cleared, the log deletion is the first activity posted to the empty log. That entry provides details about who deleted the logs, and when.

Event logs

March 4, 2021

The following articles list and describe events that can be logged by services within Citrix Virtual Apps and Desktops.

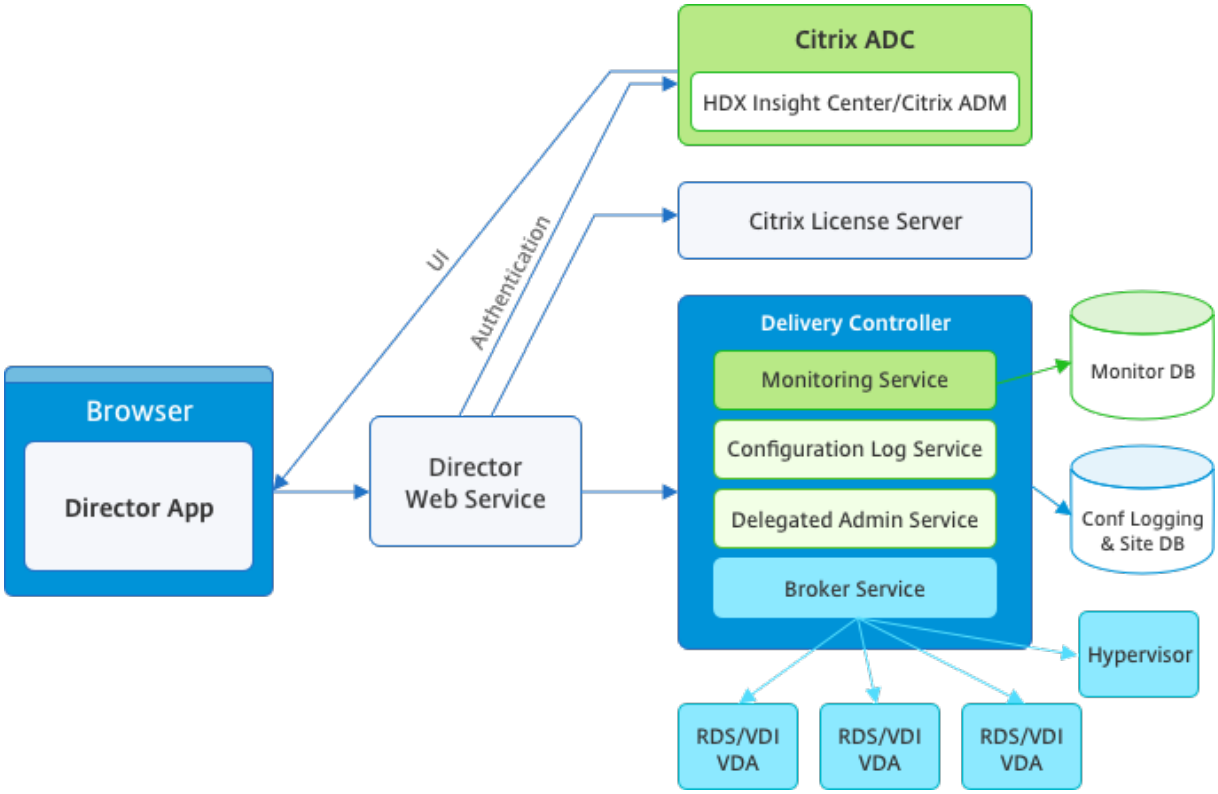
This information is not comprehensive. Readers should check individual feature articles for additional event information.

- Citrix Broker Service events
- Citrix FMA Service SDK events
- Citrix Configuration Service events
- Citrix Delegated Administration Service events

Director

April 19, 2024

Director is a monitoring and troubleshooting console for Citrix Virtual Apps and Desktops.



Director can access:

- Real-time data from the Broker Agent using a unified console integrated with Analytics, Performance Manager, and Network Inspector.
  - Analytics includes performance management for health and capacity assurance, and historical trending and network analysis, powered by Citrix ADM, to identify bottlenecks due to the network in your Citrix Virtual Apps or Desktops environment.
- Historical data stored in the Monitor database to access the Configuration Logging database.
- ICA data from the Citrix Gateway using Citrix ADM.
  - Gain visibility into the end-user experience for virtual applications, desktops, and users for Citrix Virtual Apps or Desktops.
  - Correlate network data with application data and real-time metrics for effective troubleshooting.
  - Integrate with Citrix Virtual Desktop 7 Director monitoring tool.

Director uses a troubleshooting dashboard that provides real-time and historical health monitoring of the Citrix Virtual Apps or Desktops Site. This feature allows you to see failures in real time, providing a better idea of what the end users are experiencing.

For more information regarding the compatibility of Director features with Delivery Controller (DC), VDA and any other dependent components, see Feature compatibility matrix.

> Note:
>
> With the disclosure of the Meltdown and Spectre speculative execution side-channel vulnerabilities, Citrix recommends that you install relevant mitigation patches. Note that these patches might impact SQL Server performance. For more information, see the Microsoft support article, Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities. Citrix recommends that you test the scale and plan your workloads before rolling out the patches in your production environments.

Director is installed by default as a website on the Delivery Controller. For prerequisites and other details, see the System requirements documentation for this release. For specific information on the installation and configuration of Director, see Install and configure Director.

Log on to Director

The Director website is located at https or `http://<Server FQDN>/Director`.

If one of the Sites in a multi-site deployment is down, the logon for Director takes a little longer while it attempts to connect to the Site that is down.

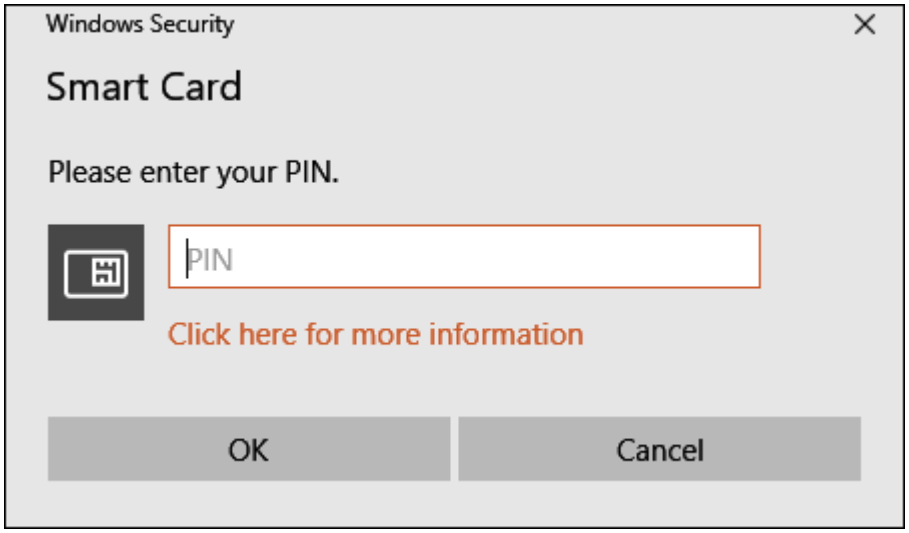
Use Director with PIV smart card authentication

Director now supports Personal Identity Verification (PIV) based smart card authentication to log on. This feature is useful for organizations and government agencies that use smart card based authentication for access control.
Smart card authentication requires specific configuration on the Director server and in Active Directory. The configuration steps are detailed in Configure PIV smart card authentication.

> Note:
>
> Smart card authentication is supported only for users from the same Active Directory domain.

After performing the required configuration, you can log on to Director using a smart card:

1. Insert your smart card into the smart card reader.
2. Open a browser and go to the Director URL, `https://<directorfqdn>/Director`.
3. Select a valid user certificate from the displayed list.
4. Enter your smart card token.



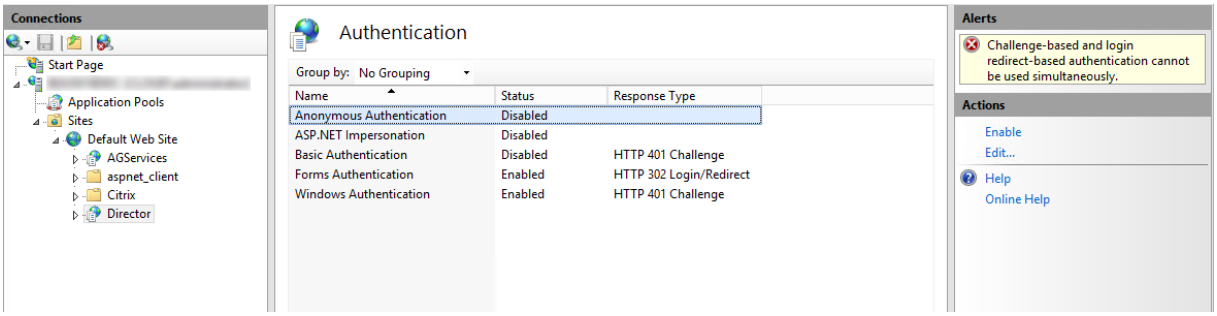
5. After you are authenticated, you can access Director without keying additional credentials on the Director logon page.

Use Director with Integrated Windows Authentication

With Integrated Windows Authentication(IWA), domain-joined users gain direct access to Director without rekeying their credentials on the Director logon page. The prerequisites for working with Integrated Windows Authentication and Director are:

- Enable Integrated Windows Authentication on the IIS website that hosts Director. When you install Director, Anonymous and Forms Authentication are enabled. To work with Integrated Windows Authentication and Director, disable Anonymous Authentication and enable Windows Authentication. Forms Authentication must remain set to Enabled for authentication of non-domain users.

    1. Start IIS manager.
    2. Go to **Sites** > **Default Web Site** > **Director**.
    3. Select **Authentication**.
    4. Right-click **Anonymous Authentication**, and select **Disable**.
    5. Right-click **Windows Authentication**, and select **Enable**.



- Configure Active Directory delegation permission for the Director machine. This is only required if Director and the Delivery Controller are installed on separate machines.

  1. On the Active Directory machine, open the Active Directory Management Console.
  2. In the Active Directory Management Console navigate to **Domain Name** > **Computers.** Select the Director machine.
  3. Right-click and select **Properties**.
  4. In Properties, select the **Delegation** tab.
  5. Select the option, **Trust this computer for delegation to any service (Kerberos only)**.

- The browser that is used to access Director must support Integrated Windows Authentication. This might require additional configuration steps in Firefox and Chrome. For more information, refer to the browser documentation.
- The Monitoring Service must be running Microsoft .NET Framework 4.5.1 or a later supported version listed in the System Requirements for Director. For more information, see System Requirements.

When a user logs off Director or if the session times out, the logon page is displayed. From the logon page, the user can set the Authentication type to **Automatic logon** or **User credentials**.

Interface views

Director provides different views of the interface tailored to particular administrators. Product permissions determine what is displayed and the commands available.

For example, help desk administrators see an interface tailored to help desk tasks. Director allows help desk administrators to search for the user reporting an issue and display activity associated with that user, such as the status of the user's applications and processes. They can resolve issues quickly by performing actions such as ending an unresponsive application or process, shadowing operations on the user's machine, restarting the machine, or resetting the user profile.

In contrast, full administrators see and manage the entire Site and can perform commands for multiple users and machines. The Dashboard provides an overview of the key aspects of a deployment, such as the status of sessions, user logons, and the Site infrastructure. Information is updated every minute. If issues occur, details appear automatically about the number and type of failures that have occurred.

For more information about the various roles and their permissions in Director, see Delegated Administration and Director

Usage data collection by Google Analytics

The Director Service starts using Google Analytics to collect usage data anonymously after Director is installed. Statistics regarding the usage of the Trends pages and OData API call analytics are collected. Analytics collection complies with the Citrix Privacy Policy. Data collection is enabled by default when you install Director.

To opt out of the Google Analytics data collection, edit the registry key, as described below on the machine where Director is installed. If the registry key doesn't already exist, create and set it to the desired value. Refresh the Director instance after changing the registry key value.
Caution: Using Registry Editor 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. Citrix recommends that you back up Windows Registry before changing it.

Location: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Name: DisableGoogleAnalytics

Value: 0 = enabled(default), 1 = disabled

You can use the following PowerShell cmdlet to disable data collection by Google Analytics:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
     DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

New features guide

Director has an in-product guide that uses Pendo to give an insight into the new features released in the current version of Director. The quick overview coupled with appropriate in-product messages helps you understand what's new in the product.

To opt out of this feature, edit the registry key, as described below on the machine where Director is installed. If the registry key doesn't already exist, create and set it to the desired value. Refresh the Director instance after changing the registry key value.

Caution: Using Registry Editor 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. Citrix recommends that you back up Windows Registry before changing it.

Location: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Name: DisableGuidedHelp

Value: 0 = enabled(default), 1 = disabled

You can use the following PowerShell cmdlet to disable the in-product guide:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

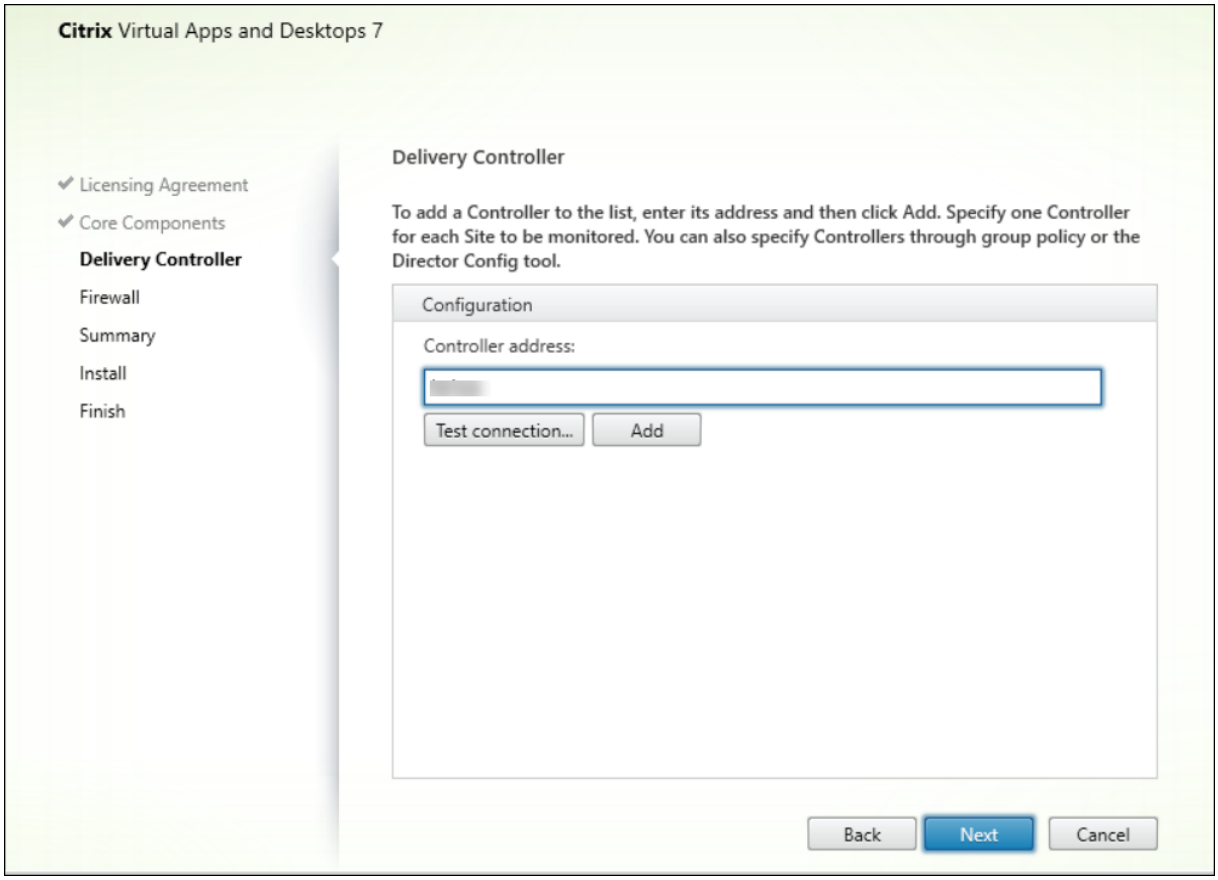
Install and configure

March 7, 2022

Install Director

Install Director using the full product ISO Installer for Citrix Virtual Apps and Desktops, which checks for prerequisites, installs any missing components, sets up the Director website, and performs basic configuration. For prerequisites and other details, see the System requirements documentation for this release. This release of Director is not compatible with Virtual Apps deployments earlier than 6.5 or Virtual Desktops deployments earlier than 7.
The default configuration provided by the ISO installer handles typical deployments. If Director was not included during installation, use the ISO installer to add Director. To add any additional components, rerun the ISO installer and select the components to install. For information on using the ISO installer, see Install core components in the installation documentation. Citrix recommends that you install using the full product ISO installer only, not the .MSI file.

When Director is installed on the Controller, it is automatically configured with localhost as the server address, and Director communicates with the local Controller by default. To install Director on a dedicated server that is remote from a Controller, you are prompted to enter the FQDN or IP address of a Controller.



> **Note:**
> Click **Add** to add the Controller to be monitored.

Director communicates with that specified Controller by default. Specify only one Controller address for each Site that you monitor. Director automatically discovers all other Controllers in the same Site and falls back to those other Controllers if the Controller you specified fails.

> **Note:**
> Director does not load balance among Controllers.

To secure the communications between the browser and the Web server, Citrix recommends that you implement TLS on the IIS website hosting Director. Refer to the Microsoft IIS documentation for instructions. Director configuration is not required to enable TLS.

Deploy and configure Director

When Director is used in an environment containing more than one Site, be sure to synchronize the system clocks on all the servers where Controllers, Director, and other core components are installed. Otherwise, the Sites might not display correctly in Director.

> Important:
>
> To protect the security of user names and passwords sent using plain text through the network, Citrix strongly recommends that you allow Director connections using only HTTPS, and not HTTP. Certain tools are able to read plain text user names and passwords in HTTP (unencrypted) network packets, which can create a potential security risk for users.

Configure permissions

To log on to Director, administrators with permissions for Director must be Active Directory domain users and must have the following rights:

- Read rights in all Active Directory forests to be searched (see Advanced configuration).
- Configured Delegated Administrator roles (see Delegated Administration and Director).
- To shadow users, administrators must be configured using a Microsoft group policy for Windows Remote Assistance. In addition:
  - When installing VDAs, ensure that the Windows Remote Assistance feature is enabled on all user devices (selected by default).
  - When you install Director on a server, ensure that Windows Remote Assistance is installed (selected by default). However, it is disabled on the server by default. The feature does not need to be enabled for Director to provide assistance to end users. Citrix recommends leaving the feature disabled to improve security on the server.
  - To enable administrators to initiate Windows Remote Assistance, grant them the required permissions by using the appropriate Microsoft Group Policy settings for Remote Assistance. For information, see CTX127388: How to Enable Remote Assistance for Desktop Director.

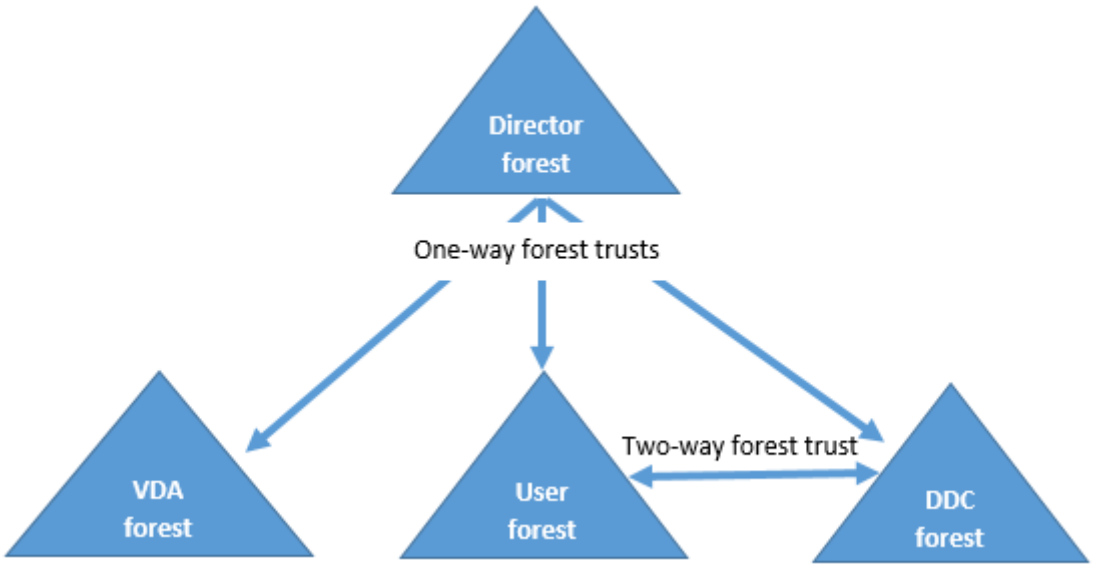
Advanced configuration

March 7, 2022

Director can support multi-forest environments spanning a forest configuration where users, Delivery Controllers (DCs), VDAs, and Directors are located in different forests. This requires proper setup of trust relationships among the forests and configuration settings.

Recommended configuration in a multi-forest environment

The recommended configuration requires creation of outgoing and incoming forest trust relationships among the forests with domain-wide authentication.



The trust relationship from the Director enables you to troubleshoot issues in user sessions, VDAs, and Delivery Controllers located in different forests.

Advanced configuration required for Director to support multiple forests is controlled through settings defined in Internet Information Services (IIS) Manager.

> Important:
>
> When you change a setting in IIS, the Director service automatically restarts and logs off users.

To configure advanced settings using IIS:

1. Open the Internet Information Services (IIS) Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Double-click a setting to edit it.
5. Click **Add** to add a new setting.

Director uses Active Directory to search for users and to look up additional user and machine information. By default, Director searches the domain or forest in which:

- The administrator's account is a member.
- The Director web server is a member (if different).

Director attempts to perform searches at the forest level using the Active Directory global catalog. If you do not have permissions to search at the forest level, only the domain is searched.

Searching or looking up data from another Active Directory domain or forest requires that you explicitly set the domains or forests to be searched. Configure the following Applications setting to the Director website in IIS Manager:


```
Connector.ActiveDirectory.Domains = (user),(server)
```

The value attributes user and server represent the domains of the Director user (the administrator) and Director server, respectively.

To enable searches from an additional domain or forest, add the name of the domain to the list, as shown in this example:

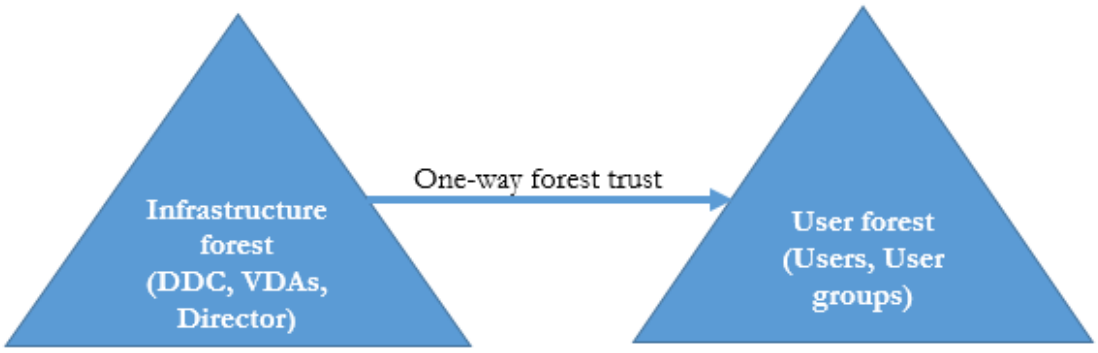
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

For each domain in the list, Director attempts to perform searches at the forest level. If you do not have permissions to search at the forest level, only the domain is searched.

Domain local group configuration

Most Citrix Service Providers (CSPs) have similar environment set-ups consisting of the VDAs, DC(s), and Director in what we can call the Infrastructure forest while the users or user-group records belong to the Customer forest. A one-way outgoing trust exists from the Infrastructure forest to the Customer forest.

CSP administrators typically create a domain local group in the Infrastructure forest and add the users or user groups in the Customer forest to this domain local group.



Director can support a multi-forest set-up like this and monitor the sessions of users configured using domain local groups.

1. Add the following Applications settings to the Director website in IIS Manager:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true Connector.
       ActiveDirectory

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   <domain1><domain2> are names of the forests in which the domain local group exists.

2. Assign the domain local group to Delivery Groups in Citrix Studio.
3. Restart IIS and log on to Director again for the changes to take effect. Now, Director can monitor and show the sessions of these users.

Add Sites to Director

If Director is already installed, configure it to work with multiple Sites. To do this, use the IIS Manager Console on each Director server to update the list of server addresses in the application settings.

Add an address of a Controller from each Site to the following setting:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
<!--NeedCopy-->
```

where SiteAController and SiteBController are the addresses of Delivery Controllers from two different Sites.

Disable the visibility of running applications in the Activity Manager

By default, the Activity Manager in Director 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 in Director. For Delegated Administrator roles, this includes Full Administrator, Delivery Group Administrator, and Help Desk Administrator.

To protect the privacy of users and the applications they are running, you can disable the Applications tab to list running applications.

> 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.

1. On the VDA, modify the registry key located at HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManager
   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.
2. On the server with Director installed, modify the setting that controls the visibility of running applications. By default, the value is "true", which allows visibility of running applications in the Applications tab. Change the value to "false", which disables visibility. This option affects only the Activity Manager in Director, not the VDA.
   Modify the value of the following setting:
   UI.TaskManager.EnableApplications = false

> Important:
>
> To disable the view of running applications, Citrix recommends making both changes to ensure that the data is not displayed in Activity Manager.

Configure PIV smart card authentication

November 30, 2020

This article lists the configuration required on the Director Server and in Active Directory to enable the smart card authentication feature.

> Note:
> Smart card authentication is supported only for users from the same Active Directory domain.

Director server configuration

Perform the following configuration steps on the Director server:

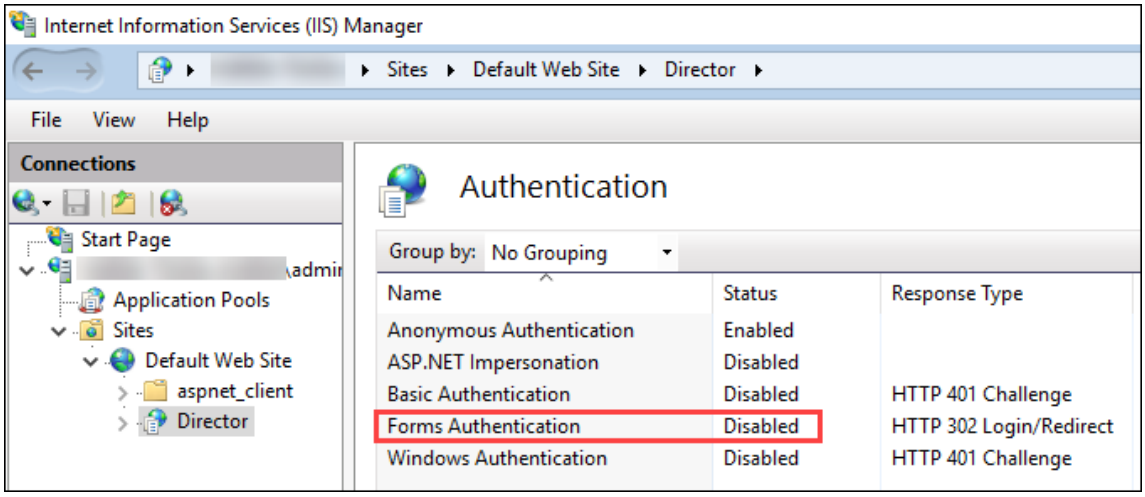
1. Install and enable the Client Certificate Mapping Authentication. Follow the **Client Certificate Mapping authentication using Active Directory** instructions in the Microsoft document, Client Certificate Mapping Authentication.
2. Disable Forms Authentication on the Director site.

   Start IIS Manager.

   Go to **Sites** > **Default Web Site** > **Director**.

   Select **Authentication**.

   Right-click **Forms Authentication**, and select **Disable.**



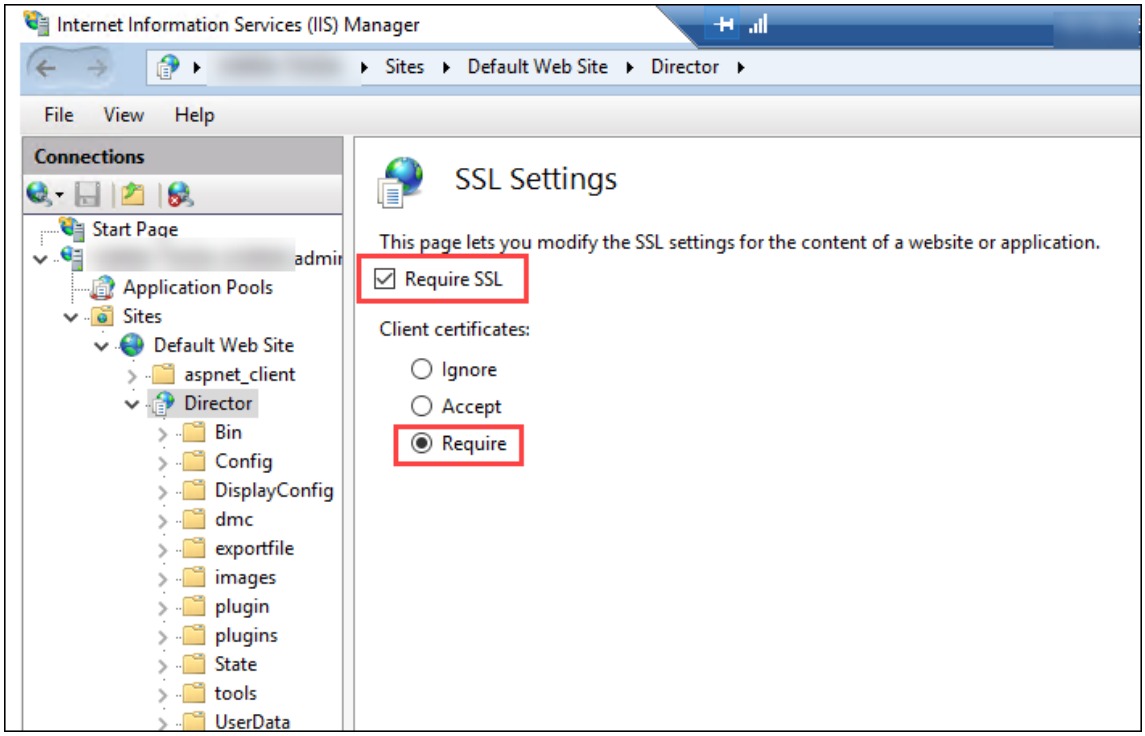
3. Configure the Director URL for the more secure https protocol (instead of http) for client certificate authentication.

   a) Start IIS Manager.

   b) Go to **Sites** > **Default Web Site** > **Director**.

   c) Select **SSL Settings.**

   d) Select **Require SSL** and **Client certificates** > **Require.**



4. Update web.config. Open the web.config file (available in c:\inetpub\wwwroot\Director) using a text editor.

Under the <system.webServer> parent element, add the following snippet as the first child element:

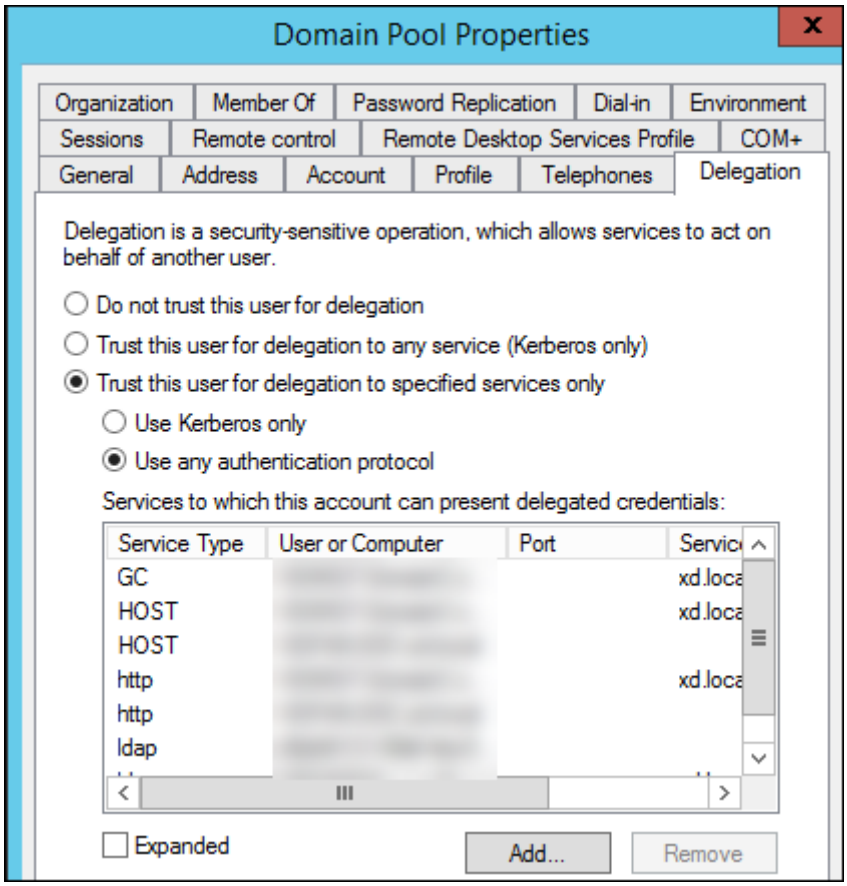
```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

Active Directory configuration

By default, Director application runs with the **Application Pool** identity property. Smart card authentication requires delegation for which the Director application identity must have Trusted Computing Base (TCB) privileges on the service host.

Citrix recommends that, you create a separate service account for Application Pool identity. Create the service account and assign TCB privileges as per the instructions in the Microsoft article, Protocol Transition with Constrained Delegation Technical Supplement.

Assign the newly created service account to the Director application pool. The following figure shows the properties dialog of a sample service account, Domain Pool.

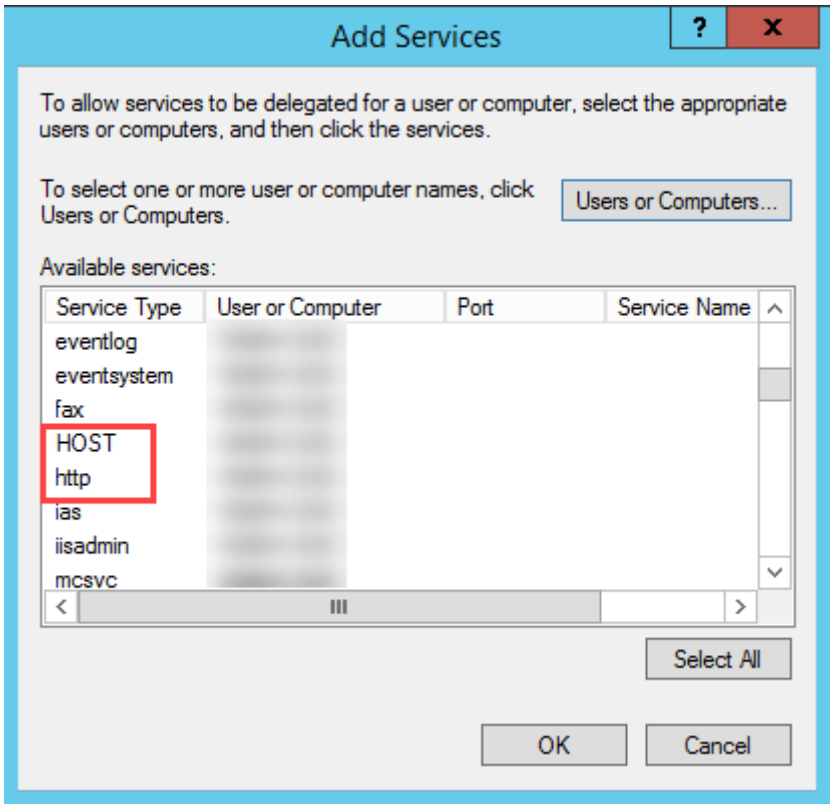


Configure the following services for this account:

- Delivery Controller: HOST, http
- Director: HOST, http
- Active Directory: GC, LDAP

To do this,

1. In the user account properties dialog, click **Add.**
2. In the **Add Services** dialog, click Users or Computers.
3. Select the Delivery Controller hostname.
4. From the **Available services** list, select HOST and http **Service Type**.



Similarly, add Service Types for **Director** and **Active Directory** hosts.

Firefox browser configuration

To use the Firefox browser, install the PIV driver available at OpenSC 0.17.0. For installation and configuration instructions, see Installing OpenSC PKCS#11 Module in Firefox, Step by Step.
For information on the usage of the smart card authentication feature in Director, see the Use Director with PIV based smart card authentication section in the Director article.

Configure network analysis

September 30, 2022

> **Note:**
> The availability of this feature depends on your organization's license and your administrator permissions.

Director integrates with Citrix ADM to provide network analysis and performance management:

- Network analysis leverages HDX Insight reports from Citrix ADM to provide an application and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.
- Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you enable this feature in Director, HDX Insight reports provide Director with additional information:

- The Network tab in the Trends page shows latency and bandwidth effects for applications, desktops, and users across your entire deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

Limitations:

- In the Trends view, HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

To enable network analysis, you must install and configure Citrix ADM in Director. Director requires Citrix ADM Version 11.1 Build 49.16 or later. MAS is a virtual appliance that run on the Citrix XenServer. Using network analysis, Director communicates and gathers the information that is related to your deployment.

For more information, see the Citrix ADM documentation.

> **Note:**
> Citrix NetScaler Insight Center has reached its End of Maintenance date as of 15th May 2018. See the Citrix Product Matrix. Integrate Director with Citrix ADM for network analysis. To migrate your NetScaler Insight Center to Citrix ADM, see Migrate from NetScaler Insight Center to Citrix ADM.

1. On the server where Director is installed, locate the DirectorConfig command line tool in C:\inetpub\wwwroot\Director\tools, and run it with parameter /configNetScaler from a command prompt.

2. When prompted, enter the Citrix ADM machine name (FQDN or IP address), the username, password, HTTPS connection type (preferred over HTTP), and choose Citrix ADM integration.
3. To verify the changes, log off and log back on.

> **Note:**
>
> For security reasons, it is recommended to create a custom role for ADM integration with Director with sufficient permission to access HDX Insight only.
>
> For more information, see Configure access policies.

Delegated Administration and Director

February 7, 2020

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.

For information about creating delegated administrators, see the main Delegated Administration article.

Administrative permissions determine the Director 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.

The built-in roles and permissions also determine how administrators use Director:

Administrator Role	Permissions in Director
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.

Administrator Role	Permissions in Director
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 as well as 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 Director and cannot view data.

Configure custom roles for Director administrators

In Studio, you can also configure Director-specific, custom roles to more closely match the requirements of your organization and delegate permissions more flexibly. For example, you can restrict the built-in Help Desk administrator role so that this administrator cannot log off sessions.

If you create a custom role with Director permissions, you must also give that role other generic permissions:

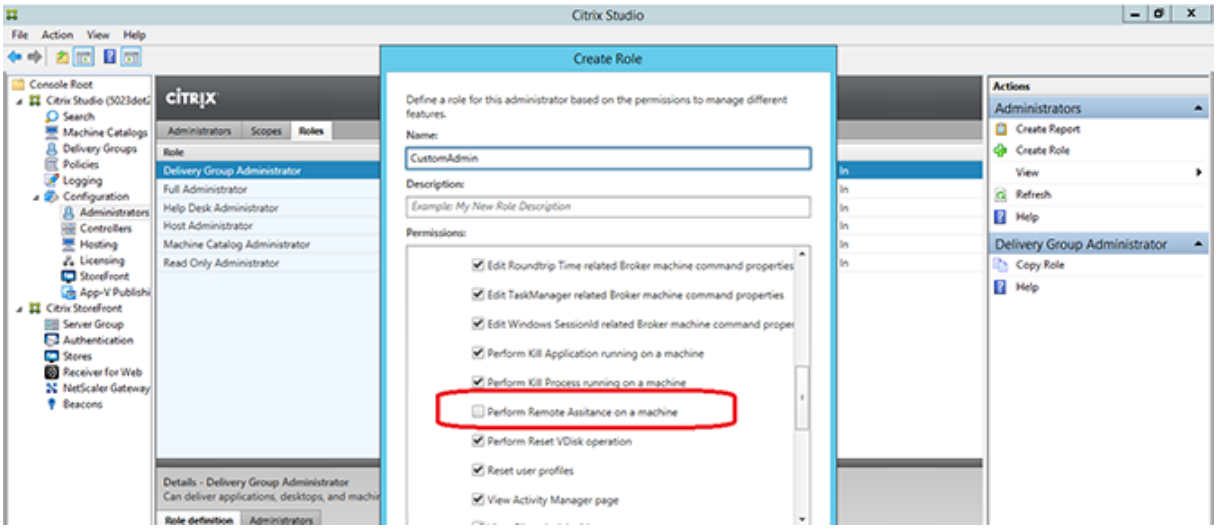
- Delivery Controller permission to log on to Director - at least read only access in Administrator node
- Permissions to Delivery Groups to view the data related to those Delivery Groups in Director - at least read only access

Alternatively, you can create a custom role by copying an existing role and include additional permissions for different views. For example, you can copy the Help Desk role and include permissions to view the Dashboard or Filters pages.

Select the Director permissions for the custom role, which include:

- Perform Kill Application running on a machine
- Perform Kill Process running on a machine
- Perform Remote Assistance on a machine
- Perform Reset vDisk operation
- Reset user profiles
- View Client Details page
- View Dashboard page
- View Filters page
- View Machine Details page
- View Trends page
- View User Details page

In this example, Shadowing (Perform Remote Assistance on a machine) is turned off.



A permission can have dependencies on other permissions to become applicable on the UI. For example, selecting the **Perform Kill Application running on a machine** permission enables the **End Application** functionality only in those panels to which the role has permission. You can select the following panel permissions:

- View Filters page
- View User Details page
- View Machine Details page
- View Client Details page

In addition, from the list of permissions for other components, consider these permissions from Delivery Groups:

- Enable/disable maintenance mode of a machine using Delivery Group membership.
- Perform power operations on Windows Desktop machines using Delivery Group membership.
- Perform session management on machines using Delivery Group membership.

Secure Director deployment

January 10, 2022

This article highlights areas that might have an impact on system security when deploying and configuring Director.

Configure Microsoft Internet Information Services (IIS)

You can configure Director with a restricted IIS configuration. Note that this is not the default IIS configuration.

Application Pool recycling limits

You can set the following Application Pool recycling limits:

- Virtual Memory Limit: 4,294,967,295
- Private Memory Limit: The size of the physical memory of the StoreFront server
- Request Limit: 4,000,000,000

Filename extensions

You can disallow unlisted file name extensions.

Director requires these file name extensions in Request Filtering:

- .aspx
- .css
- .html
- .js
- .png
- .svc

- .woff
- .woff2
- .png
- .eot
- .svg
- .ttf
- .json
- . (for redirections)

Director requires the following HTTP verbs in Request Filtering. You can disallow unlisted verbs.

- GET
- POST
- HEAD

Director does not require:

- ISAPI filters
- ISAPI extensions
- CGI programs
- FastCGI programs

> Important:
>
> - Director requires Full Trust. Do not set the global .NET trust level to High or lower.
> - Director maintains a separate application pool. To modify the Director settings, select the Director Site and modify.

Configure user rights

When Director is installed, its application pools are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. This is normal installation behavior when application pools are created.

You do not need to change these user rights. These privileges are not used by Director and are automatically disabled.

Director communications

In a production environment, Citrix recommends using the Internet Protocol security (IPsec) or HTTPS protocols to secure data passing between Director and your servers. IPsec is a set of standard extensions to the Internet Protocol that provides authenticated and encrypted communications with data

integrity and replay protection. Because IPsec is a network-layer protocol set, higher level protocols can use it without modification. HTTPS uses the Transport Layer Security (TLS) protocols to provide strong data encryption.

> Note:
>
> - Citrix strongly recommends that you do not enable unsecured connections to Director in a production environment.
> - Secure communications from Director requires configuration for each connection separately.
> - The SSL protocol is not recommended. Use the more secure TLS protocol instead.
> - You must secure communications with Citrix ADC using TLS, not IPsec.

To secure communications between Director and Citrix Virtual Apps and Desktops servers (for monitoring and reports), refer to Data Access Security.

To secure communications between Director and Citrix ADC (for Citrix Insight), refer to Configure network analysis.

To secure communications between Director and License server, refer to Secure the License Administration Console.

Director security separation

If you deploy any web applications in the same web domain (domain name and port) as Director, any security risks in those web applications could potentially reduce the security of your Director deployment. Where a greater degree of security separation is required, Citrix recommends that you deploy Director in a separate web domain.

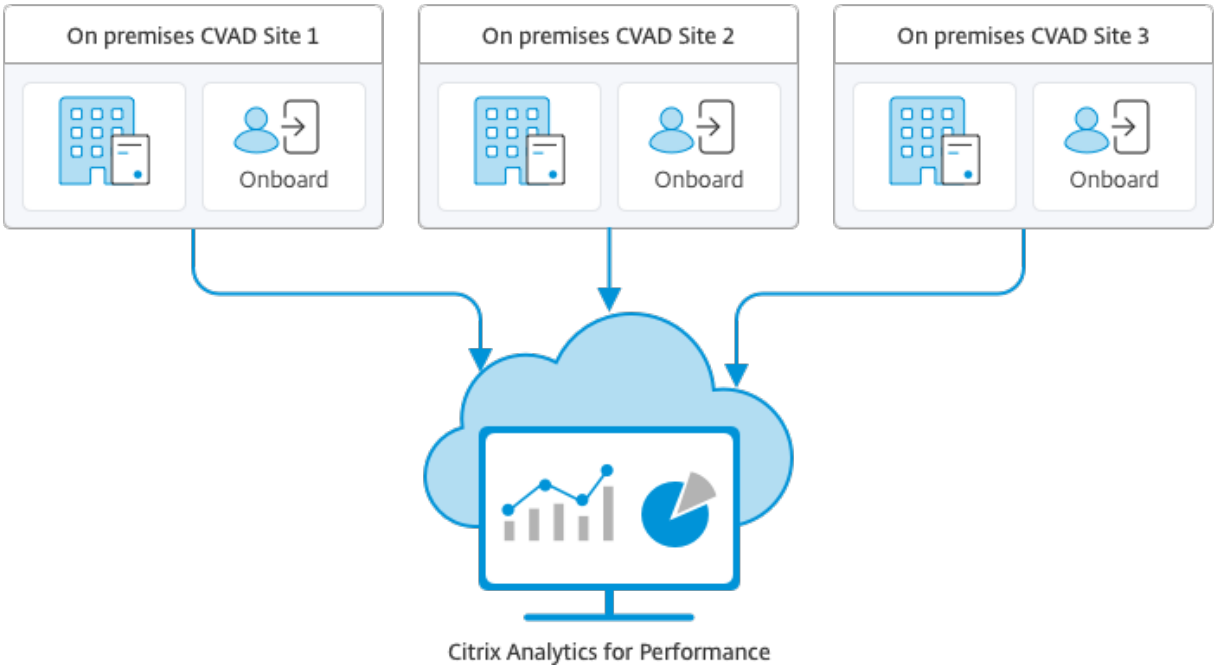
Configuring on-premises Sites with Citrix Analytics for Performance

May 27, 2024

Citrix Analytics for Performance (Performance Analytics) is the comprehensive performance monitoring solution from the Citrix Analytics Cloud Service. Performance analytics provides advanced insights and analytics built on performance metrics. Performance Analytics helps you monitor and view the usage and performance metrics of one or more Citrix Virtual Apps and Desktops Sites in your organization.

For more information about Performance Analytics, see the Performance Analytics article.

You can send performance data from your Site to Citrix Analytics for Performance on Citrix Cloud to leverage its advanced performance analytics capabilities. To view and use Performance Analytics, you must first configure your on-prem Sites with Citrix Analytics for Performance from the **Analytics** tab in **Director**. This feature requires Director on version 1909 or later, Delivery Controller and VDA on version 1906 or later.



Performance Analytics accesses data in a secure manner and no data is transferred from Citrix Cloud to the on-prem environment.

Prerequisites

To configure Citrix Analytics for Performance from Director, no new components need to be installed. Ensure that the following requirements are met:

- Your Delivery Controller and Director are on version 1912 CU2 or later. For more information, see Feature compatibility matrix.

> **Note:**
>
> - Configuring your on-premises site with Citrix Analytics for Performance from Director might fail if the Delivery Controller is running a Microsoft .NET Framework version earlier than 4.8. As a workaround, upgrade the .NET Framework in your Delivery Controller to version 4.8. LCM-9255.
> - When you configure your on-premises site running Citrix Virtual Apps and Desktops version 2012 with Citrix Analytics for Performance from Director, the configuration

> might fail after a couple of hours or after a restart of the Citrix Monitor Service in the Delivery Controller. The Analytics tab displays a Not Connected status in this case. As a workaround, create an Encryption folder in the registry on the Delivery Controller, Location: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor, Folder Name: Encryption. Ensure that the CitrixMonitor account has Full Control Access on the Encryption folder. Restart the Citrix Monitor Service.DIR-14324.

- Access to the **Analytics** tab to perform this configuration is available for full administrators only.
- For Performance Analytics to access performance metrics, outbound internet access is available on all Delivery Controllers and the machines on which Director is installed. Specifically, ensure accessibility to the following URLs:
  - Citrix Key Registration: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`
    In case, Delivery Controllers and Director machines are within an intranet and outbound internet access is via a proxy server, ensure the following:
- The proxy server must allow the preceding list of URLs.
- Add the following configuration in the Director web.config and citrix.monitor.exe.config files. Ensure that you add this configuration within the **configuration** tags:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>  -  The Director web.config is located at `C:\
    inetpub\wwwroot\Director\web.config` on the machine where
    Director is installed.  -  The citrix.monitor.exe.config is
    located at `C:\Program Files\Citrix\Monitor\Service\Citrix.
    Monitor.exe.Config` on the machine where the Delivery
    Controller is installed.
```

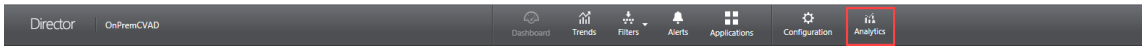
  This setting is provided by Microsoft on IIS. For more information, see `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.
  The **defaultproxy** field in the config file controls the outbound access of Director and Monitor Service. Configuration and communication with Performance Analytics requires the **defaultproxy** field to be set to **true**. It is possible that the policies in effect set this field to false. In this case, you must manually set the field to true. Take a backup of the config files before you make the changes. Restart the Monitoring service on the Delivery Controller for the changes to be affected.

- You have an active Citrix Cloud entitlement for Citrix Analytics for Performance.
- Your Citrix Cloud account is an Administrator account with rights to the Product Registration Experience. For more information about administrator permissions, see Modify Administrator Permissions.

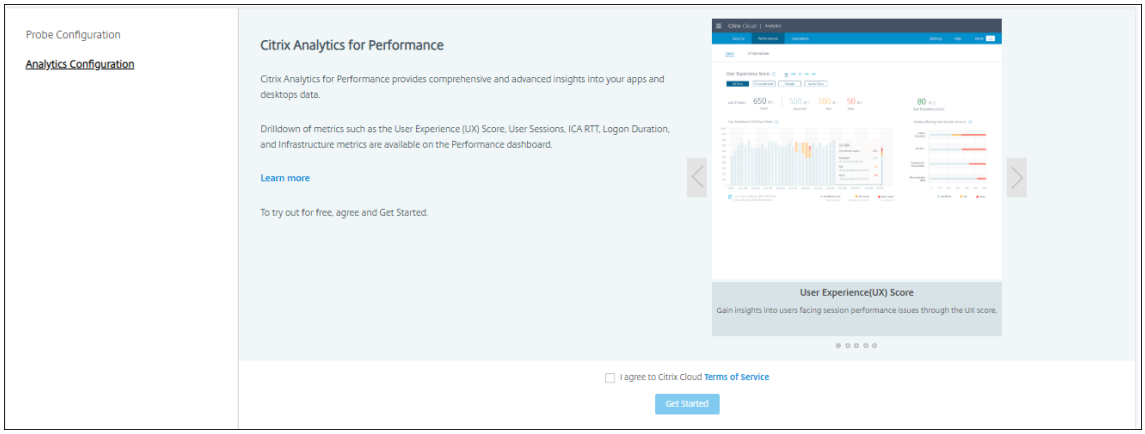
Configuration steps

After you have verified the prerequisites, do the following:

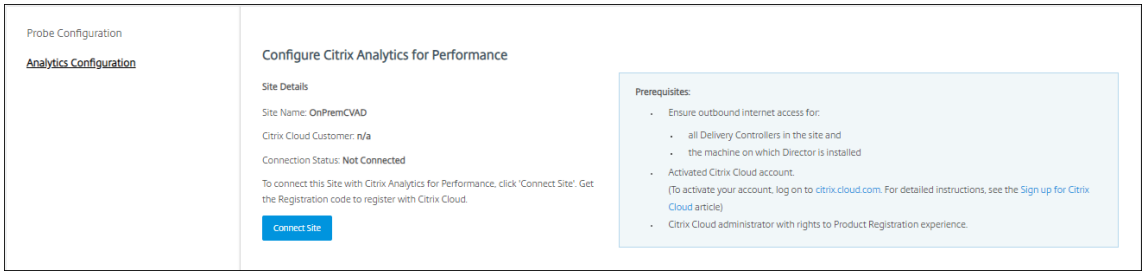
1. Log on to Director as a full administrator and select the Site which you want to configure with Performance Analytics.
2. Click the **Analytics** tab. The **Configuration** page is displayed.



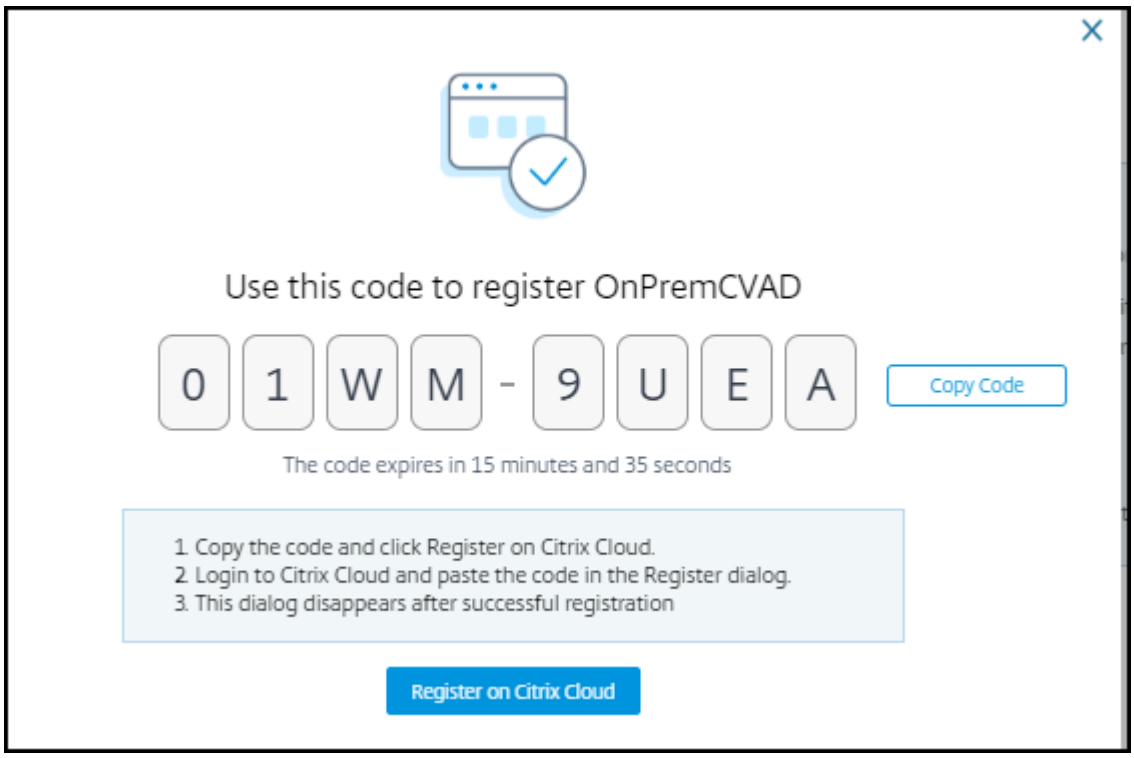
3. Review the steps, select the terms of service, and then click **Get Started**.



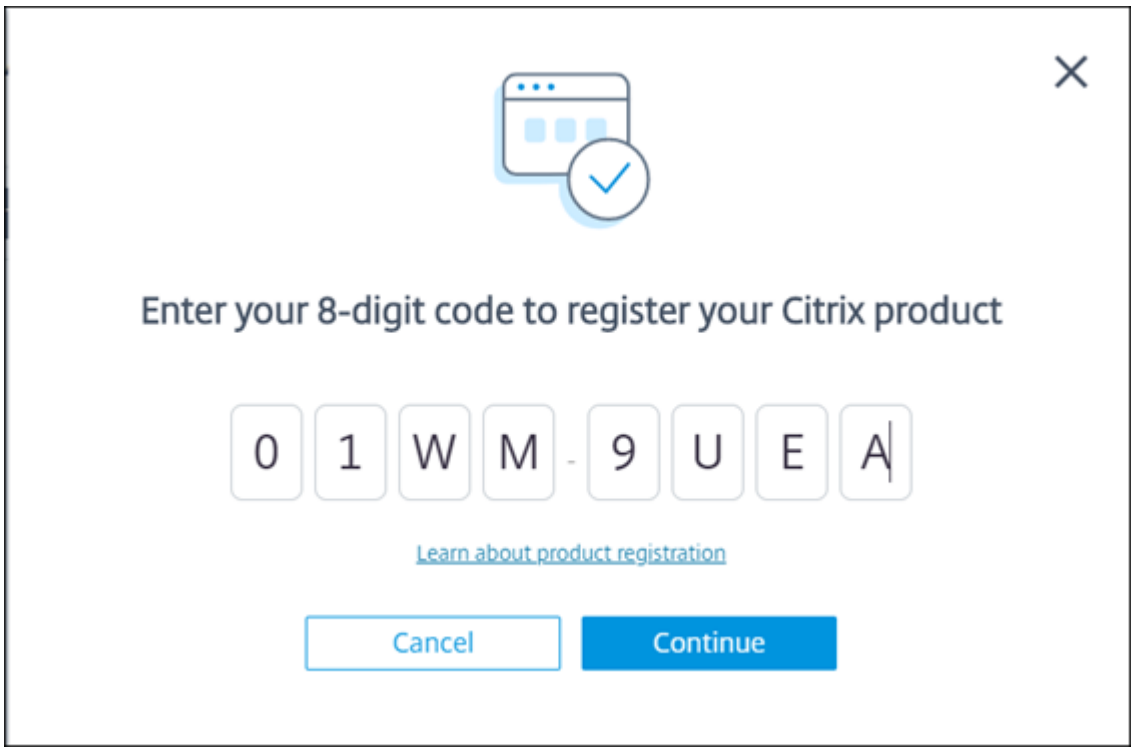
4. Review the prerequisites and ensure that they are met. Review the Site Details.
5. Click **Connect Site** to start the configuration process.



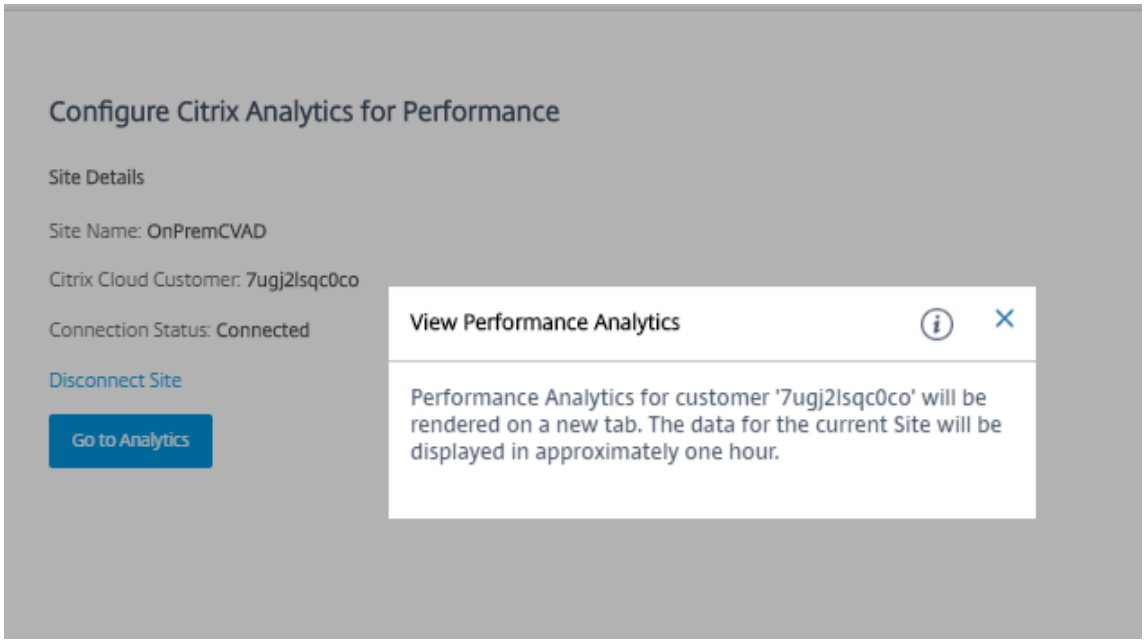
6. A unique 8-digit registration code is generated to be used to register this Site with Citrix Cloud.



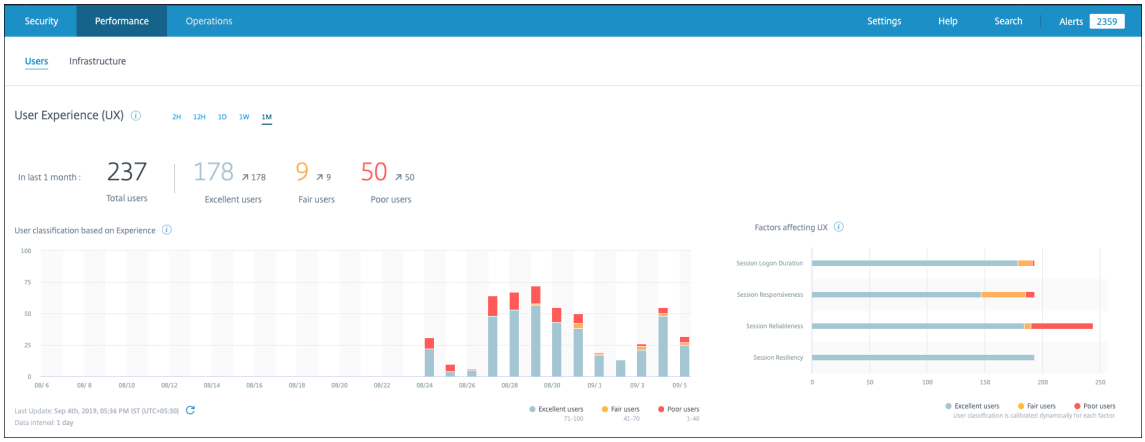
7. Click **Copy Code** to copy the code and then click **Register on Citrix Cloud**.
8. You are redirected to the Registration URL in Citrix Cloud. Log in with your Citrix Cloud credentials and select your customer.
9. Paste the copied registration code in the Product Registrations page in Citrix Cloud. Click **Continue** to register. Review the registration details and click **Register**.



10. Your on-prem Site registers with Citrix Cloud. Now, from **Director**, click **Go to Analytics** in the **Analytics** tab.



11. Performance Analytics is opened on a new tab in your browser.



If your Citrix Cloud session has expired, you might be redirected to the Citrix.com or My Citrix account logon page.

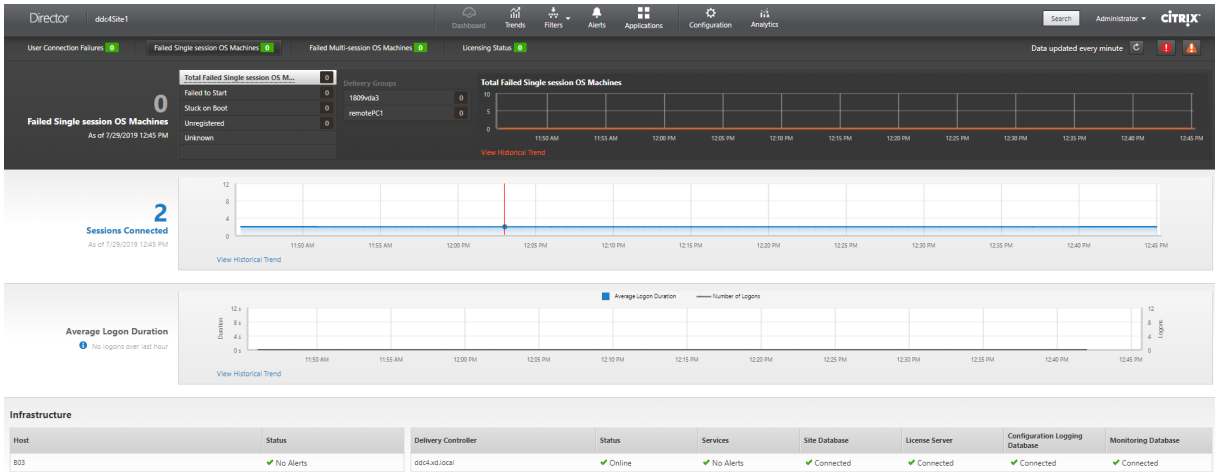
12. To register multiple Sites with Performance Analytics, repeat the preceding configuration steps for each Site from Director. Metrics for all configured Sites are displayed on the Performance Analytics dashboard.
13. To disconnect your Site from Citrix Cloud, click **Disconnect Site**. This option deletes the existing configuration.

> **Notes:**
>
> The first time you configure a Site, events from the Site might take some time (approximately an hour) to be processed; causing a delay in the display of metrics on the Performance Analytics dashboard. Thereafter, events refresh at regular intervals.
>
> Upon disconnect, data transmission from the old account continues for some time until the events from the new account are transmitted. For approximately one hour after data transmission stops, analytics related to the old account remain displayed on the Performance Analytics Dashboard.
>
> Upon expiry of entitlement to the Citrix Analytics service, it takes upto a day to stop sending the Site metrics to Performance Analytics.

Site Analytics

February 7, 2020

With full administrator permission, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a Site.



If there are currently no failures and no failures have occurred in the past 60 minutes, panels stay collapsed. When there are failures, the specific failure panel automatically appears.

> **Note:**
> Depending on your organization's license and your Administrator privileges, some options or features might not be available.

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 broken out by Delivery Groups. Connection failures includes 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 broken out by 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.

Panel	Description
Licensing Status	License Server alerts display alerts sent by the License Server and the actions required to resolve the alerts. Requires License Server Version 11.12.1 or later. Delivery Controller alerts display the details of the licensing state as seen by the Controller and are sent by the Controller. Requires Controller for XenApp 7.6 or XenDesktop 7.6 or later. You can set the threshold for alerts in Studio. Licensing status displayed in **Delivery Controllers** > **Details** > **Product Editions** > **PLT** indicates **Premium** and not **Platinum**.
Sessions Connected	Connected sessions across all Delivery Groups for the last 60 minutes.
Average Logon Duration	Logon data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Logon data for VDAs earlier than XenDesktop 7.0 is not included in this average. For more information, see Diagnose user logon issues.
Infrastructure	Lists your Site's infrastructure - hosts and Controllers. For infrastructure from Citrix Hypervisor or VMware, you can view performance alerts. For example, you can configure XenCenter to generate performance alerts when CPU, network I/O, or disk I/O usage go over a specified threshold on a managed server or virtual machine. By default, the alert repeat interval is 60 minutes, but you can configure this as well. For details, see the XenCenter Performance Alerts section in the Citrix Hypervisor product documentation.

> **Note:**
> If no icon appears for a particular metric, this indicates that this metric is not supported by the type of host you are using. 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 below):

- Control user machine power
- Prevent connections to machines

Monitor sessions

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.

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 and 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, where you can display graphical session data based on selected Delivery Groups and ranges and usage across Delivery Groups.
End idle sessions	The Sessions Filters view displays data related to all active sessions. Filter the sessions 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 of time	On the Trends view, select the **Sessions** tab to drill down to more specific usage data for connected and disconnected sessions over a longer period of time (that is, session totals from earlier than the last 60 minutes). To view this information, click **View historical trends**.

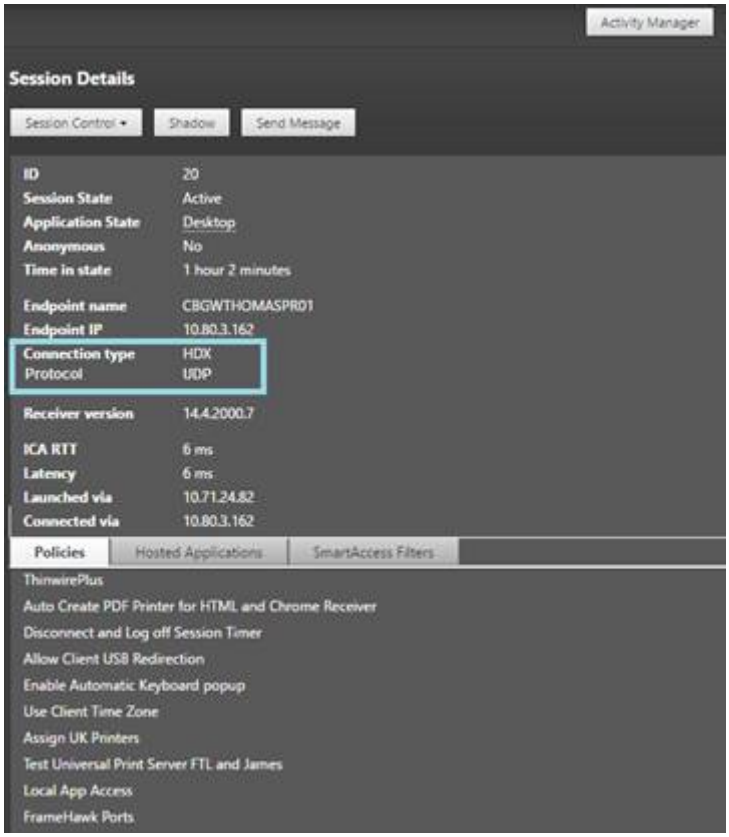
> **Note:**
> If the user device is running a legacy Virtual Delivery Agent (VDA), such as a VDA earlier than version 7, or a Linux VDA, Director cannot display complete information about the session. Instead, it displays a message that the information is not available.

Desktop Assignment Rules limitation:
Citrix Studio 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, Director 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 Director.
You can map the assigned desktop displayed in StoreFront to the Delivery Group name displayed in Director using 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
```

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.



- 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 cannot 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 contain trends represented as graphs and tables. CSV format reports contain tabular data that can be processed to generate views or can be archived.

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 name and format of the report.

Director generates the report based on the filter criteria 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 Director 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.

You can change the default limit by configuring the Director Application Settings in Internet Information Services (IIS).

Report format	Default number of records supported	Fields in Director Application Settings	Max number of records supported
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100,000	UI.ExportExcelDrilldownLimit	1,000,000
CSV	100,000 (10,000,000 in **Sessions** tab)	UI.ExportCsvDrilldownLimit	10,000,000

To change the limit of the number of records you can export:

1. Open the IIS Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Edit or add a setting for the fields UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLimit, or UI.ExportCsvDrilldownLimit as required.

Adding these field values in Application Settings overrides the default values.

> Warning:
>
> Setting field values greater than the max number of records supported can impact the performance of Export and is not supported.

Error Handling

This section gives you information on dealing with errors that you might encounter during Export operation.

- **Director has timed out**

This error could occur due to network issues or high resource usage on the Director server or with the Monitor Service.

The default timeout duration is 100 seconds. To increase the timeout duration of the Director Service, set the value of **Connector.DataServiceContext.Timeout field in** Director Application Settings in Internet Information Services (IIS):

1. Open the IIS Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Edit the value **Connector.DataServiceContext.Timeout**.

- **Monitor has timed out**

This error could occur due to network issues or high resource usage with the Monitor Service or on the SQL server.

To increase the timeout duration of the Monitor Service, run the following PowerShell commands on the Delivery Controller:

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Max concurrent Export or Preview operations ongoing**

Director supports one instance of Export or Preview. If you get the **Max concurrent Export or Preview operations ongoing** error, try the next Export operation again later.

It is possible to increase the number of concurrent Export or Preview operations, however this can impact the performance of Director and is not supported:

1. Open the IIS Manager console.

2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Edit the value **UI.ConcurrentExportLimit**.

- **Insufficient disk space in Director**

Each Export operation requires a maximum of 2 GB hard disk space in the Windows Temp folder. Retry Export after clearing space or adding more hard disk space on the Director server.

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 Director, 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 is not 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 Director as "failed to start,"and use this command to restart them.
Force Restart	Restarts the VM without first performing 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.

Command	Function
Force Shutdown	Shuts down the VM without first performing 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.
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 as soon as all users are logged off. For users who do not log off, send a message informing them that machines will be shut down at a certain time, and 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 indicating that the desktop is currently unavailable. No new connections can be made until you disable maintenance mode.

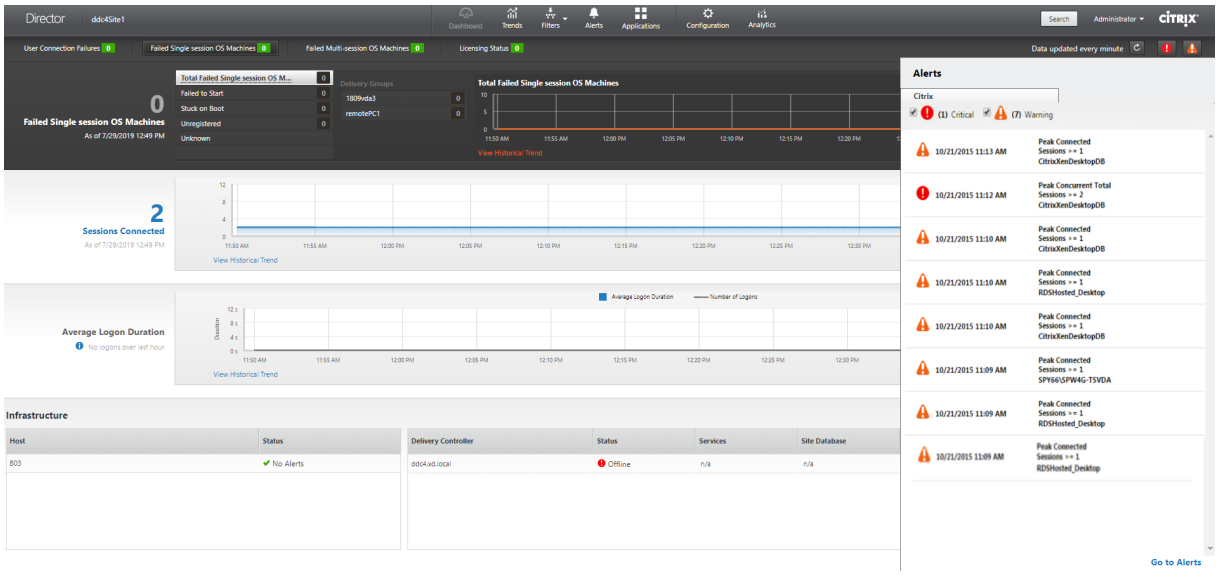
Application Analytics

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 probe results, number of instances per application, and faults and errors associated with the published applications. For more information, see the Application Analytics section in **Troubleshooting Applications**.

Alerts and notifications

August 16, 2022

Alerts are displayed in Director on the dashboard and other high level views with warning and critical alert symbols. Alerts are available for **Premium** licensed Sites. Alerts update automatically every minute; you can also update alerts on demand.



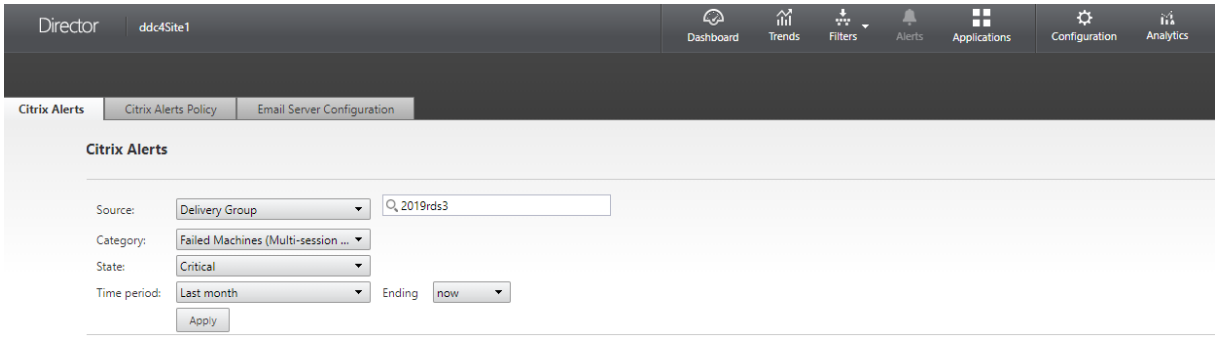
A warning alert (amber triangle) indicates that the warning threshold of a condition has been reached or exceeded.

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 Director 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

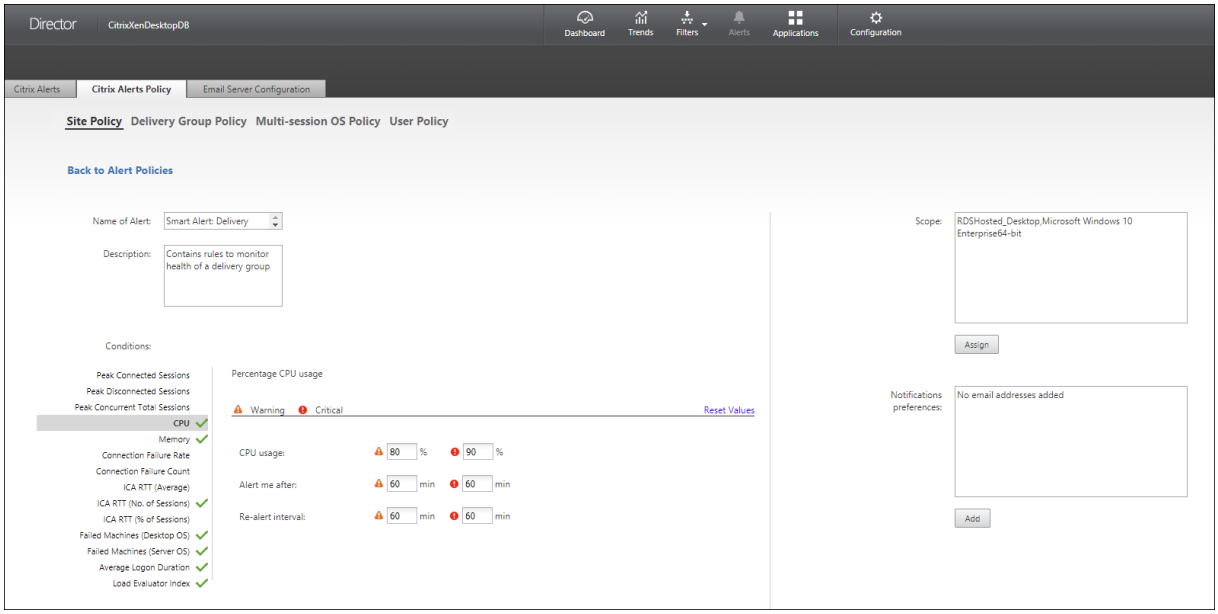
Citrix alerts are alerts monitored in Director that originate from Citrix components. You can configure Citrix alerts within Director in **Alerts** > **Citrix Alerts Policy**. As part of the configuration, you can set notifications to be sent by email to individuals and groups when alerts exceed the 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 is available for Delivery Groups and Multi-session OS VDA scope. This feature requires Delivery Controller(s) version 7.18 or later. 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.

In case you upgrade Director and your Site, the alert policies from your previous Director instance are carried over. 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.

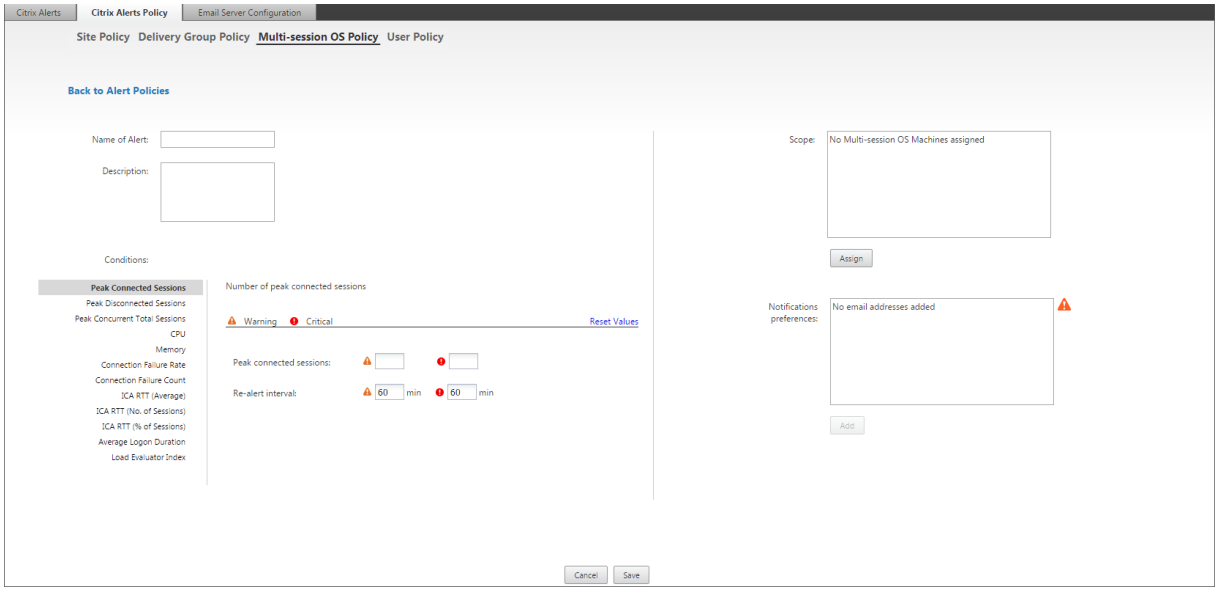


SCOM alerts

SCOM alerts display alert information from Microsoft System Center 2012 Operations Manager (SCOM) to provide a more comprehensive indication of data center health and performance within Director. For more information, see the Configure SCOM alerts integration section.

The number of alerts displayed next to the alerts icons before you expand the sidebar are the combined sum of Citrix and SCOM alerts.

Create alerts policies



To create a new alerts policy, for example, to generate an alert when a specific set of session count criteria is 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. You have to specify an email server on the **Email Server Configuration** tab in order to set email Notification preferences in Alerts Policies.
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.

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 Director 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 Director 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 Director Session Trends view in Director 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 Director 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 Director 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 Director 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, work with 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 - 400ms 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, work with 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 Director 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 Director 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

Average Logon Duration

Average logon duration for logons that occurred over the last hour.

- Check the Director 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 Director 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%

Hypervisor Alerts Monitoring

Director 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 Citrix Studio. 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.

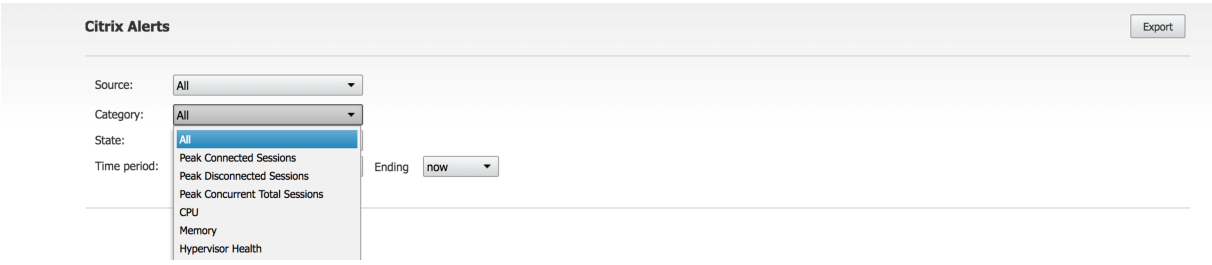
Alert	Supported Hypervisors	Triggered by	Condition	Configuration
CPU usage	Citrix Hypervisor, VMware vSphere	Hypervisor	CPU usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Memory usage	Citrix Hypervisor, VMware vSphere	Hypervisor	Memory usage alert 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.
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.

Alert	Supported Hypervisors	Triggered by	Condition	Configuration
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.

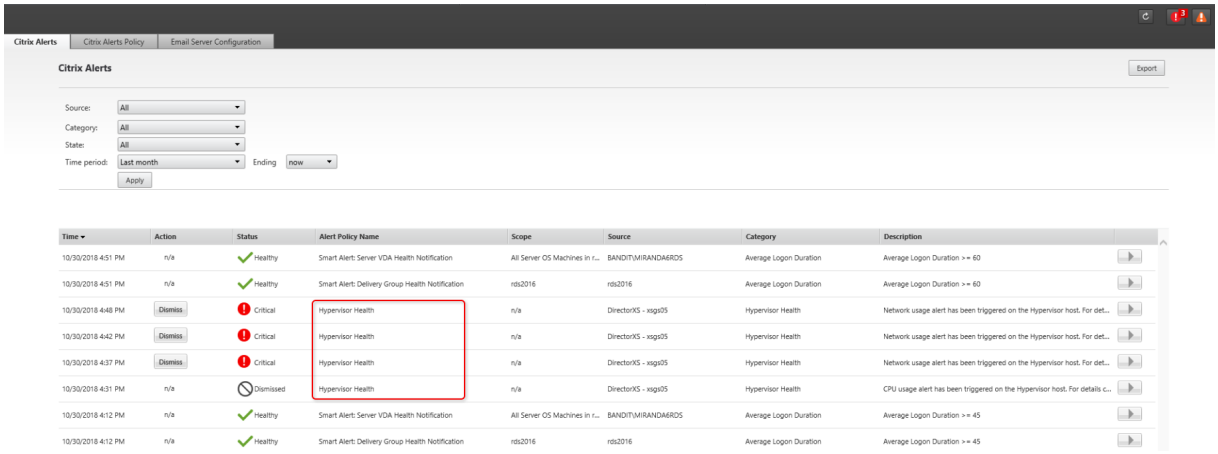
Email notification preference can be configured under **Citrix Alerts Policy > Site Policy > Hypervisor Health**. The threshold conditions for Hypervisor alert policies can be configured, edited, disabled, or deleted from the hypervisor only and not from Director. However, modifying email preferences and dismissing an alert can be done in Director.

> Important:
>
> - Alerts triggered by the Hypervisor are fetched and displayed in Director. However, changes in the life cycle/state of the Hypervisor alerts are not reflected in Director.
> - Alerts that are healthy or dismissed or disabled in the Hypervisor console continues to appear in Director and have to be dismissed explicitly.
> - Alerts that are dismissed in Director 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



This feature requires Delivery Controller version 7 1811 or later. If you are using an older version of Director with Sites 7 1811 or later, only the hypervisor alert count is displayed. To view the alerts, you must upgrade Director.

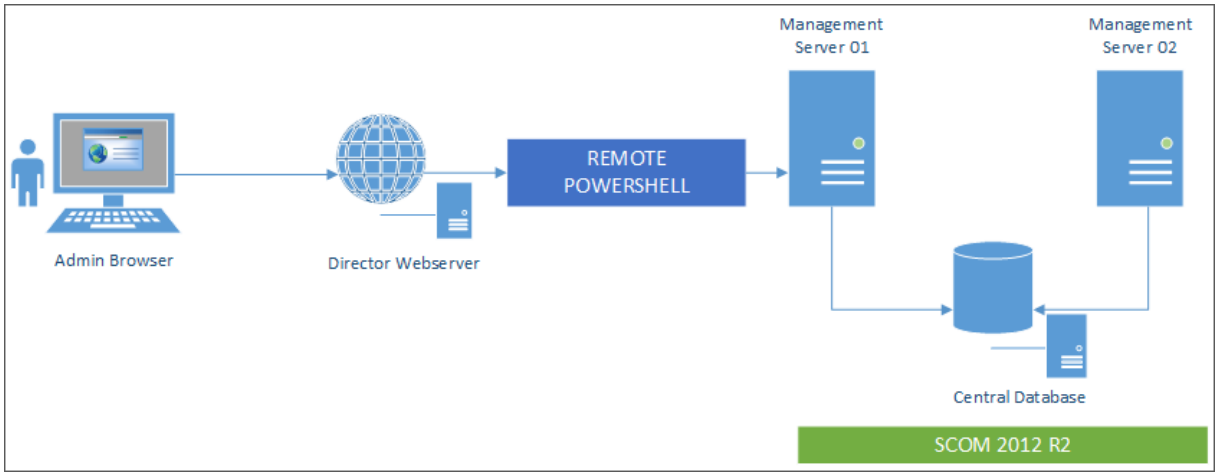
Configure SCOM alerts integration

SCOM integration with Director lets you view alert information from SCOM on the Dashboard and in other high-level views in Director.

SCOM alerts are displayed on-screen alongside Citrix alerts. You can access and drill down into SCOM alerts from SCOM tab in the side bar.

You can view historical alerts up to one month old, sort, filter, and export the filtered information to CSV, Excel, and PDF report formats. For more information, see Export reports.

SCOM integration uses remote PowerShell 3.0 or later to query data from the SCOM Management Server and it maintains a persistent runspace connection in the user's Director session. Director and SCOM server must have the same PowerShell version.



The requirements for SCOM integration are:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 or later (PowerShell version on Director and the SCOM server must match)
- Quad Core CPU with 16 GB RAM (recommended)
- A primary Management Server for SCOM must be configured in the Director web.config file. You can do this using the DirectorConfig tool.

Citrix recommends that the Director administrator account is configured as a SCOM Operator role so that full alert information can be retrieved in Director. If this is not possible, a SCOM administrator account can be configured in the web.config file using the DirectorConfig tool.

Citrix further recommends that you do not configure more than 10 Director administrators per SCOM Management Server to ensure optimal performance.

On the Director server:

1. Type **Enable-PSRemoting** to enable PowerShell remoting.
2. Add the SCOM Management Server to the TrustedHosts list. Open a PowerShell prompt and execute the following command(s):
   - Get the current list of TrustedHosts

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - Add the FQDN of the SCOM Management Server to the list of TrustedHosts. <Old Values> represents the existing set of entries returned from Get-Item cmdlet.

     Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
3. Configure SCOM using the DirectorConfig tool.

   C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom

On the SCOM Management server:

1. Assign Director administrators to a SCOM administrator role.

   a) Open the SCOM Management console and go to **Administration** > **Security** > **User Roles**.

   b) In User Roles, you can create a new User Role or modify an existing one. There are four categories of SCOM operator roles that define the nature of access to SCOM data. For example, a Read-Only role does not see the Administration pane and cannot discover or manage rules, machines or accounts. An Operator role is a full administrator role.

   > Note:
   >
   > The following operations are not available if the Director administrator is assigned to a non-operator role:

   ```
   > - If there are multiple management servers configured and the primary management server is not available, the Director administrator cannot connect to the secondary management server. The primary management server is the server configured in the Director web.config file, that is the same server as the one specified with the DirectorConfig tool in step 3 above. The secondary management servers are peer management servers of the primary server.
   > - While filtering alerts, the Director administrator cannot search for the alert source. This requires an operator level permission.
   ```

   a) To modify any User Role, right-click on the role, then click **Properties**.

   b) In the User Role Properties dialog, you can add or remove Director administrators from the specified user role.

2. Add Director administrators to the Remote Management Users group on the SCOM Management server. This allows the Director administrators to establish a remote PowerShell connection.

3. Type **Enable-PSRemoting** to enable PowerShell remoting.

4. Set the WS-Management properties limits:

   a) Modify MaxConcurrentUsers:

   In CLI:

   “‘winrm set winrm/config/winrs @{MaxConcurrentUsers = “20”}

   ```
   In PS:

   ```Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20<!--NeedCopy-->
   ```


   ```

b) Modify MaxShellsPerUser:

In CLI:

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--
NeedCopy-->
```

In PS:

“‘Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20

```
1.  Modify MaxMemoryPerShellMB:

    In CLI:

    ```winrm set winrm/config/winrs @{
 MaxMemoryPerShellMB="1024" }
 <!--NeedCopy-->
```

```
In PS:
```

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024<!--
NeedCopy-->
```

5. To ensure that SCOM integration works in mixed domain environments, set the following registry entry.

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Key: LocalAccountTokenFilterPolicy

Type: DWord

Value: 1

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.

Once SCOM integration is set up you might see the message “Cannot get the latest SCOM alerts. View the Director server event logs for more information”. The server event logs help identify and correct the problem. Causes can include:

- Loss of network connectivity at the Director or SCOM machine.
- The SCOM service is not available or too busy to respond.
- Failed authorization due to a change in permissions for the configured user.
- An error in Director while processing the SCOM data.
- PowerShell version mismatch between Director and SCOM server.


```

# Filter data to troubleshoot failures

March 4, 2021

When you click numbers on the Dashboard or select a predefined filter from the Filters menu, the Filters view opens to display data based on the selected machine or failure type.

Predefined filters cannot be edited, but you can save a predefined filter as a custom filter and then modify it. Additionally, you can create custom filtered views of machines, connections, sessions, and application instances across all Delivery Groups.

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.
    - **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 Server and Single-session OS. The session idle time measurements are available for Application instances on VDAs of Multi-session OS.

    > **Note:**
    >
    > If you have launched Desktop sessions on VDAs installed on a Windows 10 1809 computer, the Activity Manager in Director might sometimes display Microsoft Edge and Office as actively running applications while they are actually running only in the background.

2. For **Filter by**, select the criteria.
3. Use the additional tabs for each view, as needed, to complete the filter.
4. Select additional columns, as needed, to troubleshoot further.
5. Save and name your filter.
6. To access filters from multiple Director servers, store the filters on a shared folder accessible from those servers:
    - The shared folder must have modify permissions for accounts on the Director server.
    - The Director servers must be configured to access the shared folder. To do this, run **IIS Manager**. In Sites > Default Web Site > Director> Application Settings, modify the **Service.UserSettingsPath** setting to reflect the UNC path of the shared folder.

7. To open the filter later, from the **Filters** menu, select the filter type (Machines, Sessions, Connections, or Application Instances), and then select the saved filter.
8. Click **Export** to export the data to CSV format files. Data of up to 100,000 records can be exported. This feature is available in Delivery Controller(s) version 1808 and later.
9. 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.
10. 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 7.12 Failure Reasons Troubleshooting Guide.
11. In the **Machines** view, click on 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.
12. 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 Director, Delivery Controller(s), and VDAs are version 7.13 or later.

> **Note:**
> Citrix Studio 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, Director 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 Director. To map the assigned desktop displayed in StoreFront to the Delivery Group name displayed in Director, 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-->
```

Monitor historical trends across a Site

February 6, 2020

The Trends view accesses historical trend information for sessions, connection failures, machine failures, logon performance, load evaluation, capacity management, machine usage, resource utilization, and network analysis for each Site. 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.

Choose a time period for which you require the historical trend information; time period availability depends on your Director deployment as follows:

- Trend reports of up to Last year (365 days) are available in Premium licensed Sites.
- Trend reports of up to Last month (31 days) are available in Advanced licensed Sites.
- Trend reports of up to Last 7 days in non-Premium and non-Advanced licensed Sites.

> **Note:**
>
> - In all Director deployments, 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.
> - Grooming retention values of the Monitor Service control the trends data availability. The default values are available in Data granularity and retention. Customers on Premium licensed Sites can change the grooming retention to their desired number of retention days.
> - The following parameters in IIS Manager control the range of custom ending dates available for selection and can be customized. However, the data availability for selected dates depends on the grooming retention setting for the specific metric being measured.

Parameter	Default values
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

Parameter	Default values

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 Director UI after the reconnect has occurred.

The auto reconnect information helps you view and troubleshoot network connections having interruptions, and also 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 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 Delivery Controller version 7 1906 or later, and 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 Director for the following reasons:

- Workspace app is not sending auto reconnect data to VDA.
- VDA is not sending data to monitor service.
- VDA payloads is discarded by Delivery Controllers as they might not have the corresponding sessions.

> Note:
>
> Sometimes, the client IP address might not be obtained correctly if certain NSG 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.
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 Multi-session OS machine in a Delivery Group was selected), and range.

View hosted applications usage: The availability of this feature depends on your organization's license.
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-session 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, 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 number of machines displayed in Available Counter includes machines in maintenance mode.

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 Delivery Controller(s) and 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 processes consuming CPU. 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).

View network analysis data: The availability of this feature depends on your organization's license and your administrator permissions. This feature requires Delivery Controller(s) **version 7.11** or later.

From the Network tab, monitor your network analysis, which provides a user, application, and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment through HDX Insight reports from Citrix ADM. For more information, see Configure network analysis

View application failures: The Application Failures tab displays failures associated with the published applications on the VDAs.

This feature requires Delivery Controller(s) and 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.

View application probe results: The Application Probe Results tab displays the results of probe for applications that have been configured for probing in the Configuration page. Here, the stage of launch during which the application launch failure occurred is recorded.

This feature requires Delivery Controller(s) and VDAs **version 7.18** or later. For more information see Application probing.

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.

This feature requires Delivery Controller(s) **version 7.12** or later.

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 new 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 additional 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 new 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 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 Citrix Studio are available for selection in the Director 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.

Troubleshoot deployments

February 6, 2020

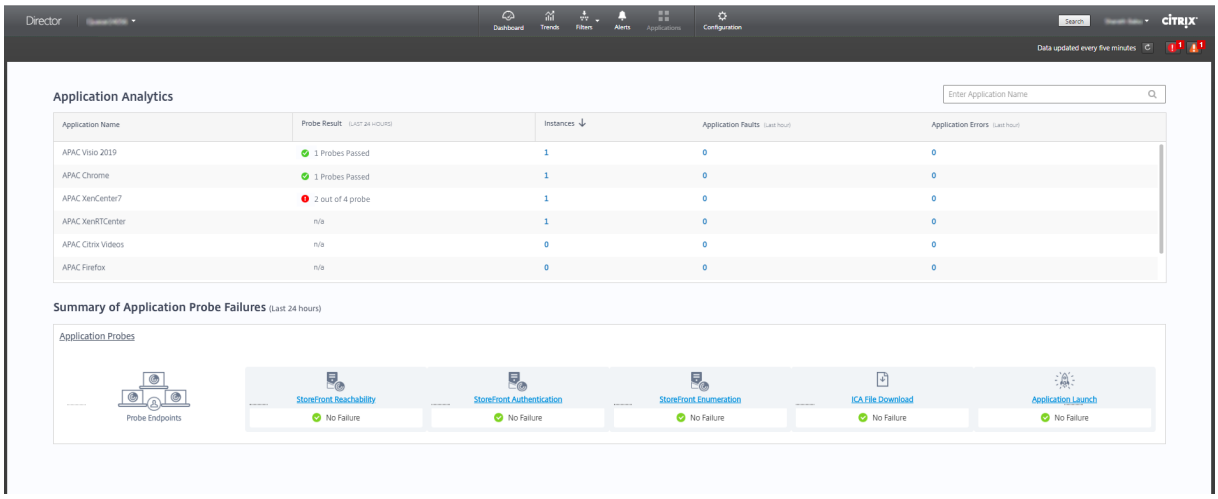
As a help desk administrator, you can search for the user reporting an issue and display details of sessions or applications associated with that user. Similarly, you can search for machines or endpoints where issues are reported. Issues can be quickly resolved by monitoring the relevant metrics and performing suitable actions. Available actions include 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 or resetting the user profile.

Troubleshoot applications

February 7, 2020

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 Delivery Controller(s) Version 7.16 or later and 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** > **Application Probe Results** page. For more details on how to configure application probes, see Application 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, Director 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

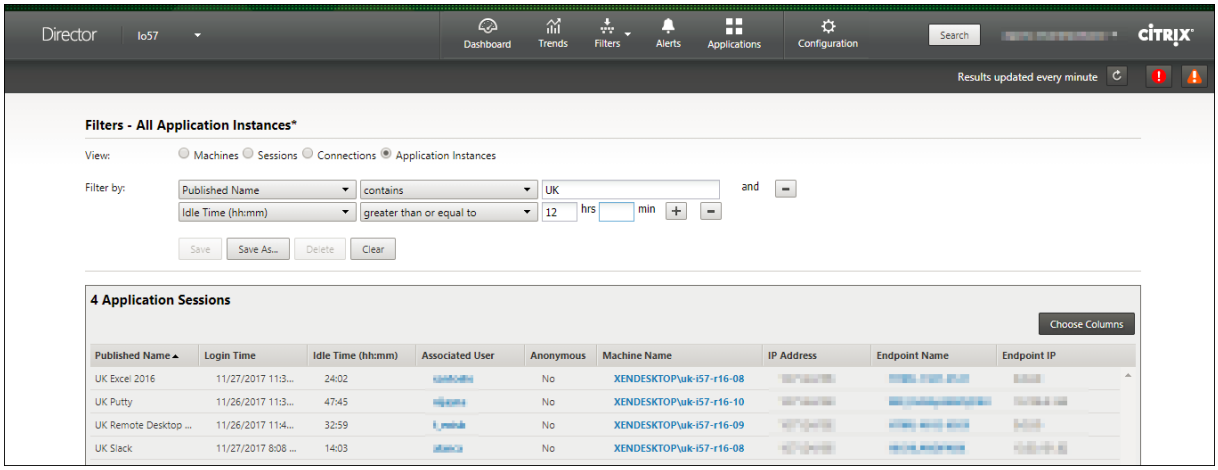
You can troubleshoot applications and sessions by using the idle time metric to identify instances that are idle beyond a specific time limit.

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 Server 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.

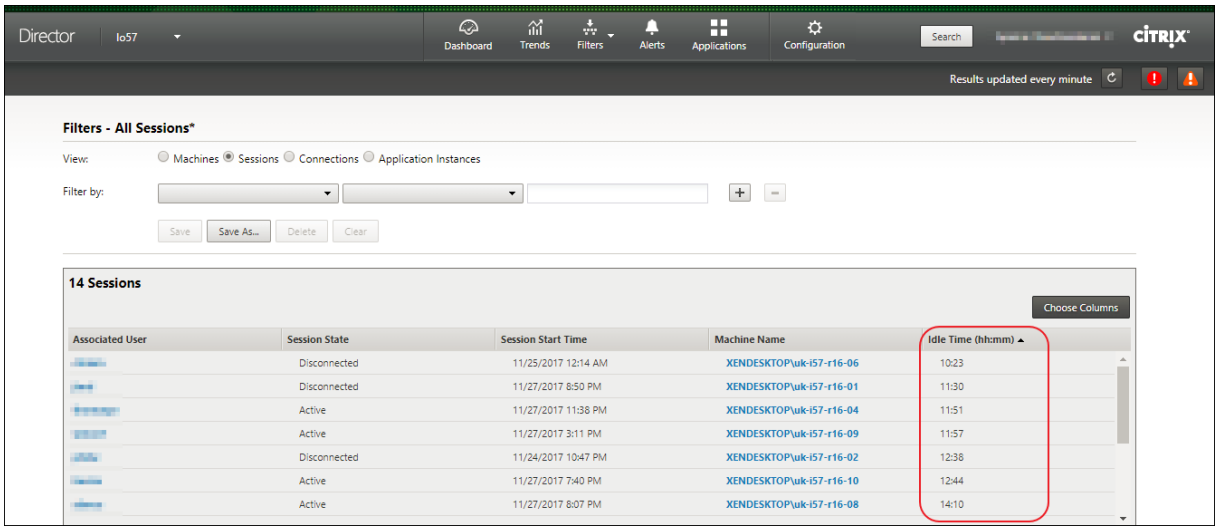
Use this information to identify the application instances that are idle beyond a specific time period and log off or disconnect them as appropriate. To do this, select **Filters > Application Instances** and select a pre-saved filter or choose **All Application Instances** and create your own filter.



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.

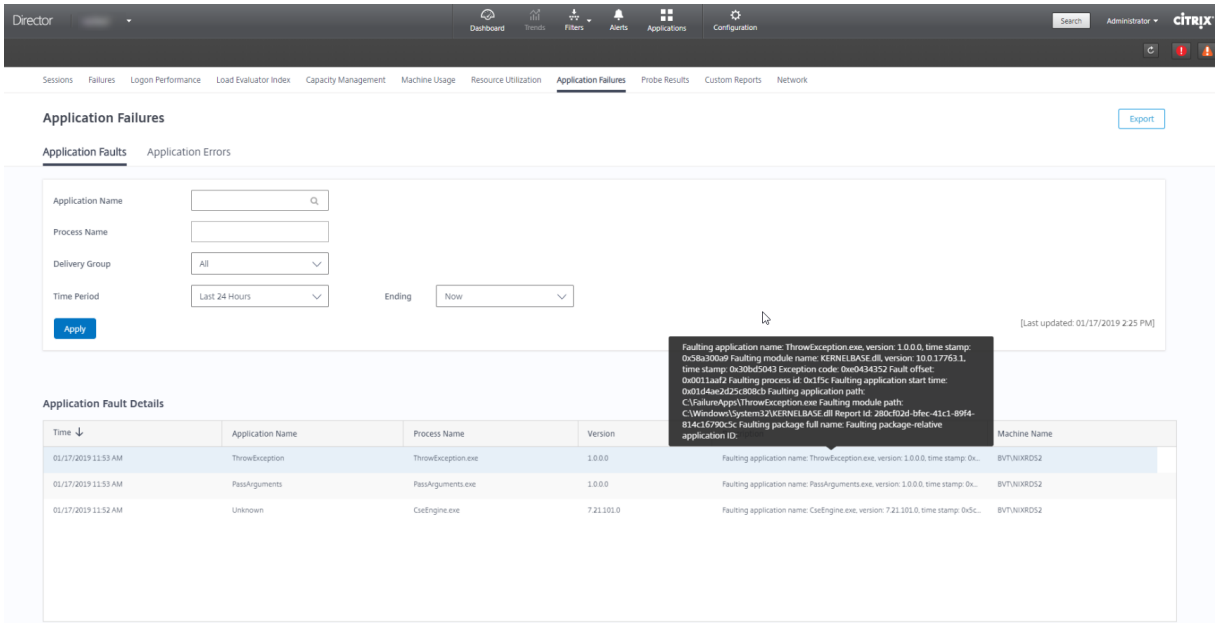
Historical application failure monitoring

The **Trends** -> **Application Failures** tab displays failures associated with the published applications on the VDAs.

Application failure trends are available for the last 2 hours, 24 hours, 7 days, and month for Premium and Advanced licensed Sites. They are available for the last 2 hours, 24 hours, and 7 days for other license types. 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 grooming retention settings for application failure monitoring, GroomApplicationErrorsRetentionDays and GroomApplicationFaultsRetentionDays are set to one day by default for both Premium and non-Premium licensed Sites. You can change this setting using the PowerShell command:

```
PowerShell command Set-MonitorConfiguration -\<setting name\> \<value \> <!--NeedCopy-->
```



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

February 7, 2020

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 Director.

Requirements:

- Delivery Controller runs version 7.18 or later.
- 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.
- Director and StoreFront support the default form-based authentication.

User accounts/permissions required to run Application Probing:

- A unique StoreFront user to probe on each endpoint machine. The StoreFront 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 existing user accounts for application probing might log off the users' active sessions.
  - Delivery Group permissions:

    - Read-only
  - Director 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

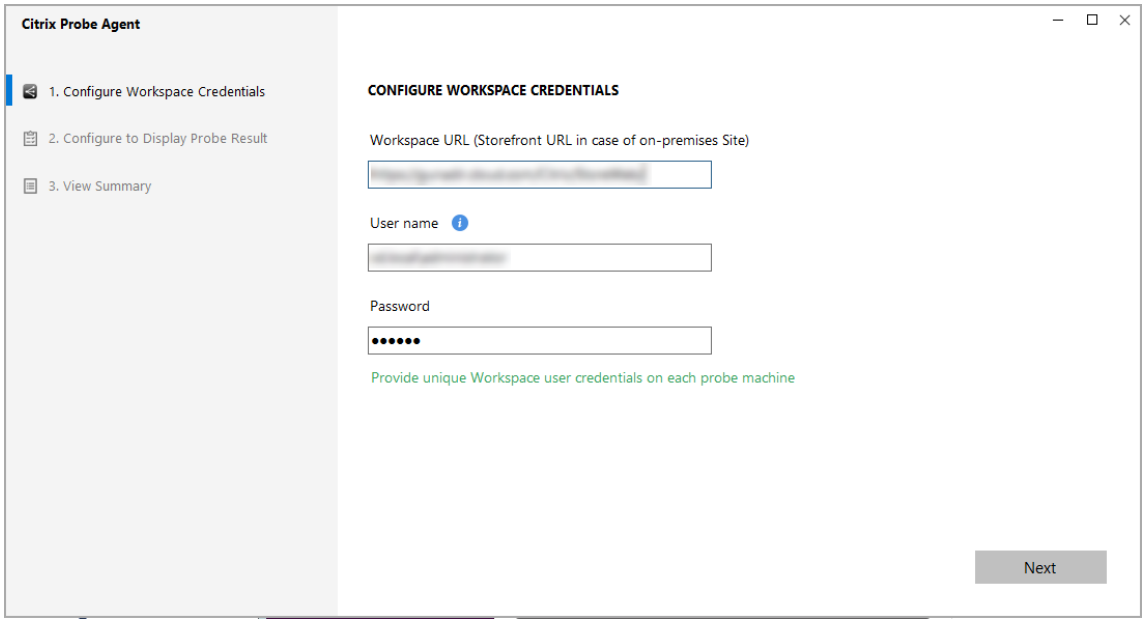
Configure Application Probing

You can schedule 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.

Step 1: Install and configure the Citrix Probe Agent

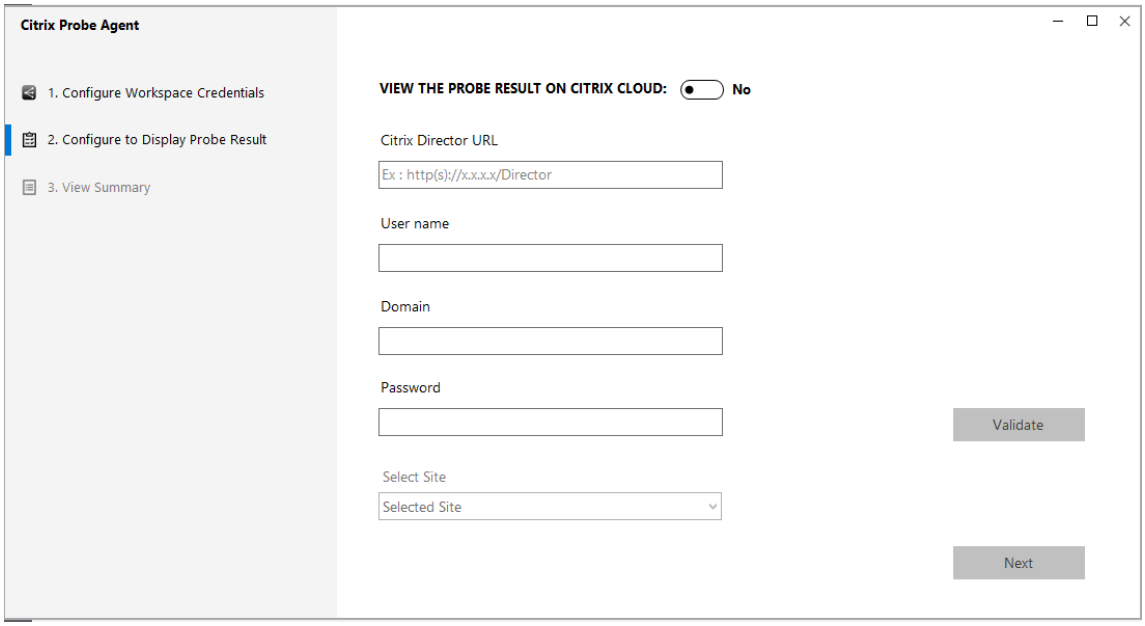
The Citrix Probe Agent is a Windows executable that simulates the actual application launch by the user through StoreFront. It tests application launches as configured in Director and reports back the results to Director.

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 StoreFront Receiver for Web credentials. Configure a unique StoreFront user on each endpoint machine. The credentials are encrypted and stored securely.



> **Note:**
> To access the Site to be probed from outside the network, type the login URL for Citrix Gateway in the StoreFront URL field. Citrix Gateway automatically routes the request to the corresponding Site StoreFront URL. This feature is available for Citrix Gateway version 12.1 and later (RfWebUI theme), and Delivery Controller(s) 1811 and later.

4. In the **Configure To Display Probe Result** tab, enter your Director credentials and click **Validate**.

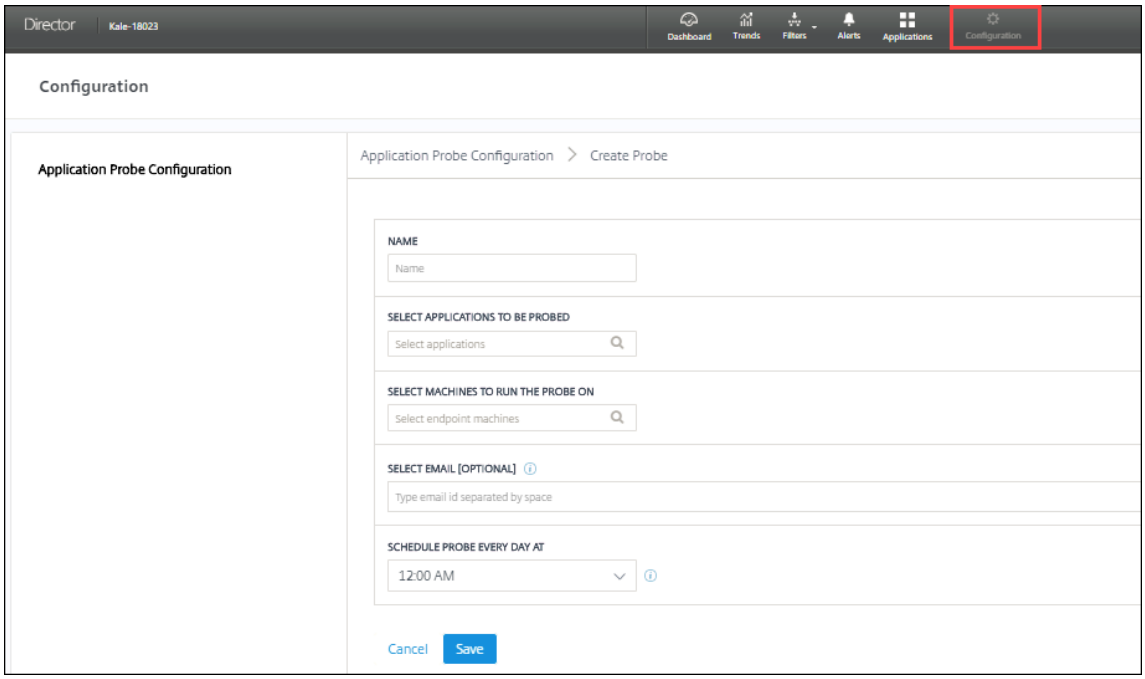


5. Select your Site and click **Next**.

Step 2: Configure Application Probing in Director

1. Go to **Configuration** > **Application Probe Configuration**.
2. Create a probe and choose:
   - the applications to be probed,
   - the endpoint machines on which the probe must run,
   - the email addresses to which the failure probe results are sent (configure your email server in **Alerts** -> **Email Server Configuration**), and
   - the time of the day at which the probe must run (as per the local time zone of the endpoint machine).

   After configuration in Director, the agent takes 10 minutes before it is ready to start probing. Then, it runs configured probes starting the next hour.



Step 3: Probe execution

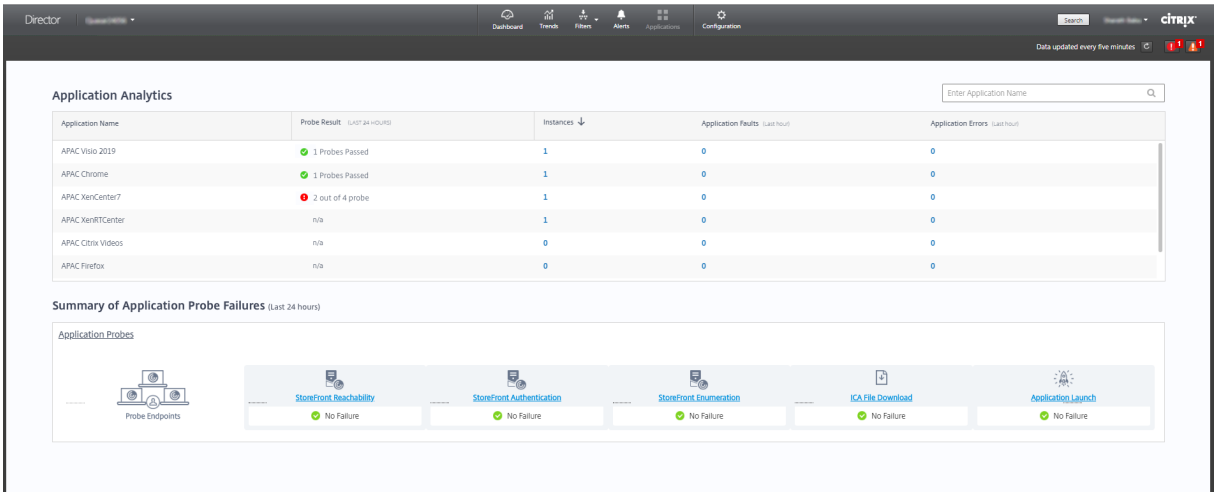
The agent executes application probing as per the probe configuration it fetches from Director periodically. It launches selected applications serially using StoreFront. The agent reports the results back to Director via the Monitor database. Failures are reported in five specific stages:

- **StoreFront Reachability** - configured StoreFront URL is not reachable.
- **StoreFront Authentication** - configured StoreFront credentials are invalid.
- **StoreFront Enumeration** - StoreFront Enumerate applications list does not contain the application to be probed.

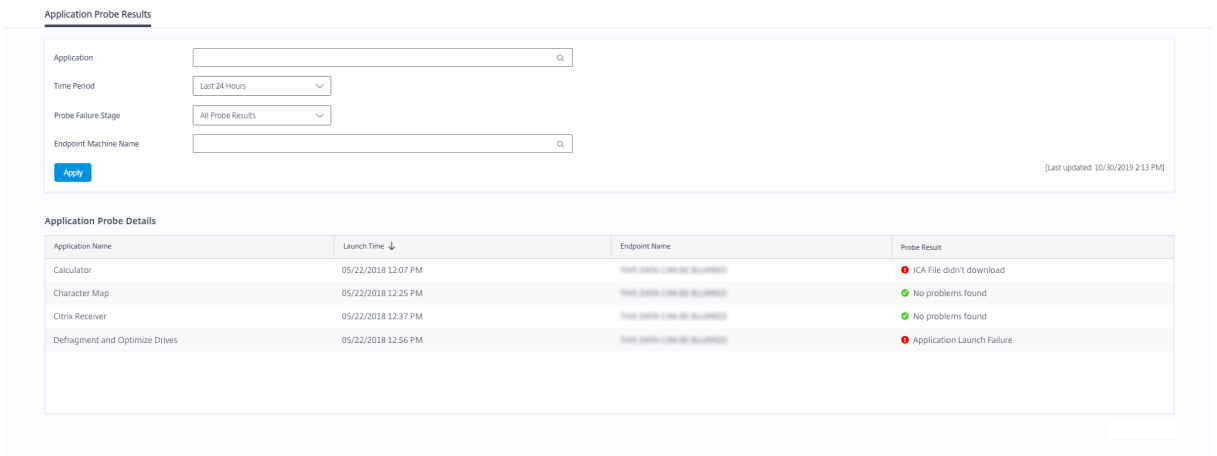
- **ICA download** - the ICA file is not available.
- **Application launch** –the application cannot be launched.

Step 4: View probe results

You can view the latest probe results in the **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 7, 2020

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 Director.

In Director'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 StoreFront and reports the results back to Director. The probe results are displayed in the Director 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 - StoreFront Reachability, StoreFront Authentication, StoreFront 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. Desktop probing is available for Premium licensed Sites. This feature requires Delivery Controller(s) version 7 1906 or later and Probe Agent 1903 or later.

Requirements:

- Delivery Controller runs version 1906 or later.
- 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.
- Director and StoreFront support the default form-based authentication.

User accounts or permissions required to run Desktop probing:

- A unique StoreFront user to probe on each endpoint machine. The StoreFront 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'active sessions.
  - Delivery Group permissions:
    - Read-only
  - Director 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

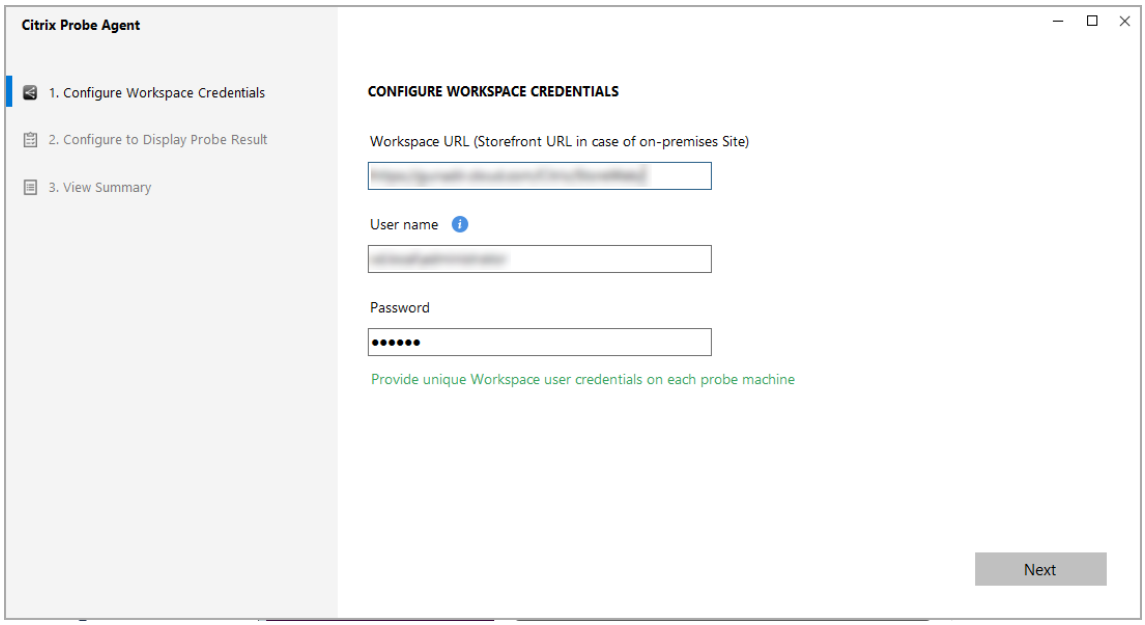
Configure desktop probing

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.

Step 1: Install and configure the Citrix Probe Agent

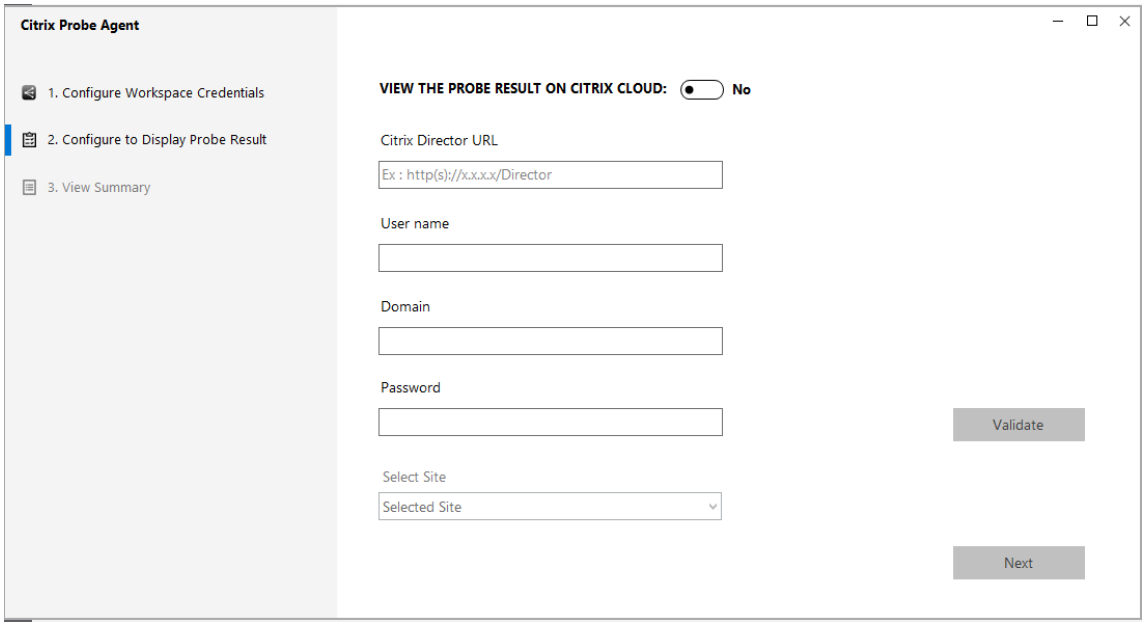
The Citrix Probe Agent is a Windows executable that simulates the actual desktop launch by the user through StoreFront. It tests desktop launches as configured in Director and reports back the results to Director.

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 StoreFront Receiver for Web credentials. Configure a unique StoreFront user on each endpoint machine. The credentials are encrypted and stored securely.



> Note:
>
> To access the Site to be probed from outside the network, type the Citrix Gateway login page URL in the StoreFront URL field. Citrix Gateway automatically routes the request to the corresponding Site StoreFront URL. This feature is available for Citrix Gateway version 12.1 or later, and Delivery Controller(s) 1811 or later.

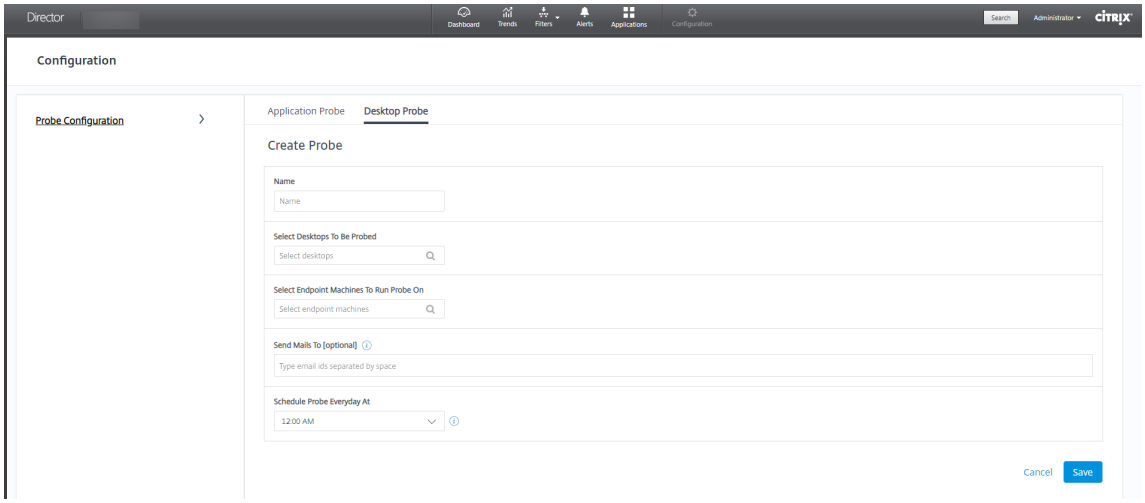
4. In the **Configure To Display Probe Result** tab, enter your Director credentials and click **Validate**.



5. Select your Site and click **Next**.

Step 2: Configure desktop probing in Director

1. Go to **Configuration** > **Desktop Probe Configuration**.
2. To create a probe, enter the details and click **Save**.



> Note:
>
> Configure your email server in **Alerts** > **Email Server Configuration**.

After desktop probing configuration is complete, the agent takes 10 minutes before it is ready to start probing. Then, it runs configured probes starting the next hour.

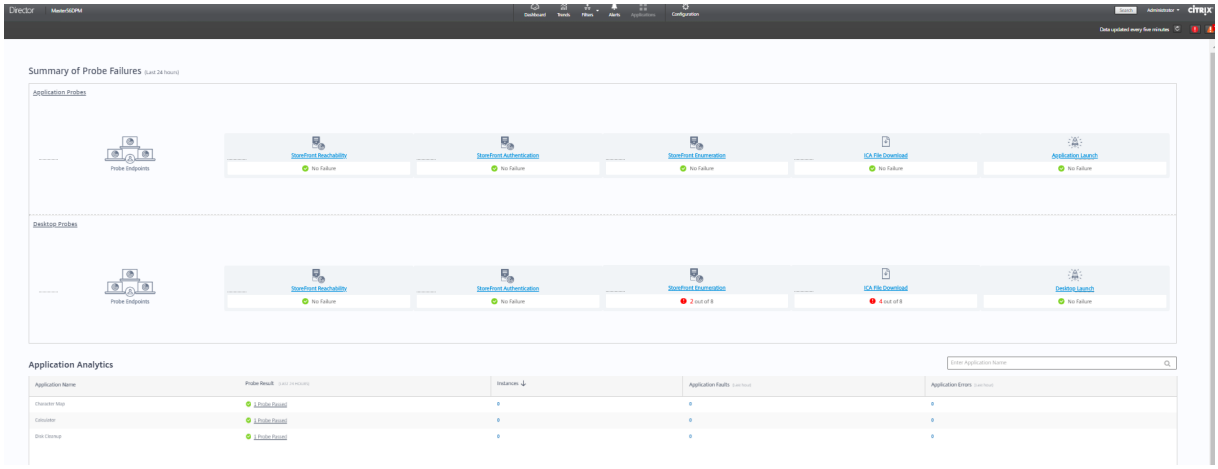
Step 3: Probe execution

The agent executes desktop probing as per the probe configuration it fetches from Director periodically. It launches selected desktops serially using StoreFront. The agent reports the results back to Director via the Monitor database. Failures are reported in five specific stages:

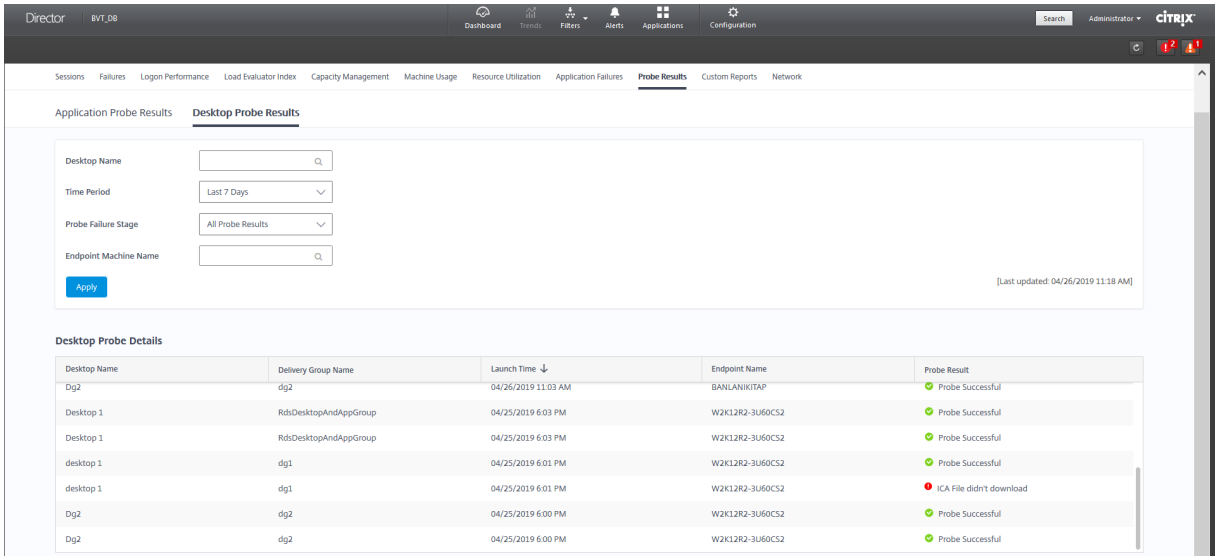
- **StoreFront Reachability** - configured StoreFront URL is not reachable.
- **StoreFront Authentication** - configured StoreFront credentials are invalid.
- **StoreFront Enumeration** - StoreFront Enumerate desktops list does not contain the desktop to be probed.
- **ICA download** - the ICA file is not available.
- **Desktop launch** –the desktop cannot be launched.

Step 4: View probe results

You can view the latest probe results in 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's 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 Director console 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 7.12 Failure Reasons Troubleshooting Guide.

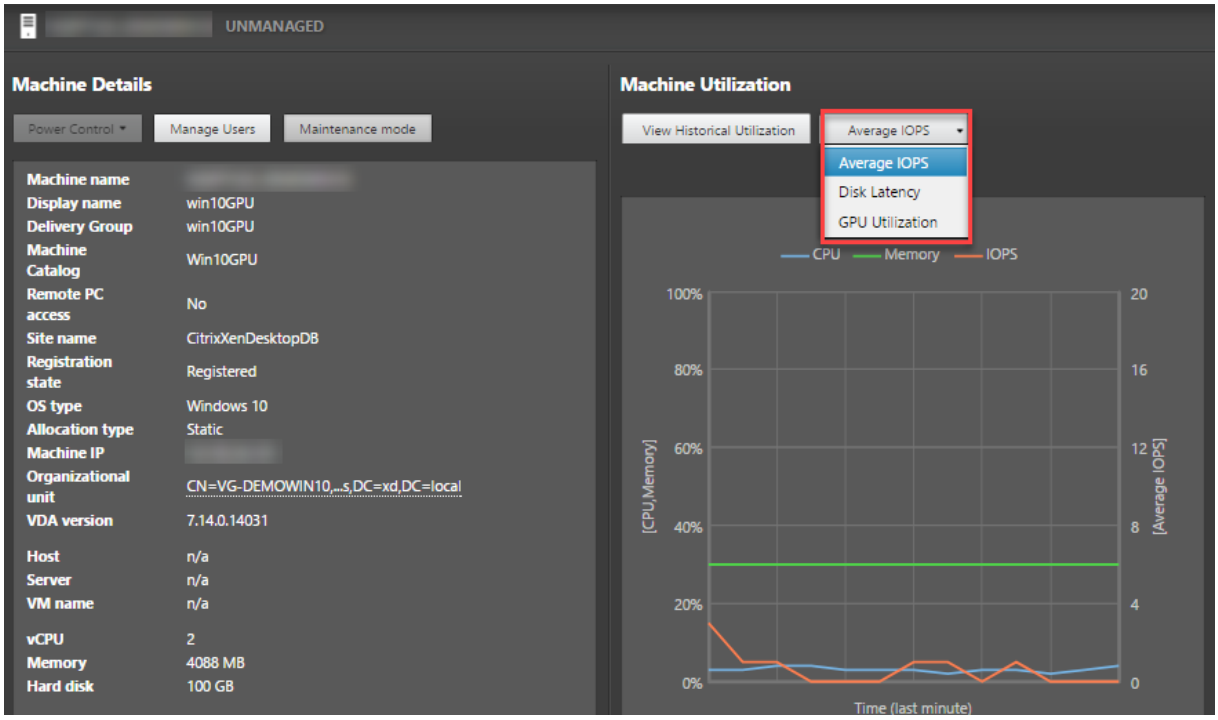
Click the machine name link to go to the **Machine Details** page.

The Machine Details page lists the machine details, infrastructure details, and details of the hotfixes applied on the machine.

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 Delivery Controller(s) and VDA versions **7.14** or 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.



Select **GPU Utilization** to see percentage utilization of the GPU, the GPU memory, and of the Encoder and the Decoder to troubleshoot GPU-related issues on Server or Single-session OS VDAs. The GPU Utilization graphs are available only for VDAs running 64-bit Windows with NVIDIA Tesla M60 GPUs, and running Display Driver version 369.17 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.

Machine-based historical resource utilization

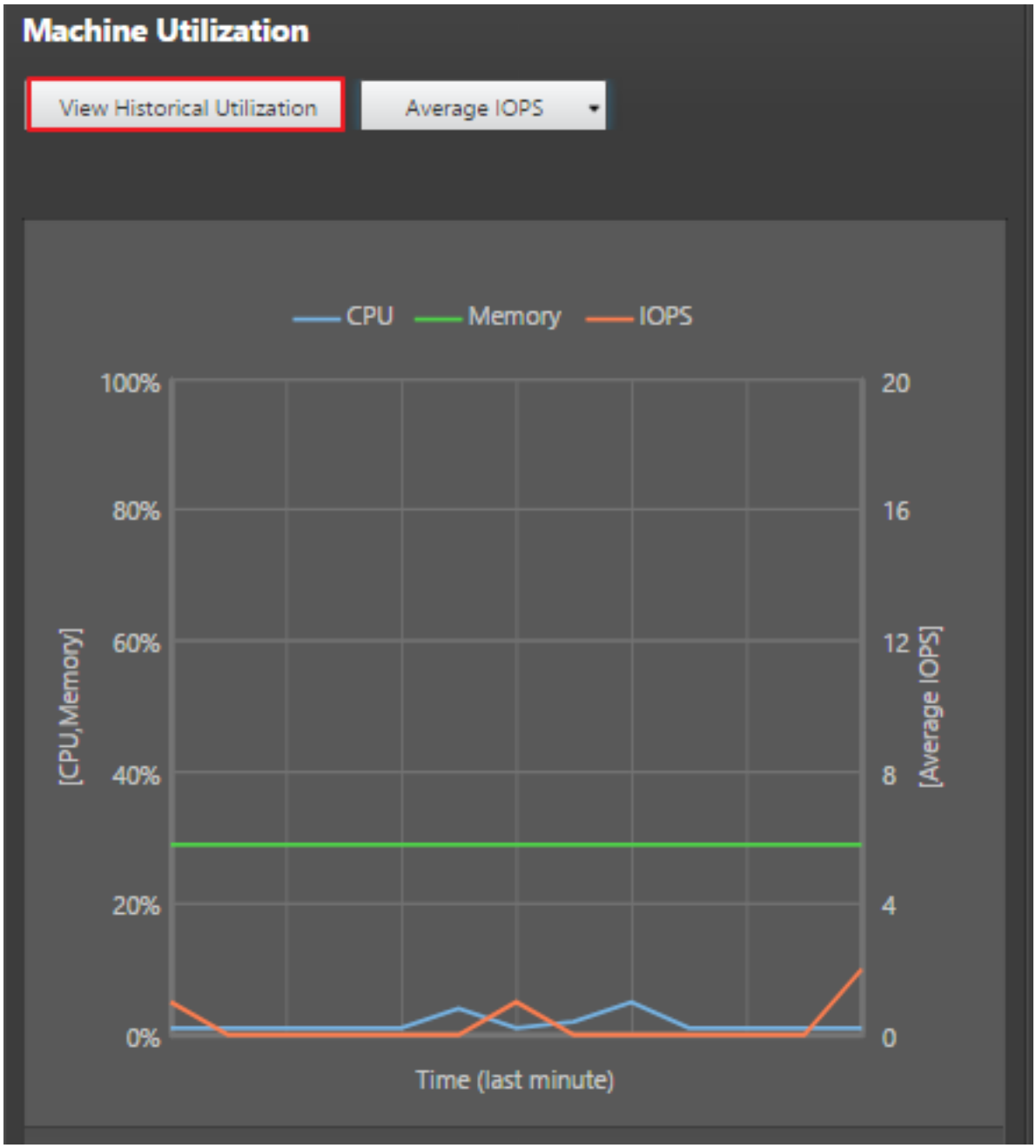
In the **Machine Utilization** panel, click **View Historical Utilization** to view the historical usage of resources on the selected machine.

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.

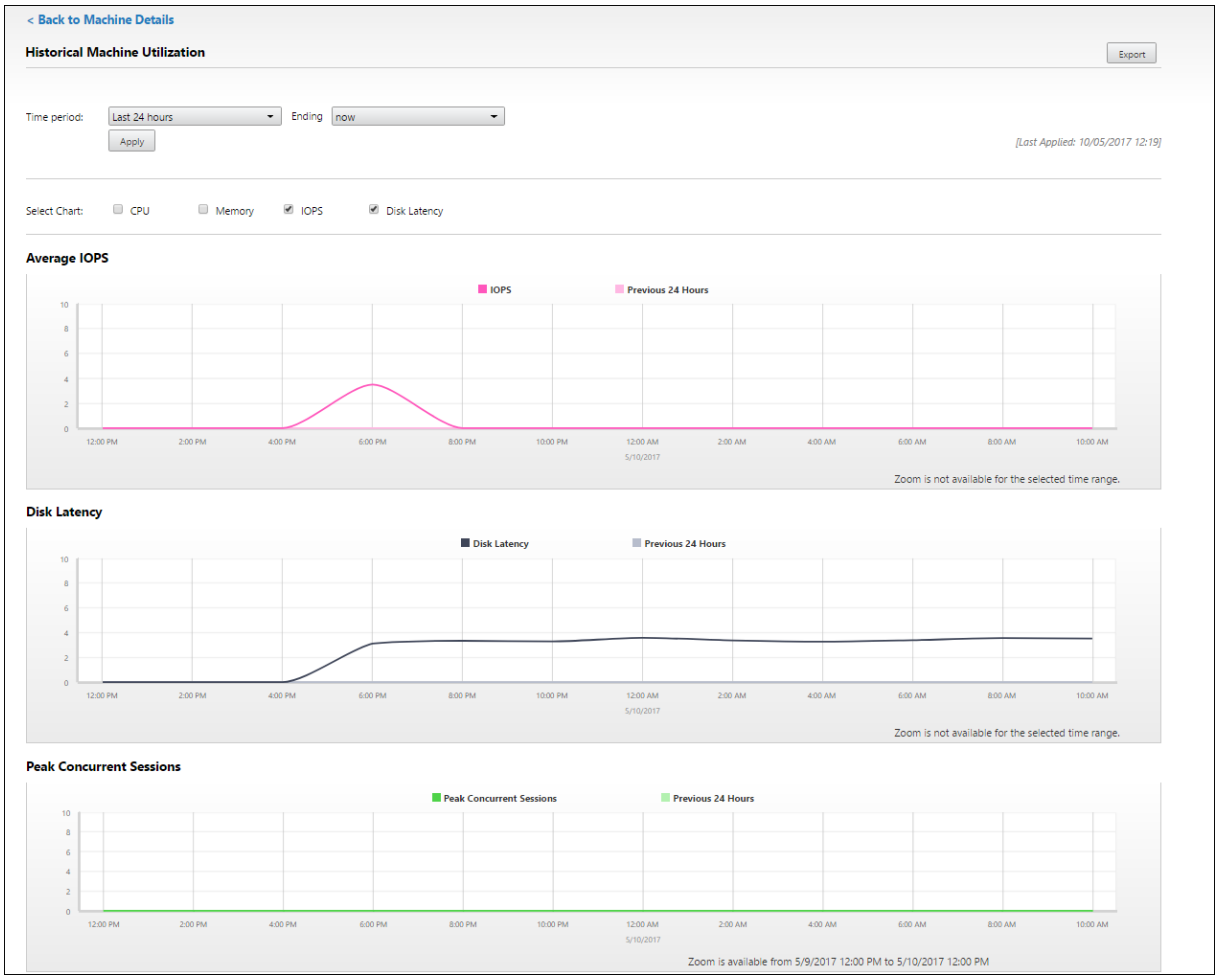


1. From the **Machine Utilization** panel in the **Machine Details** view, select **View Historical Utilization**.
2. In the **Historical Machine Utilization** page, set **Time Period** to view usage for the last 2 hours, 24 hours, 7 days, month, or year.

   > **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.

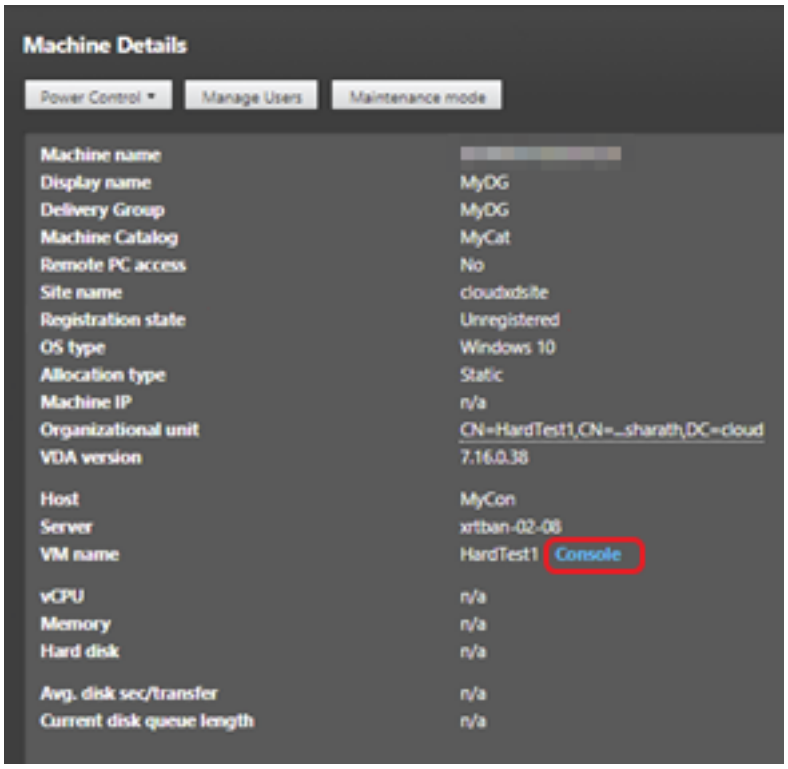
> **Note:**
> The session ID for system processes is displayed as "0000".

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 Single-session and Multi-session OS machines hosted on XenServer Version 7.3 and later directly from Director. This way, you don't require XenCenter to troubleshoot issues on XenServer hosted VDAs. For this feature to be available:

- Delivery Controller of Version 7.16 or later is required.
- The XenServer hosting the machine must be of Version 7.3 or later and must be accessible from the Director UI.



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.
- Director launches console access in a new tab, ensure that your browser settings allow pop-ups.
- For security reasons, Citrix recommends that you install SSL certificates on your browser.

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 Director
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).

Troubleshoot user issues

March 7, 2022

Use the Director's **Help Desk** view (**Activity Manager** page) to view information about the user:

- Check for details about the user's logon, connection, and applications.
- Shadow the user's machine.
- Record the ICA session.
- Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

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
Application is slow or won't respond	Resolve application failures
Connection failed	Restore desktop connections
Session is slow or not responding	Restore sessions
Record sessions	Record 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.

Search tips

When you type the user's name in a Search field, Director searches for users in Active Directory for users across all sites configured to support Director.

When you type a multiuser machine name in a Search field, Director displays the Machine Details for the specified machine.

When you type an endpoint name in a Search field, Director uses the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint, which enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

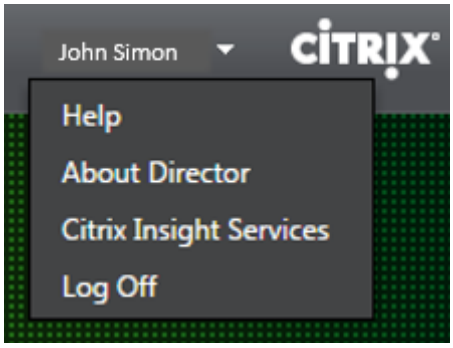
The search results also include users who are not currently using or assigned to a machine.

- Searches are not case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name (username, family name and first name, or display name), separated by a space, the results include matches for both strings. 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 Director logo.

Access Citrix Insight Services

You can access Citrix Insight Services (CIS) from the User drop-down in Director to access additional diagnostic insights. The data available in CIS comes from sources including Call Home and Citrix Scout.



Upload troubleshooting information to Citrix Technical Support

Run Citrix Scout from a single Delivery Controller or VDA to capture key data points and Citrix Diagnostics Facility (CDF) traces to troubleshoot selected computers. Scout offers the ability to securely

upload the data to the CIS platform to assist Citrix Technical Support on troubleshooting. Citrix Technical Support uses the CIS platform to reduce the time to resolve customer-reported issues.

Scout is installed with Citrix Virtual Apps and Desktops components. Depending on the version of Windows, Scout appears in the Windows Start Menu or Start Screen when you install or upgrade to Citrix Virtual Apps and Desktops.

To start Scout, from the Start Menu or Start Screen, select Citrix > Citrix Scout.

For information on using and configuring Scout, and for frequently asked questions, see CTX130147.

Diagnose session startup issues

April 19, 2024

In addition to the logon process phases mentioned in the Diagnose user logon issues section, Director displays the session startup duration. This is divided into Workspace App Session Startup and VDA Session Startup duration on the **User Details** page and **Machine 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. This feature is available on Delivery Controller version 7 1906 and later and VDAs 1903 and later.

Prerequisites

Ensure that the following prerequisites are met for session startup duration data to be displayed:

- Delivery Controller 7 1906 or later.
- VDA 1903 or later.
- Citrix End User Experience Monitoring (EUEM) service must be running on the VDA.

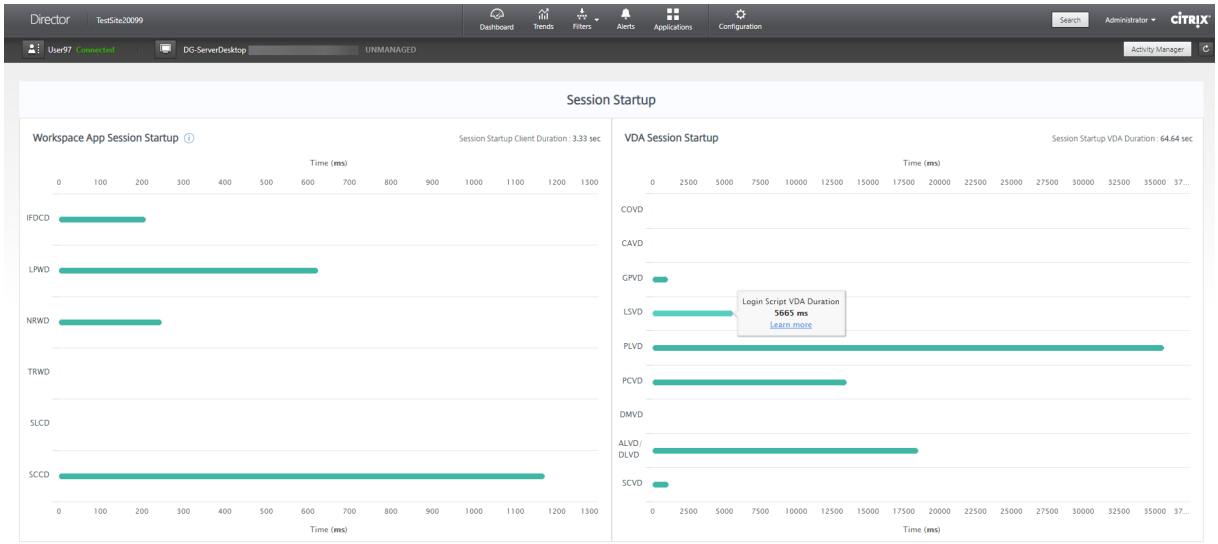
Limitations

The following limitations apply when Director 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.

- ICA File Download Duration (IFDCD) is available only when Workspace App is detected while launching from a browser.
- For session launches from Mac OS, IFDCD is available for Workspace App 1902 or 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 browser with Workspace app detected.

> Notes:
>
> - If you face issues in the sessions startup duration display after the prerequisites are met, view the Director server and VDA logs as described in CTX130320. For shared sessions (multiple applications launched in 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. This 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. In the case of 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

This 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) in the Workspace Application.
2. A request from the user is sent to StoreFront through 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 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 could 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 encompasses 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 may 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 may 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.

Consider making asynchronous the user or group's login scripts. Consider optimizing 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, consider 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. Consider using the Terminal Services home folders with redirected personal folders to mitigate this problem. In general, consider using 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. Consider reconfiguring 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 user receives keyboard and mouse control.

Session Creation VDA Duration (SCVD)

This time includes miscellaneous delay in session creation time on VDA.

Diagnose user logon issues

March 7, 2022

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 logon 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 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 currently 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.

VM start

If the session required a machine start, this is the time taken to start the virtual machine.

HDX connection

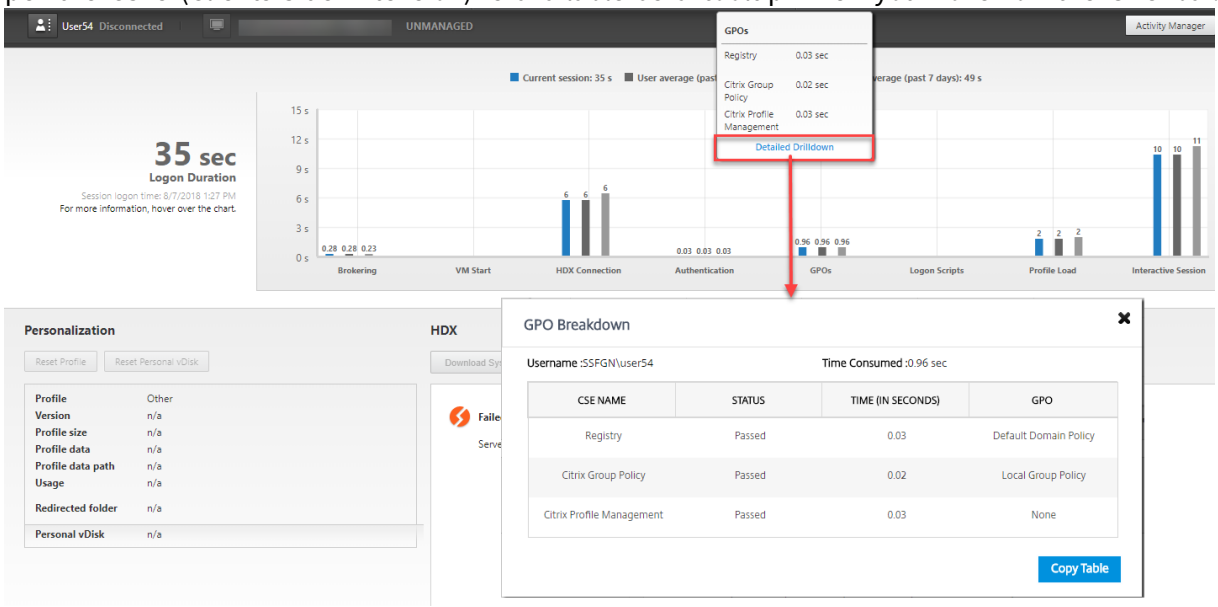
Time taken to complete the steps required in setting up the HDX connection from the client to the virtual machine.

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 article Configuring the Event Logs.

Logon scripts

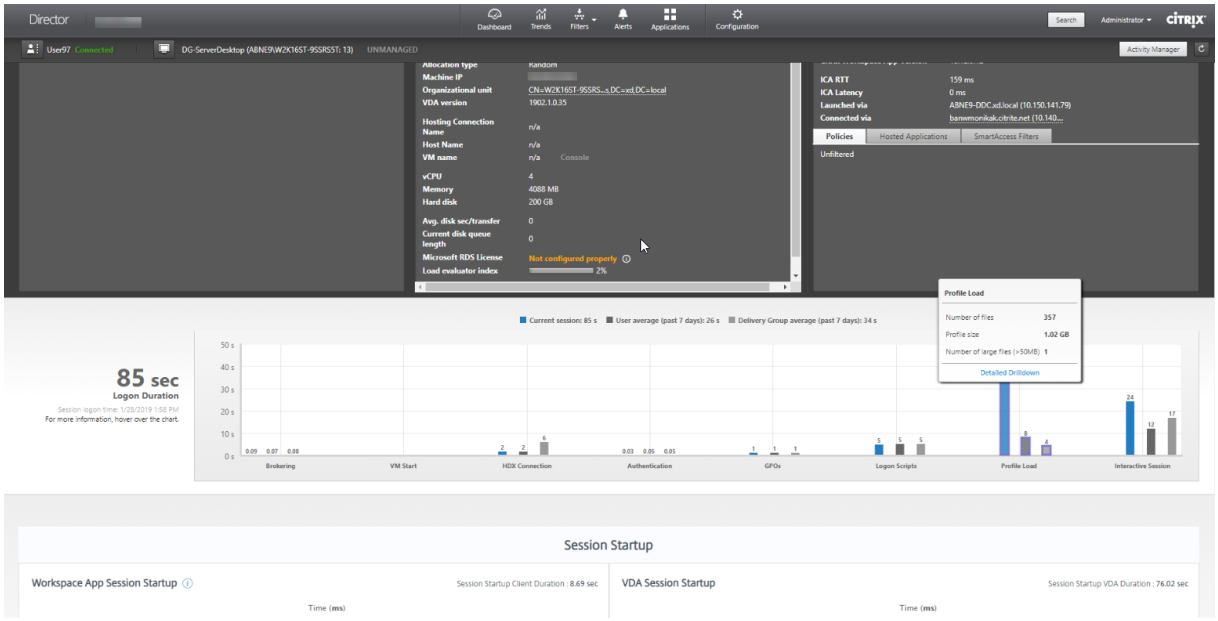
If logon scripts are configured for the session, this is the time taken for the logon scripts to be executed.

Profile load

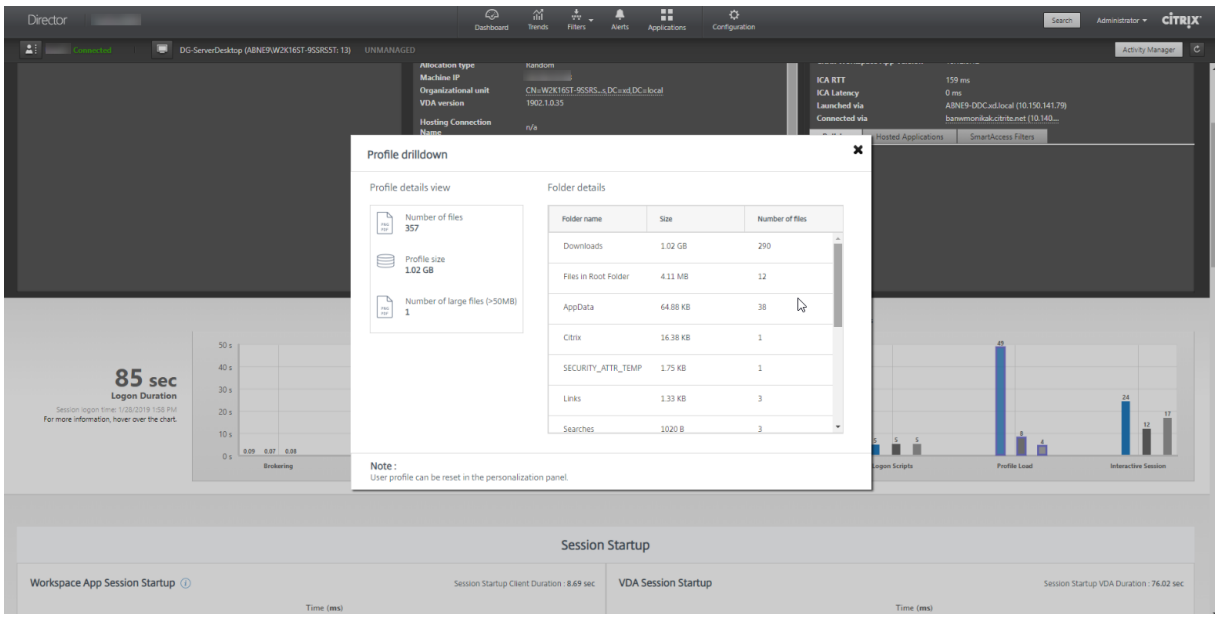
If profile settings are configured for the user or the virtual machine, this is the time taken for the profile to load.

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, an increased duration is displayed by the Profile Load bar. This increase is caused by this enhancement and does not reflect a performance degradation. This enhancement is available on VDAs 1903 or later.

Hovering over the Profile Load bar displays a tooltip showing the user profile details for the current session.



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 Delivery Controller version 7 1811 or later and VDAs 1811 or 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 folders in the profile root are displayed in the drilldown. To hide folder visibility, edit the following registry value on the VDA machine:

> Warning:
>
> Adding and 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.

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 commands 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.
- The NTUser.dat files in the root folder may not be visible to end users. However, they are included in the profile drilldown and displayed in the list of files in **Root Folder**.
- Certain hidden files in the AppData folder are not included in Profile drilldown.
- Number of files and profile size data may not match with the data in the Personalization panel due to certain Windows limitations.

Interactive Session

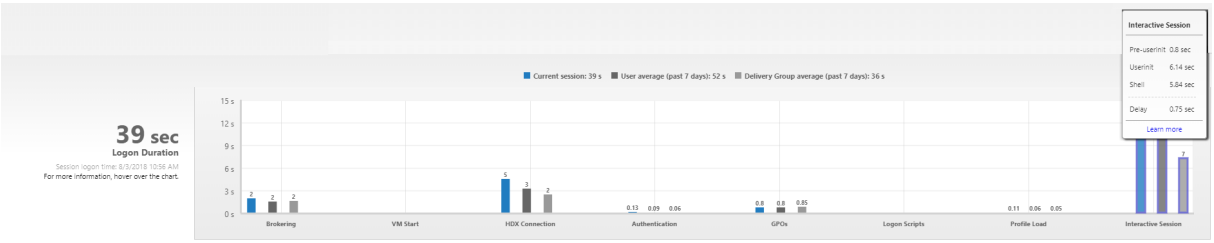
This is the time taken to "hand off" keyboard and mouse control to the user after the user profile has been loaded. It is normally the longest duration out of all the phases of the logon process and is calculated as **Interactive Session duration = Desktop Ready Event Timestamp (EventId 1000 on VDA) - User Profile Loaded Event Timestamp (EventId 2 on VDA)**. Interactive Session has three subphases: Pre-userinit, Userinit, and Shell. Hovering over Interactive Session displays a tooltip showing the subphases, the time taken for each subphase, the total cumulative time delay between these subphases, and a link to the documentation.

> 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 or later, a 'Drilldown unavailable due to server error' message is displayed. However, if you have launched sessions after 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 new 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 Audit process tracking 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, additional 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 sub-second 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.

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 VM startup 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 will be high.
- Major discrepancy between the user's logon 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 VM Start or Brokering.

Shadow users

February 6, 2020

From Director, 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.

Director launches shadowing in a new tab, update your browser settings to allow pop-ups from the Director 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:**
>
> - The VDA must be accessible from the Director UI for shadowing to work. Hence, shadowing

> is possible only for Linux VDAs in the same intranet as the Director client.
> - Director uses FQDN to connect to the target Linux VDA. Ensure that the Director 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 Director 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 the Enable or Disable features section in Install VDAs.

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 additional 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.

By default, this option is enabled for Sites in the Local intranet zone. If the Director Site is not in the Local intranet zone, consider manually adding the Site to this zone.

Send messages to users

April 23, 2020

From Director, 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**.

If the message is sent successfully, a confirmation message appears in Director. If the user's machine is connected, the message appears there.

If the message is not sent successfully, an error message appears in Director. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click Try again.

Resolve application failures

January 4, 2021

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 current status of each.

> **Note:**
> If the Applications tab is grayed out, contact an administrator with the permission to enable the tab.

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 will fail.
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 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.

Restore desktop connections

February 6, 2020

From Director, 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

February 6, 2020

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 onto it. You can also shadow the user to more closely monitor this session.

Run HDX channel system reports

February 6, 2020

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.

1. In the HDX panel, click Download System Report.
2. You can view or save the .xml report file.
    - To view the .xml file, click Open. The .xml file appears in the same window as the Director application.
    - To save the .xml file, click Save. The Save As window appears, prompting you for a location on the Director machine to download the file to.

Reset a user profile

February 7, 2020

> **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 Director, 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. If the profile is a Citrix user profile, the profile is already reset by the time the user's desktop appears. If the profile is 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:

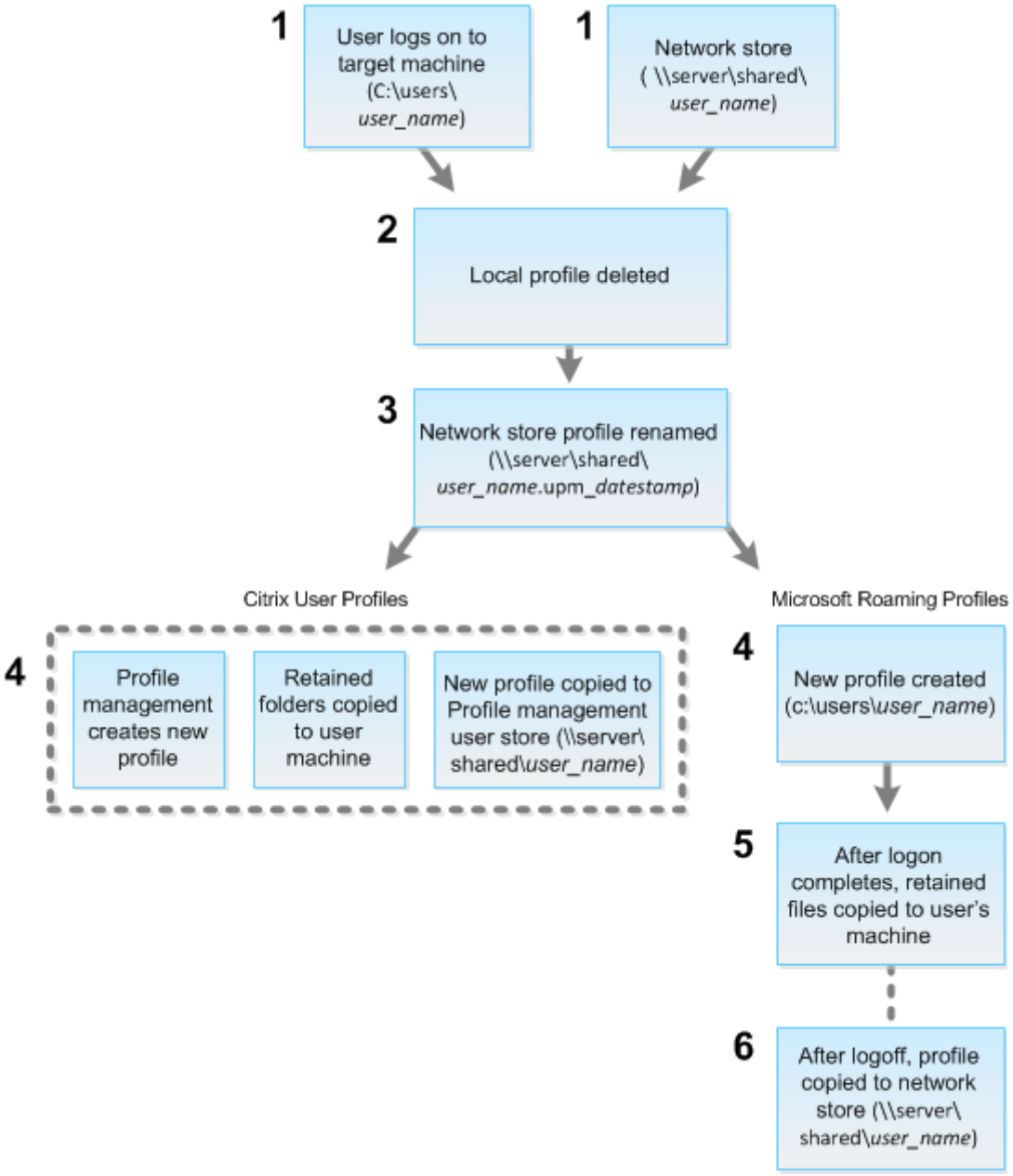
- Desktop
- Cookies
- Favorites
- Documents
- Pictures
- Music
- Videos

> **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 Director or using the PowerShell SDK), Director first identifies the user profile in use and issues an appropriate reset command. Director 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 Director 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 the user is processed by Profile management, but receives a roaming profile command, it is rejected (or vice versa).

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 required.

For Microsoft roaming profiles, a new profile is created by Windows, 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.

To reset a profile using PowerShell SDK

You can reset a profile using the Broker PowerShell SDK.

New-BrokerMachineCommand

Creates a command queued for delivery to a specific user, session, or machine. For more information about this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/.

Examples

See the following examples for details about how to use the PowerShell cmdlets to reset a profile:

Reset a Profile Management profile

- Suppose you want to reset the profile for user1. Use the New-BrokerMachineCommand PowerShell command. For example:


```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName
  "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -
  SendTrigger logon -user domain1\user1
```

> **Important:**
>
> The `CommandData $byteArray` must be in the following format: `<SID>[,<backup path>]`. If you do not provide the backup path, Profile Management generates a backup folder named by current date and time.

Reset a Windows roaming profile

- Suppose you want to reset the roaming profile for user1. Use the New-BrokerMachineCommand PowerShell command. For example:

```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName
  "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray
  -SendTrigger logon -user domain1\user1
```

Record sessions

February 7, 2020

You can record ICA sessions using the Session Recording controls from the **User Details** and **Machine Details** screen in Director. This feature is available for customers on **Premium** Sites.

To configure Session Recording on Director using the DirectorConfig tool, see the **Configure Director to use the Session Recording Server** section in Create and activate recording policies.
The Session Recording controls are available in Director only if the logged in user has the permission to modify the Session Recording policies. This permission can be set on the Session Recording Authorization console as described in Create and activate recording policies.

> **Note:**
> Changes made to the Session Recording settings through Director or the Session Recording Policy console take effect starting from the subsequent ICA session.

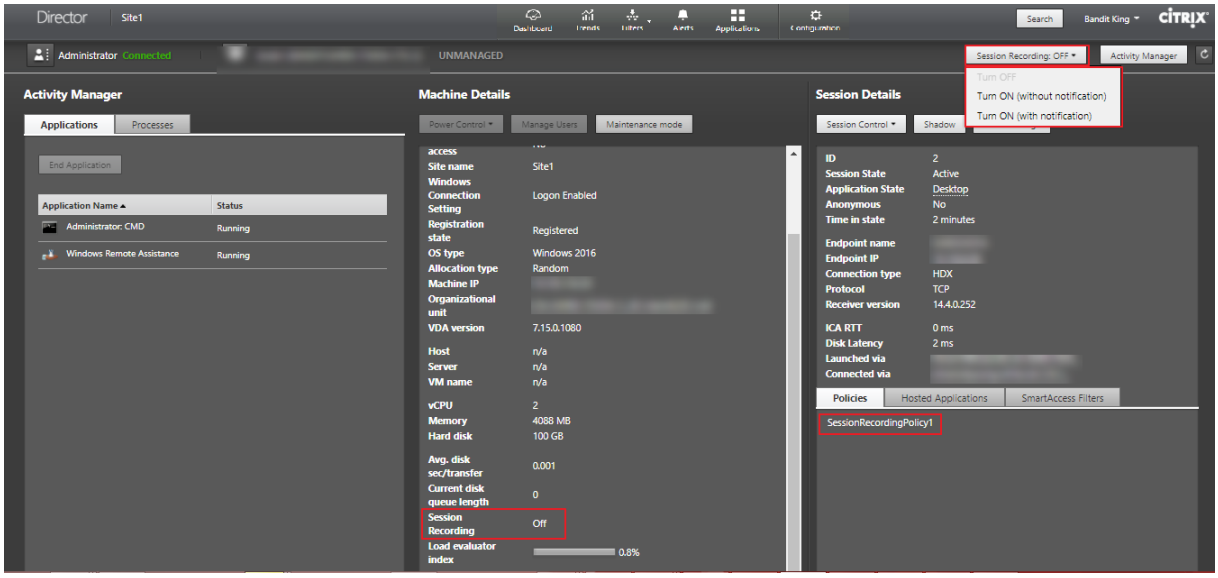
Session Recording controls in Director

You can enable Session Recording for a specific user on the **Activity Manager** or the **User Details** screen. Subsequent sessions are recorded for the specific user on all supported servers.

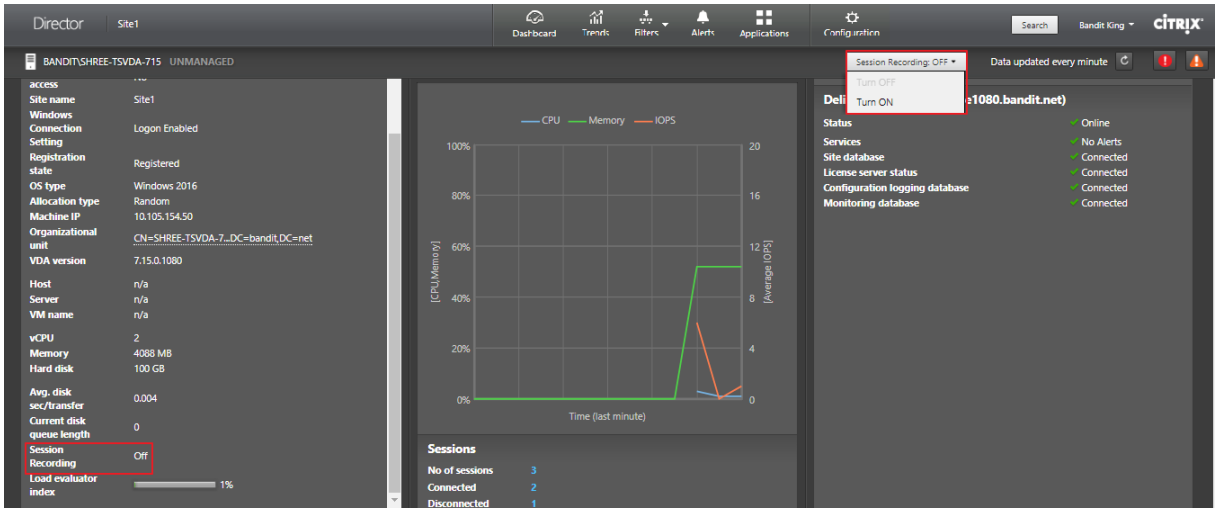
You can:

- Turn ON (with notification) - the user is notified about the session being recorded on logging on to the ICA session.
- Turn ON (without notification) - the session is recorded silently without notifying the user.
- Turn OFF - disable recording of sessions for the user.

The Policies Panel displays the name of the active Session Recording policy.



You can enable Session Recording for a specific machine from the Machine Details page. Subsequent sessions on the machine are recorded. The Machine Details panel displays the status of the Session Recording policy for the machine.



Feature compatibility matrix

August 17, 2022

Citrix Director 7 1912 is compatible with:

- Citrix Virtual Apps and Desktops 7 1909 and later
- XenApp and XenDesktop Version 7.15 LTSR

Within each Site, although you can use Director with earlier versions of Delivery Controller, all the features in the latest version of Director might not be available. Citrix recommends having Director, Delivery Controller, and the VDAs at the same version.

> **Note:**
> After you upgrade a Delivery Controller, you are prompted to upgrade the Site when you open Studio. For more information, see the **Upgrade Sequence** section in Upgrade a deployment.

The first time you log in after a Director upgrade, a version check is performed on the configured Sites. If any Site is running a version of the Controller earlier than that of Director, a message appears on the Director console, recommending a Site upgrade. Additionally, as long as the version of the Site is older than that of Director, a note continues to be displayed on the Director Dashboard indicating this mismatch.

> **Note:**
>
> Earlier versions of Citrix Director do not display policies applied to user sessions running on recent VDA versions. Citrix Director 1912 and earlier versions do not display policies applied to user sessions running on VDA versions 2003 and later. Use Citrix Director versions 2003 and later to view those policies.

Specific Director features with the minimum version of Delivery Controller (DC), VDA and other dependent components required along with License Edition are listed below.

Director Version	Feature	Dependencies - min version required	Edition
1909	Configure on-prem Sites with Citrix Analytics for Performance	DC 7 1906 and VDA 1906	All
1906	Session Auto Reconnect	DC 7 1906 and VDA 1906	All

Director Version	Feature	Dependencies - min version required	Edition
1906	Session startup duration	DC 7 1906 and VDA 1903	All
1906	Desktop probing	DC 7 1906 and Citrix Probe Agent 1903	Premium
7.9 and later	Citrix Profile Management Duration in Profile Load	VDA 1903	All
1811	Profile Drilldown	DC 7 1811 and VDA 1811	All
1811	Hypervisor Alerts Monitoring	DC 7 1811	Premium
1811	Application probing	DC 7 1811 and Citrix Application Probe Agent 1811	Premium
1811	Microsoft RDS license health	DC 7 1811 and VDA 7.16	All
1808	Export of Filters data	DC 7 1808	All
1808	Interactive Session drill down	DC 7 1808 and VDA 1808	All
1808	GPO drill down	DC 7 1808 and VDA 1808	All
1808	Machine historical data available using OData API	DC 7 1808	All
7.18	Application probing	DC 7.18	Premium (formerly Platinum)
7.18	Smart alert policies	DC 7.18	Premium (formerly Platinum)
7.18	Health Assistant link	None	All
7.18	Interactive Session drill-down	None	All
7.17	PIV smart card authentication	None	All
7.16	Application Analytics	DC 7.16 and VDA 7.15	All

Director Version	Feature	Dependencies - min version required	Edition
7.16	OData API V.4	DC 7.16	All
7.16	Shadow Linux VDA users	VDA 7.16	All
7.16	Domain local group support	None	All
7.16	Machine console access	DC 7.16	All
7.15	Application failure monitoring	DC 7.15 and VDA 7.15	All
7.14	Application-centric troubleshooting	DC 7.13 and VDA 7.13	All
7.14	Disk Monitoring	DC 7.14 and VDA 7.14	All
7.14	GPU Monitoring	DC 7.14 and VDA 7.14	All
7.13	Transport protocol on Session Details panel	DC 7.x and VDA 7.13	All
7.12	User-friendly Connection and Machine failure descriptions	DC 7.12 and VDA 7.x	All
7.12	Increased historical data availability in Enterprise edition	DC 7.12 and VDA 7.x	Enterprise
7.12	Custom Reporting	DC 7.12 and VDA 7.x	Premium (formerly Platinum)
7.11	Resource utilization reporting	DC 7.11 and VDA 7.11	All
7.11	Alerting extended for CPU, memory and ICA RTT conditions	DC 7.11 and VDA 7.11	Premium (formerly Platinum)
7.11	Export report improvements	DC 7.11 and VDA 7.x	All

Director Version	Feature	Dependencies - min version required	Edition
7.11	Integration with Citrix ADM	DC 7.11, VDA 7.x and MAS version 11.1 Build 49.16	Premium (formerly Platinum)
7.9	Logon Duration breakdown	DC 7.9 and VDA 7.x	All
7.7	Proactive monitoring and alerting	DC 7.7 and VDA 7.x	Premium (formerly Platinum)
7.7	SCOM integration	DC 7.7, VDA 7.x, SCOM 2012 R2, and PowerShell 3.0	Premium (formerly Platinum)
7.7	Windows Authentication Integration	DC 7.x and VDA 7.x	All
7.7	Single-session and Multi-session OS Usage	DC 7.7 and VDA 7.x	Premium (formerly Platinum)
7.6.300	Support for Framehawk virtual channel	DC 7.6 and VDA 7.6	All
7.6.200	Session recording integration	DC 7.6 and VDA 7.x	Premium (formerly Platinum)
7	HDX Insight integration	DC 7.6, VDA 7.x, and Citrix ADM	Premium (formerly Platinum)

Data granularity and retention

November 24, 2022

Aggregation of data values

The Monitor Service collects a variety of data, including user session usage, user logon performance details, session load balancing details, and connection and machine failure information. Data is aggre-

gated 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 of time. 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 of time, therefore are exposed as sums over a time period.

Concurrent data evaluation

Sessions must be overlapping to be considered concurrent. However, when the time interval is 1 minute, all sessions in that minute (whether or not 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 of time. These metrics are aggregated into the summary table for complete intervals. There will be 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 will have no data. Although raw data may exist for those partial intervals, it will never be summarized. You can determine the earliest and latest aggregate interval for a particular data granularity by pulling the min and max SummaryDate from a particular summary table. 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 above. They can be used for historical trends, but raw events may be more current in the state than what has been summarized for trend analysis. Any time-based comparison of summary to raw data needs to take into account that there will be no summary data for partial intervals that may occur or for the beginning and ending of the time period.
- **Missed and latent events.** Metrics that are aggregated into the summary table may 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 will be gaps in the summary data counts of current connections, but the session instances will still be 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 may be missing because it has been groomed away from summary or raw tables. Retention periods may 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 may 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 may be some discrepancy as to where data is aggregated.

Granularity and retention

The granularity of aggregated data retrieved by Director is a function of the time (T) span requested. The rules are as follows:

- 0 < T <= 1 hour uses per-minute granularity
- 0 < T <= 30 days uses per-hour granularity
- T > 31 days uses 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. Customers on Premium licensed Sites can change the grooming retention to their desired number of retention days, otherwise the default is used. In case of connectivity loss with the Site database, Monitor Service will use the default retention days for Premium entitlement as specified in the table below.

To access the settings, run the following PowerShell commands on the Delivery Controller:


```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

	Setting name	Affected grooming	Default value Premium (days)	Default value non-Premium (days)
1	GroomSessionsRetentionDays	Session, Connection records retention after Session termination	90	7
2	GroomFailuresRetentionDays	MachineFailureLog and Connection-FailureLog records	90	7
3	GroomLoadIndexesRetentionDays	LoadIndex records	90	7
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	7

	Setting name	Affected grooming	Default value Premium (days)	Default value non-Premium (days)
5	GroomSummariesRetentionDays	Desktop Group Summary, FailureLog-Summary, and LoadIn-dexSummary records. Aggregated data - daily granularity.	90	7
6	GroomMachineHotfixLogRetentionDays	Hotfixes applied to the VDA and Controller machines	90	90
7	GroomMinuteRetentionDays	Aggregated data - minute granularity	3	3
8	GroomHourlyRetentionDays	Aggregated data - hourly granularity	32	7
9	GroomApplicationInstanceRetentionDays	Application Instance history	90	0
10	GroomNotificationLogRetentionDays	Notification Log records	90	
11	GroomResourceUsageRawDataRetentionDays	Resource utilization data - raw data	1	1
12	GroomResourceUsageMinuteDataRetentionDays	Resource utilization summary data - minute granularity	7	7

	Setting name	Affected grooming	Default value Premium (days)	Default value non-Premium (days)
13	GroomResourceUsageHourDataRetentionDays	Resource utilization summary data - hour granularity	30	7
14	GroomResourceUsageDayDataRetentionDays	Resource utilization summary data - day granularity	90	7
15	GroomProcessUsageRawDataRetentionDays	Process utilization data - raw data	1	1
16	GroomProcessUsageMinuteDataRetentionDays	Process utilization data - minute granularity	3	3
17	GroomProcessUsageHourDataRetentionDays	Process utilization data - hour granularity	7	7
18	GroomProcessUsageDayDataRetentionDays	Process utilization data - day granularity	30	7
19	GroomSessionMetricsDataRetentionDays	Session metrics data	1	1
20	GroomMachineMetricDataRetentionDays	Machine metrics data	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	Machine metrics summary data	90	7
22	GroomApplicationErrorRetentionDays	Application error data	1	1

	Setting name	Affected grooming	Default value Premium (days)	Default value non-Premium (days)
23	GroomApplicationFailureRetentionDays	Application failure data	1	1

> **Caution:**
>
> Modifying values on the Monitor Service database requires restarting the service for the new values to take effect. You are advised to make changes to the Monitor Service database only under the direction of Citrix Support.

The settings GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays, and GroomSessionMetricsDataRetentionDays are limited to their default values of 1, while GroomProcessUsageMinuteDataRetentionDays is limited to its default value of 3. The PowerShell commands to set these values have been disabled, as the process usage data tends to grow quickly. Additionally, license based retention settings are as follows:

- **Premium licensed Sites -** you can update the grooming retention settings above to any number of days.
- **Advanced licensed Sites -** the grooming retention for all settings is limited to 31 days.
- **All other Sites -** the grooming retention for all settings is limited to 7 days.

Exceptions:

- GroomApplicationInstanceRetentionDays can be set only in Premium licensed Sites.
- GroomApplicationErrorsRetentionDays and GroomApplicationFaultsRetentionDays are limited to 31 days in Premium licensed Sites.

Retaining data for long periods will have 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 could 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 may be large. Excessively large amounts of data may 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 will grow very fast. For example, two years' worth of these tables would gather more than a TB of data, requiring a high-end enterprise-level database.

Citrix Director failure reasons and troubleshooting

April 19, 2024

The following tables describe the various failure categories, the reasons, and the action you need to take to resolve the issues. For more information, see Enums, error codes, and descriptions.

Connection failure errors

Category	Reason	Issue	Action
N/A	[0] Unknown. This error code is not mapped.	The Monitoring service cannot determine the reason for the reported launch or connection failure from information shared by the Brokering service.	Collect CDF logs on the controller and contact Citrix support.
[0] None	[1] None	None	N/A
[2] MachineFailure	[2] SessionPreparation	Session preparation request from the delivery controller to the VDA failed. Possible causes: Communication issues between the controller and the VDA, issues experienced by the Broker Service while creating a prepare request, or network issues resulting in the VDA not accepting the request.	Refer to troubleshooting steps listed in Knowledge center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops for common problems that cause communication issues between the controller and the VDA.

Category	Reason	Issue	Action
[2] MachineFailure	[3] RegistrationTimeout	The VDA was powered on, but a time-out occurred while it was attempting to register with the delivery controller.	Verify that the Citrix Broker Service is running on the delivery controller and that the Desktop service is running on the VDA. Start each if stopped.
[1] ClientConnection-Failure	[4] ConnectionTimeout	The client did not connect to the VDA after the VDA was prepared for session launch. The session was successfully brokered, but a time-out occurred while waiting for the client to connect to the VDA. Possible causes: Firewall settings, network interruptions, or settings that prevent remote connections.	Check the Director console to see if the client currently has an active connection, which means no user is impacted. If no session exists, review the event logs on the client and on the VDA for any errors. Resolve any issues with network connectivity between the client and the VDA.

Category	Reason	Issue	Action
[4] NoLicensesAvailable	[5] Licensing	The licensing request failed. Possible causes: Insufficient number of licenses, or the license server has been down for more than 30 days.	Verify that the license server is online and reachable. Resolve any network connectivity issues to the license server or reboot the license server if it appears to be malfunctioning. Verify that there are sufficient licenses in the environment and allocate more if necessary.
[1] ClientConnection-Failure	[6] Ticketing	A failure occurred during ticketing, indicating that the client connection to the VDA does not match the brokered request. A launch request ticket is prepared by the Broker and delivered in the ICA file. When the user attempts to launch a session, the VDA validates the launch ticket in the ICA file with the Broker. Possible causes: ICA file is corrupt or the user is attempting to make an unauthorized connection.	Verify that the user has access to the application or desktop based on user groups defined in the delivery groups. Instruct the user to relaunch the application or desktop to determine whether this is a one off issue. If the issue occurs again, review the client device event logs for errors. Verify that the VDA to which the user is attempting to connect is registered. If unregistered, review the event logs on the VDA and resolve any registration issues.

Category	Reason	Issue	Action
[1] ClientConnection-Failure	[7] Other	A session has been reported as terminated from the VDA after the client has initially contacted the VDA but before it completed the connection sequence.	Verify if the session was not terminated by the user before launch. Try relaunching the session, if the problem persists, collect CDF logs and contact Citrix support.
[1] ClientConnection-Failure	[8] GeneralFail	The session failed to launch. Possible causes: A brokered launch was requested while the broker was still starting up or initializing, or internal error during the brokering phase of a launch.	Verify that the Citrix Broker Service is running and retry launching the session.
[5] Configuration	[9] MaintenanceMode	The VDA, or the delivery group to which the VDA belongs, is set in maintenance mode.	Determine whether maintenance mode is required. Disable maintenance mode on the delivery group or machine in question if it is not needed and instruct the user to attempt to reconnect.
[5] Configuration	[10] ApplicationDisabled	The application cannot be accessed by end users because it has been disabled by the administrator.	If the application is intended to be available for production use, enable the application and instruct the user to reconnect.

Category	Reason	Issue	Action
[4] NoLicensesAvailable	[11] LicenseFeature Refused	The feature being used is not covered by the existing licenses.	Contact a Citrix sales representative to confirm the features that are covered by the existing Citrix Virtual Apps and Desktops license edition and type.
[3] NoCapacityAvailable	[13] SessionLimitReached	All VDAs are in use and there is no capacity to host more sessions. Possible causes: All VDAs are in use (for single-session OS VDAs), or all VDAs have reached the configured maximum concurrent sessions allowed (for multi-session OS VDAs).	Verify if there are any VDAs in maintenance mode. Disable maintenance mode if it is not needed to free up more capacity. Consider increasing the value of **Maximum Number of Sessions** in the Citrix policy setting to allow more sessions per server VDA. Consider adding more multi-session OS VDAs. Consider adding more single-session OS VDAs.
[5] Configuration	[14] DisallowedProtocol	The ICA and RDP protocols are not allowed.	Run the **Get-BrokerAccessPolicyRule** PowerShell command on the delivery controller and verify that the **AllowedProtocols** value has all the desired protocols listed. This issue occurs only if there is a misconfiguration.

Category	Reason	Issue	Action
[5] Configuration	[15] ResourceUnavailable	The application or desktop to which the user is attempting to connect is not available. This application or desktop might not exist, or there are no VDAs available to run it. Possible causes: The application or desktop has been unpublished, or the VDAs hosting the application or desktop have reached maximum load, or the application or desktop is set in maintenance mode.	Verify that the application or desktop is still published and the VDAs are not in maintenance mode. Determine whether the multi-session OS VDAs are at full load. If so, provision more multi-session OS VDAs. Verify that there are single-session OS VDAs available for connections. Provision more single-session OS VDAs if necessary.
[5] Configuration	[16] ActiveSessionReconnectDisabled	The ICA session is active and connected to a different endpoint. However, because the **Active Session Reconnection** is disabled, the client cannot connect to the active session.	On the delivery controller, verify that **Active Session Reconnection** is enabled. Verify that the value of **DisableActiveSessionReconnect** in the registry, under **HKEY_LOCAL_MACHINE\Software** is set to 0.
[2] MachineFailure	[17] NoSessionToReconnect	The client attempted to reconnect to a specific session but the session was terminated.	Retry the workspace control reconnection.

Category	Reason	Issue	Action
[2] MachineFailure	[18] SpinUpFailed	The VDA cannot be powered on for session launch. This is a hypervisor reported issue.	If the machine is still powered off, attempt to start the machine from Citrix Studio. If this fails, review the hypervisor connectivity and permissions. If the VDA is a PVS-provisioned machine, verify in the PVS console that the machine is running. If not, verify that the machine is assigned a Personal vDisk, log in to the hypervisor to reset the VM.
[2] MachineFailure	[19] Refused	The delivery controller sends a request to the VDA to prepare for a connection from an end user, but the VDA actively refuses this request.	Verify via ping, that the delivery controller and the VDA can successfully communicate. If not, resolve any firewall or network routing issues.

Category	Reason	Issue	Action
[2] MachineFailure	[20] ConfigurationSet Failure	The delivery controller did not send required configuration data, such as policy settings and session information, to the VDA during session launch. Possible causes: Communication issues between the controller and the VDA, issues experienced by the Broker Service while creating a configuration set request, or network issues resulting in the VDA not accepting the request.	-
[3] NoCapacityAvailable	[21] MaxTotalInstance-sExceeded	The maximum number of instances of an application has been reached. No additional instances of the application can be opened on the VDA. This issue is related to the application limits feature.	Consider increasing the application setting, **Limit the number of instances running at the same time** to a higher value if licensing permits.

Category	Reason	Issue	Action
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	The user is attempting to open more than one instance of an application but the application is configured to allow only a single instance of the application per user. This issue is related to the application limits feature.	Only one instance of the application is allowed per user by default. If multiple instances per user are required, consider clearing the **Limit to one instance per user** setting in the application setting.
[1] ClientConnectionFailure	[23] Communication error	The delivery controller attempted to send information to the VDA, such as a request to prepare for a connection, but an error occurred during the communication attempt. This can be caused due to network disruptions.	If already started, restart the Desktop service on the VDA to restart the registration process and verify that the VDA registers successfully. Confirm that the delivery controllers configured for the VDA are accurate via the details in the application event log.

Category	Reason	Issue	Action
[3] NoCapacityAvailable	[100] NoMachineAvailable Monitoring service converts [12] NoDesktopAvailable to this error code.	The VDA assigned to launch the session is in an invalid state or is unavailable. Possible causes: Power state of the VDA is unknown or unavailable, the VDA did not reboot since the last user's session, session sharing is disabled while the current session requires it to be enabled, or the VDA was removed from the delivery group or from the site.	Verify that the VDA is in a delivery group. If not, add it to the appropriate delivery group. Verify that there are sufficient VDAs registered and in ready state to be able to launch the published shared desktop or application requested by the user. Verify that the hypervisor hosting the VDA is not in maintenance mode.
[2] MachineFailure	[101] MachineNotFunctional. Monitoring service converts [12] NoDesktopAvailable to this error code.	The VDA is not operational. Possible causes: The VDA was removed from the delivery group, the VDA is unregistered, the VDA power state is unavailable, or the VDA is experiencing internal issues.	Verify that the VDA is in a delivery group. If not, add it to the appropriate delivery group. Verify that the VDA shows as powered on in Citrix Studio. If the power state is unknown for several machines, resolve any issues with connectivity to the hypervisor or host failures. Verify that the hypervisor hosting the VDA is not in maintenance mode. Restart the VDA once these issues have been addressed.

Machine failure type

Error Code	Error Code ID	Issue	Action
Unknown	-	-	-
Unregistered	3	-	-
MaxCapacity	4	The load index on the hypervisor is at its maximum capacity.	Ensure that all hypervisors are powered on. Add more capacity to the hypervisor. Add more hypervisors.
StuckOnBoot	2	The VM did not complete its boot sequence and is not communicating with the hypervisor.	Ensure that the VM booted successfully on the hypervisor. Check for other messages on the VM, such as OS issues. Ensure that the hypervisor tools are installed on the VM. Ensure that the VDA is installed on the VM.
FailedToStart	1	The VM experienced issues when trying to start on the hypervisor.	Check the hypervisor logs.
None	0	-	-

Machine deregistration reason (applicable when failure type is Unregistered or Unknown)

Error Code	Error Code ID	Issue	Action
AgentShutdown	0	The VDA experienced a graceful shutdown.	Power on the VDA if you do not expect it to be off based on existing power management policies. Review any errors in the event logs.
AgentSuspended	1	The VDA is in hibernation or sleep mode.	Take the VDA out of hibernation mode. Consider disabling hibernation for Citrix Virtual Apps and Desktops VDAs via power settings.
IncompatibleVersion	100	The VDA cannot communicate with the delivery controller due to a mismatch in the Citrix protocol versions.	Align the VDA and delivery controller versions.
AgentAddressResolutionFailed	101	The delivery controller was not able to resolve the VDA's IP address.	Verify that the VDA machine account exists in AD. If not, create it. Verify that the name and the IP address of the VDA in DNS are accurate. If not, correct them. If widespread, validate the DNS settings on the delivery controllers. Verify DNS resolution from the controller by running the `nslookup` command.

Error Code	Error Code ID	Issue	Action
	101	The delivery controller was not able to resolve the VDA's IP address.	Verify that the VDA machine account exists in AD. If not, create it. Verify that the name and the IP address of the VDA in DNS are accurate. If not, correct them.
AgentNotContactable	102	A communication issue occurred between the delivery controller and the VDA.	Use a ping to verify that the delivery controller and the VDA can successfully communicate. If not, resolve any firewall or network issues. Refer to the troubleshooting steps listed in Knowledge Center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA.

Error Code	Error Code ID	Issue	Action
	102	A communication issue occurred between the delivery controller and the VDA.	Refer to troubleshooting steps listed in Knowledge Center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA. Contact Citrix support.
AgentWrongActiveDirectoryOU	103	An Active Directory discovery misconfiguration occurred. The site-specific OU (where the site controller info is stored in AD) configured in the VDA registry is for a different Site.	Ensure the active directory configuration is correct, or check registry settings.
EmptyRegistrationRequest	104	The registration request sent from the VDA to the delivery controller was empty. This can be due to a corrupt VDA software installation.	Restart the Desktop service on the VDA to restart the registration process and verify that the VDA registers correctly via the application event log.
MissingRegistrationCapabilities	105	The VDA version is not compatible with the delivery controller.	Upgrade the VDA or remove the VDA and then reinstall it.

Error Code	Error Code ID	Issue	Action
MissingAgentVersion	106	The VDA version is not compatible with the delivery controller.	Reinstall the VDA software if the issue is impacting all machines.
InconsistentRegistrationCapabilities	107	The VDA cannot communicate its capabilities to the Broker. This can be due to incompatibility between the VDA and delivery controller versions. The registration capabilities, which change with each version, are expressed in a form that does not match the registration request.	Align the VDA and delivery controller versions.
NotLicensedForFeature	108	The feature you are attempting to use is not licensed.	Check your Citrix licensing edition, or remove the VDA and then reinstall it.
	108	The feature you are attempting to use is not licensed.	Contact Citrix support.
UnsupportedCredentialSecurityversion	109	The VDA and the delivery controller are not using the same encryption mechanism.	Align the VDA and delivery controller versions.

Error Code	Error Code ID	Issue	Action
InvalidRegistrationRequest	110	The VDA made a registration request to the Broker but the content of the request is corrupt or invalid.	Refer to the troubleshooting steps listed in Knowledge Center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA.
SingleMultiSessionMismatch	111	The VDA's operating system type is not compatible with the machine catalog or delivery group.	Add the VDA to the correct machine catalog type or delivery group containing machines with the same operating system.
FunctionalLevelTooLowForCatalog	112	The machine catalog is set to a higher VDA functional level than the installed VDA version.	Verify that the VDA's machine catalog functional level matches that of the VDA. Upgrade or downgrade the machine catalog to match that of the VDA.
FunctionalLevelTooLowForDesktopGroup	113	The delivery group is set to a higher VDA functional level than the installed VDA version.	Verify that the VDA's delivery group functional level matches that of the VDA. Upgrade or downgrade the machine catalog to match that of the VDA.

Error Code	Error Code ID	Issue	Action
PowerOff	200	The VDA did not shut down gracefully.	If the VDA is supposed to be powered on, attempt to start the VDA from Citrix Studio and verify that it boots up and registers correctly. Troubleshoot any boot or registration issues. Review the event logs on the VDA once it is back up to help determine the root cause of the shutdown.
AgentRejectedSettingsUpdate	203	Settings such as Citrix policies were changed or updated but there was an error in sending the updates to the VDA. This can occur if the updates are incompatible with the installed VDA version.	Upgrade the VDA if necessary. Review whether the updates that were applied are supported with the VDA version.
SessionPrepareFailure	206	The Broker did not complete an audit of the sessions that are running on the VDA.	If widespread, restart the Citrix Broker Service on the delivery controller.
	206	The Broker did not complete an audit of the sessions that are running on the VDA.	Contact Citrix support.

Error Code	Error Code ID	Issue	Action
ContactLost	207	The delivery controller lost connection with the VDA. This can be caused by network disruptions.	Verify that the Citrix Broker Service is running on the delivery controller and the Desktop service is running on the VDA. Start each if stopped. If already started, restart the Desktop service on the VDA to restart the registration process and verify that the VDA registers successfully. Confirm that the delivery controllers configured for the VDA are accurate via the details in the Application event log. Use a ping to verify that the delivery controller and the VDA can successfully communicate. If not, resolve any firewall or network issues.
	207	The delivery controller lost connection with the VDA. This can be caused by network disruptions.	Verify that the Desktop service is running on the VDA. Start if stopped.

Error Code	Error Code ID	Issue	Action
BrokerRegistrationLimitReached	201	The delivery controller has reached the configured maximum number of VDAs that are allowed to concurrently register with it. By default, the delivery controller allows 10,000 concurrent VDA registrations.	Consider adding delivery controllers to the Site or creating a Site. You can also increase the number of VDAs allowed to concurrently register with the delivery controller via the **HKEY_LOCAL_MACHINE\Software** registry key. See Knowledge Center article, Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446) for more information. Increasing this number might require more CPU and memory resources for the controller.
SettingsCreationFailure	208	The Broker did not construct a set of settings and configurations to send to the VDA. If the Broker is unable to gather the data, registration fails and the VDA becomes unregistered.	Check the event logs on the delivery controller for any errors. Restart the Broker Service if a specific issue is not evident in the logs. Once the Broker Service is restarted, restart the Desktop service on the affected VDAs and verify that they successfully register.

Error Code	Error Code ID	Issue	Action
	208	The Broker did not construct a set of settings and configurations to send to the VDA. If the Broker is unable to gather the data, registration fails and the VDA becomes unregistered.	Restart the Desktop service on the affected VDAs and verify that they successfully register. Contact Citrix support.
SendSettingsFailure	204	The Broker did not send settings and configuration data to the VDA. If the Broker can gather the data but is unable to send it, registration fails.	If limited to a single VDA, restart the Desktop service on the VDA to force reregistration and validate that the VDA registers successfully via the application event log. Troubleshoot any errors seen. Refer to the troubleshooting steps listed in Knowledge center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA.
AgentRequested	2	An unknown error occurred.	Contact Citrix support.

Error Code	Error Code ID	Issue	Action
DesktopRestart	201	An unknown error occurred.	Contact Citrix support.
DesktopRemoved	202	An unknown error occurred.	Contact Citrix support.
SessionAuditFailure	205	An unknown error occurred.	Contact Citrix support.
UnknownError	300	An unknown error occurred.	Contact Citrix support.
RegistrationStateMismatch	302	An unknown error occurred.	Contact Citrix support.
Unknown	-	An unknown error occurred.	Contact Citrix support.

SDKs and APIs

September 29, 2021

Several SDKs and APIs are available with this release. To access the SDKs and APIs, go to Build anything with Citrix. From there, select **Citrix Workspace** to access programming information for Citrix Virtual Apps and Desktops and its related components.

> **Note:**
>
> The Citrix Virtual Apps and Desktops SDK and the Citrix Group Policy SDK can be installed as a module or a snap-in. Several component SDKs (such as Citrix Licensing, Citrix Provisioning, and StoreFront) install using only a snap-in.

Citrix Virtual Apps and Desktops SDK

This SDK installs automatically as a PowerShell module when you install a Delivery Controller or Studio. This enables you to use this SDK's cmdlets without having to add snap-ins. (Instructions are provided below if you choose to install this SDK as a snap-in.)

Permissions

You must run the shell or script using an identity that has Citrix administration rights. Although members of the local administrators group on the Controller automatically have full administrative privi-

leges to allow Citrix Virtual Apps or Citrix Virtual Desktops to be installed, Citrix recommends that for normal operation, you create Citrix administrators with the appropriate rights, rather than use the local administrators account.

Access and run the cmdlets

1. Start a shell in PowerShell: Open Studio, select the **PowerShell** tab, and then click **Launch PowerShell**.
2. To use SDK cmdlets within scripts, set the execution policy in PowerShell. For information about PowerShell execution policy, see the Microsoft documentation.
3. If you want to use the snap-in (rather than the module), add the snap-in using the `Add-PSSnapin` (or `asnp`) cmdlet.

   V1 and V2 denote the version of the snap-in. XenDesktop 5 snap-ins are version 1. Citrix Virtual Apps and Desktops, and earlier XenDesktop 7 version snap-ins are version 2. For example, to install Citrix Virtual Apps and Desktops snap-in, type `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. To import all the cmdlets, type: `Add-PSSnapin Citrix.*.Admin.V*`

You can now use the cmdlets and help files.

- To access the help files for this SDK, select the product or component in the Categories list, and then select **Citrix Virtual Apps and Desktops SDK**.
- For PowerShell guidance, see Windows PowerShell Integrated Scripting Environment (ISE).

Group Policy SDK

The Citrix Group Policy SDK enables you to display and configure Group Policy settings and filters. This SDK uses a PowerShell provider to create a virtual drive that corresponds to the machine and user settings and filters. The provider appears as an extension to `New-PSDrive`.

To use the Group Policy SDK, either Studio or the Citrix Virtual Apps and Desktops SDK must be installed.

The Citrix Group Policy PowerShell provider is available as a module or a snap-in.

- To use the module, no additional work is needed.
- To add the snap-in, type `Add-PSSnapin citrix.common.grouppolicy`.

To access help, type: `help New-PSDrive -path localgpo:/`.

To create a virtual drive and load it with settings, type `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` where the Controller string is the fully qualified domain name of a Controller in the site you want to connect to and load settings from.

Monitor Service OData

The Monitor API allows access to the Monitor Service data using Version 3 or 4 of the OData API. You can create customized monitoring and reporting dashboards based on data queried from the Monitor Service data. OData V.4 is based on the ASP.NET Web API and supports aggregation queries.

For more information, see the Monitor Service OData API.

WCAG 2.0 Voluntary Product Accessibility Templates

May 12, 2021

Section 508 compliance and WCAG 2.0 commitment

Citrix is committed to making technology accessible to everyone. We are currently engaged in high-priority initiatives to design and engineer products with a focus on improved usability and accessibility for all customers, with or without a disability. Citrix is committed to supporting well known accessibility standards including Section 508 compliance and WCAG 2.0.

Harmonization of Section 508 compliance and WCAG 2.0

The World Wide Web Consortium (W3C) developed the *Web Content Accessibility Guidelines* or WCAG. It is a globally recognized standard ISO/IEC 40500 that provides a range of stipulations for making web content more accessible. On the domestic United States front, there is a similar requirement as well. Section 508 is part of the Federal Acquisition Regulation (FAR) that comes from the Rehabilitation Act of 1973. Like WCAG, its primary objective is to provide equivalent access to, and use of the Federal agencies'electronic and information technology (ICT) by individuals with disabilities. In January 2017, the Access Board published a rule to harmonize Section 508 and WCAG 2.0. As a result, Citrix is focusing more on the most recent updates to WCAG in order to provide the most accessible products to our customers.

Voluntary Product Accessibility Template (VPAT) documents

VPAT documents for various Citrix products and components are available for download from https://www.citrix.com/about/legal/security-compliance/section-508.html.