# XenApp and XenDesktop 7.15 LTSR

# Contents

**What's new** 13

**Cumulative Update 9 (CU9)** 13

**Fixed issues** 18

**Cumulative Update 8 (CU8)** 21

**Fixed issues** 26

**Cumulative Update 7 (CU7)** 32

**Fixed issues** 37

**Cumulative Update 6 (CU6)** 45

**Fixed issues** 50

**Cumulative Update 5 (CU5)** 61

**Fixed issues** 65

**Cumulative Update 4 (CU4)** 76

**Fixed issues** 83

**Cumulative Update 3 (CU3)** 99

**Fixed issues** 105

**Cumulative Update 2 (CU2)** 124

**Fixed issues** 128

**Cumulative Update 1 (CU1)** 143

**Fixed issues** 148

**7.15 LTSR (initial release)** 159

**Fixed issues** 165

**Known issues** 195

**Third party notices** 204

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Deprecation and removals** 205

**Section 508 Voluntary Product Accessibility Template** 209

**System requirements** 210

**Technical overview** 226

**Active Directory** 234

**Databases** 236

**Delivery methods** 243

**XenApp published apps and desktops** 245

**VM hosted apps** 247

**Network ports** 248

**HDX** 251

**Adaptive transport** 260

**Double hop in Citrix Virtual Apps and Desktops** 264

**Install and configure** 266

**Prepare to install** 268

**Microsoft Azure Resource Manager virtualization environments** 274

**Microsoft System Center Virtual Machine Manager virtualization environments** 279

**Microsoft System Center Configuration Manager environments** 283

**VMware virtualization environments** 286

**Nutanix virtualization environments** 293

**Microsoft Azure virtualization environments** 295

**Install core components** 297

**Install VDAs** 308

**Install using the command line** 325

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Install VDAs using scripts** 337

**Install VDAs with SCCM** 339

**Create a Site** 342

**Create machine catalogs** 346

**Manage machine catalogs** 359

**Create Delivery Groups** 366

**Manage Delivery Groups** 371

**Create Application Groups** 390

**Manage Application Groups** 398

**Remote PC Access** 403

**App-V** 411

**AppDisks** 422

**Publish content** 451

**Personal vDisk** 458

**Install and upgrade** 459

**Configure and manage** 463

**Tools** 474

**Displays, messages, and troubleshooting** 477

**Remove components** 487

**Upgrade and migrate** 489

**Changes in 7.x** 490

**Upgrade a deployment** 496

**Upgrade a XenApp 6.5 worker to a new VDA** 506

**Migrate XenApp 6.x** 507

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Secure** **535**

**Security considerations and best practices** **537**

**Integrate XenApp and XenDesktop with NetScaler Gateway** **545**

**Delegated Administration** **546**

**Smart cards** **553**

**Smart card deployments** **558**

**Pass-through authentication and single sign-on with smart cards** **565**

**Transport Layer Security (TLS)** **566**

**Federated Authentication Service** **579**

**Federated Authentication Service architectures overview** **605**

**Federated Authentication Service ADFS deployment** **614**

**Federated Authentication Service Azure AD integration** **619**

**Federated Authentication System how-to: configuration and management** **665**

**Federated Authentication Service certificate authority configuration** **666**

**Federated Authentication Service private key protection** **674**

**Federated Authentication Service security and network configuration** **691**

**Federated Authentication Service troubleshoot Windows logon issues** **702**

**Federated Authentication Service PowerShell cmdlets** **713**

**Graphics** **714**

**Framehawk** **716**

**HDX 3D Pro** **726**

**GPU acceleration for Windows Server OS** **728**

**GPU acceleration for Windows Desktop OS** **730**

**OpenGL Software Accelerator** **736**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Thinwire** **737**

**Multimedia** **741**

**Audio features** **744**

**Browser content redirection** **752**

**Flash redirection** **754**

**HTML5 multimedia redirection** **762**

**Windows Media redirection** **765**

**General Content Redirection** **766**

**Client folder redirection** **767**

**Host to client redirection** **768**

**Bidirectional content redirection** **775**

**Local App Access and URL redirection** **777**

**USB and client drive considerations** **785**

**Print** **795**

**Printing configuration example** **803**

**Best practices, security considerations, and default operations** **806**

**Printing policies and preferences** **808**

**Provision printers** **810**

**Maintain the printing environment** **818**

**Policies** **822**

**Work with policies** **824**

**Policy templates** **828**

**Create policies** **832**

**Compare, prioritize, model, and troubleshoot policies** **837**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Default policy settings** 841

**Policy settings reference** 867

**ICA policy settings** 871

**Auto client reconnect policy settings** 876

**Audio policy settings** 880

**Bandwidth policy settings** 882

**Bidirectional content redirection policy settings** 887

**Client sensors policy settings** 888

**Desktop UI policy settings** 889

**End user monitoring policy settings** 890

**Enhanced desktop experience policy setting** 891

**File Redirection policy settings** 892

**Flash Redirection policy settings** 896

**Graphics policy settings** 901

**Caching policy settings** 906

**Framehawk policy settings** 906

**Keep alive policy settings** 907

**Local App Access policy settings** 908

**Mobile experience policy settings** 908

**Multimedia policy settings** 909

**Multi-stream connections policy settings** 917

**Port redirection policy settings** 919

**Printing policy settings** 920

**Client printers policy settings** 922

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Drivers policy settings** 925

**Universal Print Server policy settings** 927

**Universal printing policy settings** 929

**Security policy settings** 931

**Server limits policy settings** 933

**Session limits policy settings** 933

**Session reliability policy settings** 935

**Time zone control policy settings** 937

**TWAIN devices policy settings** 938

**USB devices policy settings** 939

**Visual display policy settings** 942

**Moving images policy settings** 943

**Still images policy settings** 945

**WebSockets policy settings** 947

**Load management policy settings** 948

**Profile management policy settings** 950

**Advanced policy settings** 950

**Basic policy settings** 952

**Cross-platform policy settings** 955

**File system policy settings** 957

**Exclusions policy settings** 957

**Synchronization policy settings** 958

**Folder redirection policy settings** 960

**AppData(Roaming) policy settings** 961

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Contacts policy settings** 961

**Desktop policy settings** 962

**Documents policy settings** 962

**Downloads policy settings** 963

**Favorites policy settings** 964

**Links policy settings** 964

**Music policy settings** 965

**Pictures policy settings** 966

**Saved Games policy settings** 967

**Start menu policy settings** 967

**Searches policy settings** 968

**Video policy settings** 968

**Log policy settings** 969

**Profile handling policy settings** 973

**Registry policy settings** 976

**Streamed user profiles policy settings** 977

**Receiver policy settings** 979

**Virtual Delivery Agent policy settings** 980

**HDX 3D Pro policy settings** 982

**Monitoring policy settings** 982

**Virtual IP policy settings** 986

**Configure COM Port and LPT Port Redirection settings using the registry** 987

**Connector for Configuration Manager 2012 policy settings** 988

**Manage** 991

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Licensing** 993

**Multi-type licensing** 996

**Applications** 999

**Universal Windows Platform Apps** 1008

**Zones** 1011

**Connections and resources** 1024

**Local Host Cache** 1036

**Manage security keys** 1046

**Connection leasing** 1062

**Virtual IP and virtual loopback** 1065

**Delivery Controllers** 1069

**VDA registration** 1073

**Sessions** 1083

**Use Search in Studio** 1091

**Tags** 1091

**IPv4/IPv6 support** 1100

**User profiles** 1103

**Citrix Insight Services** 1109

**Citrix Scout** 1119

**Monitor** 1131

**Session Recording 7.15** 1132

**Get started with Session Recording** 1133

**Plan your deployment** 1134

**Security recommendations** 1137

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Scalability considerations** **1143**

**Install, upgrade, and uninstall Session Recording** **1155**

**Configure Session Recording** **1195**

**Grant access rights to users** **1200**

**Create and activate recording policies** **1200**

**Create notification messages** **1206**

**Disable or enable recording** **1207**

**Enable or disable live session playback and playback protection** **1208**

**Enable and disable digital signing** **1210**

**Specify where recordings are stored** **1210**

**Specify file size for recordings** **1211**

**Log administration activities** **1212**

**Install Session Recording with database high availability** **1215**

**View recordings** **1216**

**Open and play recordings** **1219**

**Play recorded sessions** **1220**

**Use events and bookmarks** **1224**

**Change the playback display** **1226**

**Cache recorded session files** **1228**

**Search for recordings** **1228**

**Troubleshoot Session Recording** **1230**

**Verify component connections** **1235**

**Search for recordings using the Player fails** **1238**

**Change your communication protocol** **1241**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Manage your database records** **1242**

**Configuration Logging** **1248**

**Event logs** **1253**

**Director** **1254**

**Advanced configuration** **1260**

**Monitor deployments** **1263**

**Alerts and notifications** **1276**

**Delegated Administration and Director** **1288**

**Secure Director deployment** **1291**

**Configure permissions for VDAs earlier than XenDesktop 7** **1294**

**Configure network analysis** **1296**

**Troubleshoot user issues** **1297**

**Send messages to users** **1299**

**Restore sessions** **1300**

**Reset a Personal vDisk** **1301**

**Run HDX channel system reports** **1301**

**Shadow users** **1302**

**Diagnose user logon issues** **1303**

**Record sessions** **1305**

**Restore desktop connections** **1307**

**Resolve application failures** **1307**

**Reset a user profile** **1308**

**Troubleshoot applications** **1311**

**Troubleshoot machines** **1314**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Feature compatibility matrix** **1318**

**Data granularity and retention** **1320**

**Citrix Director failure reasons and troubleshooting** **1326**

**SDKs and APIs** **1347**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# What's new

July 7, 2022

### 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 7.15 LTSR (initial release)

# Cumulative Update 9 (CU9)

July 8, 2022

Release date: July 8, 2022

### About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 9 (CU9) fixes more than 15 issues reported since the release of 7.15 LTSR CU8.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU8

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Downloads

Download 7.15 LTSR CU9

> **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.
>
> **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 CU9 from scratch?

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

Peruse the XenApp and XenDesktop 7.15 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 that your setup meets the system requirements for all components.

### Existing deployments

What do I update?

CU9 provides updates to baseline components of the 7.15 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### XenApp and XenDesktop 7.15 LTSR CU9 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.9000 | |
| VDA for Server OS | 7.15.9000 | |
| Citrix Studio | 7.15.9000 | |
| Citrix Director | 7.15.9000 | |
| Delivery Controller | 7.15.9000 | |
| Citrix Federated Authentication Service | 7.15.9000 | |
| Citrix Group Policy Management | 3.1.9000 | |
| Citrix Group Policy Client-Side Extension | 3.1.9000 | |
| Linux VDA | 7.15.6000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.9000 | |
| Provisioning Services | 7.15.45 | |
| Session Recording | 7.15.9000 | Premium Edition only |
| StoreFront | 3.12.9000 | |
| Universal Print Server | 7.15.9000 | |

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR CU9 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 2011 |
| *Browser content redirection | 15.19.2000 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 7.15 LTSR CU9 Compatible Components and Platforms | Version |
|---|---|
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.3000 |
| License Server | 11.16.6.0 build 33000 |
| Self-Service Password Reset | 1.1.20.0 |
| Workspace Environment Management | 2012 |

***Browser content redirection**

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

## Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with theXenApp and Xendesktop 7.15 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.

## XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Excluded Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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 or upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see Install and upgrade analytics.

### 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 XenApp 7.15 LTSR CU9. 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 7.15 LTSR CU9 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU9 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 XenApp 7.15 LTSR CU9 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU9 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 27, 2022

### 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 Studio

- 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]
- 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

- The site test might fail when the network connectivity among Delivery Controllers in different satellite zones is blocked. [CVADHELP-17273]
- 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

fix, restart the Host service and reopen Citrix Studio after the DBschema upgrade. [CVADHELP-17705]

- Citrix Director might not display IP addresses of some VDA machines when searched. The issue occurs when the **MonitorData.[Machine]** table contains duplicate entries. [CVADHELP-18108]

### Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU9 documentation provides specific information about the updates in this release.

### Profile Management

- After enabling the Delete excluded files or folders policy, the initial logon attempt using Profile Management might take longer. This issue occurs if the user profile contains unnecessary files slowing the logon. [CVADHELP-17230]
- Verification of Active Directory group membership might fail when user devices in offline mode connect to the network during logon. As a result, Profile Management also fails. [CVADHELP-17364]
- Changing the folder redirection path through the Citrix Profile Management policy might result in deletion of data in the legacy folder redirection path. [CVADHELP-17833]
- Attempting to launch desktops using Profile Management might fail with this error message:

  **The Group Policy Client service failed the sign-in.**

  **Access is denied.**

  [CVADHELP-18398]
- Profile Management Service might exit unexpectedly due to an unhandled exception. [CVADHELP-18813]
- On a Windows 10 20H2 desktop, when you configure the user store path with a !CTX_OSNAME! variable, Profile Management might create folder names on the user store with incorrect information. The following might be observed:
  - For Version CU3, the new profiles might contain operating system as Win10RS6.
  - For Version CU4, the new profiles might contain operating system as Win10_2009.

[CVADHELP-19016]

- When you launch Edge Chromium on a published desktop with Profile Management enabled, duplicate profiles might be created once you log back on. The issue occurs as Profile Management might fail to delete local profiles during logoff. [CVADHELP-19865]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Provisioning Services

Provisioning Services 7.15 LTSR CU9 documentation provides specific information about the updates in this release.

### StoreFront

- If the **CtxsClientVersion** cookie expires while the **CtxsClientDetectionDone** cookie is still active, existing native applications switch to HTML5, and new applications are launched with HTML5. [CVADHELP-18040]
- This fix addresses a security vulnerability in an underlying component. For more information, see Knowledge Center article CTX377814. [CVADHELP-19161]

### VDA for Desktop OS

### Keyboard

- This fix addresses Russian keyboard mapping issues on Citrix Workspace app for HTML5, Mac, and Linux clients. [CVADHELP-19012]

#### 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]
- 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]

#### Session/Connection

- When you exit a session, the server might become unresponsive. The issue occurs when you use Generic USB redirection. [CVADHELP-18204]

#### System Exceptions

- VDAs might experience a fatal exception on wdica.sys and display a blue screen. [CVADHELP-16055]
- The VDAs might experience a fatal exception on icaussb.sys and display a blue screen with bug check code, 0x3B. [CVADHELP-17339]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### VDA for Server OS

#### Keyboard

- This fix addresses Russian keyboard mapping issues on Citrix Workspace app for HTML5, Mac, and Linux clients. [CVADHELP-19012]

#### 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]
- 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]

#### Session/Connection

- When you exit a session, the server might become unresponsive. The issue occurs when you use Generic USB redirection. [CVADHELP-18204]

#### System Exceptions

- VDAs might experience a fatal exception on wdica.sys and display a blue screen. [CVADHELP-16055]
- Citrix Stack Control Service (SCService64.exe) might exit unexpectedly. [CVADHELP-18707]
- The VDAs might experience a fatal exception on icaussb.sys and display a blue screen with bug check code, 0x3B. [CVADHELP-17339]

## Cumulative Update 8 (CU8)

August 10, 2021

Release date: August 11, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 8 (CU8) fixes more than 40 issues reported since the release of 7.15 LTSR CU7.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU7

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

## Downloads

Download 7.15 LTSR CU8

> **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.
>
> **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 CU8 from scratch?

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Peruse the XenApp and XenDesktop 7.15 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 that your setup meets the system requirements for all components.

### Existing deployments

What do I update?

CU8 provides updates to baseline components of the 7.15 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.

### XenApp and XenDesktop 7.15 LTSR CU8 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.8000 | |
| VDA for Server OS | 7.15.8000 | |
| Citrix Studio | 7.15.8000 | |
| Citrix Director | 7.15.8000 | |
| Delivery Controller | 7.15.8000 | |
| Citrix Federated Authentication Service | 7.15.8000 | |
| Citrix Group Policy Management | 3.1.8000 | |
| Citrix Group Policy Client-Side Extension | 3.1.8000 | |
| Linux VDA | 7.15.6000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.8000 | |
| Provisioning Services | 7.15.39 | |
| Session Recording | 7.15.8000 | Premium Edition only |
| StoreFront | 3.12.8000 | |
| Universal Print Server | 7.15.8000 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR CU8 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 2011 |
| *Browser content redirection | 15.19.2000 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.3000 |
| License Server | 11.16.6.0 build 33000 |
| Self-Service Password Reset | 1.1.20.0 |
| Workspace Environment Management | 2012 |

#### *Browser content redirection

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with theXenApp and Xendesktop 7.15 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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 or upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see Install and upgrade analytics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp 7.15 LTSR CU8. 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 7.15 LTSR CU8 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU8 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 XenApp 7.15 LTSR CU8 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU8 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 23, 2021

### Citrix Director

- Citrix Director might show incorrect user session count information. [CVADHELP-14849]

### 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Studio

- This fix provides enhanced security by allowing only approved StoreFront and Citrix Gateway servers to communicate with the Delivery Controller. For more information, see Security keys. [CVADHELP-15729]
- Attempts to add or delete virtual machines from the existing catalogs might fail. [CVADHELP-17316]

### Delivery Controller

- This fix provides enhanced security by allowing only approved StoreFront and Citrix Gateway servers to communicate with the Delivery Controller. For more information, see Security keys. [CVADHELP-15729]
- 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]
- The Citrix Broker Service (Brokerservice.exe) might become unresponsive and go offline. [CVADHELP-16352]
- After upgrading XenApp and XenDesktop 7.15 CU6 to Citrix Virtual Apps and Desktops 1912 LTSR CU2, issues might occur when updating the database. The issue occurs when the **AdminAccountName/AdminUpn** entries are longer than 64 characters. [CVADHELP-17379]
- 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]

### Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU8 documentation provides specific information about the updates in this release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Profile Management

- Windows user credentials might remain after being removed from the Credential Manager. [CVADHELP-16083]
- Folders created before enabling Delete excluded files or folders through the Logon Exclusion Check policy but excluded by the Exclusion list –directories or Enable Default Exclusion list – directories policy might not be deleted. [CVADHELP-16439]
- New files created with the Large **File Handling - Files to be created as symbolic links** policy setting, might not sync during logoff. [CVADHELP-16526]
- With Citrix Profile Management installed, redirected folders might be recreated under the local user profile. [CVADHELP-16861]
- This fix addresses a security vulnerability in the Citrix Profile Management WMI plugin installer. For more information, see Knowledge Center article CTX319750. [CVADHELP-17728]
- This fix addresses a security vulnerability in the Citrix Profile Management installer. For more information, see Knowledge Center article CTX319750. [CVADHELP-17939]

### Provisioning Services

Provisioning Services 7.15 LTSR CU8 documentation provides specific information about the updates in this release.

### StoreFront

- This fix provides enhanced security by allowing only approved StoreFront and Citrix Gateway servers to communicate with the Delivery Controller. For more information, see Security keys. [CVADHELP-15729]
- With socket pooling enabled, attempts to log on to StoreFront might fail with this error message:

  **Cannot Complete your Request**

  The issue occurs when there is a TCP dynamic port exhaustion.

  [CVADHELP-16625]
- 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-16698]
- After upgrading StoreFront from version 7.15 LTSR CU4, VDI desktops with the same host name might appear in random order instead of serial order. [CVADHELP-16723]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you attempt to launch a user session using Citrix StoreFront services API, the parameters passed to the launch request might be incorrect. [CVADHELP-16834]

## Universal Print Server

### Server

- The Universal Print Server (UPServer.exe) might exit unexpectedly. The issue occurs because of the faulting module, prntvpt.dll. [CVADHELP-12651]

## User Profile Management VDA

- When you log on to a session, the user data might be deleted unexpectedly. The issue occurs when you change the file server address from path1 to path2 in the Citrix folder redirection path policy settings (for example, the Desktop path setting). But, path1 and path2 point to the same physical location. To prevent this issue, enable the Microsoft group policy setting **Verify old and new Folder Redirection targets point to the same share before redirecting**. For details, see the Description part of the Citrix folder redirection path policy settings. [CVADHELP-12439]

## VDA for Desktop OS

### 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]
- 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]

### Session/Connection

- When a session is recorded on Citrix Workspace app for Windows, movements of a mouse pointer might not be recorded. The issue occurs with VDA Version 7.15.400. [CVADHELP-13300]
- When you attempt to switch to a window using the taskbar preview, opening that window might take a long time. [CVADHELP-15422]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When using Generic IME for Microsoft Windows 10 20H2 with KB4586853 update, the application might exit unexpectedly. [CVADHELP-16664]
- With this fix, you can now set different input methods for each application window available under advanced keyboard settings. [CVADHELP-16731]
- When using certain third-party applications, a black screen might appear when the application opens another window. [CVADHELP-16956]

#### System Exceptions

- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x93 (INVALID_KERNEL_HANDLE). [CVADHELP-15326]
- 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]
- The Citrix Desktop Service (BrokerAgent.exe) might experience an access violation and exit unexpectedly. [CVADHELP-17055]

#### User Experience

- A black patch might appear on the screen when using Explorer. The issue occurs when connected to endpoints using certain AMD GPU models.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: MinTransientWidth

  Type: DWORD

  Value: 00000021

  [CVADHELP-17057]

### VDA for Server OS

#### Printing

- Attempting to print a PDF file from a session launched through Citrix Workspace app for Chrome might fail. [CVADHELP-15318]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When using a Remote PC Access VDA to print through Citrix Workspace app for Mac, the printer settings might be ignored. [CVADHELP-15320]
- 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]

**Session/Connection**

- When a session is recorded on Citrix Workspace app for Windows, movements of a mouse pointer might not be recorded. The issue occurs with VDA Version 7.15.400. [CVADHELP-13300]
- When you attempt to launch a session through Citrix Workspace app for HTML5, the session might run in windowed mode instead of full-screen mode. The issue occurs with VDAs running on Windows Server 2012. [CVADHELP-14865]
- When you attempt to switch to a window using the taskbar preview, opening that window might take a long time. [CVADHELP-15422]
- A webcam might not be added to the registry. In a Citrix session, this might prevent other applications from recognizing the webcam.

  Set the following registry key to allow users to tune the waiting time of **WebcamArrivalEvent**:

  - On 32-bit systems:

    HEKY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

    Name: RetryNumToWaitWebcamArrival

    Type: DWORD

    Value: By default, the registry is absent. When the registry is absent or is not read, the default value of 1000 will be used. This value indicates the default wait time length which is 20 seconds. If the value is less than 1000, then the default value (1000) will be used.
  - On 64-bit systems:

    HEKY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxRealTime

    Name: RetryNumToWaitWebcamArrival

    Type: DWORD

    Value: By default, the registry is absent. When the registry is absent or is not read, the default value of 1000 will be used. This value indicates the default wait time length which is 20 seconds. If the value is less than 1000, then the default value (1000) will be used.

    [CVADHELP-16318]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- With this fix, you can now set different input methods for each application window available under advanced keyboard settings. [CVADHELP-16731]
- When using certain third-party applications, a black screen might appear when the application opens another window. [CVADHELP-16956]

#### System Exceptions

- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x93 (INVALID_KERNEL_HANDLE). [CVADHELP-15326]
- 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]
- The Citrix Desktop Service (BrokerAgent.exe) might experience an access violation and exit unexpectedly. [CVADHELP-17055]

#### User Experience

- A black patch might appear on the screen when using Explorer. The issue occurs when connected to endpoints using certain AMD GPU models.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: MinTransientWidth

  Type: DWORD

  Value: 00000021

  [CVADHELP-17057]

### Virtual Desktop Components –Other

- App-V applications might take a long time to launch. [CVADHELP-16732]

## Cumulative Update 7 (CU7)

June 21, 2021

Release date: February 9, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 7 (CU7) fixes more than 60 issues reported since the release of 7.15 LTSR CU6.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU6

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

## Downloads

Download 7.15 LTSR CU7

> **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.
>
> **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 CU7 from scratch?

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Peruse the XenApp and XenDesktop 7.15 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 that your setup meets the system requirements for all components.

### Existing deployments

What do I update?

CU7 provides updates to baseline components of the 7.15 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.

### XenApp and XenDesktop 7.15 LTSR CU7 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.7000 | |
| VDA for Server OS | 7.15.7000 | |
| Citrix Studio | 7.15.7000 | |
| Citrix Director | 7.15.7000 | |
| Delivery Controller | 7.15.7000 | |
| Citrix Federated Authentication Service | 7.15.7000 | |
| Citrix Group Policy Management | 3.1.7000 | |
| Citrix Group Policy Client-Side Extension | 3.1.7000 | |
| Linux VDA | 7.15.6000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.7000 | |
| Provisioning Services | 7.15.33 | |
| Session Recording | 7.15.7000 | Premium Edition only |
| StoreFront | 3.12.7000 | |
| Universal Print Server | 7.15.7000 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR CU7 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 2011 |
| *Browser content redirection | 15.19.2000 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.3000 |
| License Server | 11.16.6.0 build 33000 |
| Self-Service Password Reset | 1.1.20.0 |
| Workspace Environment Management | 2012 |

#### *Browser content redirection

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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 or upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see Install and upgrade analytics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp 7.15 LTSR CU7. 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 7.15 LTSR CU7 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU7 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 XenApp 7.15 LTSR CU7 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU7 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 21, 2022

### Citrix Director

- In scenarios with poor network connectivity, when you use Director in an environment containing large sites, the IIS worker process (w3wp.exe) might consume high memory. The Director page stops loading. [CVADHELP-14959]
- After uninstalling a VDA, the namespaces for Citrix Windows Management Instrumentation (WMI) might remain. [CVADHELP-14965]
- 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.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

[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]

### Citrix Policy

- When you upgrade the Citrix Group Policy Engine from Version 1.7 to Version 7.15, the **Printer assignments** policy under **Citrix User Policies** might not be displayed. [CVADHELP-15608]

### Citrix Studio

- 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

- 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]
- In a large Citrix Virtual Apps and Desktops environment, stored procedures for Monitor database grooming might not work. The issue occurs when the size of the Monitor database is large. [CVADHELP-13287]
- Delivery Controllers might receive the following Local Host Cache Error 505 in the event log: Unknown Error. [CVADHELP-14428]
- 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]
- Attempts to create a Machine Creation Services (MCS) catalog in Azure using PowerShell might fail with this error message:

  **Could not locate item with path=Citrix.AzureRmPlugin.InventoryItemPath.**

  The issue occurs when you use Shared Azure subscriptions in conjunction with narrow scope service principals. [CVADHELP-14640]
- When you log on to a new session using Citrix Director, the logon might not appear on the **Average Logon Duration** graph available on the **Logon Performance** tab under **Trends**. However, the logon appears in the **Logon Duration by User Session** form. [CVADHELP-14740]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- vSAN storage policies might not be applied on a virtual machine created using Machine Creation Services (MCS). The issue occurs when the version of a disk attached to the machine is incorrect. [CVADHELP-14935]
- 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 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]
- This fix provides Microsoft System Center Virtual Machine Manager (SCVMM) 2019 support for Machine Creation Services (MCS). [CVADHELP-15779]

### Metainstaller

- When installing a VDA, additional components such as Personal vDisk might be installed even though you did not select them in the GUI. [CVADHELP-15572]
- 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

- With the **Profile streaming** policy enabled in Profile Management, attempts to download a file in Internet Explorer 11 might fail. [CVADHELP-12970]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you navigate to **Control Panel > System and Security > System > Change settings > Advanced > User Profiles > Settings**, the profile for the logged-in user shows a question mark for the Size field. The other user profiles show the correct sizes. [CVADHELP-13993]
- When you add Appdata\local\temp to the **Exclusion list - directories**, Profile Management does not create the Appdata\local\temp folder in the user profile and runtime errors occur for some applications such as Microsoft Outlook. The issue occurs during second or subsequent logons with the **Delete locally cached profiles on logoff** policy enabled. [CVADHELP-14054]
- Profile Management does not synchronize the subkeys of a registry key present in the **Registry inclusion list**. For example, when you add Software\Citrix to the **Registry inclusion list**, only HKEY_CURRENT_USER\SOFTWARE\Citrix is saved in the user store. The subkeys are not stored. [CVADHELP-14815]
- When a folder on the **Folders to Mirror** list is not present in the user store during logons, the local user profile is deleted. [CVADHELP-15248]
- With **Desktop** added to the **Exclusion list –directories** policy, an error might occur when users attempt to save changes in a published application or desktop. [CVADHELP-15792]

### Provisioning Services

Provisioning Services 7.15 LTSR CU7 provides specific information about the updates in this release.

### StoreFront

- On iPadOS 13 or later, StoreFront webpages might freeze when users attempt to log on. The issue occurs when the Enable classic experience policy is enabled for your StoreFront deployment. [CVADHELP-14905]
- When a custom config file is present in the store folder, the custom file might replace the content of the web.config file in the store folder. The issue occurs when you upgrade StoreFront. [CVADHELP-13485]

### VDA for Desktop OS

#### Session/Connection

- When several USB devices are redirected to a session, one of them might not work correctly. [CVADHELP-12516]
- 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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]

- If **SAS notification** is enabled, a user with multiple monitors connecting to an existing session at the console might find the monitor layout is not restored correctly. For example, if the right monitor is 1 and selected as the main monitor and the left monitor is 2, the user might find the positions swapped when reconnecting. This issue affects only RemotePC users with a physical desktop. This is due to incompatibility between two features.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: UseSDCForLocalModes

  Type: DWORD

  Value: 1

  [CVADHELP-14249]

- VDAs might unregister intermittently when IPv6 is enabled. [CVADHELP-14847]

- 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, set the registry key 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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]
- 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 time zone policy set to **Use server time zone**, the client-side time zone might still get redirected on a VDA through a user session. [CVADHELP-15628]
- 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]
- On Server VDI VDAs, the power button on the Start menu might not offer the Disconnect option. [CVADHELP-16595]

#### System Exceptions

- After you upgrade a VDA from Version 7.15 Cumulative Update 5 to Cumulative Update 6 or Version 2003, the Group Policy engine (CseEngine.exe) service might exit unexpectedly. [CVADHELP-14515]
- 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code APC_INDEX_MISMATCH (1). The issue occurs when you attempt to access a mapped client drive. [CVADHELP-15003]
- 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]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x93 (INVALID_KERNEL_HANDLE). [CVADHELP-15326]
- 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, HostMMTransport.dll. [CVADHELP-15598]

## VDA for Server OS

### Session/Connection

- When several USB devices are redirected to a session, one of them might not work correctly. [CVADHELP-12516]
- 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]
- 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]
- License statistics might not be consistent among sites. For example, there can be an apparent discrepancy between licenses consumed by Citrix Concurrent User (CCU) and licenses assigned to unique users for multiple sites. [CVADHELP-14950]
- 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, set the registry key as follows:

  - *For 32-bit systems*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    Name: KeepAliveTimer

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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]
- Microsoft Teams might fail to load in optimized mode when a clock drift is created. This drift translates into an invalid or expired Citrix certificate. As a workaround, change the HTML5 Video Redirection Service (txHdxWebSocketService) startup type to **Automatic** (Delayed Start) instead of the default **Automatic**. [CVADHELP-15298]
- 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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]

#### 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]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code APC_INDEX_MISMATCH (1). The issue occurs when you attempt to access a mapped client drive. [CVADHELP-15003]
- 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]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x93 (INVALID_KERNEL_HANDLE). [CVADHELP-15326]
- 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, HostMMTransport.dll. [CVADHELP-15598]
- 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 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]
- This fix addresses a security vulnerability in an underlying component. For more information, see Knowledge Center article CTX285059. [CVADHELP-14755]

## Cumulative Update 6 (CU6)

June 21, 2021

Release date: June 30, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 6 (CU6) fixes more than 94 issues reported since the release of 7.15 LTSR CU5.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU5

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

## Downloads

Download 7.15 LTSR CU6

> **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.
>
> **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 CU6 from scratch?

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Peruse the XenApp and XenDesktop 7.15 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 that your setup meets the system requirements for all components.

### Existing deployments

What do I update?

CU6 provides updates to baseline components of the 7.15 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU6. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU6. If Provisioning Services is not part of your deployment, you do not need to install or update it.

### XenApp and XenDesktop 7.15 LTSR CU6 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.6000 | |
| VDA for Server OS | 7.15.6000 | |
| Citrix Studio | 7.15.6000 | |
| Citrix Director | 7.15.6000 | |
| Delivery Controller | 7.15.6000 | |
| Citrix Federated Authentication Service | 7.15.6000 | |
| Citrix Group Policy Management | 3.1.6000 | |
| Citrix Group Policy Client-Side Extension | 3.1.6000 | |
| Linux VDA | 7.15.5000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.6000 | |
| Provisioning Services | 7.15.27 | |
| Session Recording | 7.15.6000 | Premium Edition only |
| StoreFront | 3.12.6000 | |
| Universal Print Server | 7.15.6000 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR CU6 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 1903 |
| *Browser content redirection | 15.15 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.3000 |
| License Server | 11.16.6.0 build 31000 |
| Self-Service Password Reset | 1.1.20.0 |
| Workspace Environment Management | 1906.0.1.1 |

#### *Browser content redirection

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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 or upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see Install and upgrade analytics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp 7.15 LTSR CU6. 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 7.15 LTSR CU6 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU6 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 XenApp 7.15 LTSR CU6 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU6 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 11, 2021

### Citrix Director

- When you log on to Citrix Director for the first time after you restart Internet Information Services (IIS), the following error message might appear on the **Trends** page:

  **No details are available.**

  [CVADHELP-12426]

- Attempts to send messages to multiple users might fail with the following error message:

  **Message cannot be sent. Unexpected server error. View Director server event logs for further information.**

  [CVADHELP-12601]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When Citrix Director attempts to set up an email configuration using an SMTP server, this error message might appear:

  **Invalid Email Server**

  [CVADHELP-14449]

- 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 Policy

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

### Citrix Studio

- Attempts to launch an App-V application might fail with the following error message:

  **Cannot start**

  The issue occurs when large App-V packages are not fully streamed to VDAs. [CVADHELP-12889]

- 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]
- When you attempt to add devices from PVS collection to a catalog in Citrix Studio, all target devices might be listed including machines that already exist in the catalog. [CVADHELP-13403]
- When you attempt to change the executable path or the icon location of an existing app assigned to an Application Group, the following error message might appear:

  **Unable to browse machines in the Delivery Group. Do you want to browse on the local machine?**

  [CVADHELP-14199]

- When you run Studio as a published app, Studio might become unresponsive. [CVADHELP-14207]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Delivery Controller

- Attempts to send messages to many users through Citrix Director might fail. This error message appears:

  **Message Cannot be sent. Data source unresponsive or reported an error.**

  The fix intends to minimize the occurrence of this issue.

  [CVADHELP-12066]

- When you attempt to view custom reports for application instances from Citrix Director, some fields might display null values instead of application end times. [CVADHELP-12733]
- Application enumeration might cause a significant increase in CPU usage on the SQL server hosting the site database. [CVADHELP-13043]
- Attempts to groom resource utilization data from a table in the Monitoring database might fail with an execution timeout. [CVADHELP-13075]
- With the **Remote PC Access Wake on LAN** feature enabled in a machine catalog, Local Host Cache might stop synchronizing data. The issue occurs when you use Microsoft System Center Configuration Manager (SCCM) as a hosting connection. [CVADHELP-13122]
- A virtual machine where a user session is running might shut down unexpectedly. The issue occurs when the Automatic Client Reconnection feature fails to trigger a Delete power action that is pending in the database. [CVADHELP-13165]
- 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]

- 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]
- Local Host Cache (LHC) files might disappear after download starts. As a result, the old files remain or LHC files fail to appear in the location C:\Windows\ServiceProfiles\NetworkService. [CVADHELP-13980]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Attempts to import synchronized configurations to the Local Host Cache database might repeatedly fail with an Error 505. [CVADHELP-14237]
- After you upgrade XenApp and XenDesktop 7.15 Cumulative Update 1 to Cumulative Update 3, attempts to import Local Host Cache (LHC) might fail with an Error 505. [CVADHELP-14429]

### Federated Authentication Service

- The GUI does not support multiple certificate authority (CA) servers. [CVADHELP-11919]

### Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU6 documentation provides specific information about the updates in this release.

### Profile Management

- Attempts to create a user profile on Microsoft Windows 10 Version 2004 might fail. [CVADHELP-14235]
- When you log on to a session using a temporary profile, an empty user profile folder might be created under C:\Users. Profile Management deletes the temporary profile on logoff, leaving behind the empty user profile folder. [CVADHELP-14297]
- With the AppData(Roaming) folder redirection policy enabled, some tiles might disappear from the Start menu. The issue occurs when you log on to a Windows Server 2016 or 2019 machine running Citrix Virtual Apps and Desktops 1912 or earlier. [CVADHELP-14336]
- With the **Logon Exclusion Check** policy enabled, Profile Management might fail to synchronize files under an excluded folder. Instead, Profile Management might delete or ignore the files on logon. The issue occurs with files that match paths containing wildcards in the **List of files to synchronize** policy. [CVADHELP-14347]

### Provisioning Services

Provisioning Services 7.15 LTSR CU6 provides specific information about the updates in this release.

### StoreFront

- When StoreFront Version 3.12 Cumulative Update 3 is configured using SAML authentication and a complex AD architecture containing multiple domains, the Federated Authentication Service (FAS) might fail to launch an application. This error message appears:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Cannot Start App.**

The issue occurs with FAS enabled on a Store.

[CVADHELP-12865]

- If you configure the StoreFront management console with SAML authentication and enter the IdP URL (for PingID) in the address field, those changes might not be saved. This error message appears:

  **Error received: An error occurred while saving changes**

  [CVADHELP-13373]

- Security Assertion Markup Language (SAML) authentication might fail when you use a third-party application as an Identity Provider (IdP).

  The following error message appears:

  **There was a failure with the mapped account.**

  [CVADHELP-13396]

- When a custom config file is present in the store folder, the custom file might replace the content of the web.config file in the store folder. The issue occurs when you upgrade StoreFront. [CVADHELP-13485]
- This fix addresses a security vulnerability in an underlying component. [CVADHELP-13602]
- Upgrades that include 2.6, 3.0.1, 3.5, 3.8 in their upgrade history to 3.12 CU* and above may fail if the Citrix StoreFront Protocol Transition service s in **Stopped** state. [CVADHELP-13626]
- When you log on to StoreFront, application enumeration might take a long time to complete. The issue occurs if you type your user name in **domain\username** format and user authentication is delegated to Delivery Controllers. [CVADHELP-13891]
- In the StoreFront console, attempts to add domain names that contain an underscore (_) to a trusted domain list might fail. [CVADHELP-14213]
- This fix addresses a security vulnerability in an underlying component. For more information, see Knowledge Center article CTX277455. [LCM-7272]
- When you install a Delivery Controller, StoreFront might not be installed by default. To install it, use the Citrix StoreFront option from the Citrix Virtual Apps and Desktops metainstaller. [LCM-7335]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Universal Print Server

### Client

- Due to an access violation, the Universal Print Server (UPServer.exe) might exit unexpectedly. [CVADHELP-10627]
- The Print Spooler service (spoolsv.exe) might enter a deadlock. As a result, the documents fail to print and Microsoft Office applications do not launch. [CVADHELP-13315]
- 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]
- The Universal Print Server (UPServer.exe) might exit unexpectedly. The issue occurs because of the faulting module, prntvpt.dll. [CVADHELP-12651]

## VDA for Desktop OS

### Keyboard

- With the Citrix generic client Input Method Editor (IME) feature enabled, an application might exit unexpectedly when you use the Chinese client IME to input special characters and numbers in the application. The issue occurs in desktop and app sessions running on Microsoft Windows 10 Version 1809 and Windows Server 2019. [CVADHELP-13961]

### Installing, Uninstalling, Upgrading

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Printing

- After you upgrade a VDA to Version 7.15 Cumulative Update 4, the Citrix Print Manager Service (CpSvc.exe) might exit unexpectedly. [CVADHELP-12888]
- When you attempt to launch an application, the Citrix Print Manager Service (CpSvc.exe) might exit unexpectedly. [CVADHELP-13945]

### 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 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 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]
- Session roaming might not work on a VDA. The issue occurs with Dell Wyse thin client devices. [CVADHELP-13003]
- 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]
- If you click the **Cancel** button when an application is capturing a video using a webcam, the application might become unresponsive. The issue occurs because of the faulting module, MFDeviceSource.dll. [CVADHELP-13062]
- 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 it, add the following registry key:

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

  Name: PacketIntegrityChecks

  Type: DWORD

  Value: 1

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

[CVADHELP-13063]

- When a session is recorded on Citrix Workspace app for Windows, movements of a mouse pointer might not be recorded. The issue occurs with VDA Version 7.15.400. [CVADHELP-13300]
- Attempts to launch a session on a VDA might fail when you use some third-party vulnerability scanners. [CVADHELP-13306]
- A VDA might become unresponsive after restart. The issue occurs when security software such as Symantec SEP enforces security scans. [CVADHELP-13832]
- 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 multi-monitor environment, applications might not display consistently on the same monitor. The issue occurs when you move to a new workstation. [CVADHELP-13657]

#### 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]

#### 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. [CVADHELP-13000]
- 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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 Server OS

#### Keyboard

- With the Citrix generic client Input Method Editor (IME) feature enabled, an application might exit unexpectedly when you use the Chinese client IME to input special characters and numbers in the application. The issue occurs in desktop and app sessions running on Microsoft Windows 10 Version 1809 and Windows Server 2019. [CVADHELP-13961]

#### Printing

- After you upgrade a VDA to Version 7.15 Cumulative Update 4, the Citrix Print Manager Service (CpSvc.exe) might exit unexpectedly. [CVADHELP-12888]
- 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]

#### 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 VDA for Server OS, the Windows RunOnce registry key might not execute. [CVADHELP-11991]
- A Delivery Controller might show invalid session information. The issue occurs when session information that a VDA sends to the Delivery Controller contains the IP address 127.0.0.1. [CVADHELP-12767]
- 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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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]

- 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 it, add 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]

- If you **click** the Cancel button when an application is capturing a video using a webcam, the application might become unresponsive. The issue occurs because of the faulting module, MFDeviceSource.dll. [CVADHELP-13062]
- 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 it, add the following registry key:

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

  Name: PacketIntegrityChecks

  Type: DWORD

  Value: 1

  [CVADHELP-13063]

- When a session is recorded on Citrix Workspace app for Windows, movements of a mouse pointer might not be recorded. The issue occurs with VDA Version 7.15.400. [CVADHELP-13300]
- Attempts to log off from a user session using Citrix Studio and Citrix Director might fail when a published application is launched in that session. [CVADHELP-13307]
- 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]
- A VDA might become unresponsive after restart. The issue occurs when security software such as Symantec SEP enforces security scans. [CVADHELP-13832]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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]
- COM port redirection might fail to work after Automatic Client Reconnection (ACR) reconnects to a session following a network disconnection. [CVADHELP-13926]
- 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]
- 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]

#### Smart cards

- Pass-through authentication with smart cards might fail intermittently. The issue occurs when you launch an HDX session on Windows Server 2016. [CVADHELP-13054]

#### 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. [CVADHELP-13000]
- VDAs might experience a fatal exception on ctxdvcs.sys and display a blue screen with bug check code 0xc0000409. [CVADHELP-13102]
- Servers might experience a fatal exception on icardd.dll, displaying a blue screen with bug check code 0x0000003B. [CVADHELP-13330]
- 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]
- 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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]

### 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]

## Cumulative Update 5 (CU5)

June 21, 2021

Release date: October 22, 2019

### About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 5 (CU5) fixes more than 120 issues reported since the release of 7.15 LTSR CU4.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU4

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

### Downloads

Download 7.15 LTSR CU5

### New deployments

How do I deploy CU5 from scratch?

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Peruse the XenApp and XenDesktop 7.15 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 that your setup meets the system requirements for all components.

### Existing deployments

What do I update?

CU5 provides updates to baseline components of the 7.15 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU5. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU5. If Provisioning Services is not part of your deployment, you do not need to install or update it.

### XenApp and XenDesktop 7.15 LTSR CU5 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.5000 | |
| VDA for Server OS | 7.15.5000 | |
| Citrix Studio | 7.15.5000 | |
| Citrix Director | 7.15.5000 | |
| Delivery Controller | 7.15.5000 | |
| Federated Authentication Service | 7.15.5000 | |
| Group Policy Management Experience | 3.1.5000 | |
| Linux VDA | 7.15.5000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.5000 | |
| Provisioning Services | 7.15.21 | |
| Session Recording | 7.15.5000 | Premium Edition only |
| StoreFront | 3.12.5000 | |
| Universal Print Server | 7.15.5000 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR CU5 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 1903 |
| *Browser content redirection | 15.15 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.3000 |
| License Server | 11.16.3.0 Build 28000 |
| Self-Service Password Reset | 1.1.10.0 |
| Workspace Environment Management | 1906.0.1.1 |

#### *Browser content redirection

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 LTSR. For information about the lifecycle of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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 or upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see Install and upgrade analytics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp 7.15 LTSR CU5. 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 7.15 LTSR CU5 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU5 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 XenApp 7.15 LTSR CU5 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU5 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

### Citrix Director

- There are two domains present in the same Active Directory forest, a parent and a child domain. The user is added to a domain local group in the child domain, which automatically belongs to the XenDesktop Delivery group. When the administrator from the parent domain logs on to the Director, the dashboard displays a list of sessions. When the administrator attempts to view the session details, the following error message appears:

  **This user doesn't have any running sessions or assigned desktops.**

  However, the administrator from the child domain does not encounter this issue. [LD0178]

- On the Citrix Director console, when you send messages to multiple users who are filtered with Published Name for application instances, this error message might appear:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Message cannot be sent. Unexpected server error. View Director server event logs for further information.** [LD1257]

- Citrix Director might not display personalization data in the user data section, and this error message appears:

  **Unexpected server error.** [LD1353]

- In a multiple session environment, when you navigate to **Filters** > **Sessions** > **All** and log off from a session, the session logs off. When you select another session with the same user name for the second time and attempt to log off, this error message appears:

  **Data source unresponsive or reported an error. View Director Server event logs for further information.** [LD1441]

- Citrix Director might show only a few table records, followed by an empty space. You can see the remaining records only after scrolling down the table. [LD1706]

### Citrix Studio

- When you select **Advanced** for **XenApp edition**, you might not be able to create a new Amazon Web Services (AWS) host connection. [LD1988]
- Attempts to delete the virtual machines from a catalog might fail with the exception **System.ArgumentNullException Value cannot be Null**. [LD2014]
- The App-V packages deployed to VDAs might be incorrectly removed from the VDAs. This fix introduces a registry key under HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features. The key controls whether to enable or disable cleanup. By default, cleanup is disabled. [LD2025]

  To enable it, add the following registry key:

  HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features

  Name: RedundantPackageCleanup

  Type: REG_SZ

  Data: True

- Attempts to add machines to a machine catalog through Citrix Studio might fail with the following exception: **Error Id: XDDS:081419B3**. The issue occurs when the machine is added from a Provisioning Services device collection containing one or more target devices that contains a NULL `domainObjectSID` attribute in the `dbo.device` table of the Provisioning Services database. [LD2029]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Configuration Logging Services

- The site configuration test report might generate an error while resolving the user Security Identifiers (SID). The issue occurs when there is a check that verifies whether the Configuration Logging SID identities can be resolved from Active Directory. [LD1569]

### Controller

- Attempts to delete a base disk image using Machine Creation Services (MCS) might fail. [LD2143]
- This fix addresses a memory leak issue that occurs in the Citrix High Availability Service when you restart a VDA. [LD1121]
- There might be a delay of several minutes when you restart a machine while using Amazon Web Services (AWS). [LD1220]
- The CPU usage of the Monitor database might be very high on the SQL Server. This issue degrades overall performance. [LD1478]
- The power action performed manually from the Citrix Studio, or any other scheduled power action, might fail when using Amazon Web Services (AWS). The issue occurs when you reset the virtual machines while the machine is powered on. [LD1548]
- Attempts to stop the Citrix Broker Service might fail. [LD1753]
- This fix addresses an issue in an underlying component. [LD1808]
- When you run the Citrix Scout report, the Citrix Analytics Service might exit unexpectedly and this error message appears:

  **The Citrix Analytics service has stopped running.** [LD1860]
- The catalog update might fail without displaying an error message or a progress bar. [LD1980]
- When you select **Advanced** for **XenApp edition**, you might not be able to create a new Amazon Web Services (AWS) host connection. [LD1988]
- Attempts to delete the virtual machines from a catalog might fail with the exception **System.ArgumentNullException Value cannot be Null**. [LD2014]
- When you navigate to **Citrix Director** > **Trends** > **Capacity management** > **Server OS Usage**, the **Peak Concurrent Server OS Desktop Instances** metric might show a session count that is beyond the actual count. The issue occurs when the **Peak Concurrent Server OS Desktop Instances** calculation counts a single session multiple times because of session reconnect. [LD2122]
- 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**FailedToCreateImagePreparationVm** [LD2158]

- 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"** [LD2160]

### Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU5 documentation provides specific information about the updates in this release.

### Profile Management

- When using Citrix Profile Management, Microsoft's bug fix to delete the firewall rules that were created during the user logon under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Ser might not work. The issue occurs because the Citrix Profile Management doesn't call Microsoft's standard API to delete the local profile. For more information about the fix, see the Microsoft Knowledge Base article KB4467684. [LD1074]
- The files that you delete from a session might not be deleted from the UPM store. [LD1270]
- There might be discrepancies in the logon duration time that Citrix Director records, compared to the event log data that VDAs provide. [LD1679]
- Profile Management does not cancel copy operations to the profile store after it fails to load a corrupt local profile `NTUSER.DAT`. Instead, Profile Management copies the corrupt registry hive to the profile store and overwrites the `NTUSER.DAT` file and its backup. [LD1816]
- Even though you add a registry path to the exclusion list, the registry path might still be saved. The issue occurs when there is a backslash (\) present at the end of the registry path. [LD1862]
- The Citrix Desktop Service (BrokerAgent.exe) might exit unexpectedly and the following exception occurs until you restart the Citrix Profile Management Service:

  **System_Management_Instrumentation_ni!WmiNative.WbemProvider.WmiNative.IWbemServices.Cr** [LD2223]

### Provisioning Services

Provisioning Services 7.15 LTSR CU5 provides specific information about the updates in this release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### StoreFront

- When you attempt to reconnect to a previously disconnected session by clicking the same icon, the session might not reconnect. This issue occurs when multiple desktops that have identical names are published to the end user. [LD1367]
- When you edit the Controller assigned to a user farm mapping and then attempt to save the changes, the Microsoft Management Console (MMC) might exit unexpectedly. The issue occurs on servers with Microsoft .NET Framework 4.7 installed. [LD1668]

### Universal Print Server

#### Client

- The Print Spooler service might exit unexpectedly. The issue occurs when `CRawStreamHeaderWriter::EndPage` and `CRawStreamHeaderWriter::StartPage` attempt to access a null object. [LC7893]
- The Universal Print Server might cause the Print Spooler service to become unresponsive. [LC9341]
- Before you print a document, choose a printer from the list of available printers in the published desktop session's print dialog box. There might be a delay until the printer starts printing the document. [LC9601]
- After installing a VDA, the printer ports under printer **Properties** might no longer appear on a mapped network printer. [LD0949]
- Attempts to print a document might be slow in some workflows. [LD1256]
- With the **Universal print driver usage** setting set to **Use universal printing only**, the client printers might not be auto-created in a session. [LD1395]

### User Profile Management VDA

- When you log on to a session, the user data might be deleted unexpectedly. The issue occurs when you change the file server address from path1 to path2 in the **Citrix folder redirection path** policy settings (for example, the **Desktop path** setting). But, path1 and path2 point to the same physical location. To prevent this issue, enable the Microsoft group policy setting **Verify old and new Folder Redirection targets point to the same share before redirecting**. For details, see the **Description** part of the Citrix folder redirection path policy settings. [LD1500]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## VDA for Desktop OS

### Keyboard

- When you use the Korean Input Method Editor (IME) to input text, the last character in the text might disappear if you click the mouse. The issue occurs when generic client IME is enabled on Citrix Receiver. [LD1380]
- When you navigate to a website and set the keyboard as hidden, the keyboard might still appear in the non-editable area of the website. [LD1382]

### Printing

- Attempts to print a document might be slow in some workflows. [LD1256]
- With the **Universal print driver usage** setting set to **Use universal printing only**, the client printers might not be auto-created in a session. [LD1395]
- 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. [LD2370]

### Session/Connection

- When you play an audio in a user session, you might hear a popping sound. The issue occurs when you play back the audio. [LD0455]
- On Citrix Receiver for Windows, you might hear sounds intermittently when you play an audio. [LD0624]
- When Adobe Acrobat Reader and Microsoft Outlook are running in a seamless mode and you maximize both, the **Menu** bar and the **Minimize**, **Restore**, and **Close** buttons in Acrobat Reader might become unresponsive. [LD1006]
- When 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**. [LD1027]
- Some third-party applications might encounter noise when you play or pause the audio. [LD1136]
- Attempts to start a session on the VDA might fail. [LD1180]
- When you install a VDA, the USB Root Hub is also installed in the Device Manager. The USB Root Hub is installed even though USB 2.0 Root Hub or USB 3.0 Root Hub is already installed. [LD1196]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- With the **Legacy graphics mode** policy enabled, attempts to connect to a VDA for the Desktop OS might fail. The issue occurs when the VDA is installed as a Server VDI on Microsoft Windows Server 2008 R2. [LD1296]
- After you restart a VDA, the Session reliability timeout policy might not be applied during the initial connection. However, attempts to apply the policy for subsequent connections might work. [LD1397]
- With Enlightened Data Transport (EDT) enabled, VDAs might exit unexpectedly with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. The issue occurs when you access user sessions externally through the Zscaler. [LD1493]
- When you change the client-side resolution, certain legacy applications such as Citrix Studio might be redrawn incorrectly in a seamless session. [LD1554]
- When you reconnect to a session, the VDA notification icon might disappear from the user device's notification area. [LD1629]
- After you upgrade XenApp and XenDesktop 7.15 LTSR Cumulative Update 2 to Cumulative Update 3, some .Net applications might become unresponsive in a published desktop session. The issue occurs with VDAs on Windows Server 2008 R2. [LD1726]
- 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 a new value. [LD1827]

  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
- The device description in Device Manager might be corrupted on a Japanese version of the Microsoft Windows operating system. [LD1834]
- An access violation can cause the wfshell.exe process to exit unexpectedly. As a result, an attempt to launch an application fails. [LD2050]

### Smart cards

- The smart card pass-through authentication might fail on Windows 8 or Windows 10. When you lock and unlock a VDA session, the user changes to a domain user from a smart card user. [LD1365]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### System Exceptions

- The Internet Explorer (iexplore.exe) process might exit unexpectedly when you run web applications that implement the location API. [LD0677]
- The Citrix software graphics process (Ctxgfx.exe) might exit unexpectedly on an AMD Opteron(tm) Processor 6128 HE. [LD0954]
- The wfshell.exe process might exit unexpectedly on a VDA. The issue occurs because of the faulting module, CtxUiMon.dll. [LD1359]
- VDAs on which XenApp and XenDesktop 7.15 LTSR is running might experience a fatal exception on ctxdvcs.sys and display a blue screen with bug check code 0x0000007E. [LD1688]
- The wfshell.exe process might exit unexpectedly on a VDA. [LD1847]
- After you apply Fix LD0624, VDAs for Desktop OS might experience a fatal exception on ctxad.sys and display a blue screen with an audio client check code. [LD1995]
- Attempts to launch applications might fail when the wfshell.exe process exits unexpectedly. The issue occurs because of the faulting module, cmpcom.dll. [LD2107]

#### User Interface

- The logon window might not appear in the foreground when the credentials have to be entered manually. [LC9861]
- With the Citrix **Disconnect** button installed, clicking the Start button might fail to open or might open slowly. [LD1149]
- When you right-click the context menu in a published application, the menu might not open at the location where the cursor is located. [LD1243]
- An issue might occur when you launch a VDA session on a Surface Pro device and enable the **Write in the handwriting panel with your fingertip** feature in the **Pen and Windows Ink** page. The font size of the text or an image that you enter might be larger than the text or an image you enter using your mouse. [LD1472]
- A window might intermittently jump around or disappear from the **VDI desktop** screen. [LD1696]

### VDA for Server OS

#### Keyboard

- When you use the Korean Input Method Editor (IME) to input text, the last character in the text might disappear if you click the mouse. The issue occurs when generic client IME is enabled on

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Citrix Receiver. [LD1380]

- When you navigate to a website and set the keyboard as hidden, the keyboard might still appear in the non-editable area of the website. [LD1382]

### Printing

- Before you print a document, choose a printer from the list of available printers in the published desktop session's print dialog box. There might be a delay until the printer starts printing the document. [LC9601]
- Attempts to print a document might be slow in some workflows. [LD1256]
- With the **Universal print driver usage** setting set to **Use universal printing only**, the client printers might not be auto-created in a session. [LD1395]

### Session/Connection

- When Adobe Acrobat Reader and Microsoft Outlook are running in a seamless mode and you maximize both, the **Menu** bar and the **Minimize**, **Restore**, and **Close** buttons in Acrobat Reader might become unresponsive. [LD1006]
- When 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**. [LD1027]
- The Citrix Broker Service might report the following error in the event log:

  The Citrix Broker Service failed to determine the base settings needed for the Virtual Desktop Agent of machine 'machine_name'.

  Exception: System.ArgumentNullException

  Parameter name: enumStr [LD1315]
- The launch time might increase when multiple Active Directory security groups are configured to limit visibility. [LD1368]
- After you restart a VDA, the Session reliability timeout policy might not be applied during the initial connection. However, attempts to apply the policy for subsequent connections might work. [LD1397]
- VDAs for Server OS might become unresponsive when the Winlogon.exe process exits unexpectedly. [LD1480]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- With Enlightened Data Transport (EDT) enabled, VDAs might exit unexpectedly with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. The issue occurs when you access user sessions externally through the Zscaler. [LD1493]
- When you change the client-side resolution, certain legacy applications such as Citrix Studio might be redrawn incorrectly in a seamless session. [LD1554]
- When you reconnect to a session, the VDA notification icon might disappear from the user device's notification area. [LD1629]
- After you upgrade XenApp and XenDesktop 7.15 LTSR Cumulative Update 2 to Cumulative Update 3, some .Net applications might become unresponsive in a published desktop session. The issue occurs with VDAs on Windows Server 2008 R2. [LD1726]
- 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 a new value. [LD1827]

  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
- The device description in Device Manager might be corrupted on a Japanese version of the Microsoft Windows operating system. [LD1834]
- An access violation can cause the wfshell.exe process to exit unexpectedly. As a result, an attempt to launch an application fails. [LD2050]

#### System Exceptions

- The Internet Explorer (iexplore.exe) process might exit unexpectedly when you run web applications that implement the location API. [LD0677]
- The Citrix software graphics process (Ctxgfx.exe) might exit unexpectedly on an AMD Opteron(tm) Processor 6128 HE. [LD0954]
- Microsoft Internet Explorer might exit unexpectedly. The issue occurs because of the faulting module, icaendpoint.dll. [LD1266]
- The wfshell.exe process might exit unexpectedly on a VDA. The issue occurs because of the faulting module, CtxUiMon.dll. [LD1359]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- VDAs on which XenApp and XenDesktop 7.15 LTSR is running might experience a fatal exception on ctxdvcs.sys and display a blue screen with bug check code 0x0000007E. [LD1688]
- The wfshell.exe process might exit unexpectedly on a VDA. [LD1847]
- Attempts to launch applications might fail when the wfshell.exe process exits unexpectedly. The issue occurs because of the faulting module, cmpcom.dll. [LD2107]

#### 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. [LD0039]

#### User Interface

- The logon window might not appear in the foreground when the credentials have to be entered manually. [LC9861]
- When you right-click the context menu in a published application, the menu might not open at the location where the cursor is located. [LD1243]
- An issue might occur when you launch a VDA session on a Surface Pro device and enable the **Write in the handwriting panel with your fingertip** feature in the **Pen and Windows Ink** page. The font size of the text or an image that you enter might be larger than the text or an image you enter using your mouse. [LD1472]

### Virtual Desktop Components - Other

- Director might show inconsistencies in the application name when retrieved in a published instance of Internet Explorer. As a result, the same application name is shown for different users who are connected to the same machine. [LD0351]
- An issue might occur if you log on to a session using the user principal name (UPN) (user@domain). When you lock the screen, you can see the SAM account (Domain\username) in the locked desktop instead of the UPN (user@ domain). [LD1141]
- Attempts to start a session on the VDA might fail. [LD1180]
- The Citrix Broker Service might report the following error in the event log:

  The Citrix Broker Service failed to determine the base settings needed for the Virtual Desktop Agent of machine ‘machine_name’.

  Exception: System.ArgumentNullException

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Parameter name: enumStr [LD1315]

- Attempts to create a catalog using a VM created through System Center Virtual Machine Manager as a template might fail. The issue occurs when the VM has Windows 10 version 1803 or later installed and you have **Secure boot** enabled on the VM. [LD1608]
- There might be discrepancies in the logon duration time that Citrix Director records, compared to the event log data that VDAs provide. [LD1679]
- The Broker Agent does not write the .gpf files to the persisted data location. [LD1691]
- The App-V packages deployed to VDAs might be incorrectly removed from the VDAs. This fix introduces a registry key under HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features. The key controls whether to enable or disable cleanup. By default, cleanup is disabled. [LD2025]

  To enable it, add the following registry key:

  HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features

  Name: RedundantPackageCleanup

  Type: REG_SZ

  Data: True

## Cumulative Update 4 (CU4)

June 21, 2021

Release date: April 23, 2019

### About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 4 (CU4) fixes more than 140 issues reported since the release of 7.15 LTSR CU3.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU3

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Downloads

Download 7.15 LTSR CU4

### New in this cumulative update

- When you upgrade Delivery Controllers and a site to 7.15 CU4, preliminary site tests run before the actual upgrade begins. These tests include verification that essential Citrix services are running properly, and that the site database is operating correctly and has been recently backed up. After the tests run, you can view a report. Then, you can fix any issues that were detected and optionally run the tests again. This helps ensure that the upgrade will proceed successfully.
- This release removes the dependency on Version 2.0 of PowerShell in stand-alone deployments of Citrix Studio and its components.

> **Note:**
> A version of PowerShell continues to be required on the machines where you install one or more of those components, but the requirement is no longer for Version 2.0. On Delivery Controllers and StoreFront servers, PowerShell 2.0 continues to be required. For more information, see [LD0184]

- If the installation of a VDA or a Delivery Controller 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.

### New deployments

How do I deploy CU4 from scratch?

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

Peruse the XenApp and XenDesktop 7.15 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Securitysections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

### Existing deployments

What do I update?

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

CU4 provides updates to baseline components of the 7.15 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU4. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU4. If Provisioning Services is not part of your deployment, you do not need to install or update it.

### XenApp and XenDesktop 7.15 LTSR CU4 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.4000 | |
| VDA for Server OS | 7.15.4000 | |
| Citrix Studio | 7.15.4000 | |
| Citrix Director | 7.15.4000 | |
| Delivery Controller | 7.15.4000 | |
| Federated Authentication Service | 7.15.4000 | |
| Group Policy Management Experience | 3.1.4000 | |
| Linux VDA | 7.15.4000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.4000 | |
| Provisioning Services | 7.15.15 | |
| Session Recording | 7.15.4000 | Platinum Edition only |
| StoreFront | 3.12.4000 | |
| Universal Print Server | 7.15.4000 | |

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 7.15 LTSR CU4 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 1903 |
| *Browser content redirection | 15.15 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.3000 |
| License Server | 11.15.0.0 Build 26000 |
| Self-Service Password Reset | 1.1.10.0 |
| Workspace Environment Management | 1811 |

***Browser content redirection**

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

**System Requirements:**

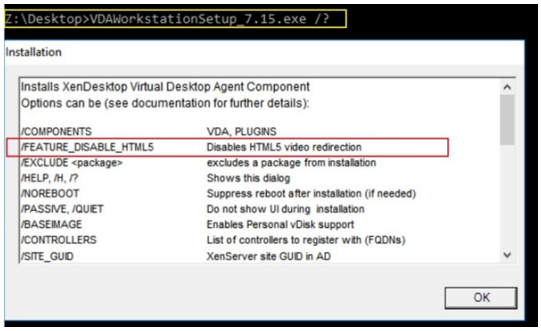
These requirements are specifically for the BCR.msi with XenApp and XenDesktop 7.15 LTSR CU4. Disregard any browser content redirection system requirements listed in any other versions of XenApp, XenDesktop, and Citrix Virtual Apps and Desktops.

- Version 7.15 LTSR CU4 on both the Delivery Controller and the VDA.
- Citrix Workspace app for Windows 1809 or later.
- BCR.msi - available from the Citrix download page.
- Chrome (with the browser content redirection extension installed from the Chrome WebStore) or Internet Explorer 11 (with the Browser Helper Object (BHO) Citrix HDXJsInjector enabled)

**Installation:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Install or upgrade the VDA with Version 7.15 LTSR CU4 by using the command line /FEATURE_DISABLE_HTML5 option.




   This option removes the HTML5 video redirection feature, which must be done before running the BCR.msi. BCR.msi adds the feature back during installation, and also adds the browser content redirection services. When this step is complete, open the services.msc console and verify that the **Citrix HDX HTML5 Video Redirection Service** is not listed.

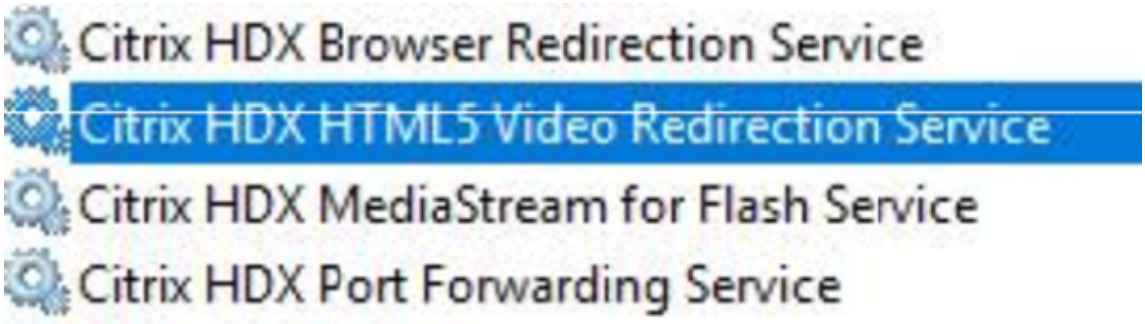
2. Start the browser content redirection installation with the BCR.msi. Depending on your system, the BCR.msi installs its files under:

   C:\Program Files\Citrix\ICAService

   or

   C:\Program Files(86)\Citrix\ICAService

   Because the installation is fast, the dialog box might close quickly. If that occurs, rerun services.msc and verify that these services were added.

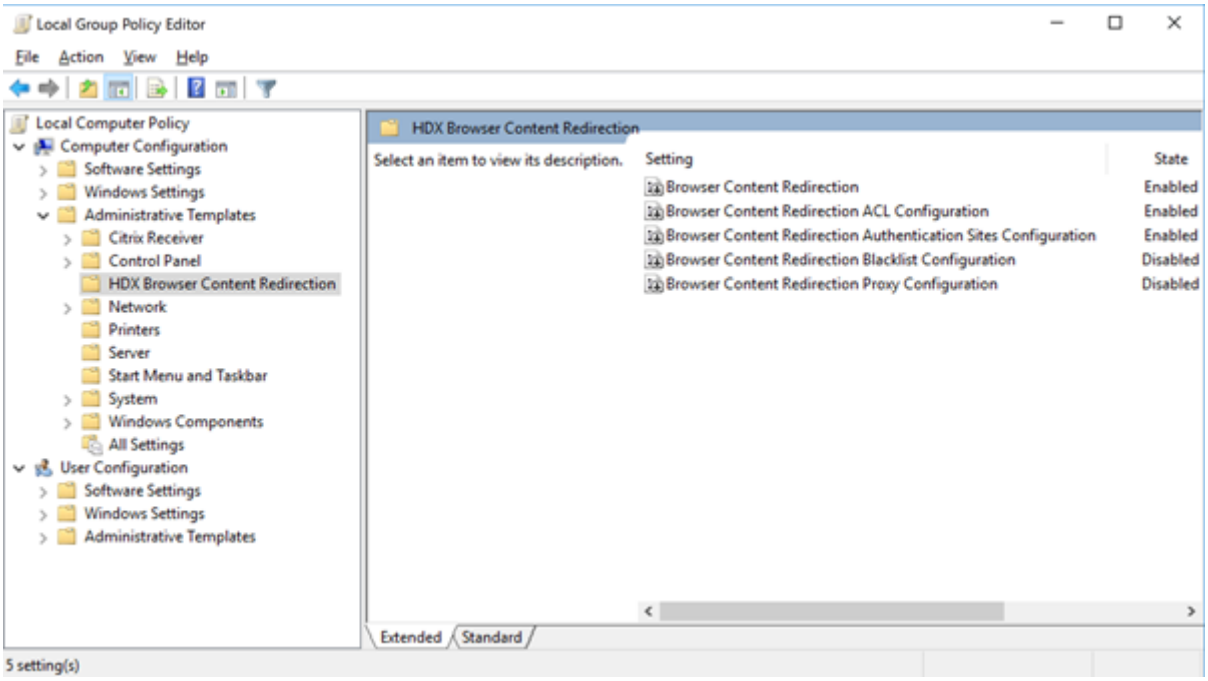



**Policies:**

You can control policies using the HKEY_LOCAL_MACHINE registries on the VDA or the **HDX Browser Content Redirection** Citrix administration template for the Group Policy Management Console.

You can download the template from the citrix.com download page under Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Components. Citrix Studio does not contain these policies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




For more policy information, see Browser content redirection policy settings. For troubleshooting information, see the Knowledge Center article, CTX230052.

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply)<br>AppDisks |

| 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. For more information, see Install and upgrade analytics.

### 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 XenApp 7.15 LTSR CU4. 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 7.15 LTSR CU4 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU4 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 XenApp 7.15 LTSR CU4 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU4 Controller, which import settings from the XML files to the new XenApp Site.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

For more information, see Migrate XenApp 6.x.

## Fixed issues

July 9, 2020

### Citrix Director

- When you navigate to **Filters** > **Sessions** in Citrix Director, check boxes are displayed instead of the session data. [LC9871]
- Custom administrators might not be able to retrieve the session details from a VDA Version 7.15 when the Citrix Director is connected to the Delivery Controller Version 7.6. [LD0134]
- The integration of NetScaler Management and Analytics System (MAS) with Citrix Director might fail. The issue occurs when any group policy changes or renames the built-in administrator account. Director uses the local administrator account to encrypt or decrypt **C:\inetpub\wwwroot\Director\bin..\plugin\hdxInsight\data.xml**. This fix addresses the issue while the changes are made in the code. After the changes are made, Director uses the machine account of the machine on which Director is installed to encrypt or decrypt **C:\inetpub\wwwroot\Director\bin..\plugin\hdxInsight\data.xml**. [LD0231]
- The Daylight Saving Time (DST) is turned on in the operating system. When you attempt to export data by selecting the CSV format to generate an export report for the previous month, the two radio buttons **Export Chart Data** and **Export Table Data** might be missing. [LD0569]
- When you navigate to **Trends** > **Resource Utilization** > **Server OS Machines** and attempt to use the scroll bar to view the complete list of machines, only a few table records are shown. The remaining records are hidden. The issue occurs when the scroll bar does not work correctly. [LD0789]
- When you create custom reports for connections in Director, some DateTime fields, such as session failure time (Session.FailureDate) and session change time (Session.ConnectionStateChangeDate), might not be converted from UTC to local time. [LD1001]
- When you search for a user in Citrix Director and if the user name is long, the name might be truncated. [LD1106]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Citrix Policy

- Attempts to use the Group Policy Management Console (GPMC, gpmc.msc) to copy a Group Policy Object (GPO) that contains Citrix Policy settings might fail. The Microsoft Management Console (MMC) exits unexpectedly. [LD0322]
- The Citrix Universal Printer object is created with the EMF Universal Print Driver inside a session even when you set the Universal Print Driver preferences to **XPS** or **Native drivers**. To enable the fix, install the Citrix Receiver for Windows 4.9.5000 LTSR Cumulative Update 5 or a later version. [LD0360]
- When you modify a policy in Citrix Studio, this error message might appear in the **Configuration Logging**.

  **Error while attempting to determine the policy change details.**

  When this error message appears, you cannot determine the details of the policy change using Configuration Logging. [LD0596]
- When a large number of site policies are configured and if the policies have the IP or the OU based filters, there might be a delay in the logon process. [LD0221]

### Citrix Studio

- This release removes the dependency on Version 2.0 of PowerShell in stand-alone deployments of Citrix Studio and its components.

> **Note:**
> A version of PowerShell continues to be required on the machines where you install one or more of those components, but the requirement is no longer for Version 2.0. On Delivery Controllers and StoreFront servers, PowerShell 2.0 continues to be required. On Windows 7 or Windows Server 2008 R2 systems, Version 3.0 or later of PowerShell is required on the machines where you install Controller components, including Citrix Studio. [LD0184]

- When you add multiple App-V packages to a site, Studio might display this error message and the administrator cannot publish new applications:

  **There was a problem communicating with the server.**
  **Get-AppLibAppVPackage : The maximum message size quota for incoming messages (41943040) has been exceeded.** [LD0232]
- When you create a machine catalog for the target device that was created on a different domain server, the target device might not be recognized. [LD0319]
- The Citrix Universal Printer object is created with the EMF Universal Print Driver inside a session even when you set the Universal Print Driver preferences to **XPS** or **Native drivers**. To enable

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

the fix, install the Citrix Receiver for Windows 4.9.5000 LTSR Cumulative Update 5 or a later version. [LD0360]

- After you rename an application within the application properties and then attempt to remove the Delivery Group from the application in Citrix Studio, this error message appears:

  **Object does not exist.**

  The issue occurs when the application property **ApplicationNameWithFolder** uses the old name after you've changed the application name, instead of replacing it with the new name. [LD0594]

- Using the **Add Machines** wizard to add one or more machines to either an existing or a new Delivery Group might return this error:

  **Machine is already allocated.**

  The message appears only when you go back to the first wizard screen at least once by clicking the Back button. [LD0924]

- You might not be able to view machines from other catalogs in a Delivery Group. The issue occurs when you add machines using the **Add Machine** wizard to either a new or an existing Delivery Group. [LD0988]
- With this fix, the cache for temporary data, Memory allocated to cache (MB): and Disk cache size (GB): are disabled by default when you create a machine catalog. [LD1120]

### Controller

- In a multi-type licensing scenario that is configured for Delivery Groups, an incorrect license type that is not configured for a Delivery Group might be checked out. [LC9086]
- This release removes the dependency on Version 2.0 of PowerShell in stand-alone deployments of Citrix Studio and its components.

> **Note:**
> A version of PowerShell continues to be required on the machines where you install one or more of those components, but the requirement is no longer for Version 2.0. On Delivery Controllers and StoreFront servers, PowerShell 2.0 continues to be required. On Windows 7 or Windows Server 2008 R2 systems, Version 3.0 or later of PowerShell is required on the machines where you install Controller components, including Citrix Studio. [LD0184]

- When a Delivery Group contains at least one VDA in drain-mode, that Delivery Group might not be selected to start a published application. [LD0194]
- When you add multiple App-V packages to a site, Studio might display this error message and the administrator cannot publish new applications:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**There was a problem communicating with the server.**
**Get-AppLibAppVPackage : The maximum message size quota for incoming messages (41943040) has been exceeded.** [LD0232]

- When using the PowerShell command **get-brokericon -filename** with the **-servername** parameter, the command returns an error message. [LD0324]
- The Citrix Virtual Apps published applications might not enumerate intermittently. As a result, a blank screen appears after the session starts or the applications fail to start. The SQL server might experience high CPU usage and the SQL Monitor might show blocked and expensive processes. [LD0336]
- The Citrix Universal Printer object is created with the EMF Universal Print Driver inside a session even when you set the Universal Print Driver preferences to **XPS** or **Native drivers**. To enable the fix, install the Citrix Receiver for Windows 4.9.5000 LTSR Cumulative Update 5 or a later version. [LD0360]
- The resource utilization data in Citrix Director might not be sorted in the correct order. The issue occurs when the SQL statements are presented in the wrong order. [LD0388]
- When you start a session, the broker might choose newly created VDAs over VDAs that were previously started. This choice can cause increased logon time. The increase occurs when the selected VM does not complete the post startup operations before the VM receives a session request. [LD0511]
- After you rename an application within the application properties and then attempt to remove the Delivery Group from the application in Citrix Studio, this error message appears:

  **Object does not exist.**

  The issue occurs when the application property **ApplicationNameWithFolder** uses the old name after you've changed the application name, instead of replacing it with the new name. [LD0594]
- When you modify a policy in Citrix Studio, this error message might appear in the **Configuration Logging**.

  **Error while attempting to determine the policy change details.**

- When this error message appears, you cannot determine the details of the policy change using Configuration Logging. [LD0596]
- Citrix Director might show incorrect user connection failures when the **FailureDate** column for sessions is set to **Null** in the **MonitorData.Session** table. As a result of this failure, the failure types are not updated in the **MonitorData.ConnectionFailureLog** table. There is a mismatch in the connection failure value that is retrieved from the Monitor Database and from the **Get-BrokerConnectionLog** output that is pulled from the Site database. [LD0726]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- If the .vhd extension is present in the upper case (.VHD), the VHD picker might not detect it as a valid vhd image. The issue occurs when you create a Machine Creation Services catalog in an Azure environment. [LD0746]
- The identity disks might be removed from the Machine Creation Services (MCS) that are present in the Amazon Web Services (AWS). [LD1043]
- When using applicable product releases, the administrator might not be able to create a host connection in Studio if NSX-T networking is enabled in the VMware environment. The issue occurs when the MCS does not enumerate the opaque network in NSX-T. [LD1102]
- The HDX connection logon data might be missing from the Logon Duration graph. [LD1113]
- The `CreateNewInstanceOnReset` is decommissioned and is no longer operational. The VM is always preserved when power cycling or when updating a machine catalog. [LD1114]
- There might be a delay of several minutes when you restart a machine while using Amazon Web Services (AWS). [LD1220]
- The Citrix Monitor Service might consume a significant amount of memory. As a result, the Delivery Controller becomes unresponsive and the call requests made from Director time out. [LD1370]

### HDX RealTime Optimization Pack

HDX RealTime Optimization Pack 7.15 LTSR CU4 documentation provides specific information about the updates in this release.

### Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU4 documentation provides specific information about the updates in this release.

### Personalization for App-V

#### Studio

- An incorrect application might launch from an App-V package when the application name is in a non-English language. [LD0222]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### VDA

- An incorrect application might launch from an App-V package when the application name is in a non-English language. [LD0222]

### Profile Management

- When you log on to the Citrix Virtual Apps server for the second time, the user profile is corrupted. The issue occurs when Profile Management cannot delete the profile at logoff because the profile is in use by the system. Restart the Profile Management Service to delete the profile. [LD0560]
- When the **CopyFileWithRetries** function fails to copy a file in a directory, the remaining files might not be copied. The issue occurs when the Citrix Profile Management service attempts to copy files from a default template profile directory to the current user's profile directory. During the copy process, the corresponding function **CopyDirectory** ends the copy operation when one file under the current directory can't be copied because of permission restrictions. As a result, other files aren't copied. [LD0648]
- The VDA for Server OS is running on Microsoft Windows 10, Version 1709 or greater. When you choose to exclude the *.tmp file for synchronization of Profile Management policy, the changes you make to any Microsoft Office documents, such as Word and PowerPoint files, might not be saved while you log out. Your changes are not retained when you log on and reopen the files. [LD0782]
- The AppData(Roaming) folder redirection might fail to work in Profile Management that is running on Microsoft Windows 10. The issue occurs when the AppData(Roaming) folder does not preexist in the file storage directory. [LD0797]

### Provisioning Services

Provisioning Services 7.15 LTSR CU4 provides specific information about the updates in this release.

### Session Recording

#### Administration

- There can be scalability and performance issues when using Session Recording. [LD0970]
- Attempts to upgrade Session Recording from Version 7.15 to Version 7.15 Cumulative Update 2 might take a long time. [LD1042]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Agent

- Attempts to install Session Recording Agent Version 7.15 Cumulative Update 3 on the French and Spanish version of the Microsoft Windows operating system might fail. [LD1161]

### Player

- When you reconnect to a disconnected session, the Session Recording Player shows the application's full path to the executable for the session. The Session Recording Player should display the published application name for the session. [LD0426]
- Session Recording Player Version 7.15 Cumulative Update 2 might fail to play recorded files and stop responding when the Session Recording Player is launched as an application. [LD0578]

## StoreFront

- When you configure a StoreFront with a base URL that contains an underscore (_) and use it with the Citrix Gateway, an error might occur. [LC9678]
- When you log on to StoreFront and refresh the Citrix Receiver for Web page, the timeout dialog box might be suppressed. [LD0214]
- Attempts to log on to StoreFront might fail with the **Cannot Complete your Request** error. The issue occurs when there is a TCP dynamic port exhaustion. [LD0573]
- After you upgrade StoreFront from Version 3.5 to Version 3.12, the following event log details might appear in the Event Viewer:

  **User name/password authentication is not enable in Store Front. Citrix.DeliveryServicesClients.Authentication.Exceptions.ProtocolNotAvailableException, Citrix.DeliveryServicesClients.Authentication, Version=3.12.0.0, Culture=neutral, PublicKeyToken=null Invalid protocol exception. The requested protocol is: ExplicitForms Protocol: ExplicitForms at Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.CreateExpli**
  [LD0608]
- The message, **There are no apps or desktops available to you at this time** remains visible even when the available apps or desktops are displayed. [LD0857]
- When using the Safari 12 and later browsers, client detection might fail on Citrix Receiver for Web because the Netscape Plugin Application Programming Interface (NPAPI) support was removed. For more information, see the Knowledge Center article CTX238286. [LD0863]
- Disable the **Desktop Viewer** toolbar for a specified Delivery Group by adding the property, **ConnectionBar=0** under each application's section of the default.ica file in the store. When you

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

disconnect and then reconnect to the session, the **Desktop Viewer** toolbar is shown again. [LD1051]

- It is only possible to modify the order of Secure Ticket Authorities (STAs) in the StoreFront management console when the option **Load balance multiple STA servers** is selected. The logic should be reversed to allow STAs order to be modified only when **Load balance multiple STA servers** is not selected. [LD1118]
- The default website setting might not appear correctly to the other nodes in an on-premises multiple-server group. As a result, the browser is forwarded to the HTTP URL for the node, rather than the correct URL. [LD1119]
- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX251988. [LD1361]

## Universal Print Server

### Client

- Before you print a document, choose a printer from the list of available printers in the published desktop session's print dialog box. There might be a delay until the printer starts printing the document. [LC9601]
- The Print Spooler service might exit unexpectedly. The issue occurs when **CRawStreamHeaderWriter::EndPage** and **CRawStreamHeaderWriter::StartPage** attempt to access a null object. [LC7893]
- After installing a VDA, the printer ports under printer Properties might no longer appear on a mapped network printer. [LD0949]

### Server

- Due to an access violation, the Universal Print Server (UPServer.exe) might exit unexpectedly and generate Event ID 7031. [LC7821]
- An access violation in **CPTStream::ThisStream** can cause the Print Spooler service to become unresponsive. [LC8856]
- Users who are members of many Active Directory groups might not be able to connect to their printers from the Universal Print Server. [LC8714]
- The Citrix Universal Print Driver advanced printing features, such as stapling and paper source, might display blank menus. [LC9711]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## VDA for Desktop OS

### HDX RealTime Windows Media Redirection

- Citrix HDX RealTime Media Engine might exit unexpectedly when you attempt to access the HDX web camera. [LD0062]
- With the **HDX MediaStream Windows Media Redirection** setting disabled, attempts to open certain video file formats through Windows Media Player can result in the following error message:

  **Windows Media Player encountered a problem while playing the file.**

  However, for some video file formats, the video aspect ratio is incorrect. [LD0279]

### Keyboard

- When you use the Chinese keyboard layout in a user session, the Input Method Editor (IME) automatically changes to the Wubi Chinese character input method. The issue occurs when the default IME is not set to **Wubi**. [LD0429]

### Printing

- After you upgrade XenApp and XenDesktop from Version 7.9 to Version 7.15, you might be unable to print documents to a different output printer tray. The print job uses the default tray to print documents even though you can choose a different tray from the Print dialog. [LC9247]
- When you send the PDF in raw data format to the print queue, the PDF might not be printed. [LC9755]
- When you attempt to print a page, the printing preferences window might not be shown correctly. The issue occurs when there are translation issues in the printing preferences window. As a result, the **Citrix** icon and the **Local Printer Settings** button name are truncated. [LD0359]
- Microsoft Windows Server 2016 fails to update the value under the registry key **HKEY_CURRENT_USER\SOFT NT\CurrentVersion\Windows\Device** when the default printer is the Citrix mapped printer. Because of this failure, the default printer might not be set for non-.net applications. [LD1032]

### Session/Connection

- Certain third-party applications might become unresponsive in a seamless session until you use the Shift+F2 key to switch the session to windowed mode and then back to seamless mode. [LC9727]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you maximize the published applications, the applications might overlap the top section of the taskbar. [LD0025]
- With the **Enable Secure ICA** setting enabled in the Delivery Group and the **DHParaml** value not present under the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Security, the applications might fail to start. This error message appears:

  **Unable to launch your application. Contact your help desk with the following information:**
  **Cannot connect to the Citrix XenApp server.protocol Driver error Desktop Viewer. The connection to "VOA Win 7 LTSR"failed with status (Unknown client error).** [LD0117]
- When processing a credit card transactions through a user device, the application and the user device can become unresponsive, or only a subset of data might be received. [LD0152]
- Attempts to start an application from a random server might fail. This error message appears:

  **Unable to launch your application. Cannot connect to the Citrix XenApp Server. The Citrix SSL Server you selected is not accepting connections.**

  The issue occurs when the server stops accepting connections on an SSL-enabled VDA. [LD0239]
- This fix addresses a memory leak issue that occurs when the **Auto connect client drives** policy is disabled. [LD0370]
- The function that terminates a thread in the TWI module (twi3.dll) might cause the server to become unresponsive. [LD0406]
- With Local App Access enabled, when you attempt to open applications in the published desktops on Microsoft Windows 10, Version 1803, the applications cannot be minimized. [LD0411]
- The user device session might stop responding for a few minutes when using certain third-party applications. [LD0419]
- You open a Google account email on an Internet Explorer, Chrome, or a Firefox browser. When you attempt to compose a new email, the **Automatic Keyboard display** feature might not work. [LD0470]
- Applications in seamless mode might become unresponsive when you change the application size from maximized to windowed or the opposite way. [LD0498]
- The target device might restart unexpectedly when the scardhook64.dll causes the exception X64_CRITICAL_PROCESS_FAULT_INVALID_POINTER_READ_IN_CALL. [LD0504]
- Attempts to reconnect to a session might fail when you set the **AutoLogon** value to a non-zero value and run the Citrix Diagnostics Facility (CDF) tracing. [LD0602]
- Part of the published application's window might not refresh. This issue can occur when any one of the Citrix published applications that are running in the background appears in the foreground. [LD0711]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you play certain third-party recording applications in a published desktop, Internet Explorer might exit unexpectedly. [LD0830]
- With this fix, the CtxUvi Hooking driver will not attempt to load MfApHook.dll on to a secure process."[LD0847]
- Published applications might be blocked while waiting for a response from the location API.

  To enable the fix by configuring the timeout value, set the following registry keys:

  - *On 32-bit systems*

    HKEY_LOCAL_MACHINES\SOFTWARE\Citrix\Location

    Name: LatlongWaitTime

    Type: REG_DWORD

    Value: Milliseconds. Default value is 60000 milliseconds. The value is the wait time allowed for getting the location information.

  - *On 64-bit systems*

    HKEY_LOCAL_MACHINES\SOFTWARE\Wow6432Node\Citrix\Location

    Name: LatlongWaitTime

    Type: REG_DWORD

    Value: Milliseconds. Default value is 60000 milliseconds. The value is the wait time allowed for getting the location information. [LD0905]

- With this fix, the CtxUvi driver might exclude the vmsp.exe process from loading Citrix dlls. For more information, see the Knowledge Center article CTX107825. [LD1024]
- An issue might occur when you press the Ctrl+Alt+Delete keys repeatedly at the local console while someone else on the user session selects **Don't allow** for the same action at the same time. A new local console screen might display for 30 seconds. As a result, the content on the console appears like an extra virtual screen for the same session. [LD1077]

### System Exceptions

- After you upgrade the target device from Version 7.6 to Version 7.15, the Internet Explorer, Windows Media Player, and the Themes service might exit unexpectedly. [LC9872]
- When you launch the VM hosted applications, the mmvdhost.exe process might exit unexpectedly. [LC9976]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen with bug check code 0x3b (SYSTEM_SERVICE_EXCEPTION). [LD0089]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [LD0119]
- An access violation can cause the VDAs to experience a fatal exception and display a blue screen. [LD0281]
- VDAs might experience a fatal exception on vd3dk.sys and display a blue screen. [LD0368]
- The wfshell.exe process might exit unexpectedly on the VDA due to the exception **DivideByZeroException**. The process displays the error message **wfshell shell has stopped working**. [LD0373]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen with bug check code 0x50. [LD0410]
- Due to a LIST_ENTRY corruption, the VDAs might experience a fatal exception on CtxUVI.sys and display a blue screen. [LD0421]
- The wfshell.exe process might exit unexpectedly when you attempt to access long URLs in a published instance of Internet Explorer. [LD0454]
- Due to a null pointer, the mmvdhost.exe process might exit unexpectedly when you log on to a VDA. [LD0474]
- The Internet Explorer (iexplore.exe) process might exit unexpectedly with the exception code **0xc00001a5**. The issue occurs when the CtxSensVcLibDll.dll faulting module unloads. [LD0485]
- When you attempt to export video clips on a VDA for Desktop OS, certain third-party applications might exit unexpectedly. [LD0506]

### User Experience

- A Microsoft Windows Version 10 client might increase the scaling of the client's high resolution monitor whose DPI scaling is set to 100. [LD0131]
- When you hover the mouse pointer over an item, the tooltip pop-up might disappear and the application loses focus. [LD0365]
- When you reconnect to a session, the lossless indicator icon disappears from the user device's notification area. To address the issue, you must set the following registry [LD0919]:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator\Interval
Type: DWORD
Value: 3 (default: 0)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## User Interface

- When you start a VM hosted app while you attempt to reconnect to a disconnected session, all but the most recently clicked applications that are present in the session are displayed. [LD0189]
- You applied Fix LD0419. When you attempt to change the cursor shape in an application without changing the cursor name, the cursor shape might not be modified. [LD0983]

## VDA for Server OS

### HDX MediaStream Windows Media Redirection

- You're using HDX MediaStream Windows Media redirection and the Windows Media Player to redirect VC-1 live streams. The live streams might fall back to server side rendering. [LD0251]
- Citrix HDX RealTime Media Engine might exit unexpectedly when you attempt to access the HDX web camera. [LD0062]
- With the **HDX MediaStream Windows Media Redirection** setting disabled, attempts to open certain video file formats through Windows Media Player can result in the following error message:

  **Windows Media Player encountered a problem while playing the file.**

  However, for some video file formats, the video aspect ratio is incorrect. [LD0279]

### Keyboard

- When you use the Chinese keyboard layout in a user session, the Input Method Editor (IME) automatically changes to the Wubi Chinese character input method. The issue occurs when the default IME is not set to **Wubi**. [LD0429]

### Printing

- After you upgrade XenApp and XenDesktop from Version 7.9 to Version 7.15, you might be unable to print documents to a different output printer tray. The print job uses the default tray to print documents even though you can choose a different tray from the Print dialog. [LC9247]
- When you send the PDF in raw data format to the print queue, the PDF might not be printed. [LC9755]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Microsoft Windows Server 2016 fails to update the value under the registry key **HKEY_CURRENT_USER\SOFT NT\CurrentVersion\Windows\Device** when the default printer is the Citrix mapped printer. Because of this failure, the default printer might not be set for non-.net applications. [LD1032]

**Session/Connection**

- Certain third-party applications might become unresponsive in a seamless session until you use the Shift+F2 key to switch the session to windowed mode and then back to seamless mode. [LC9727]
- 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. [LC9975]
- When you maximize the published applications, the applications might overlap the top section of the taskbar. [LD0025]
- With the **Enable Secure ICA** setting enabled in the Delivery Group and the **DHParaml** value not present under the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Security, the applications might fail to start. This error message appears:

  **Unable to launch your application. Contact your help desk with the following information:**
  **Cannot connect to the Citrix XenApp server.protocol Driver error Desktop Viewer. The connection to "VOA Win 7 LTSR"failed with status (Unknown client error).** [LD0117]
- When processing a credit card transactions through a user device, the application and the user device can become unresponsive, or only a subset of data might be received. [LD0152]
- Attempts to start an application from a random server might fail. This error message appears:

  **Unable to launch your application. Cannot connect to the Citrix XenApp Server. The Citrix SSL Server you selected is not accepting connections.**

  The issue occurs when the server stops accepting connections on an SSL-enabled VDA. [LD0239]
- This fix addresses a memory leak issue that occurs when the **Auto connect client drives** policy is disabled. [LD0370]
- The function that terminates a thread in the TWI module (twi3.dll) might cause the server to become unresponsive. [LD0406]
- With Local App Access enabled, when you attempt to open applications in the published desktops on Microsoft Windows 10, Version 1803, the applications cannot be minimized. [LD0411]
- VDAs for Server OS might reregister intermittently when an out-of-order notification is sent to the Delivery Controllers. [LD0466]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- You open a Google account email on an Internet Explorer, Chrome, or a Firefox browser. When you attempt to compose a new email, the **Automatic Keyboard display** feature might not work. [LD0470]
- Applications in seamless mode might become unresponsive when you change the application size from maximized to windowed or the opposite way. [LD0498]
- The target device might restart unexpectedly when the scardhook64.dll causes the exception X64_CRITICAL_PROCESS_FAULT_INVALID_POINTER_READ_IN_CALL. [LD0504]
- The enumeration of audio devices on the endpoint might time out. As a result, the session does not have audio. [LD0663]
- Part of the published application's window might not refresh. This issue can occur when any one of the Citrix published applications that are running in the background appears in the foreground. [LD0711]
- Seamless applications launch in fixed size mode. The issue occurs when the network connection is interrupted and then restored while session reliability is disabled. [LD0733]
- With this fix, the CtxUvi Hooking driver might exclude the secure processes from loading Citrix dlls. [LD0847]
- Published applications might be blocked while waiting for a response from the location API.

  To enable the fix by configuring the timeout value, set the following registry keys:

  - *On 32-bit systems*

    HKEY_LOCAL_MACHINES\SOFTWARE\Citrix\Location

    Name: LatlongWaitTime

    Type: REG_DWORD

    Value: Milliseconds. Default value is 60000 milliseconds. The value is the wait time allowed for getting the location information.

  - *On 64-bit systems*

    HKEY_LOCAL_MACHINES\SOFTWARE\Wow6432Node\Citrix\Location

    Name: LatlongWaitTime

    Type: REG_DWORD

    Value: Milliseconds. Default value is 60000 milliseconds. The value is the wait time allowed for getting the location information. [LD0905]

- With this fix, the CtxUvi driver might exclude the vmsp.exe process from loading Citrix dlls. For more information, see the Knowledge Center article CTX107825. [LD1024]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- After you upgrade the VDA to Version 7.15 Cumulative Update 3, the applications might launch slowly. The issue occurs when the user groups are configured to **Limit Visibility**. [LD1215]

#### System Exceptions

- When you launch the VM hosted applications, the mmvdhost.exe process might exit unexpectedly. [LC9976]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen with bug check code 0x3b (SYSTEM_SERVICE_EXCEPTION). [LD0089]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [LD0119]
- An access violation can cause the VDAs to experience a fatal exception and display a blue screen. [LD0281]
- The wfshell.exe process might exit unexpectedly on the VDA due to the exception **DivideByZeroException**. The process displays the error message **wfshell shell has stopped working**. [LD0373]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen with bug check code 0x50. [LD0410]
- Due to a LIST_ENTRY corruption, the VDAs might experience a fatal exception on CtxUVI.sys and display a blue screen. [LD0421]
- The wfshell.exe process might exit unexpectedly when you attempt to access long URLs in a published instance of Internet Explorer. [LD0454]
- The Internet Explorer (iexplore.exe) process might exit unexpectedly with the exception code **0xc00001a5**. The issue occurs when the CtxSensVcLibDll.dll faulting module unloads. [LD0485]

#### User Experience

- When you hover the mouse pointer over an item, the tooltip pop-up might disappear and the application loses focus. [LD0365]

#### User Interface

- When you start a VM hosted app while you attempt to reconnect to a disconnected session, all but the most recently clicked applications that are present in the session are displayed. [LD0189]
- The graphics appearing on the desktops might be corrupted. [LD1115]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Cumulative Update 3 (CU3)

June 21, 2021

Release date: October 29, 2018

## About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 3 (CU3) fixes more than 200 issues reported since the release of 7.15 LTSR CU2.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU2

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

## Downloads

Download 7.15 LTSR CU3

## New in this cumulative update

Browser content redirection is a newly compatible component of XenApp and XenDesktop 7.15 LTSR, available as a separate download. For more information about browser content direction in this cumulative update, see *Browser content redirection* under XenApp and XenDesktop 7.15 LTSR CU3 compatible components.

## New deployments

How do I deploy CU3 from scratch?

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

Peruse the XenApp and XenDesktop 7.15 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Securitysections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Existing deployments

What do I update?

CU3 provides updates to baseline components of the 7.15 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU3. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU3. If Provisioning Services is not part of your deployment, you do not need to install or update it.

### XenApp and XenDesktop 7.15 LTSR CU3 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.3000 | |
| VDA for Server OS | 7.15.3000 | |
| Delivery Controller | 7.15.3000 | |
| Citrix Studio | 7.15.3000 | |
| Citrix Director | 7.15.3000 | |
| Group Policy Management Experience | 3.1.3000 | |
| StoreFront | 3.12.3000 | |
| Provisioning Services | 7.15.9 | |
| Universal Print Server | 7.15.3000 | |
| Session Recording | 7.15.3000 | Platinum Edition only |
| Linux VDA | 7.15.3000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.3000 | |
| Federated Authentication Service | 7.15.3000 | |

### XenApp and XenDesktop 7.15 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

might ask you to upgrade to a newer version of these components within your 7.15 LTSR environments.

| 7.15 LTSR CU3 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 4.15.0 |
| *Browser content redirection | 15.15 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4.2000 |
| License Server | 11.15.0.0 Build 25000 |
| Self-Service Password Reset | 1.1.10.0 |
| Workspace Environment Management | 4.7 |

***Browser content redirection**

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA. For more information see Browser content redirection.

**System Requirements:**

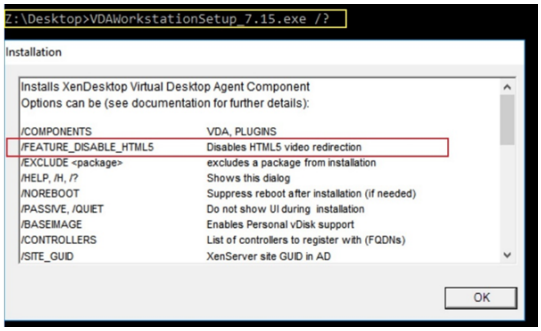
These requirements are specifically for the BCR.msi with XenApp and XenDesktop 7.15 LTSR CU3. Disregard any browser content redirection system requirements listed in any other versions of XenApp, XenDesktop, and Citrix Virtual Apps and Desktops.

- Version 7.15 LTSR CU3 on both the Delivery Controller and the VDA.
- Citrix Workspace app for Windows 1809 or later.
- BCR.msi - available from the Citrix download page.
- Chrome (with the browser content redirection extension installed from the Chrome WebStore) or Internet Explorer 11 (with the Browser Helper Object (BHO) Citrix HDXJsInjector enabled).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Installation:**

1. Install or upgrade the VDA with Version 7.15 LTSR CU3 by using the command line /FEATURE_DISABLE_HTML5 option.




   This option removes the HTML5 video redirection feature, which must be done before running the BCR.msi. BCR.msi adds the feature back during installation, and also adds the browser content redirection services. When this step is complete, open the services.msc console and verify that the **Citrix HDX HTML5 Video Redirection Service** is not listed.

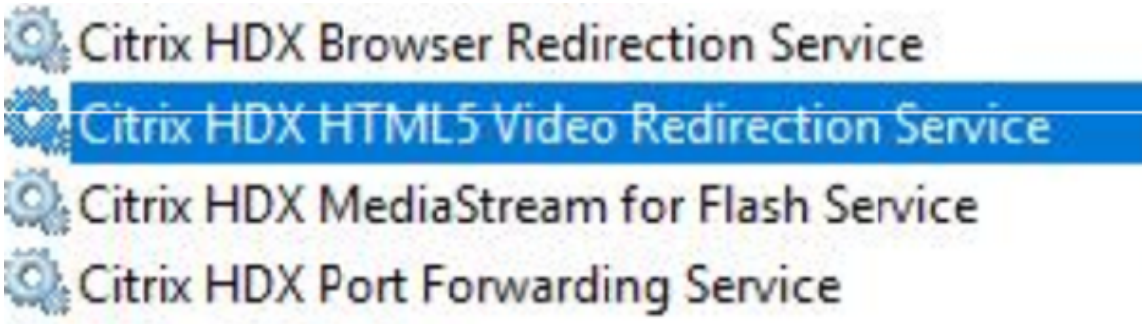
2. Start the browser content redirection installation with the BCR.msi. Depending on your system, the BCR.msi installs its files under:

   C:\Program Files\Citrix\ICAService

   or

   C:\Program Files(86)\Citrix\ICAService

   Because the installation is fast, the dialog box might close quickly. If that occurs, rerun services.msc and verify that these services were added.

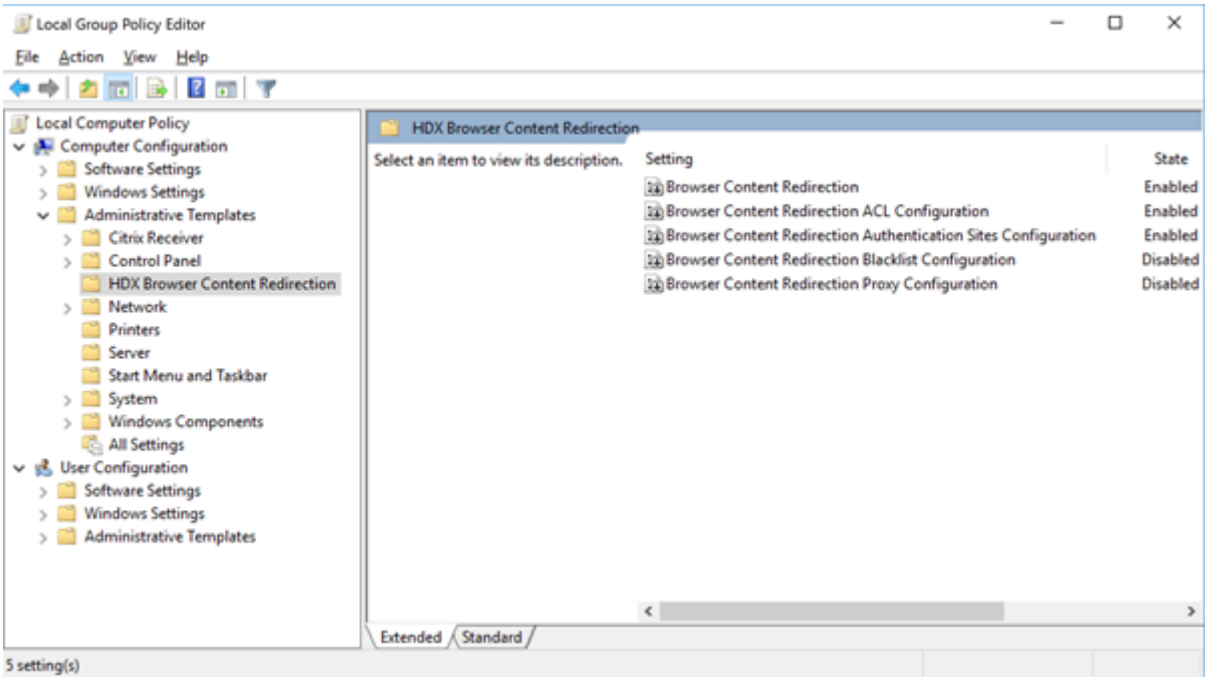



**Policies:**

You can control policies using the HKEY_LOCAL_MACHINE registries on the VDA or the **HDX Browser Content Redirection** Citrix administration template for the Group Policy Management Console.

You can download the template from the citrix.com download page under Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Components. Citrix Studio does not contain these policies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




For more policy information, see Browser content redirection policy settings. For troubleshooting information, see the Knowledge Center article, CTX230052.

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
| --- |
| Framehawk |
| StoreFront Citrix Online Integration |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply)<br>AppDisks |

| 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. For more information, see Install and upgrade analytics.

### 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 XenApp 7.15 LTSR CU3. 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 7.15 LTSR CU3 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU3 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 XenApp 7.15 LTSR CU3 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU3 Controller, which import settings from the XML files to the new XenApp Site.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

For more information, see Migrate XenApp 6.x.

## Fixed issues

July 9, 2020

### Citrix Director

- Attempts to remove the user assignment from a desktop using Citrix Studio, PowerShell, or Citrix Director by a delegated administrator with a custom role might fail. The issue occurs when custom administrators have permissions to perform the operations on the Delivery Groups but do not have permissions on the Machine Catalogs. [LC8174]
- Attempts to search for users when assigning them to machines might fail. The selected user is shown as null. [LC8395]
- Citrix Director might report Multi-Stream ICA as inactive when using the **UDP-based Data Transfer Protocol (UDT)**. The issue occurs when the HDX WMI provider is not updated to account for EDT or UDT sessions. [LC8960]
- The CPU usage of the w3wp.exe process might be very high on Citrix Director. [LC9222]
- When you set the browser language to certain non-English language and start Citrix Director, the session detail pane might show one session as active even when there are no sessions running. [LC9392]
- When using Citrix Director, Microsoft Internet Explorer 11 might display non-functional scroll bars in the **Machine Details** section of **Filters** > **Machines** > **All machines** page. [LC9505]
- In the **Trends** page in **Citrix Director**, Internet Explorer might automatically add Google Analytics (https://www.google-analytics.com) as a trusted site. This action by Internet Explorer cannot be stopped. Even when you disable the automatic uploads value **SendExperienceMetrics** under the registry key HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall, Google Analytics calls are established on the Citrix Director dashboard and on the Applications page. To disable automatic uploads, use the procedure described in Citrix Insight Services. After you apply this fix, a ping is made to Google Analytics on a Citrix Director logon, but the data doesn't upload. [LC9736]
- The reports generated in CSV format for the logon performance in Citrix Director might use the UTC time zone instead of the local time. [LC9854]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Some administrators might not be able to access some domains that were added in the web.config domain list. As a result, when you search for a user's session, an exception occurs and the session details are not displayed. [LC9865]
- The **ExportCsvDrilldownLimit** value might not be applied for custom reports in Citrix Director. [LD0004]

### Citrix Policy

- When you apply the loopback policy in merge mode to a VDA and add the StoreFront URL to a Delivery Group of the VDA in Citrix Studio, duplicate icons of published applications might appear. [LC8889]
- Attempts to create a machine catalog might fail with an exception stating that it cannot create the summary. Additionally, when using the creation catalog wizard and before the exception appears, the drop-down list that is supposed to list the domains is empty. [LC9636]
- When you run the Group Policy Results tool from the Group Policy Management console on a machine that is installed with VDA 7.15.2000, the following error message appears: **An error occurred while generating report: Not Found** [LC9825]
- The Citrix Print Manager service (cpsvc.exe) might exit unexpectedly. The issue occurs when there are garbage entries in the printing registry key that is connected to a Group Policy Object (GPO). [LC9921]
- The Group Policy engine might fail to insert all the values to the **ApplicationStartDetails** registry key. As a result, attempts to start App-V applications might fail. [LC9942]
- When registry entries are manually pre-populated to session keys under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix, the keys might not be updated upon session start. [LC9977]
- When you attempt to apply a Citrix Policy in Citrix Studio using the Organizational Unit (OU) filter, the following error message might appear: **An unknown error occurred**.

  The following exception appears:
  **Collection was modified; enumeration operation may not execute.**[LD0044]
- When you attempt to back up a Group Policy and then import the Group Policy with the Group Policy Management Console (GPMC) Version 3.1.2, the GPMC might become unresponsive. But, the policy is imported. [LD0173]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Citrix Studio

- Attempts to remove the user assignment from a desktop using Citrix Studio, PowerShell, or Citrix Director by a delegated administrator with a custom role might fail. The issue occurs when custom administrators have permissions to perform the operations on the Delivery Groups but do not have permissions on the Machine Catalogs. [LC8174]
- When one of the Delivery Controllers goes offline or becomes otherwise unavailable, Citrix Studio might take a few minutes to open and display the following message:

  **This snap-in is not responding**. [LC8993]
- Attempts to unpublish and remove App-V packages from the VDA might fail. [LC9161]
- When you attempt to view the **Machine Allocation** page for the second time after selecting **Edit Delivery Group** in the **Actions** pane, the **Machine Allocation** page might become blank and the details such as machine name and users are not displayed. [LC9465]
- Attempts to delete the **application folder** in Citrix Studio after moving the published application from **Application Group** might fail with a permission error. [LC9520]
- After upgrading Citrix Studio to Version 7.15 Cumulative Update 2, the policies might not be localized. For more information, see Knowledge Center article CTX234711. [LC9613]
- Attempts to create a machine catalog might fail with an exception stating that it cannot create the summary. Additionally, when using the creation catalog wizard and before the exception appears, the drop-down list that is supposed to list the domains is empty. [LC9636]
- When you attempt to delete App-V applications from the Delivery Group, the applications might be deleted. An error message appears. [LC9985]
- When you attempt to apply a Citrix Policy in Citrix Studio using the Organizational Unit (OU) filter, the following error message might appear: **An unknown error occurred**.

  The following exception appears:
  **Collection was modified; enumeration operation may not execute**. [LD0044]
- When you attempt to apply a Citrix policy in Citrix Studio using the Organizational Unit (OU) filter or add an OU in the catalog wizard, an exception occurs. [LD0112]

### Controller

- Attempts to remove the user assignment from a desktop using Citrix Studio, PowerShell, or Citrix Director by a delegated administrator with a custom role might fail. The issue occurs when custom administrators have permissions to perform the operations on the Delivery Groups but do not have permissions on the Machine Catalogs. [LC8174]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The VDAs might intermittently have an invalid power state in Citrix Studio. Studio shows the power state to be **OFF** even when the VDA is running. [LC8898]
- When one of the Delivery Controllers goes offline or becomes otherwise unavailable, Citrix Studio might take a few minutes to open and display the following message:

  **This snap-in is not responding** [LC8993]
- You import changes from the principal broker to the Local Host Cache (LHC) database and remove a user or machine from the Active Directory without removing it from Citrix Studio. As a result, errors might occur and the LHC isn't updated. [LC9054]
- Deadlocks might occur on XenApp with an application **Event ID 2013** during peak connection time. This error message appears:

  **An unexpected exception occurred while the Citrix Broker Service processed an HTTP request**. [LC9134]
- When you upgrade XenApp 7.6 to XenApp 7.15, the permissions for the Licensing folder on the Delivery Controller under **C:\Windows\ServiceProfiles\NetworkService\Licensing** is overwritten. [LC9445]
- The Citrix High Availability Service (HighAvailabilityService.exe) memory usage might exceed 2 GB. [LC9446]
- When you send a reboot command to the target VDA from Citrix Studio, the target VDA might shut down. [LC9479]
- Attempts to delete the **application folder** in Citrix Studio after moving the published application from **Application Group** might fail with a permission error. [LC9520]
- The Virtual desktop infrastructure (VDI) that is hosted on the ESXi hosts might go into an unknown power state and does not power on automatically. The issue occurs after the virtual machines (VMs) are moved to the ESXi hosts after the ESXi hosts are taken out of maintenance mode. [LC9619]
- Attempts to create a machine catalog might fail with an exception stating that it cannot create the summary. Additionally, when using the creation catalog wizard and before the exception appears, the drop-down list that is supposed to list the domains is empty. [LC9636]
- Citrix Studio does not show the **Start** option. As a result, the Remote PC fails to power on. [LC9702]
- Using this performance enhancement for the Monitor service, reduces the high CPU consumption on the SQL server when the Monitor database is large. [LC9726]
- The Machine Creation Services (MCS) provisioned virtual machines (VMs) might not be created with **Secure Boot** enabled. This issue might occur even when the Master template was created using Extensible Firmware Interface (EFI) and with **Secure Boot** enabled. [LC9841]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- By default, the Amazon Web Services (AWS) ID of the Machine Creation Services (MCS) provisioned machine is non-persistent. This might cause the power management actions of the virtual machine to fail on the AWS.

  To configure the persistence of the AWS ID, the following options are available:

  - To enable the persistent of the AWS ID, set the Host connection's advance property's Connection option to **CreateNewInstanceOnReset=False**.
  - To disable the persistent of the AWS ID, set the Host connection's advance property's Connection option to **CreateNewInstanceOnReset=True** or delete the option.

  A ten second wait time is required when the option is changed to take effect. [LC9960]

- Attempts to create an application using the **New-BrokerApplication** command with the -AdminFolder parameter might not create the specified folder in certain scenarios. [LC9982]
- When you attempt to delete App-V applications from the Delivery Group, the applications might be deleted. An error message appears. [LC9985]
- In a large environment where many Application Groups are used, when you click the Applications tab in Studio, the session times out while fetching **Get-BrokerApplicationGroup** output. As a result, the following exception appears:

  **Database could not be connected**.

  Before throwing the exception, Studio becomes unresponsive while enumerating the Application Groups. [LD0012]

- When you attempt to apply a Citrix Policy in Citrix Studio using the Organizational Unit (OU) filter, the following error message might appear: **An unknown error occurred**.

  The following exception appears:
  **Collection was modified; enumeration operation may not execute**. [LD0044]

- Attempts to recreate the Local Host Cache with a Delivery Group name that contains special characters might fail with an **Event ID 505**. [LD0068]
- The Citrix Studio hosting connection might give a warning message to use the HTTPS for XenServer hosting connections even though the HTTPS connections are not supported. [LD0210]
- After you upgrade XenApp and XenDesktop to Version 7.15, the initial reboot schedules might start immediately instead of starting during the next scheduled event. [LD0308]

### HDX RealTime Optimization Pack

HDX RealTime Optimization Pack 7.15 LTSR CU3 documentation provides specific information about the updates in this release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Identity Assertion

- Attempts to access the authentication certificate that is available in the session to log on might fail. [LC9728]
- When using a Federated Authentication Service in-session certificate to authenticate a TLS 1.1 (or earlier) connection, the connection can fail. Event ID 305 is logged, indicating an unsupported hash ID. The Federated Authentication Service does not support the SHAMD5 hash. [LD0018]

### Installer

- Attempts to install the VDA in the environment that already has Adobe Acrobat Reader 2015 DC application installed can result in the following error message:

  **The Program can't start because mfc120u.dll is missing from your computer. Try reinstalling the program to fix the problem**. [LC9979]

### Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU3 documentation provides specific information about the updates in this release.

### Profile Management

- When you configure folder redirection using Microsoft Active Directory policy by clicking **Reset Profile** in Citrix Director, the redirected folders are also reset. As a result, certain folders such as **Documents**, **Pictures**, **Music**, **Videos**, and **Favorites** are renamed. But, folders such as **Start Menu**, **Contacts**, **Downloads**, **Links**, **Searches**, and **Saved Games** are not renamed. [LC9237]
- The Profile Management Service might exit unexpectedly with exception code 0xc0000374. [LC9355]
- Profile Management might not synchronize certain settings on the VDA that is running on Microsoft Windows 10, version 1709. [LC9503]
- When the **Active Write back** registry policy is enabled, the default policy of the registry exclusion including Software\Microsoft\AppV\Client\Integration and Software\Microsoft\AppV\Client\Publishing might not work. [LC9550]
- You have full permission to the default user profile. During the first logon, Profile Management might delete the excluded folders that are configured through a policy from the default user

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

profile. The issue occurs when the logon exclusion check is configured to delete the excluded files and folders. [LC9575]

- Profile Management configured with Active write back Registry processes all the registries and records all the changes into a temporary file regardless of whether the registries are being excluded or included. As a result, there is a high CPU usage. [LC9624]
- 7.15 LTSR CU2 sessions might launch as a black screen. The issue occurs with sessions running on XenApp and XenDesktop 7.15 LTSR CU2 and 7.17 VDAs when Profile Management is enabled. For more information and a workaround, see Knowledge Center article CTX235100. [LC9648]
- The Folder to Mirror policy in Profile Management might fail to work. [LC9691]
- With Profile Management enabled, blank icons might appear in the Start menu in the published desktops. The issue occurs during second or subsequent logons.

  **Note:** This fix is effective only on fresh installations. For upgrade scenarios, you must configure the **Folder to Mirror** policy manually either in the HDX Group Policy Editor or in the Active Directory Policy Editor. [LC9692]
- The AppData(Roaming) folder redirection might fail to work on Profile Management and this error message appears:

  **Access is Denied**.

  The issue occurs when the Profile Management does not link **AppData/Roaming** correctly to the shared folder and attempts to append /Application Data/Roaming erroneously. [LC9830]

### Provisioning Services

Provisioning Services 7.15 LTSR CU3 provides specific information about the updates in this release.

### Remote Broker Provider

- By default, the Amazon Web Services (AWS) ID of the Machine Creation Services (MCS) provisioned machine is non-persistent. This might cause the power management actions of the virtual machine to fail on the AWS.

  To configure the persistence of the AWS ID, the following options are available:

  - To enable the persistent of the AWS ID, set the Host connection's advance property's Connection option to **CreateNewInstanceOnReset=False**.
  - To disable the persistent of the AWS ID, set the Host connection's advance property's Connection option to **CreateNewInstanceOnReset=True** or delete the option.

  A ten second wait time is required when the option is changed to take effect. [LC9960]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Session Recording

### Administration

- A user from **domain B** logs on to the Session Recording server on domain A and attempts to update the Session Recording property. The machine GUID is not produced and an error occurs. The issue occurs because the user is in **domain B**, but the Session Recording server is in **domain A**. [LC9562]

### Agent

- The published instance of Microsoft Internet Explorer might be shown as **explorer.exe** on the Session Recording player list. The correct file name is **Iexplore.exe**. [LC9622]

## StoreFront

- When you zoom the browser to 125%, the custom logo might disappear. [LC9018]
- With **OverrideIcaClientname** enabled, attempts to establish a remote session from the Remote Desktop client might fail. The issue occurs when the license is not renewed. One of these error messages might appear:

  "The remote session could not be established from remote desktop client WR_XxXXxXXX because its license could not be renewed."

  OR

  "The remote session could not be established from remote desktop client WR_XxXXxXXX because its temporary license has expired."[LC9246]
- Attempts to enumerate applications might fail after updating the Delivery Controller certificate to TLS v1.2. [LC9337]
- When you select a configured Site during the setup of XenDesktop, a default store might be created in StoreFront that uses the default Authentication Service. If you remove this store, users of Citrix Receiver for Windows cannot add any other store and this error message appears:

  "A protocol error occurred while communicating with the Authentication Service."[LC9404]
- Attempts to log on to StoreFront might fail with the error **Cannot Complete your Request**. The issue occurs when the published applications have custom icons with minimum resolutions. [LC9521]
- When you use the StoreFront SDK to customize certain features and configure aggregation of the store, the logon might fail with the error **Cannot Complete your Request**. [LC9561]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The session prelaunch might not work after you configure **Resource Filtering by Keywords**. [LC9642]
- The ICA file might show VDA fully qualified domain name (FQDN) in the UDPICAPort entry even when using the NetScaler Gateway connection. [LC9760]

## Universal Print Server

### Client

- The Universal Print Server might cause the Print Spooler service to become unresponsive. [LC9341]

## User Profile Management VDA

- After upgrading the VDA from Version 7.13 to Version 7.15.2000, Citrix Director might not show the redirected folders. The issue occurs when the folder redirection is still working. [LC9968]
- The CPU usage of the brokeragent.exe process might be high. [LD0310]

## VDA for Desktop OS

### HDX

- The Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might exit unexpectedly and the video is not redirected on the HTML5 page. [LC8825]
- When a published application that is running on a VDA is using a generic path such as %ProgramFiles% or %ProgramFiles(x86)%, a new duplicated application window might open while reconnecting the session. [LC9741]

### Printing

- An access violation in **CpSvc!CDispatcher::UpdateCounters** can cause the Citrix Print Manager service (cpsvc.exe) to exit unexpectedly. [LC8804]
- The default printer might not be set for non .net applications. Microsoft Windows Server 2016 fails to update the value under the registry key **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device** when the default printer is the Citrix mapped printer. [LC8984]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The default printer might be incorrectly set in a session. The issue occurs when the default printer switches to any other random printer. [LC8999]
- When reconnecting to a session, the printers that are mapped into a session might load slowly while using legacy printer names. [LC9079]
- In certain Microsoft Excel files, when you navigate to **Excel** > **Print**, and then select any auto-create client printer using the Citrix Universal Printer EMF driver, the characters in the print preview image might appear smaller. [LC9700]
- The Citrix Print Manager service (cpsvc.exe) might exit unexpectedly. The issue occurs when **CpWSGetPrinterConnectionsFromPolicy** passes a null pointer to the comparison string **[MS]_wcsicmp**. [LC9796]

#### Session/Connection

- The web camera might become unresponsive inside a user session. The issue occurs when you perform any of these actions:
  - When using certain third-party applications to select a webcam in a user session, the webcam video frames become unresponsive.
  - When using the GraphEdit tool to start a virtual webcam and selecting the Use clock option in the menu.
  - When analyzing the Citrix Diagnostics Facility (CDF) traces, you see that only one video sample is delivered when the delivery pipeline between the VDA and Citrix Receiver for Windows is established. [LC8382]
- Disabling Citrix Hooks might fail to take effect when several executables are added to **ExcludedImageNames** under the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook**. [LC8614]
- Citrix Director might report Multi-Stream ICA as inactive when using the **UDP-based Data Transfer Protocol (UDT)**. The issue occurs when the HDX WMI provider is not updated to account for EDT or UDT sessions. [LC8960]
- Inconsistent mouse movement might occur in a multi-monitor environment using H configuration. You start a Microsoft Skype for Business session and start sharing the screen with the other user. The Citrix graphic driver receives an incorrect mouse location from the operating system.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

  Name: DisableAppendMouse

  Type: DWORD

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Data: 00000001

However, when you use the HDX session after setting the registry key, certain features that programmatically set the mouse pointer location might not work as expected. The features are:

- Mouse Snap To feature.
- The capability to synchronize mouse location between users with GotoMeeting screen sharing.
- The capability to synchronize mouse location between users with Skype for Business screen sharing. [LC8976]

- In certain scenarios, VDAs might reregister automatically with Event ID 1048. For example, when you start two applications with similar names –Lotus Notes and Lotus Notes Standard and close the second application that you have started, it removes the entry of the first application from the registry. When this information is sent to the Delivery Controller through a notification, then that notification is rejected and results in reregistration. [LC9223]
- The HDX RealTime Connector might exit unexpectedly. The video preview window closes or the video preview window shows a black box for a brief time and then closes. The issue occurs when there is no HDX RealTime Media Engine installed on the endpoint. [LC9282]
- The Citrix Audio Service might exit unexpectedly and then restart again. When you reconnect to the same session from the second end point (thin client), the new devices are not mapped correctly to the session. [LC9381]
- If you select the Clear or Delete clipboard function in a published application that is running on a VDA, the VDA clipboard clears but the text remains on the endpoint clipboard. [LC9434]
- When you disconnect a user session from the first end point and then reconnect to the same session from the second end point (thin client), the client side audio devices might be listed in an incorrect order within the VDA.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  Name: CleanMappingWhenDisconnect

  Type: DWORD

  Value: 1 [LC9440]

- The published application sessions might disconnect and user sessions might not log off correctly from the VDAs. When the issue occurs, you might not be able to reconnect and cannot disconnect from Citrix Studio. To remedy this situation, set the sessions to Hidden using the PowerShell command or restart the VDA. [LC9444]
- When using a VDA version 7.15.1000, an abnormal number of CPU instructions that originate from twi3.dll might pass through the Winlogon.exe process. [LC9450]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- With the Client drive redirection policy disabled, when you start an application for the second time from the user device, the application might take a long time to start. [LC9477]
- When you attempt to reconnect to an existing session that is active from a different endpoint, this error message appears:

  **Connection interrupted; receiver will attempt to reconnect for 5 minutes**.

  The issue occurs on Microsoft Windows 7 that has VDA 7.15 installed. [LC9485]
- A web based application is opened using Microsoft Internet Explorer or Mozilla Firefox browser. When you open certain tabs in the application, the entire desktop might become unresponsive. [LC9508]
- The **Server Total** instance performance counter might be missing from the **ICA Session** counters. [LC9537]
- File type association with Local App Access enabled might not work when the files are on the distributed file system (DFS) drive. [LC9538]
- The Event ID 31 **Start Listening for Connections** might not be passed to the **Event Viewer**. [LC9556]
- With **Unicode keyboard layout mapping** enabled, the published applications cannot be logged off. [LC9590]
- When you switch between the keyboard layouts, a pop-up window might appear. Set the following registry key to suppress the pop-up window:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  Name: HideNotificationWindow

  Type: DWORD

  Value: 1 [LC9592]
- A published application might close intermittently immediately after you start the application due to an unexpected failure. The issue occurs when the information about active processes is retrieved. [LC9661]
- After upgrading XenApp and XenDesktop from version 7.6 to version 7.15 LTSR Cumulative Update 1, certain services might stop or exit unexpectedly, or become unresponsive intermittently during logon. [LC9679]
- The VDAs might become unresponsive after installing XenApp and XenDesktop 7.15 LTSR Cumulative Update 2. [LC9701]
- After you disable certain ciphers through the Microsoft registry HKEY_LOCAL_MACHINE\SYSTEM\CurrentCont the TLS might not be enabled. [LC9743]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you access a Windows workstation through a Remote PC Access and disconnect from the Remote PC Access session, the workstation might not be locked. Therefore, the workstation is accessible to anyone who can physically reach the workstation. [LC9812]
- The **Kana** language input key on the Japanese Input Method Editor (IME) might be automatically enabled when you log on to a VDA. [LC9932]
- With this fix, the whitelist process mechanism is added to SCardHook. When the whitelist is defined in the registry, only processes that are included in the whitelist can use smart card redirection.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  Name: HookProcessWhitelist

  Type: REG_SZ

  Value: <process name> [LC9961]
- When you disconnect a user session from the first endpoint and then reconnect to the same session from a thin client, the client side audio devices might be listed in an incorrect order within the VDA.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  Name: CleanMappingWhenDisconnect

  Type: DWORD

  Value: 1 [LD0458]

**System Exceptions**

- Servers might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22 (FILE_SYSTEM). [LC7726]
- With Enlightened Data Transport (EDT) enabled, servers might experience a fatal exception on tdica.sys and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LC8794]
- Servers might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x000000D1(DRIVER_IRQL_NOT_LESS_OR_EQUAL). [LC8830]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen. [LC9695]
- The wfshell.exe process might exit unexpectedly when attempting to start a published application. The issue occurs when the bidirectional content redirection policy is enabled, while no URLs are provided. [LC9705]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Microsoft Windows Server 2008 R2 might experience a fatal exception and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. The issue occurs when XenApp and XenDesktop 7.15 LTSR CU2 is installed on the Microsoft Windows Server. [LC9849]
- Servers might experience a fatal exception on picavc.sys and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LD0006]

#### User Experience

- When you resize and attempt to move the published application from one monitor to another, a white border might appear around the application. [LC9570]
- Configure a VDA to use the **Unicode keyboard layout mapping** and establish an HDX session from Citrix Receiver with local IME enabled. When you type any character and then select some or all the output characters in a published application, the new characters are inserted before the selected characters instead of replacing them. [LC9591]
- When you change the resolution of the screen and reconnect to the published application from a VDA for Desktop OS, the application window might be truncated. [LC9947]
- In a multi-monitor environment, in certain scenarios the screen does not lock as expected. [LD0186]

#### User Interface

- When an application window in a seamless session becomes unresponsive, the taskbar icon of the application window might be removed and recreated. [LC9807]

### VDA for Server OS

#### HDX

- The Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) might exit unexpectedly and the video is not redirected on the HTML5 page. [LC8825]
- When a published application that is running on a VDA is using a generic path such as %ProgramFiles% or %ProgramFiles(x86)%, a new duplicated application window might open while reconnecting the session. [LC9741]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Printing

- An access violation in **CpSvc!CDispatcher::UpdateCounters** can cause the Citrix Print Manager service (cpsvc.exe) to exit unexpectedly. [LC8804]
- The default printer might not be set for non .net applications. Microsoft Windows Server 2016 fails to update the value under the registry key HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device when the default printer is the Citrix mapped printer. [LC8984]
- The default printer might be incorrectly set in a session. The issue occurs when the default printer switches to any other random printer. [LC8999]
- When reconnecting to a session, the printers that are mapped into a session might load slowly while using legacy printer names. [LC9079]
- In certain Microsoft Excel files, when you navigate to Excel > Print, and then select any auto-create client printer using the Citrix Universal Printer EMF driver, the characters in the print preview image might appear smaller. [LC9700]
- The Citrix Print Manager service (cpsvc.exe) might exit unexpectedly. The issue occurs when **CpWSGetPrinterConnectionsFromPolicy** passes a null pointer to the comparison string **[MS]_wcsicmp**. [LC9796]

### Session/Connection

- After upgrading the VDA from Version 7.12 to Version 7.13, the badge readers might stop working. [LC7667]
- The web camera might become unresponsive inside a user session. The issue occurs when you perform any of these actions:
  - When using certain third-party applications to select a webcam in a user session, the web-cam video frames become unresponsive.
  - When using the GraphEdit tool to start a virtual webcam and selecting the Use clock option in the menu.
  - When analyzing the Citrix Diagnostics Facility (CDF) traces, you see that only one video sample is delivered when the delivery pipeline between the VDA and Citrix Receiver for Windows is established. [LC8382]
- Disabling Citrix Hooks might fail to take effect when several executables are added to **ExcludedImageNames** under the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook**. [LC8614]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- A spurious XenApp session might be created on a VDA for Server OS when a Remote Desktop session disconnects and reconnects. [LC8706]
- Inconsistent mouse movement might occur in a multi-monitor environment using H configuration. You start a Microsoft Skype for Business session and start sharing the screen with the other user. The Citrix graphic driver receives an incorrect mouse location from the operating system.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

  Name: DisableAppendMouse

  Type: DWORD

  Value: 00000001

  However, when you use the HDX session after setting the registry key, certain features that programmatically set the mouse pointer location might not work as expected. The features are:

  - Mouse Snap To feature.
  - The capability to synchronize mouse location between users with GotoMeeting screen sharing.
  - The capability to synchronize mouse location between users with Skype for Business screen sharing. [LC8976]
- In certain scenarios, VDAs might reregister automatically with Event ID 1048. For example, when you start two applications with similar names –Lotus Notes and Lotus Notes Standard and close the second application that you have started, it removes the entry of the first application from the registry. When this information is sent to the Delivery Controller through a notification, then that notification is rejected and results in reregistration. [LC9223]
- The HDX RealTime Connector might exit unexpectedly. The video preview window closes or the video preview window shows a black box for a brief time and then closes. The issue occurs when there is no HDX RealTime Media Engine installed on the endpoint. [LC9282]
- You start Microsoft Excel 2007 in a published desktop, open a macro enabled .xslm file, and resize the file in windowed mode on the Desktop Viewer. The session might become unresponsive. The issue occurs when using the keyboard shortcut **Alt+Enter**. [LC9379]
- The Citrix Audio Service might exit unexpectedly and then restart again. When you reconnect to the same session from the second end point (thin client), the new devices are not mapped correctly to the session. [LC9381]
- If you select the Clear or Delete clipboard function in a published application that is running on a VDA, the VDA clipboard clears but the text remains on the endpoint clipboard. [LC9434]
- The published application sessions might disconnect and user sessions might not log off correctly from the VDAs. When the issue occurs, you might not be able to reconnect and cannot

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

disconnect from Citrix Studio. To remedy this situation, set the sessions to Hidden using the PowerShell command or restart the VDA. [LC9444]

- When using a VDA version 7.15.1000, an abnormal number of CPU instructions that originate from twi3.dll might pass through the Winlogon.exe process. [LC9450]
- With the Client drive redirection policy disabled, when you start an application for the second time from the user device, the application might take a long time to start. [LC9477]
- A web based application is opened using Microsoft Internet Explorer or Mozilla Firefox browser. When you open certain tabs in the application, the entire desktop might become unresponsive. [LC9508]
- The **Server Total** instance performance counter might be missing from the **ICA Session** counters. [LC9537]
- File type association with Local App Access enabled might not work when the files are on the distributed file system (DFS) drive. [LC9538]
- With **Unicode keyboard layout mapping** enabled, the published applications cannot be logged off. [LC9590]
- When you switch between the keyboard layouts, a pop-up window might appear. Set the following registry key to suppress the pop-up window:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  Name: HideNotificationWindow

  Type: DWORD

  Value: 1 [LC9592]

- A published application might close intermittently immediately after you start the application due to an unexpected failure. The issue occurs when the information about active processes is retrieved. [LC9661]
- In multiple domains or multi-forest environments, you might not be able to start the second application when the local groups are configured for limited visibility. [LC9665]
- After upgrading XenApp and XenDesktop from version 7.6 to version 7.15 LTSR Cumulative Update 1, certain services might stop or exit unexpectedly, or become unresponsive intermittently during logon. [LC9679]
- The VDAs might become unresponsive after installing XenApp and XenDesktop 7.15 LTSR Cumulative Update 2. [LC9701]
- After you disable certain ciphers through the Microsoft registry HKEY_LOCAL_MACHINE\SYSTEM\CurrentCont
  the TLS might not be enabled. [LC9743]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- You plug in a USB storage device during session logon and redirect with generic mode. The drive might still exist after you unplug the USB device. [LC9783]
- The **Kana** language input key on the Japanese Input Method Editor (IME) might be automatically enabled when you log on to a VDA. [LC9932]
- With this fix, the whitelist process mechanism is added to SCardHook. When the whitelist is defined in the registry, only processes that are included in the whitelist can use smart card redirection.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  Name: HideNotificationWindow

  Type: REG_SZ

  Value: <process name> [LC9961]
- The wfshell.exe process might exit unexpectedly. As a result, the published applications fail to start. [LD0102]
- After you upgrade the VDA to Version 7.15 Cumulative Update 2 or upgrade from Version 7.15 Cumulative Update 1 to Cumulative Update 2, the configured values **AnonymousUserIdleTime** and **MaxAnonymousUsers** under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Cont might be removed. [LD0378]

### Smart Cards

- You set the registry value DisableLogonUISuppression to 0 under the registry key HKEY_LOCAL_MACHINE\SO Virtual Desktop Agent. When you start a published application, the VDA might require you to type the smart card pin. The message **Please wait for the local session manager** appears in Citrix Receiver for Windows and eventually times out because the **DisableLogonUISuppression** value 0 suppresses the LogonUI PIN prompt. As a result, the PIN prompt never appears.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  Name: DisableLogonUISuppressionForSmartCardPublishedApps

  Type: DWORD

  Value: 1 [LC9059]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### System Exceptions

- Servers might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22 (FILE_SYSTEM). [LC7726]
- With Enlightened Data Transport (EDT) enabled, servers might experience a fatal exception on tdica.sys and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LC8794]
- Servers might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x000000D1(DRIVER_IRQL_NOT_LESS_OR_EQUAL). [LC8830]
- VDAs might experience a fatal exception on wdica.sys and display a blue screen. [LC9695]
- The wfshell.exe process might exit unexpectedly when attempting to start a published application. The issue occurs when the bidirectional content redirection policy is enabled, while no URLs are provided. [LC9705]
- When you start an application, the wfshell.exe process might exit unexpectedly. The issue occurs because of the faulting module, icaendpoint.dll. [LC9737]
- Microsoft Windows Server 2008 R2 might experience a fatal exception and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. The issue occurs when XenApp and XenDesktop 7.15 LTSR CU2 is installed on the Microsoft Windows Server. [LC9849]
- Servers might experience a fatal exception on picavc.sys and display a blue screen with bug check code **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LD0006]

### User Experience

- When you attempt to open a hyperlink from certain third-party applications (such as Aurion) that are running on a VDA for Server OS, an extra string %1 might be added at the beginning of the URL. [LC8952]
- When you resize and attempt to move the published application from one monitor to another, a white border might appear around the application. [LC9570]
- Configure a VDA to use the **Unicode keyboard layout mapping** and establish an HDX session from Citrix Receiver with local IME enabled. When you type any character and then select some or all the output characters in a published application, the new characters are inserted before the selected characters instead of replacing them. [LC9591]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### User Interface

- A legal notice appears at the start of the logon screen in a user session. With Local App Access enabled, when you click **Ok** on the logon screen to continue, the screen might show the legal notice for several seconds before proceeding with the logon. [LC9408]
- When an application window in a seamless session becomes unresponsive, the taskbar icon of the application window might be removed and recreated. [LC9807]
- When you attempt to start a published application, the Citrix Receiver for Windows screen might appear in the bottom right corner. [LC9817]

### Virtual Desktop Components - Other

- Attempts to unpublish and remove App-V packages from the VDA might fail. [LC9161]
- The cache overflow in Machine Creation Services Storage Optimization (MCSIO) can result in poor performance of XenServer virtual machines. [LC9351]
- The WMI queries that are running on the VDA might become unresponsive for an indefinite amount of time. [LC9510]
- Attempts to run multiple instances of the same App-V application in the same session might fail. The issue occurs when the process that is running is different than the defined process in the manifest file. [LC9652]
- When the Microsoft Edge browser is running on the VDA, multiple application entries might be seen under the **Activity Manager** in Citrix Director while you search for the user. [LC9673]

## Cumulative Update 2 (CU2)

June 21, 2021

Release date: April 17, 2018

### About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 2 (CU2) fixes more than 150 issues reported since the release of 7.15 LTSR CU1.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR CU1

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

### Downloads

Download 7.15 LTSR CU2

### New deployments

How do I deploy CU2 from scratch?

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

Peruse the XenApp and XenDesktop 7.15 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Securitysections 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 7.15 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU2. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU2. If Provisioning Services is not part of your deployment, you do not need to install or update it.

### XenApp and XenDesktop 7.15 LTSR CU2 baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.2000 | |
| VDA for Server OS | 7.15.2000 | |
| Delivery Controller | 7.15.2000 | |
| Citrix Studio | 7.15.2000 | |
| Citrix Director | 7.15.2000 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| Group Policy Management Experience | 3.1.2000 | |
| StoreFront | 3.12.2000 | |
| Provisioning Services | 7.15.3 | |
| Universal Print Server | 7.15.2000 | |
| Session Recording | 7.15.2000 | Platinum Edition only |
| Linux VDA | 7.15.2000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.2000 | |
| Federated Authentication Service | 7.15.2000 | |

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR CU2 Compatible Components and Platforms | Version |
|---|---|
| App Layering | 4.10.0 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.4 |
| License Server | 11.14.0.1 Build 23101 |
| Self-Service Password Reset | 1.1.10.0 |
| Workspace Environment Management | 4.6 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 7.15 LTSR CU2 Compatible Components and Platforms | Version |
|---|---|

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 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 Features |
|---|
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
|---|
| Personal vDisk: Excluded for Windows 10 machines; For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. For more information, see Install and upgrade analytics.

### 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 XenApp 7.15 LTSR CU2. 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 7.15 LTSR CU2 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU2 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 XenApp 7.15 LTSR CU2 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU2 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 22, 2022

### Citrix Director

- When you filter the machines by DNS name, Citrix Director might not display any machines or show duplicate entries of the machines. The issue occurs when the machine is first added to

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

the Monitor database but is concurrently added from two different Delivery Controllers. As a result, two machine entries are created. [LC4905]

- An exception might occur when you, as a custom administrator, cannot retrieve the Remote PC setting from the machine catalog. The issue occurs when you have permission to manage the machine catalog, but the scope does not contain the particular catalog. [LC8170]
- When you navigate to **Filters** > **Sessions** in Citrix Director and attempt to resize the browser, the entire table might be incorrectly aligned. [LC8624]
- The CSV file becomes unusable when you export data from Citrix Director. This issue might occur when you set any non-English versions of Microsoft Windows as the Director display language because commas might be used as both value and decimal separators. [LC8625]
- When you start Citrix Director, the following error message appears in the **Infrastructure** tab:

  "Cannot retrieve the data. Lost connection with web server. Check your network connection and try again."[LC8752]
- Citrix Director site names are truncated when there are multiple sites configured. [LC9258]

## Citrix Policy

- When you open a second instance of Group Policy Editor (gpedit.msc), the Citrix Policies node does not open and the following error message might appear:

  "Unhandled exception in managed code snap-in."[LC7600]
- When you apply Citrix policies through the Group Policy Management Console (GPMC), the policies might not appear under the GPMC policy settings. However, when editing the Group Policy Object (GPO), you can see the policies and the settings are enabled. [LC8282]
- Using Citrix Group Policy Management 3.1 to add the **Printer Assignments** setting to a **User Policy** in Active Directory might cause a window resizing issue. The window might begin to auto resize horizontally after you open it until it extends to the corner of the screen. As a result, editing the policy can be difficult because you cannot reach all of the columns. [LC8684]
- When files in the local policies cache folder (%ProgramData%/CitrixCseCache) are set to "Read-only,"the policy settings might not be applied successfully. [LC8750]
- Attempts to start App-V applications in single user admin mode from VDAs might fail. The issue occurs when the value of the **ApplicationStartDetails** registry key is empty or if the application details are missing from the registry key. [LC8798]
- Attempts to add machines to a Delivery Group by using the NETBIOS name for user associations might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC9393]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Citrix Studio

- When you attempt to add an application from the Linux VDA manually, the following error message might appear:

  "Value cannot be null while publishing the application."

  However, the application is added successfully when you click "OK"in the error message that appears. [LC7910]
- Attempts to remove applications from a Delivery Group might fail when the applications are located in the sub folder of the **Application** node in Citrix Studio. [LC8705]
- Attempts to add machines to a Delivery Group by using the NETBIOS name for user associations might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC9393]

### Controller

- Extraneous characters might appear at the end of "Service Display Name"and "Service description"of certain Citrix services installed on a Japanese operating system. [LC5208]
- When attempting to retrieve data for sessions from Citrix Director, null entries appear in the Monitor database. As a result, certain data is not displayed in Citrix Director and the following error message appears:

  "Failed to retrieve data"[LC6273]
- When you attempt to add an application from the Linux VDA manually, the following error message might appear:

  "Value cannot be null while publishing the application."

  However, the application is added successfully when you click "OK"in the error message that appears. [LC7910]
- After upgrading the Delivery Controller to Version 7.15 LTSR, the old basedisk that is created after a machine catalog update is not removed from the hypervisor's image. [LC8637]
- The Citrix Broker Service (Brokerservice.exe) might exit unexpectedly. The issue occurs because of the faulting module, LicPolEng.dll. [LC8638]
- When you provision the virtual machines (VMs) with the minimum required VMware privileges through Machine Creation Services, attempts to delete the VMs might fail. This failure might occur even with the minimum granted permissions for VMware. [LC8868]
- When you attempt to create a machine catalog that uses premium storage, the option to select the E-Series or L-Series type virtual machine size might not be available. [LC9052]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When an Active Directory user who is assigned with zone preference is deleted, attempts to import the broker configuration to the secondary broker might fail. The import operation can also fail after upgrading XenDesktop to the latest version. [LC9269]
- Attempts to add machines to a Delivery Group by using the NETBIOS name for user associations might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC9393]

### HDX MediaStream Flash Redirection

- With HDX MediaStream Flash Redirection enabled, when you reconnect a VDA session with Qumu.com, the Flash content might not be loaded in Microsoft Internet Explorer. [LC9193]

### Installer

- Attempts to change the installation directory path in Delivery Controller might not work for **XaXdProxy.msi**. [LC8691]

### Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU2 documentation provides specific information about the updates in this release.

### Profile Management

- After restarting the Profile Management Service, Citrix Director might not show the user logon and personalization information. [LC6942]

### Provisioning Services

Provisioning Services 7.15 LTSR CU2 documentation provides specific information about the updates in this release.

### StoreFront

- With the "Auto launch desktop"setting enabled, the "Multiple launch prevention"option might not work. As a result, subsequent requests to launch the same instance of the desktop fail. [LC7430]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- After upgrading StoreFront 2.6 installed on a non-default drive, users' application subscription data might not be retained. [LC8046]
- After you restart the StoreFront MMC console, the value of the **Show desktop viewer** check box might be incorrectly displayed. [LC8520]
- If you execute a **Set-STFWebReceiverSiteStyle** command with a PNG file (transparency is supported) to customize StoreFront, the PNG file is converted to a JPEG file. The JPEG file format might lose transparency support. [LC8677]
- If you execute a **Set-STFWebReceiverApplicationShortcuts** command to set the trusted URLs for application shortcuts in Citrix Receiver for Web sites, a forward slash ("/") might be added to the end of the URL. [LC8761]
- When you use the **Set-STFWebReceiverSiteStyle** command to customize StoreFront, the style.css might be changed incorrectly in the Custom folder. As a result, the StoreFront console is not able to read the customization. [LC8776]
- Authentication failure might occur on the StoreFront servers. The issue occurs because of TCP dynamic port exhaustion. [LC8795]
- Attempts to change the StoreFront logo using the **Set-STFWebReceiverSiteStyle** command might fail. [LC8994]
- Attempts to upgrade StoreFront might fail when read only files are present within the custom file directory of any instance of Citrix Receiver for Web sites. [LC9252]

## VDA for Desktop OS

### HDX 3D Pro

- With HDX 3D Pro and custom resolution enabled on a VDA that is running on Microsoft Windows 10, a gray screen might appear intermittently when you log on. [LC8417]

### HDX MediaStream Flash Redirection

- With HDX MediaStream Flash Redirection enabled, when you reconnect a VDA session with Qumu.com, the Flash content might not be loaded in Microsoft Internet Explorer. [LC9193]

### HDX MediaStream Windows Media Redirection

- With HDX MediaStream Windows media Redirection disabled, attempts to open certain video file formats through Windows Media Player can cause the video that is playing to be vertically flipped. [LC9194]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### HDX RealTime

- RealTime Connector is installed. When using applications that use a redirected webcam, such as Skype for Business, the webcam that is installed on a VDA for Desktop OS might be redirected and detected during an initial session launch. However, when you reconnect to the user session, the webcam is no longer detected. The issue occurs when RealTime Media Engine is not installed on the user device. [LC8793]

### Keyboard

- When you start an application on an Android device and you are in the text field, the keyboard might not appear automatically. Also, you must always touch the keyboard button for opening or closing. [LC8936]

### Printing

- Attempts to print on both sides of the paper with the printer settings using Microsoft Word might fail. [LC7501]
- Attempts to print a document from a published instance of Microsoft Internet Explorer might fail. [LC8093]
- With French as the display language installed on a VDA, attempts to print a document might fail. [LC8209]
- A printer that is redirected from a user device might not be redirected after you reconnect to the session. [LC8762]
- Attempts to restart the Citrix Print Manager service (cpsvc.exe) might fail when you stop the Print Spooler service while launching the first session. [LC9192]

### Session/Connection

- When reading a file from a mapped client drive, the old, cached file length might be returned if the file length was changed outside of the client session. Additionally, null characters are inserted for any deleted characters.

  To enable the fix, set the following registry value to "0":

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters;
  Name: CacheTimeout;
  Type: REG_DWORD;

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Value: Default value is 60 seconds. If CacheTimeOut is set to "0," the file length is reloaded immediately and if not it is loaded after the defined timeout. [LC6314]

- A session running on a VDA for Desktop OS might become unresponsive when using legacy graphics mode. When the issue occurs, you might not be able to update anything on the Desktop Viewer, but the Desktop Viewer is not in an unresponsive state. Also, after 30-60 minutes, the previously unresponsive session recovers. [LC7777]
- When you launch an application with session lingering enabled, the session might log off after the application appears. [LC8245]
- When you attempt to start a VDA for Desktop OS, the desktop might start and then disappear after a few seconds. [LC8373]
- Windows Explorer might close unexpectedly in one of the following cases:
  - When selecting a large number of files whose names contain more than 260 characters and then selecting the "Send to > Fax recipient" option.
  - When attempting to open third-party applications.
  - When attempting to combine files by using Nitro PDF. [LC8423]
- Changes you make to Advanced System Settings under Visual Effects apply to the current VDA for Desktop OS session but might not be retained for subsequent sessions. To make such changes persistent, set the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Type: DWORD;
  Value: 1 [LC8049, LC8658]
- After you disconnect a session, monitor1 might incorrectly display as the primary monitor on the next local log on. This behavior might occur when you log on locally to a Remote PC Access VDA in a multi monitor environment and configure monitor2 as the primary monitor, connect through a user device, and then disconnect a session using the Desktop Viewer. [LC8675]

  To enable the fix, set the following registry key on the VDA for Desktop OS:

  Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: UseSDCForLocalModes

  Type: REG_DWORD

  Data: 1
- When you attempt to start a published application that is running on Microsoft Windows Server 2012 or 2016, you might be locked out. [LC8681]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you start an application in multi-monitor environment, a logon banner might appear that encompasses both monitors. When using a single monitor, the logon banner window is shown in full screen. [LC8741]
- With Local App Access enabled, when you attempt to open applications on the published desktops that are running on Microsoft Windows 10, the applications cannot be minimized. [LC8813]
- The DLP software might fail to scan files with the UNC link. [LC8893]
- After you start a published application, the Num Lock key does not work. The issue occurs when the LED of the Num Lock key is visible on the user device but numbers are not working inside a user session. The issue occurs in certain scenarios when the client requested LED update comes earlier than the time the newly created remote desktop initializes its LED state. When this happens, the WinsStation might not update its LED state and the LED state is out of sync between endpoint and VDA. [LC8921]
- Attempts to start applications and desktops might fail. The issue occurs when the VDA for Server OS becomes unresponsive.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard;
  Name: EnableSCardHookVcResponseTimeout;
  Type: DWORD;
  Value: 1 [LC8969]
- Attempts to open VM hosted applications might fail. [LC9001]
- Attempts to reconnect to a session might fail. [LC9040]
- When you use the WFAPI SDK **WFQuerySessionInformation** command in a session to retrieve the installed VDA version information, the command might not work. [LC9041]
- After upgrading XenApp and XenDesktop from Version 7.14 through 7.15, attempts to switch between the tabs of a published application might cause the application to become unresponsive. Also, if you resize the seamless window to a smaller size and then expand the window, it takes some time to paint all the elements within the window. [LC9078]
- A published application might close intermittently immediately after you start the application. [LC9167]
- When reconnecting to a seamless application within a Millennium suite with a different screen resolution than the initial connection, the application might resize incorrectly. As a result, the window might be truncated. [LC9214]
- Attempts to connect to a Windows 10 Version 1709 published desktop through a user device might result in a gray screen. When you attempt to connect through the hypervisor's console

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

to a published desktop, a black screen with a spinning wheel appears. However, connecting through an RDP to a published desktop works successfully. [LC9215]

- Attempts to start applications from Citrix Receiver for Mac might fail. The issue occurs when the client license (LicenseRequestClientLicense) cannot be fetched. [LC9286]
- With HDX 3D Pro enabled, attempts to start a XenDesktop might fail intermittently. The issue occurs when there is a GPU failure. [LC9343]
- The session display from a user session to an unmanaged Remote Desktop session might be incorrect when smooth roaming. [LC9471]

#### Smart Cards

- When using a smart card, certain third-party applications might become unresponsive instead of showing the PIN prompt. [LC8805]

#### System Exceptions

- Servers might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x22. [LC6177]
- Servers might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA). [LC6985]
- Servers might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x22. [LC7574]
- Servers might experience a fatal exception on vdtw30.dll and display a blue screen with stop code SYSTEM_SERVICE_EXCEPTION (3b). [LC8087]
- Servers might experience a fatal exception, displaying a blue screen, on pdcrypt2.sys with bugcheck code 0x3B. The issue occurs when launching a VDA. [LC8328]
- With HDX 3D Pro and GPU hardware encoding enabled and when using the NVIDIA GPUs, the Citrix software graphics process (Ctxgfx.exe) might exit unexpectedly. The issue occurs when using high resolution screens. LC8435]
- The VDA for Server OS might experience a fatal exception on picadm.sys and display a blue screen. [LC8708]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bugcheck code 0x22. [LC8749]
- When you log on for the first time after restarting the VDA, an unexpected access violation exception might occur. The Citrix software graphics process (Ctxgfx.exe) exits unexpectedly. As a result, the quality of the image and text appearing in the VDA might be blurry. [LC9005]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Windows Explorer might close unexpectedly in one of the following cases:
  - When selecting a large number of files whose names contain more than 260 characters and then selecting the **Send to** > **Fax recipient** option.
  - When attempting to open third-party applications.
  - When attempting to combine files by using Nitro PDF. [LC9076]

#### User Experience

- When you copy content from any application that is running on a client and paste it into an application in a user session, that content might not be pasted. Also, the **Paste** button might be disabled. [LC8516]
- The screen might not refresh with the logon prompt after you attempt to log on to a session that was locked previously. [LC8774]

#### User Interface

- Desktop wallpaper appears even after setting the "Desktop wallpaper"policy to "Prohibited." [LC8398]

#### Miscellaneous

- This fix addresses minor performance and quality improvements for Enlightened Data Transport (EDT). [LC9278]

### VDA for Server OS

#### HDX MediaStream Windows Media Redirection

- With HDX MediaStream Windows media Redirection disabled, attempts to open certain video file formats through Windows Media Player can cause the video that is playing to be vertically flipped. [LC9194]

#### HDX RealTime

- RealTime Connector is installed. When using applications that use a redirected webcam, such as Skype for Business, the webcam that is installed on a VDA for Desktop OS might be redirected

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

and detected during an initial session launch. However, when you reconnect to the user session, the webcam is no longer detected. The issue occurs when RealTime Media Engine is not installed on the user device. [LC8793]

### Keyboard

- When you start an application on an Android device and you are in the text field, the keyboard might not appear automatically. Also, you must always touch the keyboard button for opening or closing. [LC8936]

### Printing

- Attempts to print on both sides of the paper with the printer settings using Microsoft Word might fail. [LC7501]
- Attempts to print a document from a published instance of Microsoft Internet Explorer might fail. [LC8093]
- With French as the display language installed on a VDA, attempts to print a document might fail. [LC8209]
- Attempts to restart the Citrix Print Manager service (cpsvc.exe) might fail when you stop the Print Spooler service while launching the first session. [LC9192]

### Server/Site Administration

- The Citrix Stack Control Service (SCService64.exe) might exit unexpectedly when the VDA checks for the group membership of the user when there are two or more groups with the same name in multiple domains. The issue occurs when the string "DnsDomainName"is empty in the DS_DOMAIN_TRUSTSW structure. [LC8484]

### Session/Connection

- The following warning message might appear in the system event log when launching XenApp 7.6 Long Term Service Release Cumulative Update 2 VDA for Server OS or the previous versions:

  "An attempt to connect to the SemsService has failed with error code 0x2."[LC6311]
- When reading a file from a mapped client drive, the old, cached file length might be returned if the file length was changed outside of the client session. Additionally, null characters are inserted for any deleted characters.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To enable the fix, set the following registry value to "0":

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters;
Name: CacheTimeout;
Type: REG_DWORD;
Value: Default value is 60 seconds. If CacheTimeOut is set to "0,"the file length is reloaded immediately and if not it is loaded after the defined timeout. [LC6314]

- After undocking a laptop, session sharing might fail. The issue occurs when the VDA reregisters with the Delivery Controller while an-out-of-order notification is triggered during auto client reconnect. [LC7450]
- A session running on a VDA for Desktop OS might become unresponsive when using legacy graphics mode. When the issue occurs, you might not be able to update anything on the Desktop Viewer, but the Desktop Viewer is not in an unresponsive state. Also, after 30-60 minutes, the previously unresponsive session recovers. [LC7777]
- After closing a published application with an App-V client installed on the VDA and the configuration settings "EnablePubilishingRefreshUI"and "Session Lingering"enabled in the session, a black window might remain open on an iOS device. The issue occurs when the session is in active lingering state. [LC8080]
- When you launch an application with session lingering enabled, the session might log off after the application appears. [LC8245]
- Servers might become unresponsive on RPM.dll and the following error message appears:

  "Event ID 1009, picadm: Timeout waiting for response message from client"[LC8339]
- Windows Explorer might close unexpectedly in one of the following cases:
  - When selecting a large number of files whose names contain more than 260 characters and then selecting the "Send to > Fax recipient"option.
  - When attempting to open third-party applications.
  - When attempting to combine files by using Nitro PDF. [LC8423]
- Citrix Director might report multiple connection failures. The issue occurs when the expansion of groups assigned to control the limited visibility of an application is used for each user. This expansion process takes a long time to complete and can be observed in large networks having many groups that span multiple domains. [LC8652]
- The COM ports might fail to map on Version 7.15 of the VDAs. [LC8656]
- When you attempt to start a published application that is running on Microsoft Windows Server 2012 or 2016, you might be locked out. [LC8681]
- When you start an application in multi-monitor environment, a logon banner might appear that encompasses both monitors. When using a single monitor, the logon banner window is shown

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

in full screen. [LC8741]

- With Local App Access enabled, when you attempt to open applications on the published desktops that are running on Microsoft Windows 10, the applications cannot be minimized. [LC8813]
- When you connect a user device to a VDA, the desktop might not be displayed. Instead, a gray screen appears on the desktop. [LC8821]
- The DLP software might fail to scan files with the UNC link. [LC8893]
- After you start a published application, the Num Lock key does not work. The issue occurs when the LED of the Num Lock key is visible on the user device but numbers are not working inside a user session. The issue occurs in certain scenarios when the client requested LED update comes earlier than the time the newly created remote desktop initializes its LED state. When this happens, the WinsStation might not update its LED state and the LED state is out of sync between endpoint and VDA. [LC8921]
- Attempts to start applications and desktops might fail. The issue occurs when the VDA for Server OS becomes unresponsive.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard;
  Name: EnableSCardHookVcResponseTimeout;
  Type: DWORD;
  Value: 1 [LC8969]
- Attempts to open VM hosted applications might fail. [LC9001]
- When you use the WFAPI SDK **WFQuerySessionInformation** command in a session to retrieve the installed VDA version information, the command might not work. [LC9041]
- After upgrading XenApp and XenDesktop from Version 7.14 through 7.15, attempts to switch between the tabs of a published application might cause the application to become unresponsive. Also, if you resize the seamless window to a smaller size and then expand the window, it takes some time to paint all the elements within the window. [LC9078]
- A published application might close intermittently immediately after you start the application. [LC9167]
- When reconnecting to a seamless application within a Millennium suite with a different screen resolution than the initial connection, the application might resize incorrectly. As a result, the window might be truncated. [LC9214]
- Attempts to start applications from Citrix Receiver for Mac might fail. The issue occurs when the client license (LicenseRequestClientLicense) cannot be fetched. [LC9286]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Smart Cards

- When using a smart card, certain third-party applications might become unresponsive instead of showing the PIN prompt. [LC8805]

### System Exceptions

- Servers might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x22. [LC6177]
- Servers might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA). [LC6985]
- Servers might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x22. [LC7574]
- The Service Host (svchost.exe) process might experience an access violation and exit unexpectedly. The issue occurs because of the faulting module, icaendpoint.dll. [LC7694]
- Servers might experience a fatal exception on vdtw30.dll and display a blue screen with stop code SYSTEM_SERVICE_EXCEPTION (3b). [LC8087]
- Servers might experience a fatal exception, displaying a blue screen, on pdcrypt2.sys with bugcheck code 0x3B. The issue occurs when launching a VDA. [LC8328]
- With HDX 3D Pro and GPU hardware encoding enabled and when using the NVIDIA GPUs, the Citrix software graphics process (Ctxgfx.exe) might exit unexpectedly. The issue occurs when using high resolution screens. [LC8435]
- Servers might experience a fatal exception, displaying a blue screen, on icardd.dll with bugcheck code 0x0000003B. [LC8492]
- The VDA for Server OS might experience a fatal exception on picadm.sys and display a blue screen. [LC8708]
- Servers might experience a fatal exception, displaying a blue screen, on icardd.dll with bugcheck code 0x0000003B. [LC8732]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bugcheck code 0x22. [LC8749]
- When you log on for the first time after restarting the VDA, an unexpected access violation exception might occur. The Citrix software graphics process (Ctxgfx.exe) exits unexpectedly. As a result, the quality of the image and text appearing in the VDA might be blurry. [LC9005]
- Windows Explorer might close unexpectedly in one of the following cases:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When selecting a large number of files whose names contain more than 260 characters and then selecting the **Send to** > **Fax recipient** option.
- When attempting to open third-party applications.
- When attempting to combine files by using Nitro PDF. [LC9076]

#### User Experience

- When you copy content from any application that is running on a client and paste it into an application in a user session, that content might not be pasted. Also, the **Paste** button might be disabled. [LC8516]
- On the VDA for Server OS, the mouse cursor might disappear from the session. This issue occurs when the cursor changes to the **Text Select** cursor and the background color is the same as the color of the **Text Select** cursor. The default background color in Microsoft Windows for editable areas is white, while the default **Text Select** cursor color is also white. As a result, the cursor might no longer be visible. [LC8807]
- Microsoft Windows might continue to retain the editable password field during session logon even after submitting the correct credentials. [LC9407]

#### User Interface

- Desktop wallpaper appears even after setting the "Desktop wallpaper"policy to "Prohibited." [LC8398]

#### Miscellaneous

- Certain third-party applications that are used to check the session display of a Linux VDA might not display all pixels. [LC8419]
- RunOnce registry keys might not be implemented correctly. [LC9260]
- This fix addresses minor performance and quality improvements for Enlightened Data Transport (EDT). [LC9278]

### Virtual Desktop Components - Other

- The LastPasswordset attribute on Active Directory might not update correctly when using the VDA version 7.15 LTSR. [lC8387]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- After the Delivery Controller is upgraded to Version 7.15, active sessions for anonymous users show that a logon is in progress. This situation results in an incorrect load index for the VDA. [LC8771]
- Started applications might not appear in the Activity Manager in Citrix Director in a double hop scenario. [LC8985]
- Registration status between the Delivery Controller and the VDA might be inconsistent, causing re-registration when the VDA launches. [LC9216]

### Miscellaneous

When the Citrix Telemetry Service is disabled or stopped, and you use a metainstaller to upgrade XenApp and XenDesktop 7.15 LTSR to Cumulative Update 1 (CU1), the following warning message might appear:

"We cannot start the Citrix service that enables you to enroll in Call Home. See CTX218094 for guidance."[LCM-3642]

## Cumulative Update 1 (CU1)

June 21, 2021

Release date: December 04, 2017

### About this release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 1 (CU1) fixes more than 80 issues reported since the initial release of the 7.15 LTSR.

7.15 LTSR (general information)

Issues fixed since XenApp and XenDesktop 7.15 LTSR (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Before you upgrade from 7.6 LTSR CU5

The main benefit to upgrading from 7.6 LTSR CU5 to 7.15 LTSR CU1 is that the base 7.15 LTSR contains many more features than the base 7.6 LTSR. However, if you are considering this upgrade, be advised that a small subset of fixes that are included in 7.6 LTSR CU5 is not present in 7.15 LTSR CU1. That's because 7.15 LTSR CU1 was released before 7.6 LTSR CU5. For a list of fixes that are applicable to 7.15 but not included in 7.15 LTSR CU1, see List of fixes present in 7.6 LTSR CU5 but not in 7.15 LTSR CU1. If your deployment depends on specific fixes included in 7.6 LTSR CU5, Citrix recommends that you review this list before you upgrade.

### New deployments

How do I deploy CU1 from scratch?

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

Peruse the XenApp and XenDesktop 7.15 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Securitysections 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 13 baseline components of the 7.15 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU1. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU1. If Provisioning Services is not part of your deployment, you do not need to install or update it.

### XenApp and XenDesktop 7.15 LTSR CU1 baseline components

| 7.15 LTSR CU1 Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15.1000 | |
| VDA for Server OS | 7.15.1000 | |
| Delivery Controller | 7.15.1000 | |
| Citrix Studio | 7.15.1000 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 7.15 LTSR CU1 Baseline Component | Version | Notes |
|---|---|---|
| Citrix Director | 7.15.1000 | |
| Group Policy Management Experience | 3.1.1000 | |
| StoreFront | 3.12.1000 | |
| Provisioning Services | 7.15.1 | |
| Universal Print Server | 7.15.1000 | |
| Session Recording | 7.15.1000 | Platinum Edition only |
| Linux VDA | 7.15.1000 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15.1000 | |
| Federated Authentication Service | 7.15.1000 | |

### XenApp and XenDesktop 7.15 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 7.15 LTSR environments.

| 7.15 LTSR Compatible Components and Platforms | Version |
|---|---|
| AppDNA | 7.16 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.13 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.14 |
| HDX RealTime Optimization Pack | 2.2.100 |
| License Server | 11.14.0.1 Build 22103 |
| Workspace Environment Management | 4.4 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 7.15 LTSR Compatible Components and Platforms | Version |
|---|---|
| App Layering | 4.6 |
| Self-Service Password Reset | 1.1 |

### Compatible versions of Citrix Workspace app

All currently supported versions of Citrix Workspace app are compatible with the XenApp and Xendesktop 7.15 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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components will be available through regular current releases.

| Excluded Features |
|---|
| Framehawk |
| StoreFront Citrix Online Integration |

| Excluded Components |
|---|
| Personal vDisk: Excluded for Windows 10 machines; •For Windows 7 machines, limited LTSR support until January 14, 2020 (CU requirements apply) |
| AppDisks |

| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. For more information, see Install and upgrade analytics.

### 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 XenApp 7.15 LTSR CU1. 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 7.15 LTSR CU1 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 CU1 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 XenApp 7.15 LTSR CU1 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.15 CU1 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 7.6 LTSR CU5 but not in 7.15 LTSR CU1

If you're considering an upgrade from 7.6 LTSR CU5 to 7.15 LTSR CU1, be advised that a small subset of fixes that are included in 7.6 LTSR CU5 is not present in 7.15 LTSR CU1. If your deployment depends on specific fixes included in 7.6 LTSR CU5, Citrix recommends that you review this list before you upgrade.

- LC6311
- LC6985
- LC7430
- LC7450

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- LC7574
- LC7600
- LC7777
- LC7911
- LC8046
- LC8080
- LC8130
- LC8170
- LC8281
- LC8339
- LC8492
- LC8732
- LC8750
- LC8774

## Fixed issues

April 22, 2022

XenApp and XenDesktop 7.15 LTSR Cumulative Update 1 (CU1) fixes more than 80 issues reported since the initial release of the 7.15 LTSR:

### Citrix Director

- When you open the Director Console and search for users for the first time, the loading bar does not appear. In subsequent searches, the bar appears as expected. [LC8190]

### Citrix Policy

- Attempts to add a new USB redirection rule to a user policy in Active Directory might fail. The issue occurs when the scroll bar is not available. [LC8112]
- When attempting to manage the "Printer Assignments"policy, the following issues might occur:
  - The exception "InvalidCastException"occurs when adding or editing the printer assignments policy.
  - The exception "InvalidOperationException"occurs when adding a new session printer.
  - Attempts to remove a session printer from the printer assignment policy fails. This issue occurs when the "Remove"option is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - When you stop typing in the search box of the "Printer Assignment"policy, the search action does not start.
  - The session printer override setting checkboxes (PrintQuality, PaperSize, Scale, and TrueTypeOption) are always selected even though you have cleared them in previously. [LC8146]

### Citrix Studio

- When you attempt to add user-assigned machines to a Delivery Group, unassigned machines might be displayed on the "Machine allocation"page. [LC6755]
- Attempts to access machine catalogs in Citrix Studio can cause Citrix Studio to exit unexpectedly and the following exception occurs:

  "Error Id: XDDS:ABB14FD9"[LC7961]
- The text for the "Use storage local to the hypervisor"option in the "Add Connection and Resources"wizard that is running on a non-English version of the Windows operating system might be truncated. [LC8041]
- After upgrading Citrix Studio to Version 7.14.1, the "Used By"column (referring to the Delivery Group that the application is used by) for existing App-V packages might appear blank. [LC8075]
- When you click the Delivery Group hyperlink in Citrix Studio, you might not be redirected to the selected Delivery Group node. [LC8095]
- When attempting to manage the "Printer Assignments"policy, the following issues might occur:
  - The exception "InvalidCastException"occurs when adding or editing the printer assignments policy.
  - The exception "InvalidOperationException"occurs when adding a new session printer.
  - Attempts to remove a session printer from the printer assignment policy fails. This issue occurs when the "Remove"option is disabled.
  - When you stop typing in the search box of the "Printer Assignment"policy, the search action does not start.
  - The session printer override setting checkboxes (PrintQuality, PaperSize, Scale, and TrueTypeOption) are always selected even though you have cleared them in previously. [LC8146]
- After upgrading the Delivery Controller to Version 7.15, attempts to launch Citrix Studio on the Delivery Controller might fail and the following error message appears:

  "MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand" [LC8396]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you select the Delivery Groups node in Citrix Studio and then select the Application tab, the hyperlink in the Application tab might not work. [LC8555]

### Controller

- If a Delivery Group contains one more VDAs in maintenance mode, you might not be able to select the Delivery Group to launch published applications. [LC6943]
- After updating a machine catalog that was created using Machine Creation Services (MCS), virtual machines hosted on vSAN 6 or later might fail to start. The following error message appears in the VMware console:

  "A general system error occurred: PBM error occurred during PreProcessReconfigureSpec: pbm.fault.PBMFault; Error when trying to run pre-provision validation; Invalid entity."[LC7860]
- Attempts to access machine catalogs in Citrix Studio can cause Citrix Studio to exit unexpectedly and the following exception occurs:

  "Error Id: XDDS:ABB14FD9"[LC7961]
- Citrix Director might display an incorrect number of disconnected sessions at the top of every hour. [LC8006]
- The "AllowRestart"policy for sessions on Server OS does not allow you to log off from the disconnected sessions. When you restart a disconnected session, the session is reconnected to the previous session instead of starting a new one. [LC8090]
- When attempting to manage the "Printer Assignments"policy, the following issues might occur:
  - The exception "InvalidCastException"occurs when adding or editing the printer assignments policy.
  - The exception "InvalidOperationException"occurs when adding a new session printer.
  - Attempts to remove a session printer from the printer assignment policy fails. This issue occurs when the "Remove"option is disabled.
  - When you stop typing in the search box of the "Printer Assignment"policy, the search action does not start.
  - The session printer override setting checkboxes (PrintQuality, PaperSize, Scale, and TrueTypeOption) are always selected even though you have cleared them in previously. [LC8146]
- The Monitoring Service might fail to insert new session data into the monitoring database. [LC8191]
- The Logon Duration by User Session panel under **Director** > **Trends** > **Logon Performance** might display only partial logon records. [LC8265]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- After upgrading the Delivery Controller to Version 7.15, attempts to launch Citrix Studio on the Delivery Controller might fail and the following error message appears:

  "MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand" [LC8396]

- In a large XenApp and XenDesktop environment, the stored procedure for Monitor database grooming does not work correctly if the size of the Monitor database is large. [LC8770]

### HDX MediaStream Flash Redirection

- With HDX MediaStream Flash Redirection enabled, Flash videos might fail to play on MSN.com and News.com. [LC6823]

### Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU1 documentation provides specific information about the updates in this release.

### Profile Management

- Profile Management can cause a black screen to appear when you attempt to launch a Microsoft Windows 10 session. With this fix, you must configure the policy "Directories to synchronize"and add the folder "*AppData\Local\Microsoft\Windows\Caches*."[LC7596]
- When you log off from a VDA running on Microsoft Windows 10, the ntuser.dat file might be in use and not be copied to the Profile Management store. As a result, the changes made to the "HKEY_CURRENT_USER"registry key are lost. [LC8068]
- With the "Delete locally cached profiles on logoff"policy enabled and "Delay before deleting cached profiles"set to two minutes, attempting to log off and log on to a session within two minutes using the same user account might create a new local profile. [LC8388]

### Provisioning Services

Provisioning Services 7.15 LTSR CU1 documentation provides specific information about the updates in this release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## StoreFront

- With "TWIMode"set to "Off"for some applications, all applications are launched in windowed mode when using Citrix Receiver for Chrome. [LC7558]
- When there are two or more stores in StoreFront, clicking "Configure Remote Access Settings" on the first or second store might duplicate that store name on the most recently added store. [LC8089]
- When you configure stores with shared authentication in StoreFront, attempts to link a new NetScaler Gateway appliance to a store can cause the existing NetScaler Gateway appliances that are already linked to be removed. When you attempt to log on to the stores, the following error message appears:

  "Your logon has expired. Please log on again to continue."

  Additionally, the StoreFront console shows duplicate store names. [LC8219]
- When importing a store with HTML5 configuration using "Import-STFConfiguration"PowerShell command, import might complete successfully. However, attempts to launch an application using Citrix Receiver for HTML5 fail. [LC8290]
- The StoreFront server might show null entries for Receiver for Web sites in the console. The issue occurs when the store name begins with the text "discovery"in the URL. [LC8320]
- With the W3C logging service enabled, attempts to make changes to the StoreFront configuration might fail and the following error message appears:

  "An error occurred while saving your changes."[LC8370]
- With socket pooling enabled and the Site database connectivity inconsistent, the sockets in StoreFront might get exhausted when you continuously log on and log off. [LC8514]

## VDA for Desktop OS

### HDX MediaStream Flash Redirection

- With HDX MediaStream Flash Redirection enabled, Flash videos might fail to play on MSN.com and News.com. [LC6823]
- Attempts to save Microsoft Office files such as Microsoft Excel spreadsheets that are running in a session with HDX seamless apps enabled can cause the files to exit unexpectedly. [LC8572]

### HDX Plug and Play

- USB devices that report the same serial number for more than one device such as Syn-Tech ProKee V2 might not get redirected to a VDA session. The following CDF trace appears:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

"Failed to assign the instance ID, error 0xc000000d."[LC8264]

### Printing

- Attempts to launch a published application might fail when the application is waiting for a mutex object in Citrix Print Manager service (cpsvc.exe). [LC6829]
- The Citrix Print Manager service (cpsvc.exe) might exit intermittently. [LC7535]
- When you roam a session between clients, session printers cannot be deleted. For example, when you configure the policy "Printer assignments"–printer A for client A and printer B for client B, printer A might not be deleted when you roam from client A to client B. [LC8077]

### Server/Site Administration

- On VDA 7.12 or later versions, when you attempt to suppress the display of the language bar in a seamless session by setting the seamless flag to "0x00040000"(disables the language bar agent) under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI, the language is no longer hidden. [LC8349]

### Session/Connection

- With local app access enabled, using the interactive logon disclaimer policy might result in a black or gray screen lasting for 45 seconds. [LC6518]
- Attempts to reconnect to an application might fail. The issue occurs when any of the disconnected applications became unresponsive when the session disconnected initially. [LC6550]
- When you lock a dual-monitor session using HDX 3D Pro, only the primary monitor is locked. [LC7767]
- When you establish a Skype for Business video call, a blue window border might appear after intersecting with the window of a third party application. [LC7773]
- With local app access enabled, using the interactive logon disclaimer policy might result in a black or gray screen. [LC7798]
- Certain published applications might not cover the entire screen when maximized. [LC7854]
- When performing an insert operation between two Microsoft Excel 2010 worksheets running on a Version 7.9 VDA, the Excel window might become unresponsive. [LC7912]
- In certain scenarios, seamless applications might not appear in seamless mode or certain features might not work. [LC8030]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- With HDX 3D Pro enabled on a VDA and the policy "Message text for users attempting to log on" enabled when the logon screen appears, attempts to launch a published desktop might fail and a gray screen appears.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig;
  Name: HKLM_DisableMontereyFBCOnInit;
  Value: DWORD;
  Type: 1 to enable [LC8082]

- With local app access enabled, using the interactive logon disclaimer policy can cause the desktop viewer to show a gray screen when connecting to a VDA. [LC8136]
- When using applications that use a redirected webcam, such as Skype for Business or a VLC media player, the webcam might be redirected and detected during an initial session launch. However, when you reconnect to the user session, the webcam is no longer detected. Instead, a gray screen appears in place of the video preview. [LC8588]

#### Smart Cards

- When you log on to a session using a smart card, the session might become unresponsive until you disconnect and reconnect the session. [#LC8036]

#### System Exceptions

- The wfshell.exe process might exit unexpectedly, pointing to the taskbar grouping module. [LC6968]
- With the USB redirection policy enabled, VDAs might experience a fatal exception, displaying a blue screen with bugcheck code SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC7999]
- VDAs might experience a fatal exception, displaying a blue screen with bugcheck code 0x7E. The issue occurs when you leave the VDA session idle for some time. [LC8045]
- Servers might experience a fatal exception, displaying a blue screen, on picavc.sys with bugcheck code SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC8063]

#### User Experience

- When reconnecting to a seamless application session, the application windows might not appear correctly on the client side. Instead, the session graphics are drawn inside a small rectangle on the client side. [LC7857]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Windows Media Player might display Microsoft AVI (.avi) files format as vertically flipped. [LC8308]
- When a published application is maximized on the screen of a third monitor, the application might not cover the entire screen. Instead, a black border appears. [LC8472]
- The Seamless applications that are hosted on the VDA 7.15 might show a gray or a black frame in the background while moving the application window. [LC8551]

#### User Interface

- If you open a spreadsheet with more than one workbook in Excel 2010, the taskbar displays only the most current workbook. [LC7557]

### VDA for Server OS

#### HDX MediaStream Flash Redirection

- Attempts to save Microsoft Office files such as Microsoft Excel spreadsheets that are running in a session with HDX seamless apps enabled can cause the files to exit unexpectedly. [LC8572]

#### HDX Plug and Play

- USB devices that report the same serial number for more than one device such as Syn-Tech ProKee V2 might not get redirected to a VDA session. The following CDF trace appears:

  "Failed to assign the instance ID, error 0xc000000d."[LC8264]

#### Printing

- Attempts to launch a published application might fail when the application is waiting for a mutex object in Citrix Print Manager service (cpsvc.exe). [LC6829]
- The Citrix Print Manager service (cpsvc.exe) might exit intermittently. [LC7535]
- When you roam a session between clients, session printers cannot be deleted. For example, when you configure the policy "Printer assignments"–printer A for client A and printer B for client B, printer A might not be deleted when you roam from client A to client B. [LC8077]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Server/Site Administration

- On VDA 7.12 or later versions, when you attempt to suppress the display of the language bar in a seamless session by setting the seamless flag to "0x00040000"(disables the language bar agent) under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI, the language is no longer hidden. [#LC8349]

### Session/Connection

- Attempts to reconnect to an application might fail. The issue occurs when any of the disconnected applications became unresponsive when the session disconnected initially. [LC6550]
- When you click "Cancel"on the progress bar of a session launch, wrong session information can remain on the Delivery Controller. As a result, the actual session is not created on the VDA and you might not be able to launch a new session. [LC6779]
- The microphone might be redirected intermittently in the user session even after setting the "Client microphone redirection"policy value to "Prohibited."

  This fix addresses the issue. However, if you continue to observe the issue, apply the following registry key on the device with the microphone:

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\icatcp\AudioConfig;
    Name: MaxPolicyAge;
    Type: DWORD;
    Value: Maximum time (in seconds) allowed between the last policy evaluation and the time of endpoint activation. Default is 30 seconds.
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\icatcp\AudioConfig;
    Name: PolicyTimeout;
    Type: DWORD;
    Value: Maximum time (in milliseconds) that the system waits for policies after determining that the policies are not up to date. Default is 4,000 milliseconds. When the timeout occurs, the system reads the policies and continues with initialization. Setting this value to (0) bypasses the Active Directory policies check and processes policies immediately. [LC7495]

- When you establish a Skype for Business video call, a blue window border might appear after intersecting with the window of a third party application. [LC7773]
- Certain published applications might not cover the entire screen when maximized. [LC7854]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- After upgrading to Versions 7.13, 7.14, or 7.15 of a VDA when using vGPU, a black area might appear in published applications or desktops running on the Microsoft Windows Server operating system. [LC7875]
- When performing an insert operation between two Microsoft Excel 2010 worksheets running on a Version 7.9 VDA, the Excel window might become unresponsive. [LC7912]
- In certain scenarios, seamless applications might not appear in seamless mode or certain features might not work. [LC8030]
- With local app access enabled, using the interactive logon disclaimer policy can cause the desktop viewer to show a gray screen when connecting to a VDA. [LC8136]
- VDAs for Server OS might reregister intermittently when an out-of-order notification is sent to the Delivery Controllers. [LC8228]
- When using applications that use a redirected webcam, such as Skype for Business or a VLC media player, the webcam might be redirected and detected during an initial session launch. However, when you reconnect to the user session, the webcam is no longer detected. Instead, a gray screen appears in place of the video preview. [LC8588]

#### Smart Cards

- When you log on to a session using a smart card, the session might become unresponsive until you disconnect and reconnect the session. [LC8036]

#### System Exceptions

- The wfshell.exe process might exit unexpectedly, pointing to the taskbar grouping module. [LC6968]
- The Windows Shell Experience Host might exit unexpectedly when you click the volume control on the taskbar. [LC7000]
- The Service Host (svchost.exe) process might experience an access violation and exit unexpectedly. The issue occurs because of the faulting module, icaendpoint.dll. [LC7900]
- With the USB redirection policy enabled, VDAs might experience a fatal exception, displaying a blue screen with bugcheck code SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC7999]
- Servers might experience a fatal exception, displaying a blue screen, on picavc.sys with bugcheck code SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC8063]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### User Experience

- When reconnecting to a seamless application session, the application windows might not appear correctly on the client side. Instead, the session graphics are drawn inside a small rectangle on the client side. [LC7857]
- Windows Media Player might display Microsoft AVI (.avi) files format as vertically flipped. [LC8308]
- When a published application is maximized on the screen of a third monitor, the application might not cover the entire screen. Instead, a black border appears. [LC8472]
- The Seamless applications that are hosted on the VDA 7.15 might show a gray or a black frame in the background while moving the application window. [LC8551]

#### User Interface

- When using the Connection Center to log off from a seamless session with unsaved data, a black window appears with the following message:

  "Programs still need to close"- with the two options - "Force Logoff"or "Cancel."The "Cancel" option does not work.

  After installing this fix, the Cancel option works as designed. [LC6075]
- If you open a spreadsheet with more than one workbook in Excel 2010, the taskbar displays only the most current workbook. [LC7557]
- The logoff screen might not appear when you attempt to log off from a Microsoft Windows Server 2008 R2 desktop session. You might be able to log off from the session, but the session appears as though it is disconnected unexpectedly. [LC8016]

### Virtual Desktop Components - Other

- Citrix Director might display an incorrect number of disconnected sessions at the top of every hour. [LC8006]
- The Monitoring Service might fail to insert new session data into the monitoring database. [LC8191]
- The Logon Duration by User Session panel under **Director** > **Trends** > **Logon Performance** might display only partial logon records. [LC8265]
- The System Center Configuration Manager (SCCM) client might exit unexpectedly after upgrading Microsoft Windows 10 from Build 1511 to Build 1703 with a VDA installed on it. [LC8632]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The rearm of Microsoft Office 2016 might be broken on Microsoft Windows 10 when using Machine Creation Services (MCS). [LC8680]
- In a large XenApp and XenDesktop environment, the stored procedure for Monitor database grooming does not work correctly if the size of the Monitor database is large. [LC8770]

## 7.15 LTSR (initial release)

March 22, 2021

Release date: April 04, 2017

### About this release

The XenApp and XenDesktop 7.15 Long Term Service Release (LTSR) includes new versions of the Windows VDAs and new versions of several XenApp and XenDesktop core components.
You can:

- **Install or upgrade a XenApp or XenDesktop Site**

Use the ISO for this release to install or upgrade all the core components and Virtual Delivery Agents. 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 have a XenApp or XenDesktop 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.

For instructions, see Prepare to install or Upgrade a deployment.

The XenApp and XenDesktop download pages for this release also include updated versions of the following software. For more information on the features and installation instructions, see the component's documentation.

StoreFront

AppDNA

Citrix SCOM Management Pack for XenApp and XenDesktop

For an overview of features that have been added since the XenApp and XenDesktop 7.6 LTSR release, see XenApp and XenDesktop 7.15 LTSR Feature Summary Comparison.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The product release also includes the following new, modified, and enhanced features since XenApp and XenDesktop 7.14.1.

#### VDA installation on machines without Microsoft Media Foundation

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 offered in a message. In the command line, you can use the /no_mediafoundation_ack option to acknowledge the limitation.

#### Upgrading a XenApp 6.5 worker to a new VDA

After migrating a XenApp 6.5 farm, you can upgrade a XenApp 6.5 worker to a new VDA. Previously, running the XenApp and XenDesktop installer on the worker server automatically removed the XenApp 6.5 software and then installed the new VDA. Now, you first remove HRP7 and the XenApp 6.5 software from the server., using separate processes. Then, you install the new VDA. For details, see Upgrade a XenApp 6.5 worker to a new VDA.

#### MCS supports generation 2 VMs

When using Microsoft System Center Virtual Machine Manager to provide VMs, you can now use Machine Creation Services (MCS) to provision generation 2 VMs.

#### Local Host Cache

During a new installation of XenApp and XenDesktop, Local Host Cache is enabled by default. Connection leasing is disabled by default.

After an upgrade, the Local Host Cache setting is unchanged. For example, if Local Host Cache was enabled in the earlier version, it remains enabled in the upgraded version. If Local Host Cache was disabled (or not supported) in the earlier version, it remains disabled in the upgraded version.

#### Director

**Application Failure monitoring.** Director extends the Trends view with the **Application Failures** tab to display historical failures associated with published applications. You can see faults and errors that have occurred while launching or running of a selected application or process during a selected time

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

period. This information enables you to comprehend and troubleshoot application-specific issues. For more information, see Historical application failure monitoring in Troubleshoot applications.

By default, failures of applications hosted on Server 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 Desktop OS VDAs, and List of applications excluded from failure monitoring. For more information, see Policies for application failure monitoring in Monitoring policy settings.

This feature requires Delivery Controller(s) and VDAs version 7.15 or later. Desktop OS VDAs of Windows Vista or later, and Server OS VDAs of Windows Server 2008 or later are supported.

#### Virtual Delivery Agents (VDAs) 7.15

After upgrading your VDAs from version 7.9, 7.11, 7.12, 7.13, or 7.14 you do not need to update the machine catalog's functional level. The default (7.9 (or newer ...)) remains the current functional level. For information, see VDA versions and functional levels.

#### Session Recording 7.15

Load balancing for Session Recording: This experimental feature, present in XenApp and XenDesktop 7.14, is not included in this release.

### New deployments

How do I deploy 7.15 LTSR from scratch?

You can set up a brand-new XenApp or XenDesktop environment using the 7.15 LTSR metainstaller.* Before you do that, we recommend that you familiarize yourself with the product:

Read the XenApp and XenDesktop 7.15 Long Term Service Release documentation and pay close attention to the Technical overview, Install and configure, and Secure sections before you start planning your deployment. Make sure your setup meets the system requirements for all components. Follow Install and configure for deployment instructions.

* Note: Provisioning Services and Session Recording are available as separate downloads and installers.

### Existing deployments

What do I update?

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

XenApp and XenDesktop 7.15 LTSR provides updates to all baseline components of 7.6 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to 7.15 LTSR. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services component. If Provisioning Services is not part of your deployment, you do not need to install or update it.

Since the original 7.6 LTSR release, we have added a metainstaller that lets you update the existing components of your LTSR environment from a unified interface. Following the Upgrade instructions, use the metainstaller to update the LTSR components of your deployment.

### XenApp and XenDesktop 7.15 LTSR baseline components

| 7.15 LTSR Baseline Component | Version | Notes |
|---|---|---|
| VDA for Desktop OS | 7.15 | |
| VDA for Server OS | 7.15 | |
| Delivery Controller | 7.15 | |
| Citrix Studio | 7.15 | |
| Citrix Director | 7.15 | |
| Group Policy Management Experience | 3.1 | |
| StoreFront | 3.12 | |
| Provisioning Services | 7.15 | |
| Universal Print Server | 7.15 | |
| Session Recording | 7.15 | Platinum Edition only |
| Linux VDA | 7.15 | See the Linux VDA documentation for supported platforms |
| Profile Management | 7.15 | |
| Federated Authentication Service | 7.15 | |

### XenApp and XenDesktop 7.15 LTSR 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

might ask you to upgrade to a newer version of these components within your 7.15 LTSR environments.

| 7.15 LTSR Compatible Components and Platforms | Version |
|---|---|
| AppDNA | 7.15 |
| Citrix SCOM Management Pack for License Server | 1.2 |
| Citrix SCOM Management Pack for Provisioning Services | 1.19 |
| Citrix SCOM Management Pack for StoreFront | 1.12 |
| Citrix SCOM Management Pack for XenApp and XenDesktop | 3.13 |
| HDX RealTime Optimization Pack | 2.3 |
| License Server | 11.14.0 Build 21103 |
| Workspace Environment Management | 4.4 |
| App Layering | 4.3 |
| Self-Service Password Reset | 1.1 |

#### 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.

### XenApp and XenDesktop 7.15 LTSR notable exclusions

The following features, components, and platforms are not eligible for 7.15 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components will be available through regular current releases.

| Excluded Features |
|---|
| Framehawk |
| StoreFront Citrix Online Integration |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Excluded Features |
| --- |
| |

| Excluded Components |
| --- |
| Personal vDisk: Excluded for Windows 10 machines; Personal vDisk: Excluded for Windows 10 machines;<br>AppDisks |

| 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.

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 XenApp 7.15 LTSR (or a later supported release). 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 7.15 LTSR core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.15 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 XenApp 7.15 LTSR Site in stages: some now and others later.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Run PowerShell import cmdlets on the new XenApp 7.15 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 22, 2022

The following issues have been fixed since Version 7.14.1:

Fixed issues compared to 7.14.1

Fixed issues compared to 7.6 LTSR CU4

### Fixed issues compared to 7.14.1

#### Citrix Director

- When navigating to the **Trends** > **Failures** > **Connection** tab in Citrix Director, the following error message might appear:

  "Unexpected error. Check your network connection or view Director server event logs for further information."[LC7755]

- Attempts to view policy information for certain sessions in Citrix Director can fail and the following error message appears:

  "Cannot retrieve the data"[LC8207]

#### Citrix Policy

- Group Policy Objects that contain both Citrix and Microsoft settings might not be enforced. This issue occurs when the extension unit in the list contains more than two GUIDs. [LC7533]

#### Citrix Studio

- Attempts to add computer accounts to new or existing machine catalogs might fail when using GUI mode instead of using PowerShell commands. The issue occurs when the directory searcher tool does not bind the correct object while finding the NetBIOS name.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For example, if the domain name is xyz.ad.airxyz.aa and the NetBIOS name is xyz-Ad, the NetBIOS name is accepted as xyz instead of xyz-Ad when using GUI mode. As a result, the machine account cannot be added for both existing and new computer accounts. [LC6679]

- After upgrading Citrix Delivery Controller to Version 7.12, attempts to add machines from Citrix Provisioning Services (PVS) to a catalog might fail in a multi-domain environment. The issue occurs when PVS does not return the domain name along with the device name. When Citrix Studio searches for the account name in the local domain, the account cannot be found. [LC6818]
- Attempts to publish App-V applications might fail. [LC7421]
- When an administrator attempts to add an App-V application from an isolation group to the Delivery Group or attempts to create an isolation group, the following error message might appear in Citrix Studio:

  "An unknown error occurred."[LC7594]
- Attempts to add machines to a Delivery Group by using the "NETBIOS"name for user association might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC7830]

### Controller

- After upgrading Citrix Delivery Controller to Version 7.12, attempts to add machines from Citrix Provisioning Services (PVS) to a catalog might fail in a multi-domain environment. The issue occurs when PVS does not return the domain name along with the device name. When Citrix Studio searches for the account name in the local domain, the account cannot be found. [LC6818]
- Attempts to add machines to an existing Machine Creation Services catalog might not follow the round robin method for multiple storages that can be selected to accept the new machines. [LC7456]
- Attempts by custom administrators to create an isolation group might fail and the following error message appears:

  "You do not have the permissions required to complete this request. For more information, contact your XenDesktop Site administrator."[LC7563]
- When an administrator attempts to add an App-V application from an isolation group to the Delivery Group or attempts to create an isolation group, the following error message might appear in Citrix Studio:

  "An unknown error occurred."[LC7594]
- Attempts to disable TLSv1.0 on Citrix Delivery Controller can cause loss of communication to the VMware vCenter hypervisor. [LC7686]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Attempts to add machines to a Delivery Group by using the "NETBIOS"name for user association might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC7830]

### Profile Management

- When you attempt to open files in a profile with Profile Streaming enabled, the file might appear empty after you log on. [LC6996]
- Servers might experience a fatal exception, displaying a blue screen, on upmjit.sys with bugcheck code 0x135. [LC7841]
- UserProfileManager.exe might exit unexpectedly when you log on to a VDA. [LC7952]

### StoreFront

- Attempts to reconnect to disconnected sessions might fail within a multi-Site aggregation deployment. As a result, you might receive a second instance of the same resource. [LC7453]
- When a part of the source of an aggregated application is disabled, the application might be unexpectedly hidden from the end user. [LC7675]
- Attempts to disable the "Account Self-Service"option in StoreFront might not take effect, even though the option appears as disabled. [LC7744]
- Attempts to remove shared authentication from Stores in StoreFront might result in the following error message while saving the changes:

  "An error occurred while saving your changes."[LC7781]

### Universal Print Server

#### Client

- The print spooler service might become unresponsive and, as a result, Universal Printing does not work. The issue occurs when a timeout is reached while waiting for a transaction response from the spooler service. [LC5209]
- When using Profile Management, changes made to Citrix Universal Print Server printers (adding, removing, and renaming) in a session on one server might not be correctly reflected in subsequent sessions on another server. [LC7645]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Server

- Attempts to print a document might fail and the following error message appears:

  "Windows cannot print due to a problem with the current printer setup."[LC6825]

- When using certain printers, Microsoft Notepad might display the message "The handle is invalid"and fail to print. The issue occurs if "Use only printer model specific drivers"is configured in the Citrix policy "Universal print driver usage"and if "Enabled with no fallback to Windows' native remote printing"is configured in the Citrix policy "Universal Print Server enable."[LC7623]

### VDA for Desktop OS

#### Installing, Uninstalling, Upgrading

- After upgrading the VDA from Version 5.6.400 to Version 7.9, restarting the VDA can cause the mirror drivers installed by the previous version to be left behind. [LC6295]
- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7555]
- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7587]

#### Printing

- The Citrix Print Manager service (cpsvc.exe) might become unresponsive and exit unexpectedly when new users log on. [LC6933]
- After upgrading the VDA from Version 7.9 to Version 7.12 or later, attempts to print from Microsoft Internet Explorer by using the Citrix Universal Print Driver might print only to tray 1 instead of printing to the tray that is selected. [LC7463]

#### Session/Connection

- When multiple webcams of the same model are installed on the VDA for Desktop OS, only the latest webcam might be recognized by the session and mapped. [LC5008]
- A removable client drive might not be returned by the WFAPI SDK on the VDA for Desktop OS. [LC6877]
- The window positions might not be retained when you reconnect to a published desktop session and are using multiple monitors. [LC7644]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you switch sessions between multiple monitors in full-screen mode with legacy graphics mode enabled and without Desktop Viewer configured, only one monitor might appear to be running the session. [LC7907]

#### Smart Cards

- Occasionally, removing a smart card reader might not trigger the user session to get locked, even though smart card removal is configured to lock the user session. [LC7411]

#### System Exceptions

- VDAs might experience a fatal exception, displaying a blue screen, on vd3dk.sys with bugcheck code 0X00000050. [LC6833]
- VDAs might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x7F while shutting down a session. [LC7545]
- The Service Host (svchost.exe) process might experience an access violation and exit unexpectedly. The issue occurs because of the faulting module, scardhook64.dll. [LC7580]
- Servers might experience a fatal exception, displaying a blue screen, on vdtw30.dll with stop code 0xc0000006. [LC7608]
- VDAs might experience a fatal exception, displaying a blue screen, on tdica.sys with a bugcheck code. [LC7632]
- This fix addresses a memory issue with the wdica.sys file that can cause servers to exit unexpectedly. [LC7666]

#### User Experience

- This fix provides improved support for sounds that play for a short period of time when using high quality audio.

  **Note**:

  - This fix does not take effect in sessions running on Windows Server 2008 R2.
  - For this fix to work, you must use Citrix Receiver 4.4 for Windows Long Term Service Release (LTSR) CU5 or later versions and the VDA version of XenApp and XenDesktop 7.6 LTSR CU4 or later. [LC5842]

- When performing an insert operation between two Microsoft Excel 2010 worksheets running on a Version 7.9 VDA, the Excel window might become unresponsive. [LC7481]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- In a multi-monitor environment, define the external monitor as the "Main Display"of Windows and position it to the right of the secondary laptop or tablet monitor in the display settings of the Control Panel. When you start a published application that appears on the external monitor and move this application to the tablet monitor or a laptop that is attached to the external monitor, opening or closing the lid of the tablet or a laptop can cause the published application to become black.

  To enable the fix, you must set the following registry key value on the VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire; Name: EnableDrvTw2NotifyMonitorOrigin; Type: REG_DWORD; Value: 1 (to enable) and 0 (to disable; 0 is the default value). By default, the registry value is missing. [LC7760]

#### User Interface

- URL shortcut icons might be displayed as blank when using a touch-optimized desktop. [LC6663]
- If you open a spreadsheet with more than one workbook in Excel 2010, the taskbar displays only the most current workbook. [LC7557]

### VDA for Server OS

#### Installing, Uninstalling, Upgrading

- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7555]
- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7587]

#### Printing

- The Citrix Print Manager service (cpsvc.exe) might become unresponsive and exit unexpectedly when new users log on. [LC6933]
- After upgrading the VDA from Version 7.9 to Version 7.12 or later, attempts to print from Microsoft Internet Explorer by using the Citrix Universal Print Driver might print only to tray 1 instead of printing to the tray that is selected. [LC7463]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Server/Site Administration

- The following error message might appear for child domain users while launching an application through Web Interface or StoreFront:

  "You have not been granted access to this published application."[LC7566]

### Session/Connection

- When multiple webcams of the same model are installed on the VDA for Desktop OS, only the latest webcam might be recognized by the session and mapped. [LC5008]
- Attempts to reconnect to a session can fail intermittently and cause the VDAs for Server OS to go into "Initializing"status. The issue occurs when the VDA is registered again with a Delivery Controller. [LC6647]
- Active sessions might be disconnected on the XenApp servers when the Delivery Controller loses connectivity. The issue occurs when VDAs fails to track the status of sessions that move from "pre-launch"to "active"status correctly. As a result, when the Delivery Controller is restarted, it attempts to clear the resources from the VDAs, and sessions in the pre-launch status are disconnected or logged off while the applications are being actively used. [LC6819]
- When you launch a published application on Microsoft Windows Server 2016, a black screen might appear for several seconds before the application becomes visible. [LC7947]

### System Exceptions

- VDAs might experience a fatal exception, displaying a blue screen, on picadm.sys with bugcheck code 0x7F while shutting down a session. [LC7545]
- The Service Host (svchost.exe) process might experience an access violation and exit unexpectedly. The issue occurs because of the faulting module, scardhook64.dll. [LC7580]
- Servers might experience a fatal exception, displaying a blue screen, on vdtw30.dll with stop code 0xc0000006. [LC7608]
- VDAs might experience a fatal exception, displaying a blue screen, on tdica.sys with a bugcheck code. [LC7632]
- This fix addresses a memory issue with the wdica.sys file that can cause servers to exit unexpectedly. [LC7666]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### User Experience

- This fix provides improved support for sounds that play for a short period of time when using high quality audio.

  **Note**:

  - This fix does not take effect in sessions running on Windows Server 2008 R2.
  - For this fix to work, you must use Citrix Receiver 4.4 for Windows Long Term Service Release (LTSR) CU5 or later versions and the VDA version of XenApp and XenDesktop 7.6 LTSR CU4 or later. [LC5842]

- When performing an insert operation between two Microsoft Excel 2010 worksheets running on a Version 7.9 VDA, the Excel window might become unresponsive. [LC7481]
- In a multi-monitor environment, define the external monitor as the "Main Display"of Windows and position it to the right of the secondary laptop or tablet monitor in the display settings of the Control Panel. When you start a published application that appears on the external monitor and move this application to the tablet monitor or a laptop that is attached to the external monitor, opening or closing the lid of the tablet or a laptop can cause the published application to become black.

  To enable the fix, you must set the following registry key value on the VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire; Name: EnableDrvTw2NotifyMonitorOrigin; Type: REG_DWORD; Value: 1 (to enable) and 0 (to disable; 0 is the default value). By default, the registry value is missing. [LC7760]

#### User Interface

- URL shortcut icons might be displayed as blank when using a touch-optimized desktop. [LC6663]
- If you open a spreadsheet with more than one workbook in Excel 2010, the taskbar displays only the most current workbook. [LC7557]

### Virtual Desktop Components - Other

- Attempts to publish App-V applications might fail. [LC7421]
- Attempts to launch App-V applications in Single Admin mode might fail. The issue occurs when the application name contains special characters. [LC7897]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Fixed issues compared to 7.6 LTSR CU4

### Citrix Director

- Citrix Director with Windows Integrated Authentication (WIA) might not work with a Kerberos Constrained Delegation setup. [LC5196]
- A "System unavailable"error occurs after attempting to log onto Citrix Director. [LC5385]
- Citrix Director might not display session details. The issue occurs when using Published content as the application type. [LC6577]

### Citrix Policy

- The Citrix Policy processing might stop responding, which causes user sessions to become unresponsive. When this occurs, connection requests to Receiver and Remote Desktop (RDP) fail. [LA4969]
- On systems with Fix LC1987 (GPCSExt170W2K8R2X64006 or its replacement) installed, Active Directory (AD) policies that contain both Citrix and Microsoft settings might not be enforced.

  **Note**: This fix addresses the issue for AD policies you create after installing this update. It also addresses it for *existing* policies where Citrix settings were configured before Microsoft settings. It does not address it for existing AD policies where Microsoft settings were configured *before* Citrix settings. For those AD policies, you must open the affected policies and save the Citrix settings. [LC2121]
- With this feature enhancement, the Citrix Group Policy Engine generates additional event log messages while processing Citrix policies. [LC3664]
- When upgrading from 7.6 to either versions 7.8 or 7.9, certain color schemes in Citrix Studio might appear too dark for text to display properly. [LC5690]
- After installing the Citrix Federated Authentication Service, attempts to configure the **Security Access Control Lists** on the StoreFront server under **User Rules** can cause the Configuration window to become unresponsive. [LC5788]
- The CPU and memory consumption of Microsoft Excel might spike while opening a file with the XLSM file extension with macros. As a result, attempts to open the file fail. [LC6142]
- Group Policy Objects that contain both Citrix and Microsoft settings might not be enforced. This issue occurs when the extension unit in the list contains more than two GUIDs. [LC7533]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Citrix Studio

- When multiple users create policies in a multiple studio session, the latest policy created overwrites the earlier policy when Citrix Studio is refreshed. [LA5533]
- Citrix Studio might not recognize the XenDesktop App Edition License and the following error message appears:

  "Can't find a valid license
  No suitable licenses are available. Check the license server address and that the product edition and model are correct."[LC0822]
- When attempting to add cross-domain users to a Delivery Group, Citrix Studio resolves their actual domain to the local domain account. [LC1886
- Attempts to publish an application in Citrix Studio 7.7 by using command line arguments that contain quotations (") might result in an error message. [LC4525]
- Citrix Studio might offer the Catalog Rollback option even when no catalog update has been done. Opting to roll back causes an exception. [LC4791]
- Attempts to add machines to a Machine Catalog from Citrix Studio can fail and an error message appears. The issue does not occur when you add machines using the XenDesktop Setup wizard. [LC5030]
- When two applications have the same ApplicationID, refreshing App-V applications can cause Citrix Studio to set the App-V package name incorrectly. [LC5261]
- When a Delivery Controller goes offline or becomes otherwise unavailable, Citrix Studio might operate slowly. [LC5335]
- After upgrading XenApp or XenDesktop to 7.7 from 7.6, a prompt to upgrade might occasionally appear in Citrix Studio. [LC5478]
- When you close and then attempt to reopen an instance of Version 7.9 of Citrix Studio that is configured with App-V servers containing many packages, Studio remains in an expanding state and fails to open. [LC5643]
- Using Citrix Studio, you can add only one App-V server to a Site. To add additional App-V servers to the Site, you must use PowerShell. [LC5767]
- After upgrading Citrix Studio from 7.8 to 7.9, applications you add after the upgrade appear with no package name or version. [LC5958]
- Adding an application through the Applications node in Citrix Studio might cause an error where the application is not added. As a workaround, use the Delivery Group node to add applications. [LC5975]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When trying to create a new XenDesktop Site through Citrix Studio and pointing to the SQL AlwaysOn Listener, the following error might appear:

  "The replica server <servername> could not be contacted. Check the database status on the SQL server. Ensure database server allows remote connections and the firewall is not blocking connections."[LC6010]

- If you remove an existing published App-V package from Citrix Studio and attempt to add a different version of the same App-V package with the same name and publishing location to the Delivery Group, the package might enumerate with a red exclamation point and the following error message appears:

  "Failed to load application data for the application "APPLICATION NAME""[LC6254]

- Attempts to add a Delivery Controller in a mirrored database setup by using the option to add an additional controller from Citrix Studio and the PowerShell command "Add-XDController" might fail. [LC6563]

- Attempts to add computer accounts to new or existing machine catalogs might fail when using GUI mode instead of using PowerShell commands. The issue occurs when the directory searcher tool does not bind the correct object while finding the NetBIOS name.

  For example, if the domain name is xyz.ad.airxyz.aa and the NetBIOS name is xyz-Ad, the NetBIOS name is accepted as xyz instead of xyz-Ad when using GUI mode. As a result, the machine account cannot be added for both existing and new computer accounts. [LC6679]

- After upgrading Citrix Delivery Controller to Version 7.12, attempts to add machines from Citrix Provisioning Services (PVS) to a catalog might fail in a multi-domain environment. The issue occurs when PVS does not return the domain name along with the device name. When Citrix Studio searches for the account name in the local domain, the account cannot be found. [LC6818]

- When upgrading a XenApp Site, the license model might change from XenApp to XenDesktop unexpectedly. [LC6981]

- The "Start-Transcript"command might fail for "Get-XDSite"and other XenDesktop high level administrative PoSH commands when run in PowerShell 5. [LC7006]

- When an administrator attempts to add an App-V application from an isolation group to the Delivery Group or attempts to create an isolation group, the following error message might appear in Citrix Studio:

  "An unknown error occurred."[LC7594]

- Attempts to add machines to a Delivery Group by using the "NETBIOS"name for user association might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC7830]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Controller

- Deploying virtual machines using Machine Creation Services in Citrix Studio fails, displaying the following error message:

  "Error Id: XDDS:0F7CB924."[LC4930]

- When users attempt to deleted the pooled catalog created on XenServer and then run the catalog update, the base disks are not removed from storage and the number of base disks might increase. [LC0577]
- Session reliability cannot be disabled by using either Active Directory Group Policy Object (GPO) or through Citrix Studio on VDA 7.x sessions that start by using XenDesktop 5.6 Desktop Delivery Controller (DDCs). [LC0878]
- When creating a new pooled machine by using the Machine Creation Services from a master image with custom VMX and nvram settings, the settings are not copied to the new virtual machines. [LC0967]
- The PrepareSession task that is executed by the Broker Service might time out when used in XenDesktop 5.6 environments, causing StoreFront to fail. [LC1055]
- This fix addresses a timing issue that can occur when the hypervisor is congested while formatting a PvD disk volume during initial machine creation. [LC3275]
- Creating virtual machines with Machine Creation Services using VMware vSphere 6.0 and vSAN 6 storage might fail. [LC4563]
- The WaitForTask response causes the exception VimApi.MissingProperty which does not allow the update of Machine Catalogs. [LC4573]
- Attempts to add machines to a Machine Catalog from Citrix Studio can fail and an error message appears. The issue does not occur when you add machines using the XenDesktop Setup wizard. [LC5030]
- After upgrading the VDA to Version 7.8, attempts to perform the update inventory operation might fail and the following error message appears:

  "Update inventory failed with :An internal error occurred Error code 0x2."[LC5051]

- Extraneous characters might appear at the end of "Service Display Name"and "Service description"of certain Citrix services installed on a Japanese operating system. [LC5208]
- When two applications have the same ApplicationID, refreshing App-V applications can cause Citrix Studio to set the App-V package name incorrectly. [LC5261]
- After upgrading XenApp or XenDesktop to 7.7 from 7.6, a prompt to upgrade might occasionally appear in Citrix Studio. [LC5478]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- An ampersand (&) in the title of an application causes the StoreFront XML to become corrupt and display no applications or icons. [LC5505]
- When you close and then attempt to reopen an instance of Version 7.9 of Citrix Studio that is configured with App-V servers containing many packages, Studio remains in an expanding state and fails to open. [LC5643]
- After upgrading to XenDesktop 7.9, logging on might occasionally fail due to the NetScaler broker's not sending credentials correctly. [LC5753]
- Using Citrix Studio, you can add only one App-V server to a Site. To add additional App-V servers to the Site, you must use PowerShell. [LC5767]
- After installing the Citrix Federated Authentication Service, attempts to configure the **Security Access Control Lists** on the StoreFront server under **User Rules** can cause the Configuration window to become unresponsive. [LC5788]
- Changing the SDK port of Flexcast Management Architecture services such as Analytics, Broker, Log, etc. causes Citrix Studio to not connect properly. [LC6005]
- When trying to create a new XenDesktop Site through Citrix Studio and pointing to the SQL AlwaysOn Listener, the following error might appear:

  "The replica server <servername> could not be contacted. Check the database status on the SQL server. Ensure database server allows remote connections and the firewall is not blocking connections."[LC6010]
- Citrix Director might show a number of unregistered machines on the dashboard that does not match with the report on the Trends page. [LC6184]
- The Monitoring Service fails to insert new session data into the Monitoring database when the Load Evaluator Index policy is enabled. This can lead to Citrix Director not displaying up-to-date information for sessions such as Logon Duration, Current Number of Active Sessions, and others. While the problem shows in Citrix Director, it is caused by an issue in the Delivery Controller. The current version of the Controller addresses the issue. [LC6241]
- Attempts to remove a hosting unit can cause the replication of AppDisks on any other hosting unit to fail. As a result, the machines in the Delivery Group with AppDisks fail to start. [LC6433]
- After restarting the Citrix Monitoring Service or the Citrix Delivery Controller, event id 1013 might appear:

  "Initial database housekeeping failed with: System.NullReferenceException: Object reference not set to an instance of an object."

  The issue occurs when the Citrix Monitor Service is stopping. [LC6438]
- Attempts to use certain third-party applications such as RayStation on a Citrix Delivery Controller might fail and the following error message appears:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

"The communication object, System.ServiceModel.Channels.ServiceChannel, cannot be used for communication because it is in the Faulted state."[LC6552]

- Attempts to add a Delivery Controller in a mirrored database setup by using the option to add an additional controller from Citrix Studio and the PowerShell command "Add-XDController" might fail. [LC6563]
- Attempts to delete MCS catalogs on VMware VSANs might fail. [LC6691]
- Memory consumption of the Monitoring Service can spike, causing servers to be unresponsive. [LC6705]
- After upgrading Citrix Studio from previous versions or when you do a fresh install of Citrix Studio Version 7.12, the Delivery Controller might cause Citrix Studio to be stuck in a mandatory upgrade loop. [LC6737]
- When using version 7.12 of Machine Creation Services to create VMs, XenTools fails to be installed, preventing graceful shutdown of the VMs. [LC6769]
- After upgrading Citrix Delivery Controller to Version 7.12, attempts to add machines from Citrix Provisioning Services (PVS) to a catalog might fail in a multi-domain environment. The issue occurs when PVS does not return the domain name along with the device name. When Citrix Studio searches for the account name in the local domain, the account cannot be found. [#LC6818]
- Permissions to publish App-V packages might be denied for administrators who do not have full permission with the following exception:

  "Citrix.Console.Models.Exceptions.PermissionDeniedException: You do not have the required permissions to perform this operation."[LC6897]
- The HighAvailabilityService.exe process might consume high memory. [LC6918]
- When upgrading a XenApp Site, the license model might change from XenApp to XenDesktop unexpectedly. [LC6981]
- The "Start-Transcript"command might fail for "Get-XDSite"and other XenDesktop high level administrative PoSH commands when run in PowerShell 5. [LC7006]
- This fix addresses a memory issue in Citrix Host Service. [LC7516]
- Attempts by custom administrators to create an isolation group might fail and the following error message appears:

  "You do not have the permissions required to complete this request. For more information, contact your XenDesktop Site administrator."[LC7563]
- When an administrator attempts to add an App-V application from an isolation group to the Delivery Group or attempts to create an isolation group, the following error message might appear in Citrix Studio:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

"An unknown error occurred."[LC7594]

- Attempts to install the VDA on Microsoft Windows Server might fail when the Microsoft Remote Desktop Session Host role service is already installed. [LC7680]
- Attempts to disable TLSv1.0 on Citrix Delivery Controller can cause loss of communication to the VMware vCenter hypervisor. [LC7686]
- Attempts to add machines to a Delivery Group by using the "NETBIOS"name for user association might fail. Instead, the domain name might appear. The issue occurs when the NETBIOS name uses the wrong URL. [LC7830]

## Licensing

- The license server might fail the Payment Card Industry (PCI) compliance scan for clickjacking because the "X-Frame-Options"header type is not set. [LC1983]
- Attempts to add a domain group whose name contains more than 32 characters might fail. [LC1986]
- If the NetBios domain name contains an ampersand (&), attempts to open the Licensing tab in Studio might fail with the following error message:

  "Citrix license server unavailable"[LC2728]

## Profile Management

- Attempts by certain third party applications to rename or move files during logon or logoff might fail. For example, if there are files file0, file1, and file2 in the local profile, attempts to rename file2 to file3, file1 to file2, and file0 to file1 might fail during the logoff process if file2 already exists on the pending area or user store. [LC0465]
- When users log off, the Profile Management (UserProfileManager.exe) service occasionally fails. [LC0625]
- The "LOGON DURATION"panel in the Performance Monitor (Perfmon) counter might record the data for user logons that are not managed by the Profile Management. [LC0779]
- The Profile Management might not synchronize the files with the user store after a certain period of time. [LC1338]
- After enabling the following logging options, no debugging information is recorded in the log file:

  - Policy: Active Directory actions
  - Policy: Policy values at logon and logoff

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - Policy: Registry difference at logoff [LC2003]

- If a user enables Profile Versioning as described in https://support.microsoft.com/en-us/kb/2890783, the Profile Management might not migrate for the following reasons:

  - The Microsoft roaming profile is created with the extension "V4"
  - The UPM profile was not migrated and created from the "Default user"template. [LC2427]

- After resetting the user profile in Desktop Director, folder redirection does not work when users log on for the first time. Folder redirection does work when users subsequently log on. [LC2602]
- The Profile Management (UserProfileManager.exe) service might close unexpectedly. [LC2979]
- After applying Fix LC0625, the Profile Management (UserProfileManager.exe) service might close unexpectedly. [LC3058]
- On Windows 8.1, attempts to download files using Internet Explorer 11 fail if Enhanced Protected Mode is enabled. [LC3464]
- File locks can occur in Profile Management during the logoff process with the following error message:

  "The process cannot access the file because it is being locked by another process."

  Attempts to delete files locked by Profile Management might fail until the locks are released. [LC3532]

- Profile Management can exit unexpectedly while the user device is in the process of shutting down. [LC3626]
- XenApp servers might become unresponsive in the farm until the server is restarted. [LC4318]
- When attempting to log on to a XenApp 7.7 server using RDP, the server might become unresponsive on the welcome screen. [LC5169]
- After upgrading a VDA from Version 7.6.1000 or earlier to Version 7.7 or later, attempts to delete, repair, or reinstall Profile Management or the VDA might fail. [LC5207]
- When logging off, Profile Management occasionally locks files/folders on the server, causing applications to fail to launch. Locally cached profiles also do not get deleted. [LC5266]
- Profile Management occasionally locks files in user profiles. When this happens, users receive a temporary profile while trying to reconnect until the lock on their profile is released. [LC5278]
- Locally cached profiles might not delete when users log off. [LC5470]
- When the license server is offline, files using the user redirection folder on the server are lost. [LC5595]
- Users'files are lost when the license trial period ends without renewal. [LC5775]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Profile Management might incorrectly raise a "NetworkDetection"flag indicating that the network might be lost. This fix introduces an extra check to ensure that the network is not available instead of temporarily being unavailable. [LC5943]
- Occasionally, the user logon screen becomes unresponsive on Windows Server 2012 R2. [LC6149]
- Attempts to migrate roaming profiles into Profile Management might fail. The issue occurs when an incorrect version number is added to the profile. [LC6150]
- The application icons might appear as grayed out when you attempt to copy the icons from the Profile Management user profile store through a WAN connection. [LC6152]
- File type associations might fail to roam in Profile Management enabled sessions running on Microsoft Windows 10 and Windows Server 2016. [LC6736]
- With the "Delete local cache at logoff"policy enabled on Microsoft Windows 10 or Windows Server 2016, the NTUSER.DAT file might fail to be deleted at logoff, causing another local profile to be created at the next logon. [LC6765]
- When using Profile Management on Microsoft Windows Server 2016 and usrclass.dat is included, the Start menu might not work. [LC6914]
- When you attempt to open files in a profile with Profile Streaming enabled, the file might appear empty after you log on. [LC6996]
- Profile Management can cause a black screen to appear when you attempt to launch a Microsoft Windows 10 session. With this fix, you must configure the policy "Directories to synchronize"and add the folder "*AppData\Local\Microsoft\Windows\Caches*."[LC7596]

## Provisioning Services

### Console Issues

- With this fix, the "Schedule the next vDisk update to occur on"option and "Apply vDisk updates as soon as they are directed by the server"option are no longer available for Provisioning Services. [LA4166]
- Attempts to create virtual machines through the XenDesktop setup wizard might fail in a non-English Microsoft System Center Virtual Machine Manager (SCVMM) environment. [LC5451]
- Attempts to create an ISO with the New-BootDeviceManager PowerShell script can fail and the following error message appears: "ISOFileName must be called with the name of the new ISO file to create."[LC5559]
- When using clustered volume storage, the Streamed VM Setup wizard does not honor the volume selection and can create target devices on random volumes. [LC5890]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Attempts to close the Provisioning Services Console after running the XenDesktop Setup wizard or the Streamed VM Setup wizard can result in an exception. [LC6048]
- After upgrading to PVS 7.11 from version 7.6, users in other domains might not be able to log on to the console. [LC6216]
- Server communication time out. In some cases, login times can become excessively long (for example, greater than 2 minutes). This can cause server timeout issues between the PVS Console and the SoapServer. By default, the timeout for such connections is 2 minutes. However, you can increase this value by modifying the registry value HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<timeout in seconds>. If the login time is greater than approximately 4 minutes, users will also experience timeouts from the Microsoft MMC containing the PVS Console (these timeouts can be dismissed).

  One cause for this issue is unreachable domains in Active Directory, where there is a 30 second timeout applied each time an attempt to connect to an unreachable domain is made. This can quickly add up to several minutes if there are multiple unreachable domains. In general, unreachable domains are created by adding a test or experimental domain to Active Directory, then removing it at a later time. Although the domain is gone, it is still reported by Active Directory when enumerating domains or authorization groups.

  Unreachable domains can also be caused by a domain controller being temporarily shut down and disconnected from the network, so not all unreachable domains should be blacklisted.

  The best way to determine whether there are unreachable domains is by looking at the CDF trace for the PVS_DLL_ADSUPPORT module and checking for “Unreachable Domain”and “Server Referral”errors. If any of these are found, check the domains to ensure that they are not in use any more, and if not, add the domain names to the blacklist.

  The blacklist is a JSON format file called “%ProgramData\Citrix\Provisioning Services\blacklist.json” . For example:

```
{


"Domains":

[

"sub.xs.local",

"sb.xs.local"

]

 }

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
16    <!--NeedCopy-->
```

Where the two domains **sub.xs.local** and **sb.xs.local** will be excluded from domain and group enumeration. After the file is updated, you must restart the SoapServer and any running consoles in order to load the updated values. [LC6249]

- After configuring the Provisioning Services Console, the label names might be missing in the target device properties. [LC6864]

### Server Issues

- In VMware ESX deployments, the XenDesktop Setup wizard can throw an exception, preventing users from setting up templates and machines properly. [LA2499]
- Two PVS servers might not be able to see the replication status of a vDisk on the opposite server, but each server shows the status of its own vDisks properly. [LC4317]
- The Citrix PXE service might ignore the entries in the BOOTPTAB file. [#LC4600]
- When using a BDM partition, target devices running on VMware do not attempt to log on to all servers in the list if the top-most server is unreachable. [LC4736]
- Attempts to create virtual machines through the XenDesktop setup wizard might fail in a non-English Microsoft System Center Virtual Machine Manager (SCVMM) environment. [LC5451]
- If not all partitions on a hard drive are being cloned, the final partitions that are being cloned might fail. [LC5452]
- When running replication status for two PVS servers from the PVS console, the status for both servers is shown as incomplete. [LC5700]
- When using clustered volume storage, the Streamed VM Setup wizard does not honor the volume selection and can create target devices on random volumes. [LC5890]
- After upgrading to PVS 7.11 from version 7.6, users in other domains might not be able to log on to the console. [LC6216]
- Server communication time out. In some cases, login times can become excessively long (for example, greater than 2 minutes). This can cause server timeout issues between the PVS Console and the SoapServer. By default, the timeout for such connections is 2 minutes. However, you can increase this value by modifying the registry value HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<timeout in seconds>. If the login time is greater than approximately 4 minutes, users will also experience timeouts from the Microsoft MMC containing the PVS Console (these timeouts can be dismissed).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

One cause for this issue is unreachable domains in Active Directory, where there is a 30 second timeout applied each time an attempt to connect to an unreachable domain is made. This can quickly add up to several minutes if there are multiple unreachable domains. In general, unreachable domains are created by adding a test or experimental domain to Active Directory, then removing it at a later time. Although the domain is gone, it is still reported by Active Directory when enumerating domains or authorization groups.

Unreachable domains can also be caused by a domain controller being temporarily shut down and disconnected from the network, so not all unreachable domains should be blacklisted.

The best way to determine whether there are unreachable domains is by looking at the CDF trace for the PVS_DLL_ADSUPPORT module and checking for "Unreachable Domain"and "Server Referral"errors. If any of these are found, check the domains to ensure that they are not in use any more, and if not, add the domain names to the blacklist.

The blacklist is a JSON format file called "%ProgramData\Citrix\Provisioning Services\blacklist.json" . For example:

```
{

"Domains":

[

"sub.xs.local",

"sb.xs.local"

\]

 }

<!--NeedCopy-->
```

Where the two domains **sub.xs.local** and **sb.xs.local** will be excluded from domain and group enumeration. After the file is updated, you must restart the SoapServer and any running consoles in order to load the updated values. [LC6249]

### Target Issues

- The auto update feature of the Provisioning Services Target device generates the following application error message (Event ID: 0) in the target's Event Viewer if the update is not available. "No update server found. Stopping client service."[LC0450]
- The target device software does not recognize the AppDisk drive and uses the AppDisk drive for write cache, which can cause conflicts. [LC5409]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you configure a vDisk to use "Write Cache on RAM"and set the RAM cache size to 4,096 MB or 4,097 MB, booting from a Hyper-V GEN-2 virtual machine can cause target devices to experience a fatal exception, displaying a blue screen. [LC6707]

### StoreFront

- If the Administrator changes the group policy setting, MaxPasswordAge, the StoreFront default domain service does not reload the new value. In StoreFront, the user may be shown the incorrect "number of days until password expiry".

  **Note**: This issue is fixed, however it can take up to an hour for the new value to load. [DNA-41380]

- With StoreFront 3.5 installed, the folder color in the categories view might no longer use the custom color defined in the StoreFront management console. It reverts to the default color. [LC5001]
- StoreFront might exit unexpectedly when managing Citrix Receiver for Web sites. The issue occurs when the style.css is customized for Citrix Receiver for Web. [LC5589]
- Enabling Federated Authentication Service on StoreFront might cause logon errors. [LC5708]
- Even with Citrix Receiver for HTML5 enabled in Citrix StoreFront, the StoreFront console might display "Not Used"instead of displaying the HTML version. [LC6626]
- When you select a configured Site during the setup of XenDesktop, a default store might be created in StoreFront that uses the default Authentication Service. If you remove this store, users of Citrix Receiver for Windows cannot add any other stores and the following error message might appear:

  "A protocol error occurred while communicating with the Authentication Service."[LC6664]

- If you configure Self-Service Password Reset (SSPR) for a specific store from the StoreFront console, the configuration applies to all stores, not just to the specific store you selected. [LC6987]
- Attempts to reconnect to disconnected sessions might fail within a multi-Site aggregation deployment. As a result, you might receive a second instance of the same resource. [LC7453]
- When any of the sources of an aggregated application are disabled, the application might be unexpectedly hidden from the end user. [LC7675]
- Attempts to disable the "Account Self-Service"option in StoreFront might not take effect, even though the option appears as disabled. [LC7744]
- Attempts to remove shared authentication from Stores in StoreFront might result in the following error message while saving the changes:

  "An error occurred while saving your changes."[LC7781]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Universal Print Server

### Client

- When using Profile Management, changes made to Citrix Universal Print Server printers (adding, removing, and renaming) in a session on one server might not be correctly reflected in subsequent sessions on another server. [LC7645]

### Server

- Attempts to print from Microsoft Internet Explorer might fail with the following error message when using the Citrix Universal Print Driver:

  "There was an internal error and Internet Explorer is unable to print this document."[LC4735]

- Attempts to print a document might fail and the following error message appears:

  "Windows cannot print due to a problem with the current printer setup."[LC6825]

- When using certain printers, Microsoft Notepad might display the message "The handle is invalid"and fail to print. The issue occurs if "Use only printer model specific drivers"is configured in the Citrix policy "Universal print driver usage"and if "Enabled with no fallback to Windows' native remote printing"is configured in the Citrix policy "Universal Print Server enable."[LC7623]

## VDA for Desktop OS

### Content Redirection

- Attempting to capture images using DirectShow fails, causing the application to exit unexpectedly. [LC6667]

### HDX Broadcast

- HDX audio devices might be randomly disabled when starting a session. [LC5281]

### Installing, Uninstalling, Upgrading

- After upgrading the VDA from Version 5.6.400 to Version 7.9, restarting the VDA can cause the mirror drivers installed by the previous version to be left behind. [LC6295]
- When upgrading from VDA Version 5.6 to 7.x, an incorrect legacy video driver might get installed. [LC6363]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When using version 7.12 of Machine Creation Services to create VMs, XenTools fails to be installed, preventing graceful shutdown of the VMs. [LC6769]
- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7555]
- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7587

#### Keyboard

- Citrix Receiver for Linux might not support Spanish DNIe identity cards. [LC6547]
- With HDX 3D Pro enabled on a VDA, the keyboard shortcuts "Alt+p"and "Alt+s"might not work. [LC6826]

#### Printing

- When you attempt to print two copies or more of a document, only one copy might print. The issue occurs if "Use only printer model specific drivers"is configured in the Citrix policy "Universal print driver usage"and if "Enabled with no fallback to Windows' native remote printing" is configured in the Citrix policy "Universal Print Server enable."[LC6023]
- The Citrix Print Manager service (cpsvc.exe) might become unresponsive and exit unexpectedly when new users log on. [LC6933]
- After upgrading the VDA from Version 7.9 to Version 7.12 or later, attempts to print from Microsoft Internet Explorer by using the Citrix Universal Print Driver might print only to tray 1 instead of printing to the tray that is selected. [LC7463]

#### Server/Site Administration

- Changes you make to "Advanced System Settings"under "Visual Effects"apply to the current VDA for Desktop OS session but might not be retained for subsequent sessions. To make such changes persistent, set the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Type: DWORD;
  Value: 1 [LC8049]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Session/Connection**

- The Client USB Device Redirection Rules policy can fail to apply. The issue occurs when the number of user-entered characters in the policy exceeds 1002. [LC1144]
- Attempts to reconnect to a VDA session after a network interruption might fail. The issue occurs after upgrading VDA to Version 7.8. [LC5040]
- With Framehawk enabled, the scroll button on a mouse might not perform any action in a XenDesktop 7.8 VDA session. The corresponding VDA side fix is available in XenDesktop 7.9. [LC5302]
- A VDA might experience a fatal exception of type 0x50 (Page_Fault_In_NonPaged_Area) on Citrix display driver vdodk.sys. [LC5074]
- When AppDisk is attached to a virtual machine that is running on a non-English version of the Microsoft Windows operating system, a "Restart Now or Restart Later"prompt might appear. With this fix, the prompt disappears. [LC5403]
- After reconnecting to a disconnected multiple monitor session, the display screens turn black and custom settings revert to the defaults. [LC5556]
- After upgrading a VDA from Version 7.6.300 to Version 7.8, clipboard sync might stop working. [LC5699]
- With Framehawk enabled, the Scroll button on a mouse might not perform any action in a XenDesktop 7.9 VDA session. [LC5779]
- When configured for Federated Authentication Services, a VDA might stop accepting connections and become unresponsive at the "Welcome"screen until it is restarted. [LC5978]
- Citrix Receiver might not progress beyond "Connection Established. Negotiate Capabilities" when launching an app. [LC6021]
- Changes you make to "Advanced System Settings"under "Visual Effects"apply to the current VDA session but might not be retained for subsequent sessions. To make such changes persistent, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Type: DWORD;
  Value: 0 [LC6163]
- Attempts to disconnect from a RemotePC session running on a touch-enabled device can result in a black screen that cannot be recovered. [LC6384]
- Citrix Receiver for Linux might not support Spanish DNIe identity cards. [LC6547]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When locking a remote PC session with SecureDoc installed on Windows 10, the lock screen appears for up to two minutes. During that time, you cannot interact with the session. [LC6668]
- When you disconnect and reconnect to a Citrix Receiver for Mac session several times while playing, the audio might not work. [LC6678]
- A removable client drive might not be returned by the WFAPI SDK on the VDA for Desktop OS. [LC6877]
- A gray screen might appear when using legacy graphics mode on a XenDesktop 7.13 Windows 7 VDA. [LC7477]
- When you switch sessions between multiple monitors in full-screen mode with legacy graphics mode enabled and without Desktop Viewer configured, only one monitor might appear to be running the session. [LC7907]

#### System Exceptions

- The VDA for Server OS might experience a fatal exception on TDICA.sys, displaying a blue screen. [LC6898]
- Servers might experience a fatal exception, displaying a blue screen, on vdtw30.dll with stop code 0xc0000006. [LC7608]
- VDAs might experience a fatal exception, displaying a blue screen, on tdica.sys with a bugcheck code. [LC7632]
- This fix addresses a memory issue with the wdica.sys file that can cause servers to exit unexpectedly. [LC7666]

#### Smart Cards

- When switching between user sessions and Microsoft Remote Desktop sessions, in-session smart card-aware applications such as Microsoft Outlook and Microsoft Word might not be able to use smart cards. As a result, various error messages might appear. Also, testing the in-session smart card support with "CertUtil /scinfo"in a Command window might result in the following error message:

  "The Microsoft Smart Card Resource manager is not running."[LC5839]
- Smart card pass-through might fail intermittently. [LC6147]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### User Experience

- If you open a spreadsheet in Excel 2010 with more than one workbook, the taskbar displays only the most current workbook. [LC5370]
- Only the top left corner of the screen displays when using legacy graphics mode on a XenDesktop 7.11 Windows 7 VDA. [LC6532]
- When performing an insert operation between two Microsoft Excel 2010 worksheets running on a Version 7.9 VDA, the Excel window might become unresponsive. [LC7481]

#### User Interface

- When using the Connection Center to log off from a seamless session with unsaved data, a black window appears with the following message:

  "Programs still need to close"- with the two options - "Force Logoff"or "Cancel."The "Cancel" option does not work.

  After installing this fix, the Cancel option works as designed. [LC6075]
- With the "Automatic keyboard display"policy set to enabled and the "Launch touch-optimized desktop"policy set to prohibited, starting a published desktop from an iPad can cause the document viewer to display at 80%. When you close certain applications on the desktop, the document viewer can display at 100%. [LC6460]
- If you open a spreadsheet with more than one workbook in Excel 2010, the taskbar displays only the most current workbook. [LC7557]

### VDA for Server OS

#### Content Redirection

- Attempting to capture images using DirectShow fails, causing the application to exit unexpectedly. [LC6667]

#### Installing, Uninstalling, Upgrading

- After upgrading from VDA 7.11 for Desktop OS to VDA 7.12 for Desktop OS, the following error message might appear while launching certain application.

  "wfapi.dll is missing"[LC6874]
- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7555]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Certain WMI classes might be renamed after installing Version 7.12 or 7.13 of the VDA on a non-English version of the Microsoft Windows operating system. [LC7587]

### Printing

- Citrix Print Manager exits unexpectedly when attempting to map a network printer using the CreateClientPrinter command. [LC4685]
- When you attempt to print two copies or more of a document, only one copy might print. The issue occurs if "Use only printer model specific drivers"is configured in the Citrix policy "Universal print driver usage"and if "Enabled with no fallback to Windows' native remote printing" is configured in the Citrix policy "Universal Print Server enable."[LC6023]
- The Citrix Print Manager service (cpsvc.exe) might become unresponsive and exit unexpectedly when new users log on. [LC6933]
- After upgrading the VDA from Version 7.9 to Version 7.12 or later, attempts to print from Microsoft Internet Explorer by using the Citrix Universal Print Driver might print only to tray 1 instead of printing to the tray that is selected. [LC7463]

### Server/Site Administration

- If users move between sessions that are on different network subnets, the printer list contains printers from both subnets, instead of the subnet to which users are currently logged on. [LC2308]
- The following error message might appear for child domain users while launching an application through Web Interface:

  "You have not been granted access to this published application."[LC7566]
- Changes you make to "Advanced System Settings"under "Visual Effects"apply to the current VDA for Desktop OS session but might not be retained for subsequent sessions. To make such changes persistent, set the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Type: DWORD;
  Value: 1 [LC8049]

### Session/Connection

- On systems with Fix LC2702 (included in Hotfix Rollup Pack 6) applications can fail to save on client mapped drives and generate corrupt files instead. [LC3976]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Launching a process with WinDbg.exe might fail when Streaming Profiler or Offline Plugin is installed. The issue occurs because RadeAPHook hooks the setting for HKEY_LOCAL_MACHINE\SOFTWARE\Mic NT\CurrentVersion\Image File Execution Options\<*processname*> and HKEY_LOCAL_MACHINE\SOFTWARE\W NT\CurrentVersion\Image File Execution Options\<*processname*>.

  To enable the fix, create the following registry key:

- *For 32-bit Windows:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook;
  Name: EnableReadImageFileExecOptionsExclusionList;
  Type: Reg_SZ;
  Value: *<List of executables to be excluded from hooking with respect to the Image File Execution Options setting, separated by commas without spaces. For example, windbg.exe,application_1.exe.>*

- *For 64-bit Windows for 32-bit applications:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  Name: EnableReadImageFileExecOptionsExclusionList
  Type: Reg_SZ
  Value: *<List of executables to be excluded from hooking with respect to the Image File Execution Options setting, separated by commas without spaces. For example, windbg.exe,application_1.exe.>*

  *[LC4750]

- When starting a new session, attempts by the Citrix Audio Redirection Service to connect to a virtual channel session that contains invalid information might fail. [LC5024]

- With Framehawk enabled, the scroll button on a mouse might not perform any action in a XenDesktop 7.8 VDA session. The corresponding VDA side fix is available in XenDesktop 7.9. [LC5302]

- After upgrading a VDA from Version 7.6.300 to Version 7.8, clipboard sync might stop working. [LC5699]

- With Framehawk enabled, the Scroll button on a mouse might not perform any action in a XenDesktop 7.9 VDA session. [LC5779]

- When configured for Federated Authentication Services, a VDA might stop accepting connections and become unresponsive at the "Welcome"screen until it is restarted. [LC5978]

- Changes you make to "Advanced System Settings"under "Visual Effects"apply to the current VDA session but might not be retained for subsequent sessions. To make such changes persistent, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Type: DWORD;
  Value: 0 [LC6163]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The following warning message might appear in the system event log when launching XenApp 7.6 Long Term Service Release Cumulative Update 2 VDA for Server OS or the previous versions:

  "An attempt to connect to the SemsService has failed with error code 0x2."[LC6311]

- A non-operational XenApp session might be created when a Remote Desktop session takes over a console session on a VDA for Server OS. [LC6617]
- Attempts to reconnect to a session can fail intermittently and cause the VDAs for Server OS to go into "Initializing"status. The issue occurs when the VDA is registered again with a Delivery Controller. [LC6647]
- When locking a remote PC session with SecureDoc installed on Windows 10, the lock screen appears for up to two minutes. During that time, you cannot interact with the session. [LC6668]
- When you disconnect and reconnect to a Citrix Receiver for Mac session several times while playing, the audio might not work. [LC6678]
- When you launch a published application on Microsoft Windows Server 2016, a black screen might appear for several seconds before the application becomes visible. [LC7947]

**Smart Cards**

- When switching between user sessions and Microsoft Remote Desktop sessions, in-session smart card-aware applications such as Microsoft Outlook and Microsoft Word might not be able to use smart cards. As a result, various error messages might appear. Also, testing the in-session smart card support with "CertUtil /scinfo"in a Command window might result in the following error message:

  "The Microsoft Smart Card Resource manager is not running."[LC5839]

**System Exceptions**

- The VDA for Server OS might experience a fatal exception on TDICA.sys, displaying a blue screen. [LC6898]
- Servers might experience a fatal exception, displaying a blue screen, on vdtw30.dll with stop code 0xc0000006. [LC7608]
- VDAs might experience a fatal exception, displaying a blue screen, on tdica.sys with a bugcheck code. [LC7632]
- This fix addresses a memory issue with the wdica.sys file that can cause servers to exit unexpectedly. [LC7666]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### User Experience

- If you open a spreadsheet in Excel 2010 with more than one workbook, the taskbar displays only the most current workbook. [LC5370]
- When performing an insert operation between two Microsoft Excel 2010 worksheets running on a Version 7.9 VDA, the Excel window might become unresponsive. [LC7481]

#### User Interface

- When using the Connection Center to log off from a seamless session with unsaved data, a black window appears with the following message:

  "Programs still need to close"- with the two options - "Force Logoff"or "Cancel."The "Cancel" option does not work.

  After installing this fix, the Cancel option works as designed. [LC6075]
- With the "Automatic keyboard display"policy set to enabled and the "Launch touch-optimized desktop"policy set to prohibited, starting a published desktop from an iPad can cause the document viewer to display at 80%. When you close certain applications on the desktop, the document viewer can display at 100%. [LC6460]
- If you open a spreadsheet with more than one workbook in Excel 2010, the taskbar displays only the most current workbook. [LC7557]

### Virtual Desktop Components - Other

- The session type of the VM hosted app session of a user might change from "Application"to "Desktop"unexpectedly. As a result, attempts to reconnect to an application fail. [LC5461]
- When launching an App-v package using the Microsoft App-V 5.0 infrastructure integrated with XenDesktop, the App-V package might fail to synchronize and the following exception occurs:

  "Cannot start <applicationname>"[LC5483]
- Attempts to load an App-V application through the network might result in the following error message:

  "Index was out of range. Must be non-negative and less than the size of the collection."[LC5828]
- After upgrading from Version 7.7 of XenApp to Version 7.8, attempts to launch App-V applications might fail. The issue occurs when the value of the "TargetIn"boolean is set to "0"instead of "1." Also, setting the value manually might not have any effect. When you refresh the application, it might revert. [LC5861]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When you add an App-V package that contains multiple applications to Citrix Studio and publish all the applications inside the package, only the first application might start in the user session. [LC5863]
- The App-V application can be started only by a single user. Attempts by another user to start the same application on the same server might fail. [LC6414]
- App-V-sequenced applications might not be contained within the actual App-V package even if they are referenced by the package (InTarget=False.) As a result, the application launch does not apply to any dependent Connection Groups that are required for that application to function correctly. [LC6534]
- After upgrading from XenApp/XenDesktop 7.11 to 7.12, existing Delivery Group restart schedules are not being honored. [LC6766]
- Attempts to launch App-V applications from a mapped drive might fail. [LC6961]
- Attempts to publish App-V applications might fail.

  [LC7421]
- Attempts to create machine catalogs might fail when Microsoft Message Queuing is installed on the VDA master image and the following error message appears in Citrix Studio:

  "Image Preparation did not complete. Status 'NotSet"[LC7528]
- Attempts to launch App-V applications in Single Admin mode might fail. The issue occurs when the application name contains special characters. [LC7897]

### Other fixed issues

- Group policies in Citrix Studio are missing if the UPM - Software\Microsoft\Speech_OneCore policy under Profile Management > Registry > Default Exclusions was configured before upgrading the Delivery Controller from 7.11 to 7.14, from 7.12 to 7.14, or from 7.13 to 7.14. [UPM-538]
- Attempts to install or upgrade to Session Recording Version 7.14 using the XenApp and XenDesktop full product installer fail on Windows Server 2008 and the following error message appears: "Microsoft Message Queuing failed."[SRT-1782]
- After upgrading Controllers, the power state of a VDA might indicate "Unknown."[DNA-37756]

## Known issues

July 2, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Known issues that are described in the 7.15 baseline, and in the 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.

### Known issues in Cumulative Update 9

There are no new known issues in CU9.

### Known issues in Cumulative Update 8

- When using this VDA version, Citrix policies applied to a machine by OU can sometimes fail to apply. [CVADHELP-19826]
- If the secure XML keys are not created in the registry, the local host cache database might be missing or corrupted. To recreate the local host cache databases, see CTX228758. [LCM-9660]
- If StoreFront is installed on the same server as the Delivery Controller, attempts to upgrade Storefront after upgrading the Delivery Controller will fail. However, upgrading StoreFront succeeds if you upgrade Storefront before upgrading the Delivery Controller.

  As a work around, if you need to upgrade Storefront after upgrading the Delivery Controller, stop Citrix Telemetry Service before running the Storefront upgrade. [LCM-9706]
- 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]

### Known issues in Cumulative Update 7

- When attempting to update the Licensing CEIP option using the `Set-LicCEIPOption` cmdlet, the operation fails with a `CommunicationError`. As a workaround, the CEIP option can be enabled through Citrix Licensing Manager. For more information, see Knowledge Center article CTX220679.

### Known issues in Cumulative Update 6

- Citrix Workspace app 1912 and later does not support HDX-FlashRedirection, which is part of the XenApp and XenDesktop 7.15 LTSR CU6 release. HDX-FlashRedirection is available only with Citrix Workspace app 1911 and earlier. You can also use Citrix Receiver 4.9 LTSR with 7.15 LTSR CU6. [LCM-8140]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The CU6 release includes a later version of the Self-Service Password Reset service. The later version of the service introduces a new functionality that detects the security configurations of the central store. When you create the central store or the service on Windows Server 2008 R2, a warning dialog appears. The issue occurs because Windows Server 2008 R2 does not support SMB encryption and thus fails the security detection. The issue does not block further actions. As a workaround, create the central store and the service on Windows Server 2012 or later that supports SMB encryption. [LCM-8179]
- Citrix Director might fail to enumerate policy information when you view session details associated with a 7.15 LTSR CU6 VDA. The issue occurs when the version of Citrix Director is earlier than VDA version 7.15 LTSR CU6. As a workaround, use Citrix Director version 7.15 LTSR CU6. Alternatively, modify the following registries on the VDA and then restart it.

  - Registry Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

    Name: SaveRsopToFile

    Type: REG_DWORD

    Value: 1
  - Registry Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

    Name: SaveRsopToMemory

    Type: REG_DWORD

    Value: 0
  - Registry Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

    Name: SaveRsopToRegistry

    Type: REG_DWORD

    Value: 0

  [LCM-8201]

### Known issues in Cumulative Update 5

- Attempts to upgrade a Windows 7 VDA from 7.6 LTSR CU8 to this release might result in a fatal exception, displaying a blue screen. No workaround is available.

  Perform any one of the following workarounds when you upgrade a Windows 7 VDA from 7.6 LTSR CU8 to this release:

  - Uninstall 7.6 LTSR CU8 and then install 7.15 LTSR CU5.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - Manually disable the Citrix WDDM driver on Windows 7 machines and then upgrade to this release. To disable the Citrix WDDM driver, perform the following steps:
    * Open `Device Manager`.
    * Click `Display adapters` and then expand the selection.
    * Right-click `Citrix Display Driver (Citrix Systems - WDDM)` and then select `Disable`. [LCM-6798]

- On a VDA that is running Windows 7 or Windows Server 2008 R2, a VC++ error might occur when you launch an App-V application. The issue occurs because the App-V client relies on a specific version of VC++ 2013 to function.

  As a workaround, apply the Microsoft hotfix https://support.microsoft.com/en-in/help/4014009/march-2017-servicing-release-for-microsoft-desktop-optimization-pack. Alternatively, install the App-V client first and then install the Cumulative Update 5 version of the VDA. [LCM-6809]

- Citrix Scout might fail to run health checks for Delivery Controllers that are running Windows 2008 R2. As a result, the following message appears: Check failed. The issue occurs when there is no internet connectivity on the Delivery Controller. As a workaround, download the check scripts and then run the scripts manually. For details, see the Knowledge Center article CTX263240. [LCM-6837]

### Known issues in Cumulative Update 4

- The custom admin scripts of the Citrix XenDesktop Admin module that targets PowerShell 2.0 might fail. The issue occurs because the module no longer supports PowerShell 2.0.
- On the Spanish version of the Microsoft Windows operating system, the component initialization might fail. The issue occurs when you run the preliminary site tests while upgrading the Delivery Controller from any Version 7.6 Cumulative Update to Version 7.15 Cumulative Update 4.
- Citrix Director might not display all the rows of records in the Trends tables. Director displays a limited number of records followed by an extra empty space. However, you can scroll down to find the remaining records. [LCM-5841]

### Known issues in Cumulative Update 3

- For a list of Citrix known issues with the Windows 10 October 2018 Update (v1809), see Knowledge Center article CTX234973.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- In an AWS environment, Server VDA rollbacks to a XenApp and XenDesktop 7.15 LTSR CU2 image or snapshot might fail. As a workaround, extend the rollback timeout to a timeout value of 30 minutes with the following PowerShell cmdlet:

  Set-ProvServiceConfigurationData –Name ImageManagemntPrep_preparationTimeout –Value 30 [LCM-4364]

- After you upgrade to XenApp and XenDesktop 7.15 LTSR CU3, a site upgrade failure might occur when the site's License Server is not updated to the version that is released as a part of CU3. There are no notifications by the product installer during the upgrade. [LCM-5467]

- After completing the XenDesktop wizard, the Machine Catalog in Studio is empty and the streaming IP address appears instead of the management IP address, which is incorrect. To use the management IP address, set the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices
Name: UseManagementIpInCatalog
Type: DWORD
Value: 1

[LD0125]

### Known issues in Cumulative Update 2

- On Windows 2016 VDAs, users logging in with smart cards might not be able to see all available users at logon. The issue is the result of the default size of the logon window, which is 600x520. For more information and a workaround, see Knowledge Center article CTX204070. [LCM-3951]

- For a list of known issues with Windows 10 Redstone 4 (Insider Preview builds), see Knowledge Center article CTX231942.

- After upgrading Citrix Studio to Version 7.15 Cumulative Update 2, the policies might not be localized. For more information, see Knowledge Center article CTX234711. [LC9613]

- 7.15 LTSR CU2 sessions might launch as a black screen. The issue occurs with sessions running on XenApp and XenDesktop 7.15 LTSR CU2 and 7.17 VDAs when Profile Management is enabled. For more information and a workaround, see Knowledge Center article CTX235100. [LC9648]

### Known issues in Cumulative Update 1

- User-configurable registry keys such as picadm and MultiStreamIca under HKEY_LOCAL_MACHINE might be deleted or overwritten by the default value while installing Cumulative Updates. [CVADHELP-16481]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The StoreFront management console does not open after an upgrade to StoreFront 3.12.1000 (XenApp and XenDesktop 7.15 LTSR CU1) from StoreFront 3.12 (XenApp and XenDesktop 7.15 LTSR), or after an install of StoreFront 3.12.1000. The StoreFront management console displays the error "MMC could not create the snap-in. The snap-in might not have been installed correctly."To work around this issue, follow the steps described in CTX233206. [LC8935]
- When installing a driver signed with a SHA-256 certificate on a Windows 7 or Windows Server 2008 R2 machine, a Microsoft WHQL (Windows Hardware Quality Labs) message might appear. To resolve the issue, install the following Microsoft hotfixes on the machine:
  - Windows 7 (one hotfix): Microsoft hotfix
  - Windows Server 2008 R2 (two hotfixes): hotfix one and hotfix two [LCM-2836]
- When the Citrix Telemetry Service is disabled or stopped, and you use a metainstaller to upgrade XenApp and XenDesktop 7.15 LTSR to Cumulative Update 1 (CU1), the following warning message might appear:
  "We cannot start the Citrix service that enables you to enroll in Call Home. See CTX218094 for guidance."[LCM-3642]
- Profile Management can cause a black screen to appear when you attempt to launch a Microsoft Windows 10 session. With this fix, you must configure the policy "Directories to synchronize"and add the folder "*AppData\Local\Microsoft\Windows\Caches*."For additional information and a workaround, see Knowledge Center article CTX234144. [LC9030]

### Known issues in 7.15 LTSR (initial release)

The XenApp and XenDesktop 7.15 LTSR release contains the following issues:

#### VDA

- If SAS notification⋆ is enabled, a user with multiple monitors connecting to an existing session at the console might find the monitor layout is not restored correctly. For example, if the right monitor is 1 and selected as the main monitor and the left monitor is 2, the user might find the positions swapped when reconnecting. This issue affects only RemotePC users with a physical desktop. This is due to incompatibility between two features. [CVADHELP-14249]

  ⋆ SAS notification is the feature that announces to a console user on RemotePC that another user is attempting to connect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### App-V

- In Studio, when deleting one or more App-V applications from the Applications node, or from a selected Delivery Group, the message "An unknown error occurred"appears. You can safely ignore the message; the applications are deleted. [DNA-29702]
- You cannot remove an App-V application from a Delivery Group if a child process launched for that application, but failed to close when the application closed. The error indicates the application is in use. To determine the process name, run Get-AppVVirtualProcess. Then end that process with Task Manager or Stop-AppVClientPackage. [DNA-23624]
- When you remove an App-V package from the Application Library, it is removed from the Studio display, but not from the VDA. As a workaround, run the following cmdlets from the VDA, with elevated administrative privilege:

  Import-Module AppvClient
  Get-AppVClientPackage -all
  #Identify the PackageId and VersionId of the package to be removed
  Remove-AppVClientPackage -PackageId <*packageid*> -VersionId <*versionid*> [DNA-47379]
- Due to the way that Microsoft App-V behaves, when you publish multiple sequenced versions of the same app using the single admin or the dual admin management method, only one version of the app is able to launch at a time per user on the VDA. Whichever version a user launches first, determines the version which runs later for them. The same behavior occurs even when Citrix components are not involved and the user starts the sequenced apps from desktop shortcuts which point to different paths. To date we (Citrix) have seen this occur for different versions of Mozilla Firefox and Google Chrome browsers. [APPV-60]

### Citrix Director

- In a multiple session environment, when you navigate to **Filters** > **Sessions** > **All** and log off from a session, the session logs off. When you select another session with the same user name for the second time and attempt to log off, this error message appears:

  **Data source unresponsive or reported an error. View Director Server event logs for further information.** [LC8826]

### Install and upgrade

- When you upgrade VDA 7.14 to VDA 7.15, the keys created under the registry key HKEY_LOCAL_MACHINE\Softw for Citrix policy settings that are applied using **Administrative Template** might be deleted from the VDA. [LCM-3876]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- When installing components using the AutoSelect application on the installation media, the autorun.log file might contain errors and exceptions about insufficient rights. Provided the installation completed successfully, you can ignore these errors. However, to avoid them, launch AutoSelect using **Run as administrator**. [DNA-45937]
- When upgrading a XenDesktop 5.6 deployment to XenDesktop 7.15 LTSR, group policy is missing. As a workaround, first upgrade from XenDesktop 5.6 to XenDesktop 7.13. Then upgrade from 7.13 to 7.15 LTSR [DNA-44818]
- When installing a Controller and you select **I want to connect to Smart Tools and Call Home** on the **Smart Tools** page of the installation wizard, Call Home might not be enabled. As a workaround, either use the schedule feature in Citrix Scout or enable Call Home using PowerShell. [CAM-9907]
- When installing a Delivery Controller on Windows Server 2012 R2 or Windows Server 2016, if you choose to connect to Smart Tools, and have more than one organization linked with your Citrix Cloud account, the logon process may not complete after you enter your Citrix Cloud credentials. As a workaround, complete one of the following:
  - Ensure the Windows Server and Internet Explorer have the latest updates.
  - Clear the Internet Explore browser option: Internet Options > Security > Local Intranet > Sites> Include all sites that bypass the proxy server. [CAM-9816]
- If StoreFront was originally installed using the executable from the installation media, StoreFront does not appear as eligible for upgrade when you use the full-product installer for a later version. As a workaround, upgrade StoreFront using the executable from the installation media. [#DNA-47816]
- When upgrading the Delivery Controller from a version earlier than 7.13, to version 7.13 and later, an error (exception) may be seen if the "Auto client reconnect timeout"setting is configured in any of the policies. This error happens if the "Auto client reconnect timeout"setting value is outside the permitted range 0 and 300, which was first introduced in version 7.13. To prevent this error, use the Citrix Group Policy PowerShell Provider to unconfigure the setting, or to set it to a value within the specified range. For an example, see CTX22947. [DNA-52476]
- When you select machines and add them to existing Delivery Groups, Studio allows you to add machines from incompatible Machine Catalogs to the same Delivery Group. (If you first select a Delivery Group and add machines to it, Studio correctly prevents machines from incompatible Machine Catalogs being added.) [DNA-39589]

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

old one which changes the `DeleteOnTermination` flag to *False*. [PMCS-4953]

- When using a Federated Authentication Service in-session certificate to authenticate a TLS 1.1 (or earlier) connection, the connection can fail. Event ID 305 is logged, indicating an unsupported hash ID. The Federated Authentication Service does not support the SHAMD5 hash. To work around this issue, use TLS 1.2 connections. This issue affects XenApp and XenDesktop 7.9 through this version. [DNA-47628]
- The policy settings are not saved in the Printer driver mapping and compatibility policy. As a workaround, use the Citrix Group Policy PowerShell Provider to edit this setting. For more information on the workaround, see CTX226589. [DNA-47423]
- Windows Event Log Error: "Windows is unable to verify the image integrity of the file MfApHook64.dll". For more information, see CTX226397. [HDX-9063]
- 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]
- Published content will not start successfully when initiated from Citrix Receiver. Content launched through the StoreFront web client (or Web Interface) launches as expected. [LC6316, RFWIN-4957]
- 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. [DNA-37964]
- Multicast might fail to display video when using Citrix Receiver for Windows newer than version 4.6. Audio is still available. As a workaround, add this registry key on the endpoint:

HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream;
Name: DisableVMRSupport;
Type: DWORD;
Value: 4; [HDX-10055]

### Printing

- Stopping or restarting the Citrix Print Manager Service may leave the CpSvc.exe process in an unresponsive state. As a workaround, stop the CpsSvc.exe process before stopping or restarting the service in the Services snap-in, or restart the VDA to avoid this issue. [HDX-10071]
- 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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Windows 10 and Windows 8 platforms. For more information, see Knowledge Center article CTX213540. [335153]

### Session Recording

- When Machine Creation Services (MCS) or Provisioning Services (PVS) creates multiple VDAs with the configured master image and Microsoft Message Queuing (MSMQ) installed, those VDAs can have the same QMId under certain conditions. This might cause various issues, for example:
  - Sessions might not be recorded even if the recording agreement is accepted.
  - The Session Recording Server might not be able to receive session logoff signals and therefore, sessions might always be in Live status.

See the Session Recording installation articles for a workaround. [528678]

### Third-party issues

- Citrix and Microsoft have identified an issue when starting seamless applications from a Server VDA running Windows Server 2016. When a user starts an application published from this VDA, Citrix Receiver displays a black screen covering the workspace of the monitor for several seconds before starting the application. For more information, see CTX225819.

  **Warning**: If you are using Azure Active Directory (AAD), do not make the registry change described in CTX225819. Making this change may cause session launch failures for AAD users. [HDX-5000]

- In a stress test environment, out of 20,000 logons, Microsoft Windows WinLogon.exe might crash intermittently with a frequency of <0.001%. [HDX-9938]

## Third party notices

July 13, 2018

This release of XenApp and XenDesktop may include third party software licensed under the terms defined in the following documents:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**XenApp and XenDesktop Third Party Notices (PDF Download)**

**Non-Commercial Software Disclosure For FlexNet Publisher 2016 R1 (11.14.0.0)**

**FLEXnet Publisher Documentation Supplement: Open Source Software Licenses applicable to FlexNet Publisher 11.14.0 (PDF Download)**

**Session Recording Third Party Notices (PDF Download)**

## Deprecation and removals

April 15, 2021

The announcements in this article are intended to give you advanced notice of platforms, Citrix products, and features which are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. This list is subject to change in subsequent releases and might not include every deprecated feature or functionality.

The following platforms, Citrix products, and features are *deprecated*. This does not mean that they are removed immediately. Citrix continues to support them in this XenApp and XenDesktop 7.15 Long Term Service Release (LTSR). Deprecated items will be removed in a Current Release following this LTSR. Alternatives for deprecated items are suggested where possible.

For details about product lifecycle support, see the Product Lifecycle Support Policy article.

| Item | Deprecation announced in | Removed in | Alternative |
|---|---|---|---|
| StoreFront browser support for Microsoft Edge Legacy | 7.15 LTSR CU7 | - | Upgrade to Microsoft Edge (based on Chromium). |
| Browser content redirection | 7.15 LTSR CU7 | - | Upgrade to 1912 LTSR. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Item | Deprecation announced in | Removed in | Alternative |
|---|---|---|---|
| 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). | 7.15 LTSR CU6 | 7.15 LTSR CU6 | Use the Citrix Licensing Manager. |
| Removal of Citrix Smart Tools Agent from Citrix Virtual Apps and Desktops installation media. | 1903 and 7.15 LTSR CU4 | 7.15 LTSR CU4 | — |
| Citrix Receiver for Web classic experience ( “green bubbles”user interface). | 7.15 LTSR (and StoreFront 3.12) | — | Citrix Receiver for Web unified experience. |
| VDAs on Windows 10 version 1511 (Threshold 2) and earlier Windows desktop OS releases, including Windows 8.x and Windows 7 | 7.15 LTSR (and 7.12) | 7.16 | Install desktop OS VDAs on Windows 10 version 1607 (Redstone 1) or newer Semi-Annual Channels. If using 1607 LTSB, we recommend a 7.15 VDA. |
| VDAs on Windows Server 2008 R2 and Windows Server 2012 (including Service Packs). | 7.15 LTSR (and 7.12) | 7.16 | Install server OS VDAs on supported versions such as Windows Server 2012 R2 or Windows Server 2016. |
| Delivery Controllers on Windows Server 2012 and 2008 R2 (including Service Packs). | 7.15 LTSR | — | Install Delivery Controllers on an alternative supported operating system |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Item | Deprecation announced in | Removed in | Alternative |
|---|---|---|---|
| Studio on Windows 7 (including Service Packs). | 7.15 LTSR | 7.18 | Install Studio on an alternative supported operating system. |
| Flash Redirection. | 7.15 LTSR | — | Citrix Workspace app 1912 and later does not support HDX-FlashRedirection, which is part of the XenApp and XenDesktop 7.15 LTSR CU6 release. HDX-FlashRedirection is available only with Citrix Workspace app 1911 and earlier. You can also use Citrix Receiver 4.9 LTSR with 7.15 LTSR CU6. |
| DirectX Command Remoting (DCR). | 7.15 LTSR | 7.16 | Use Thinwire. |
| Citrix Online Integration (Goto product) with StoreFront. | 7.14 (and StoreFront 3.11) | StoreFront 3.12 | From StoreFront 3.12, this feature cannot be configured in the StoreFront management console. If you upgrade to StoreFront 3.12, you can continue to use this feature. To change your configuration, use the PowerShell cmdlet, Update-DSGenericApplications. For more information, see Integrate Citrix Online applications with stores. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Item | Deprecation announced in | Removed in | Alternative |
|---|---|---|---|
| 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 7.13. |
| 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. |
| VDAs on Windows 8.1 and earlier Windows desktop releases. | 7.12 | — | Install server OS VDAs on supported versions such as Windows Server 2012 R2 or Windows Server 2016. |
| XenDesktop 5.6 used on Windows XP. No VDA installations on Windows XP will be supported. | 7.12 | — | Install VDAs on a supported Windows version. |
| 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. |
| Installing core components (other than Studio) on 32-bit machines: Delivery Controller, Director, StoreFront, and License Server. | 7.12 | 7.16 | Use 64-bit machines. |
| Connection leasing. | 7.12 | 7.16 | Use Local Host Cache. |
| Legacy Thinwire mode | 7.12 | 7.16 | Use Thinwire. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Item | Deprecation announced in | Removed in | Alternative |
|---|---|---|---|
| HDX Desktop Composition Redirection (DCR) | 7.12 | — | — |
| 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. |

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

## Section 508 Voluntary Product Accessibility Template

March 11, 2020

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## System requirements

January 5, 2023

### 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 StoreFront, host systems, Citrix Workspace apps and plug-ins, and Provisioning Services) are described in their respective documentation.

**Important:** Review the Prepare to install article before beginning an installation.

> **Note:**
>
> *Support for Windows operating systems: Citrix XenApp and XenDesktop and associated components are supported only on operating system versions that are supported by their manufacturer. Customers might be required to purchase extended support from their operating system manufacturer.

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 CTX119253.

For components and features that can be installed on Windows Servers, Server Core and Nano Server installations are not supported, unless specifically noted.

For components and features that can be used on Windows 10 machines, the following Windows 10 servicing options and editions are supported:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Semi-annual Channel: Pro, Enterprise, Education, Mobile Enterprise (the IoT Core Pro Edition is supported only for Citrix Workspace app).
- Long-term Servicing Channel (LTSC): Enterprise LTSB Edition

For further details, see CTX224843.

### 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 will vary, depending on your configuration. This includes the features you use, plus the number of users, and other factors. Using only the minimum can result in slow performance.

For example, the amount of disk space needed on the Controller for connection leasing (which is enabled by default) depends on the number of users, applications, and the mode: 100,000 RDS users with 100 recently-used applications require approximately 3 GB for connection leases; deployments with more applications may require more space. For dedicated VDI desktops, 40,000 desktops require at least 400-500 MB. In all cases, Citrix suggests providing several GBs of additional space.

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 |
| 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 XenApp and XenDesktop deployment has unique needs. Generally, sizing a

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

XenApp VM is based on the hardware and not the user workloads (except for RAM; you'll need more RAM for applications that consume more). The Citrix Tech Zone contains the latest guidance on VDA sizing.

### Microsoft Visual C++ Runtime versions

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

If you've already installed Citrix components that automatically install the Visual C++ 2015 Runtime, those components will 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 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions*

Requirements:

- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only)
- Microsoft .NET Framework 4.5.2 (4.6 through 4.8 are also supported)
- CU3 and earlier: Windows PowerShell 2.0
- CU4 and later: both Windows PowerShell 2.0 and Windows PowerShell 3.0 or later
- Microsoft Visual C++ 2015 Runtime, 32- 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 supports XenApp and XenDesktop 7.15 LTSR CU6 and later versions.
- SQL Server 2019, Express, Standard, and Enterprise Editions supports Provisioning Services 7.15 LTSR CU7 and later versions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- SQL Server 2017, Express, Standard, and Enterprise Editions.
- SQL Server 2016 SP1 through SP3, Express, Standard, and Enterprise Editions.
- SQL Server 2014 SP1 through SP3, Express, Standard, and Enterprise Editions. By default, SQL Server 2014 SP2 Express is installed when installing the Controller, if an existing supported SQL Server installation is not detected.
- 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, a SQL Server Express database is installed by default for use with the Local Host Cache feature. This installation is separate from the default SQL Server Express installation for the Site database.

For more information, see the following articles:

- Databases
- CTX114501
- Database sizing guidance
- Local Host Cache

### Citrix Studio

Supported operating systems:

- Windows 10 (see edition support in the *Introduction* section)
- Windows 8.1, Professional and Enterprise Editions*
- Windows 7 Professional, Enterprise, and Ultimate Editions*
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions*

Requirements:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.8 are also supported)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Microsoft Management Console 3.0 (included with all supported operating systems)
- Windows PowerShell 2.0 (CU 3 and earlier)
- Windows PowerShell 3.0 or later (CU 4 and later)

### Citrix Director

Supported operating systems:

- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions*

Requirements:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.8 are also supported).
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 only)
- 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 these are not already installed, you are prompted for the Windows Server installation media, then they are 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 Plugin are installed on the VDA (Additional Components section in the installation wizard) and that the Citrix Profile Management Service is 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. You must 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

The recommended optimal screen resolution for viewing Director is 1366 x 1024.

### Virtual Delivery Agent (VDA) for Desktop OS

Supported operating systems:

- Windows 10, (see edition support in the *Introduction* section. The following features are not supported on Windows 10: desktop composition redirection and legacy graphics mode.
- Windows 8.1, Professional and Enterprise Editions*
- Windows 7 SP1, Professional, Enterprise, and Ultimate Editions*

Requirements:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.8 are also supported)
- Microsoft .NET Framework 3.5.1 (Windows 7 only)
- Microsoft Visual C++ 2013 and 2015 Runtimes, 32- and 64-bit
- PowerShell 3.0 or later

Remote PC Access uses this VDA, which you install on physical office PCs. This VDA supports Secure Boot for XenDesktop 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 features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most supported Windows desktop OS editions, Media Foundation support is already installed and cannot be removed. However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party. For more information, see Prepare to install.

During VDA installation, you can choose the HDX 3D Pro mode of the VDA for Windows Desktop OS. That mode is particularly suited for use with DirectX and OpenGL-driven applications and with rich media such as video. See the HDX 3D Pro section for additional support information.

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 Desktop OS on a supported server operating system. See Server VDI for guidance.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Virtual Delivery Agent (VDA) for Server OS

Supported operating systems:

- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, 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 4.5.2 (4.6 through 4.8 are also supported)
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only)
- Microsoft Visual C++ 2013 and 2015 Runtimes, 32- and 64-bit
- PowerShell 3.0 or later

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 will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most Windows Server versions, the Media Foundation feature is installed through the Server Manager (for Windows Server 2012 and later: ServerMediaFoundation; for Windows Server 2008 R2: DesktopExperience). 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.

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

- Flash Redirection
- Windows Media Redirection
- HTML5 Video Redirection
- HDX Realtime Webcam Redirection

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

### Hosts / virtualization resources

Some XenApp and XenDesktop features may not be supported on all host platforms or all platform versions. For example, AppDisks are supported with XenServer, VMware, and System Center Virtual Machine Manager hosts. See the feature documentation for details.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

**IMPORTANT:** The following *major.minor* versions are supported, including updates to those versions. CTX131239 contains the most current hypervisor version information, plus links to known issues.

#### XenServer

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

#### 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.

#### 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.

#### Amazon Web Services (AWS)

- You can provision applications and desktops on supported Windows server operating systems.
- Citrix supports the Amazon Relational Database Service (RDS). See the Citrix Ready marketplace and Citrix and AWS for additional information.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### CloudPlatform

- The minimum supported version is 4.2.1 with hotfixes 4.2.1-4.
- Deployments were tested using XenServer 6.2 (with Service Pack 1 and hotfix XS62ESP1003) and vSphere 5.1 hypervisors.
- CloudPlatform does not support Hyper-V hypervisors.
- CloudPlatform 4.3.0.1 supports VMware vSphere 5.5.
- See the CloudPlatform documentation (including the Release Notes for your CloudPlatform version) for more information.

#### Microsoft Azure

#### Microsoft Azure Resource Manager

### 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
- Windows Server 2003
- Windows 2000 native (not supported for domain controllers)

### HDX

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

Echo cancellation is supported on Citrix Workspace app for Windows.

See the specific HDX feature support and requirements below.

#### HDX Desktop Composition Redirection

The Windows user device or thin client must support or contain:

- DirectX 9
- Pixel Shader 2.0 (supported in hardware)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 32 bits per pixel
- 1.5 GHz 32-bit or 64-bit processor
- 1 GB RAM
- 128 MB video memory on the graphic card or an integrated graphics processor

HDX queries the Windows device to verify that it has the required GPU capabilities, and then automatically reverts to server-side desktop composition if it does not. List the devices with the required GPU capabilities that do not meet the processor speed or RAM specifications in the GPO group for devices excluded from Desktop Composition Redirection.

The minimum available bandwidth is 1.5 Mbps; the recommended bandwidth is 5 Mbps. Those values incorporate end-to-end latency.

#### HDX Windows Media delivery

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and realtime 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 Flash Redirection

> **Note:**
>
> Citrix Workspace App 1912 and later does not support HDX-FlashRedirection, which is part of the XenApp and XenDesktop 7.15 LTSR CU6 release. HDX-FlashRedirection is available only with Citrix Workspace App 1911 and earlier.

The following clients and Adobe Flash Players are supported:

- Citrix Workspace app for Windows (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for Other Browsers, sometimes referred to as an NPAPI (Netscape Plugin Application Programming Interface) Flash Player.
- Citrix Workspace app for Linux (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for other Linux or Adobe Flash Player for Ubuntu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Citrix Online plug-in 12.1 (for legacy Flash Redirection features) - Legacy Flash Redirection features require Adobe Flash Player for Windows Internet Explorer (sometimes referred to as an ActiveX player).

The major version number of the Flash Player on the user device must be greater than or equal to the major version number of the Flash Player on the server. If an earlier version of the Flash Player is installed on the user device, or if the Flash Player cannot be installed on the user device, Flash content is rendered on the server.

The machines running VDAs require:

- Adobe Flash Player for Windows Internet Explorer (the ActiveX player)
- Internet Explorer 11 (in non-Modern UI mode). You can use Internet Explorer versions 7-10, but Microsoft supports (and Citrix recommends using) version 11. Flash redirection requires Internet Explorer on the server; with other browsers, Flash content is rendered on the server.
- Protected mode disabled in Internet Explorer (Tools > Internet Options > Security tab > Enable Protected Mode check box cleared). Restart Internet Explorer to effect the change.

#### HDX 3D Pro

When installing a VDA for Windows Desktop OS, you can choose to install the HDX 3D Pro version.

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); and with Microsoft Hyper-V in Windows Server 2016 where it is referred to as Discrete Device Assignment (DDA).
- vGPU is available with Citrix XenServer, Nutanix AHV, and VMware vSphere; see https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html.

Citrix recommends that the host computer have 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 are supported by the GPU on the host computer. However, for optimum performance with the minimum recommended user device and GPU specifications, Citrix recommends a maximum monitor resolution for user devices 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.

#### HDX video conferencing requirements for webcam video compression

Supported clients: Citrix Workspace app for Windows, Citrix Workspace app for Mac, and Citrix Workspace app for Linux.

Supported video conferencing applications:

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HDFaces
- Google+ Hangouts
- IBM Sametime
- Media Foundation-based video applications on Windows 8.x, Windows Server 2012, and Windows Server 2012 R2
- Microsoft Lync 2010 and 2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.
- Webcam drivers, obtained from the camera manufacturer if possible.

## Session Recording

### Session Recording administration components

You can install the Session Recording administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) on a single server or on different servers.

#### Session Recording Database

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*

Supported Microsoft SQL Server versions:

- Microsoft SQL Server 2016 SP1 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2014 SP2 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2012 SP3 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2008 R2 SP3 Enterprise, Express, and Standard editions

Requirement: .NET Framework 4.7.2

#### Session Recording Server

Supported operating systems:

- Windows Server 2016

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*

Other requirements:

- Internet Information Services (IIS) 10, 8.5, 8.0, or 7.5
- .NET Framework Version 4.7.2
- If the Session Recording Server uses HTTPS as its communications protocol, add a valid certificate. Session Recording uses HTTPS by default, which Citrix recommends.
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled.
- For Administrator Logging: Latest version of Chrome, Firefox, or Internet Explorer 11

#### Session Recording Policy Console

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Requirement: .NET Framework 4.7.2

### Session Recording Agent

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*
- Windows 10
- Windows 8.1*
- Windows 7 SP1*

Requirements:

- XenApp/XenDesktop 7.15 with Platinum license

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- XenApp/XenDesktop 7.6.4000 with Platinum license (VDA for Windows Server OS only; VDA for Windows Desktop OS not supported)
- .NET Framework 4.7.2
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled

### Session Recording Player

Supported operating systems:

- Windows 10
- Windows 8.1*
- Windows 7 SP1*

Requirement: .NET Framework 4.7.2

For optimal results, install Session Recording Player on a workstation with:

- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- 2GB RAM minimum; additional RAM and CPU/GPU resources can improve performance when playing graphics-intensive recordings, especially when recordings contain many animations

The seek response time depends on the size of the recording and your machine's hardware specifications.

### 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 2016
- Windows Server 2012 R2 and 2012
- Windows Server 2008 R2 SP1*

Requirement: Microsoft Visual C++ 2013 Runtime, 32- and 64-bit

For VDAs for Windows Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Other

StoreFront 3.12.2000 is the minimum supported version with this release. To use the zone preference feature, you must be using minimum StoreFront 3.12.2000 or later and NetScaler Gateway 11.0-65.x.

> **Note:**
>
> When you attempt to install StoreFront 3.12.5000 using a silent installation, the installer might exit unexpectedly. The issue occurs when PowerShell version 3.0 or later is not installed on the server.

When using Provisioning Services with this release, the minimum supported Provisioning Services version is 7.15.3.

The minimum supported License Server version for XenApp and XenDesktop 7.15 LTSR CU6 is 11.15.0.0 Build 24100. For more information on previous CU versions, see Licensing.

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 XenApp or XenDesktop core component installed), that machine must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.

If you plan to use Citrix Scout on Windows 7 or Windows 2008 R2 machines, you must install PowerShell 3.0 on those machines. For complete requirements, see Citrix Scout.

Multiple network interface cards are supported.

By default, Citrix Workspace app for Windows is installed when you install a VDA.

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

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

See the Self-Service Password Reset documentation for support and requirements information.

Client folder redirection - Supported operating systems:

- Server: Windows Server 2008 R2 SP1, Windows Server 2012, and Windows Server 2012 R2
- Client (with latest Citrix Workspace app for Windows): Windows 7, Windows 8, and Windows 8.1

Mixed DPIs with multi-monitors. The use of different DPIs between monitors is not supported in Citrix XenDesktop and XenApp environments. You can verify the DPI (% scaling) using 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 will configure the monitors appropriately. For more information, see CTX201696.

This version of XenApp and XenDesktop is not compatible with AppDNA 7.8 and AppDNA 7.9. Citrix recommends using the current AppDNA release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Technical overview

January 5, 2023

XenApp and XenDesktop are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

XenApp and XenDesktop 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.

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

## Key XenApp and XenDesktop components

This article is most helpful if you're new to XenApp or XenDesktop. If you currently have a 6.x or earlier XenApp farm, or a XenDesktop 5.6 or earlier site, see the Changes in 7.x article, 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 XenApp or XenDesktop 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 virtual machines hosted on 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 virtual 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp or XenDesktop 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 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, verify that a Citrix license is available for the user or session, and apply whatever policies have been 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 Windows server and desktop operating systems. VDAs for Windows server operating systems allow multiple users to connect to the server at one time. VDAs for Windows desktop operating systems allow only one user to connect to the desktop at a time. Linux VDAs are also available.

**Citrix StoreFront:**

StoreFront authenticates users to Sites hosting resources, 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 users have a consistent experience across multiple devices.

**Citrix Receiver:**

Installed on user devices and other endpoints (such as virtual desktops), Citrix Receiver provides users with quick, secure, self-service access to documents, applications, and desktops from any of the user'

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

s devices, including smartphones, tablets, and PCs. Citrix Receiver provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications. For devices that cannot install Citrix Receiver software, Citrix Receiver for HTML5 provides a connection through a HTML5-compatible web browser.

**Citrix Studio:**

Studio is the management console that enables you to configure and manage your XenApp and XenDesktop deployment. This console eliminates the need for separate management consoles to manage delivery of applications and desktops. Studio provides wizards to guide you through environment setup, creating your 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 XenApp or XenDesktop Sites.

Director displays:

Real-time session data from the Broker Service in the Controller. This includes data the Broker Service gets from the broker agent in the VDA.

Historical Site data from the Monitor Service in the Controller.

Data about HDX traffic (also known as ICA traffic) captured by HDX Insight from the NetScaler, if your deployment includes a NetScaler and your XenApp or XenDesktop edition includes HDX Insight.

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. You must create 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, and VMs you use to host the XenApp and XenDesktop components. A hypervisor is installed on a host computer dedicated entirely to running the hypervisor and hosting virtual machines.

XenApp and XenDesktop support various hypervisors and cloud services.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Although many XenApp and XenDesktop deployments require a hypervisor, you don't need one to provide Remote PC Access. You also don't need a hypervisor when you are using Provisioning Services (PVS to provision VMs.

For more information about:

- Ports, see Network ports.
- Databases, see Databases.
- Windows services in XenApp and XenDesktop components, see Configure user rights.
- Supported hypervisors and cloud services, see System requirements.

### Additional components

The following additional components, not shown in the illustration above, can also be included in XenApp or XenDesktop deployments. For more information, see their documentation.

**Provisioning Services (PVS):**

PVS 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 device. 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.

**NetScaler Gateway:**

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

**NetScaler SD-WAN:**

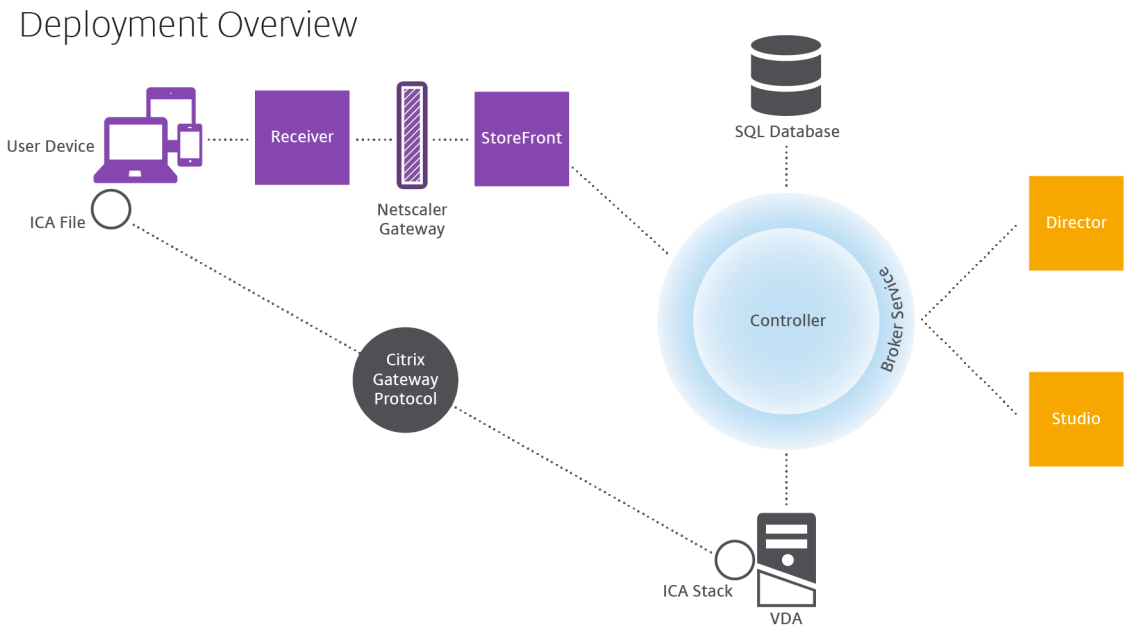
In deployments where virtual desktops are delivered to users at remote locations such as branch offices, Citrix NetScaler SD-WAN technology can be employed to optimize performance. (This technology was formerly Citrix CloudBridge, Branch Repeater, or WANScaler.) Repeaters accelerate performance across wide-area networks. With repeaters in the network, users in the branch office experience LAN-like performance over the WAN. NetScaler SD-WAN can prioritize different parts of the user experience. 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, 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 to the Site using StoreFront, their credentials are passed through to the Broker Service on the Controller. The Broker Service then obtains their profiles and available resources based on the policies set for them.

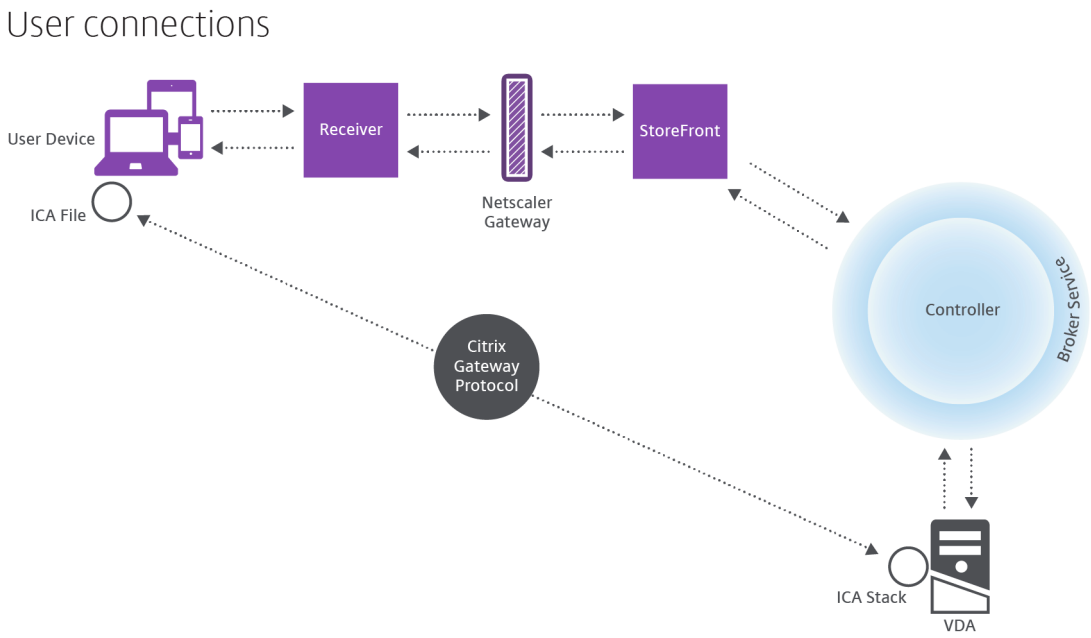
### How user connections are handled

To start a session, the user connects either through Citrix Receiver, which is installed on the user's device, or a StoreFront Citrix Receiver for 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 the Broker Service. Citrix recommends that administrators place an SSL certificate on StoreFront to encrypt the credentials coming from Citrix Receiver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 Receiver 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 Receiver. A set of required parameters is collected on StoreFront. These parameters are then sent to Citrix Receiver, either as part of the Receiver-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 Receiver, StoreFront, and Controller).

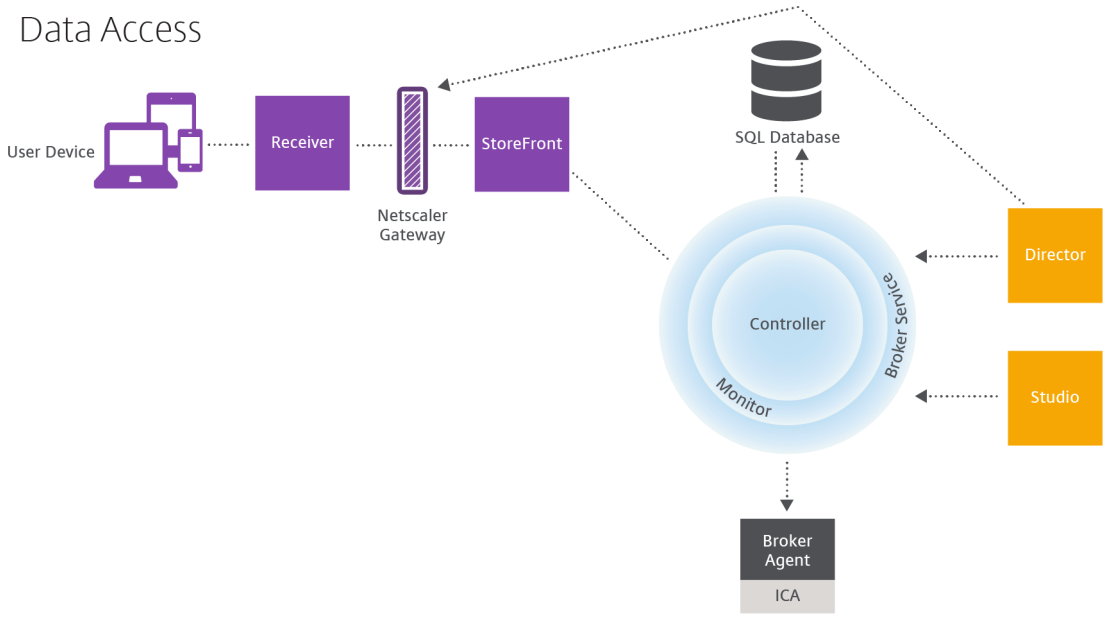
The connection between Citrix Receiver and the VDA uses the Citrix Gateway Protocol (CGP). If a connection is lost, the Session Reliability feature enables the user to reconnect to the VDA rather than having to relaunch through the management infrastructure. Session Reliability can be enabled or disabled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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### How data access works

Every 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 to the same real-time data plus historical data stored in the Monitoring database. Director 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, so 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 NetScaler Gateway to get information on the HDX data.

### Deliver desktops and applications: machine catalogs, Delivery Groups, and Application Groups

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 some or all of the machines in the catalogs), and which users can access them.

**Machine catalogs:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 users. All of 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 (PVS 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:

- **Server OS machines**: Virtual or physical machines based on a server operating system. Used for delivering XenApp published apps (known as server-based hosted applications), and XenApp published desktops (known as server-hosted desktops). These machines allow multiple users to connect to them at one time.
- **Desktop OS machines**: Virtual or physical machines based on a desktop operating system. Used for delivering VDI desktops (can optionally be personalized), VM-hosted apps (applications from desktop OSs) and hosted physical desktops. Only one user at a time can connect each of these desktops.
- **Remote PC Access**: Enables remote users to access their physical office PCs from any device running Citrix Receiver. The office PCs are managed through the XenDesktop deployment, and require user devices to be specified in a whitelist.

For more information, see 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## Active Directory

October 29, 2018

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. To use Policy Modeling, the domain controller must be running on Windows Server 2003 to Windows Server 2012 R2; this does not affect the domain functional level.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

> **Tip**
>
> 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 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. The SupportMultipleForest key is only necessary on the VDA. 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.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 a 32-bit or 64-bit VDA, locate the registry key HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAger
  - Name: ListOfSIDs
  - Type: REG_SZ
  - Data: Security Identifier (SID) of the Controllers

When external trusts are in place, make the following changes on the VDA:

1. Locate the file <ProgramFiles>\Citrix\Virtual Desktop Agent\brokeragentconfig.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

January 5, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

A XenApp or XenDesktop 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.

When you add a Delivery Controller to a site, be sure to add logon credentials for that machine to any replica SQL Servers that you use for high availability.

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, keep the Site database in the primary zone. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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.

> **Note**
>
> 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 required, 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.

For most production deployments, and any deployment that uses Microsoft high availability features, use supported non-Express editions of SQL Server installed on machines other than the server where

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 below.

You can change the location of the Configuration Logging and Monitoring databases 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 the Delivery Controllers article.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.
- High availability features should be configured, 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 permis-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

sions 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 |
| 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.

### Database address formats

You can specify a database address in one of the following forms:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- `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.

### For more information

Sizing the Site database and configuring connection strings when using SQL Server high availability solutions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Delivery methods

July 2, 2018

It's challenging to meet the needs of every user with one virtualization deployment. XenApp and XenDesktop allow administrators to customize the user experience with a variety of methods sometimes referred to as FlexCast models.

This collection of delivery methods —each with its own advantages and disadvantages —provide the best user experience in any use-case scenario.

**Mobilize Windows applications on mobile devices:**

Touch-screen devices, such as tablets and smartphones, are now standard in mobility. These devices can cause problems when running Windows-based applications that typically utilize full-size screens and rely on right-click inputs for full functionality.

XenApp with Citrix Receiver offers a secure solution that allows mobile-device users access to all the functionality in their Windows-based apps without the cost of rewriting those apps for native mobile platforms.

The XenApp published apps delivery method utilizes HDX Mobile technology that solves the problems associated with mobilizing Windows applications. This method allows Windows applications to be refactored for a touch experience while maintaining features such as multitouch gestures, native menu controls, camera, and GPS functions. Many touch features are available natively in XenApp and XenDesktop and do not require any application source code changes to activate.

These features include:

- Automatic display of the keyboard when an editable field has the focus
- Larger picker control to replace Windows combo box control
- Multitouch gestures, such as pinch and zoom
- Inertia-sensed scrolling
- Touchpad or direct-cursor navigation

**Reduce PC refresh costs:**

Upgrading physical machines is a daunting task many businesses face every three to five years, especially if the business needs to maintain the most up-to-date operating systems and applications. Growing businesses also face daunting overhead costs of adding new machines to their network.

The VDI Personal vDisk delivery method provides fully personalized desktop operating systems to single users on any machine or thin client using server resources. Administrators can create virtual machines whose resources —such as processing, memory, and storage —are stored in the network's data center.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

This can extend the life of older machines, keep software up to date, and minimize downtime during upgrades.

**Secure access to virtual apps and desktops for contractors and partners**:

Network security is an ever-growing problem, especially when working with contractors, partners, and other third-party contingent workers who need access to a company's apps and data. The workers may also need loaner laptops or other devices, which cause additional cost concerns.

Data, applications, and desktops are stored behind the firewall of the secure network with XenDesktop and XenApp, so the only thing the end user transmits is user-device inputs and outputs, such as keystrokes, mouse clicks, audio, and screen updates. By maintaining these resources in a data center, XenDesktop and XenApp offer a more secure remote access solution than using the typical SSL VPN.

With a VDI with Personal vDisk deployment, administrators can utilize thin clients or users' personal devices by creating a virtual machine on a network server and providing a single-user desktop operating system. This allows IT to maintain security with third-party workers without the need of purchasing expensive equipment.

**Accelerate migration**:

When switching to a new operating system, IT can face the challenge of delivering legacy and incompatible applications.

With virtual-machine-hosted apps, users can run older applications through Citrix Receiver on the upgraded virtual machine without any compatibility issues. This allows IT additional time to resolve and test application compatibility issues, ease users into the transition, and make help desk calls more efficient.

Additional benefit for using XenDesktop during migration include:

- Reducing complexity for desktops
- Improving IT's control
- Enhancing end-user flexibility in terms of device usage and workspace location

**Enable designers and engineers by virtualizing professional 3D graphics apps**:

Many design firms and manufacturing companies rely heavily on professional 3D graphics applications. These companies face financial strain from the costs of powerful hardware to support this type of software and also logistic problems that come with the sharing of large design files via FTP, email, and similar methods.

The hosted physical desktop delivery method provides a single desktop image to workstations and blade servers without the need of hypervisors to run graphic-intensive 3D applications on a native operating system.

All files are saved in a central data center within the network, so sharing large design files to other users in the network is faster and more secure because the files are not being transferred from one

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

workstation to another.

**Transform call centers**:

Businesses that need large-scale call centers face the difficult challenge of maintaining adequate staffing for peak periods while not overprovisioning machines during less busy hours.

The pooled VDI delivery method provides multiple users access to a standardized desktop dynamically at a minimal cost when provisioning a large number of users. The pooled machines are allocated on a per-session, first-come, first-served basis.

There is less day-to-day management of these virtual machines because any change made during the session is discarded when the user logs off. This also increases security.

The hosted desktops delivery method is another viable option for transforming call centers. This method hosts multiple user desktops on a single server-based operating system.

This is a more cost-efficient method than pooled VDI, but with hosted desktops, users are restricted from installing applications, changing system settings, and restarting the server.

## XenApp published apps and desktops

July 2, 2018

Use server OS machines to deliver XenApp published apps and published desktops.

**Use case:**

- You want inexpensive server-based delivery to minimize the cost of delivering applications to a large number of 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 may 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 datacenter.
- Most cost effective application delivery solution.
- Hosted applications are managed centrally and users cannot modify the application, providing a user experience that is consistent, safe, and reliable.
- Users must be online to access their applications.

**User experience:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- User requests one or more applications from StoreFront, their Start menu, or a URL you provide to them.
- Applications are delivered virtually and display seamlessly in high definition on user devices.
- Depending on profile settings, user changes are saved when the user's application session ends. Otherwise, the changes are deleted.

**Process, host, and deliver applications:**

- Application processing takes place on hosting machines, rather than on the user devices. The hosting machine can be a physical or a virtual machine.
- Applications and desktops reside on a server OS machine.
- Machines become available through machine catalogs.
- Machines from catalogs are organized into Delivery Groups that deliver the same set of applications to groups of users.
- Server OS machines support Delivery Groups that host either desktops or applications, or both.

**Session management and assignment:**

- Server 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 additional applications, no additional sessions are required because a user can run multiple application 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.

To deliver XenApp published apps and desktops:

1. Install the applications you want to deliver on a master image running a supported Windows server OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
3. Create a Delivery Group to deliver the applications and desktops to users. If you are delivering applications, select those you want to deliver.

See the installation and configuration articles for details.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# VM hosted apps

July 2, 2018

Use Desktop 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 a large number of users per host server (or hypervisor), while providing 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 datacenter, providing a more cost effective application delivery solution.
- On log on, 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 desktop 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 may increase the amount of server resources for processing applications and increase the amount of storage for users' personal vDisks.

**User experience:**

The same seamless application experience as hosting shared applications on Server OS machines.

**Process, host, and deliver applications:**

The same as server OS machines except they are virtual desktop OS machines.

**Session management and assignment:**

- Desktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

To deliver VM hosted apps:

1. Install the applications you want to deliver on a master image running a supported Windows desktop OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
3. When defining the desktop experience for the catalog, decide whether you want users to connect to a new VM each time they log in or connect to the same machine each time they log in.
4. Create a Delivery Group to deliver the application to users.
5. From the list of application installed, select the application you want to deliver.

See the installation and configuration articles for details.

## Network ports

November 5, 2020

The following table lists the default network ports used by XenApp and XenDesktop 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 Communication Ports Used by Citrix Technologies.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For port information about other components such as StoreFront and Provisioning Services, see the component's current "System requirements" article.

The table lists 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 https://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 will 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 Receivers |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Component | Usage | Protocol | Default incoming port | Notes |
|---|---|---|---|---|
| VDA | ICA/HDX over WebSocket | TCP | 8008 | Citrix Receiver for HTML5, and Citrix Receiver for Chrome 1.6 and earlier only |
| VDA | ICA/HDX audio over UDP Real-time Transport | UDP | 16500..16509 | |
| 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 | |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Component | Usage | Protocol | Default incoming port | Notes |
|---|---|---|---|---|
| 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

October 14, 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> registry before you edit it.

Citrix HDX includes a broad set of technologies that provide a high-definition user experience.

**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.

### Experience HDX capabilities from your virtual desktop

- See how Flash Redirection, one of three HDX multimedia redirection technologies, accelerates delivery of Adobe Flash multimedia content:

    1. Download Adobe Flash player (https://get.adobe.com/flashplayer/) and install it on both the virtual desktop and the user device.
    2. On the Desktop Viewer toolbar, select **Preferences**. In the Desktop Viewer Preferences dialog box, select the **Flash** tab and select **Optimize content**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. To experience how Flash Redirection accelerates the delivery of Flash multimedia content to virtual desktops, view a video on your desktop from a website containing Flash videos, such as YouTube. Flash Redirection is seamless so that users do not know when it is running. You can check to see whether Flash Redirection is being used. Look for a block of color that appears momentarily before the Flash player starts, or by right-clicking on the video and looking for Flash Redirection in the menu.

- See how HDX delivers high definition audio:

  1. Configure your Citrix client for maximum audio quality; see the Citrix Receiver documentation for details.
  2. Play music files with 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 https://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 Server OS and Windows Desktop OS machines, plus Remote PC Access desktops.
- This content describes how to optimize the user experience further, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Limitation

When you're using Windows Media Player and Remote Audio & Video Extensions (RAVE) enabled inside a session, a black screen might display if you right-click on the video content and select **Always show Now Playing on top**.

### 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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 transparency 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.

### Tablet mode for touch screen devices

By default, any touch enabled device that connects/roams to a Windows 10 VDA starts in tablet mode.

Tablet mode requires a minimum of version XenServer 7.2. XenServer 7.2 integrates with the XenDesktop 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. For more information, see https:/docs.citrix.com/en-us/xenserver/current-release/downloads/release-notes.pdf.

The tablet mode offers a user interface that is better suited to touch screens:

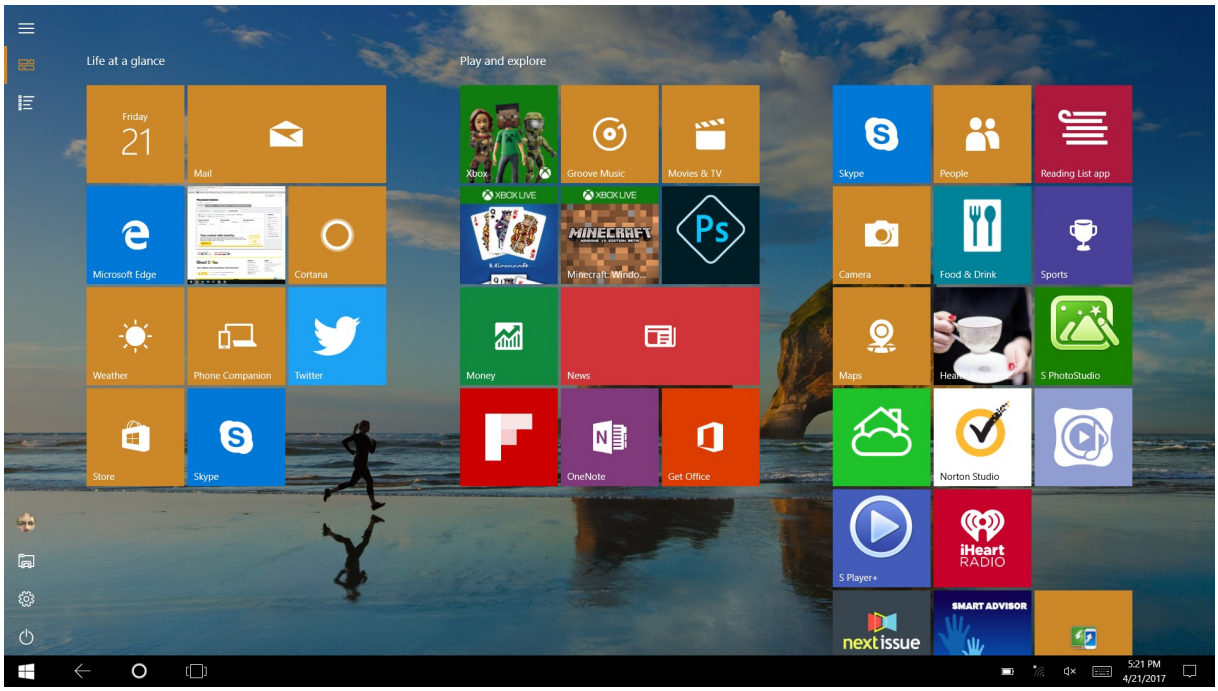
- Slightly larger buttons.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The Start screen and any apps you start open in a full screen.
- Taskbar contains a back button.
- Icons removed from the task bar.

You have access to the File Explorer.

Web Receivers do not support table mode.




Run the XenServer CLI command to allow laptop/tablet switching:

```
xe vm-param-set uuid=\<VM\\_UUID\> platform:acpi\\_laptop\\_slate=1
```

To disable or enable tablet mode, configure this registry setting on XenApp and XenDesktop:

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

Name: CitrixEnhancedUserExperience
Type: REG_DWORD

Value:
0 (Disable)
1 (Enable)

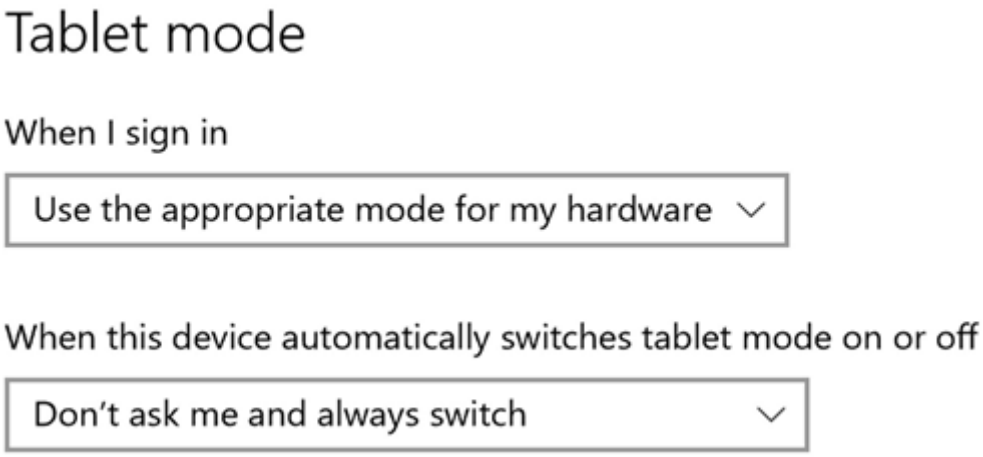
**Before starting a session:**

We recommend that you navigate to **Settings >System >Tablet Mode** on the VD 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If you don't set these options before starting the session, set the options after you start the session and restart the VDA.




### 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 XenApp and XenDesktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Citrix Receiver 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 H.264 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 (QoS)-supported routers. Four TCP streams (real time, interactive, background, and bulk) and two User Datagram Protocol (UDP) streams (voice and Framehawk display remoting) are available to carry ICA traffic between the user device and the server. 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 (QoS) is supported only when multiple session reliability ports, or the CGP ports, are configured.

> **Caution:**
>
> 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):

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 (QoS).
- 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.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. To use normal Unicode keyboard layout mapping, set DWORD value DisableWindowHook = 0.

### Related information

- Graphics
- Multimedia
- General content redirection
- Adaptive transport

## Adaptive transport

October 29, 2018

### Introduction

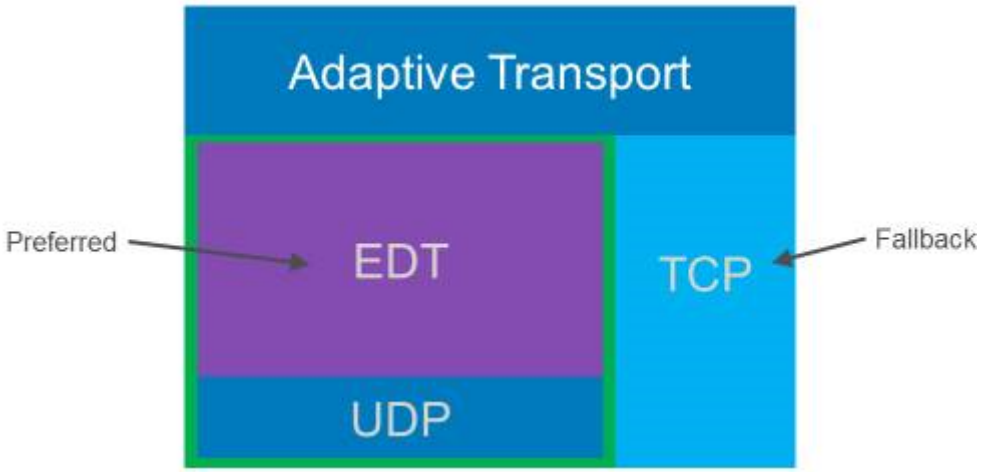
Adaptive transport is a new data transport mechanism for XenApp and XenDesktop. It is faster, more scalable, improves application interactivity, and is more interactive on challenging long-haul WAN and internet connections. Adaptive transport maintains high server scalability and efficient use of bandwidth. By using adaptive transport, ICA virtual channels automatically respond to changing network conditions. They intelligently switch the underlying protocol between the new Citrix protocol called Enlightened Data Transport (EDT) and TCP to deliver the best performance. It improves data throughput for all ICA virtual channels including Thinwire display remoting, file transfer (Client Drive Mapping), printing, and multimedia redirection. The same setting is applicable for both LAN and WAN conditions.

When set to **Preferred**, data transport over EDT is used as primary and fallback to TCP.

By default, adaptive transport is disabled (**Off**) and TCP is always used.

For testing purposes, you can set **Diagnostic mode**, in which case only EDT is used, and fallback to TCP is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Interoperability with Citrix SD-WAN WAN optimization

Citrix SD-WAN WAN optimization (WANOP) offers cross-session tokenized compression (data deduplication), including URL-based video caching. WANOP provides significant bandwidth reduction 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 XenApp and XenDesktop server scalability.

> **Important:**
>
> When TCP is used as the data transport protocol, Citrix WANOP supports the optimizations described in the previous paragraph. When using Citrix WANOP on network connections, choose TCP. By using TCP flow control and congestion control, WANOP ensures equivalent interactivity to EDT at high latency and moderate packet loss.

### Requirements and considerations

- XenApp and XenDesktop: Minimum version 7.13
- VDA for Desktop OS: Minimum version 7.13
- VDA for Server OS: Minimum version 7.13
- StoreFront: Minimum version 3.9
- Citrix Receiver for Windows: Minimum version 4.7
- Citrix Receiver for Mac: Minimum version 12.5
- Citrix Receiver for iOS: Minimum version 7.2
- Citrix Receiver for Linux: Version 13.6 for Direct VDA Connections only and 13.7 for DTLS support using NetScaler Gateway (or DTLS for direct VDA connections).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Citrix Receiver for Android: Version 3.12.3 for Direct VDA Connections only and 3.13 for DTLS support using NetScaler Gateway (or DTLS for direct VDA connections).
- IPv4 VDAs only. IPv6 and mixed IPv6 and IPv4 configurations are not supported.
- NetScaler: Minimum version 11.1-51.21. For more information on NetScaler configuration, see Configuring NetScaler Gateway to support Advanced Transport.

### Configuration

1. Install XenApp and XenDesktop.
2. Install StoreFront.
3. Install the VDA (for Desktop OS or Server OS)
4. Install Citrix Receiver for Windows (Citrix Receiver for Mac or Citrix Receiver for iOS).
5. In Studio, enable the policy setting, HDX Adaptive Transport (it is disabled by default). We also recommend that you do not enable this feature as a universal policy for all objects in the Site.
    - 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 falls back to TCP is disabled. We recommend this setting only for troubleshooting.
        - **Off.** TCP is forced on, and EDT is disabled.
6. Click Next, and complete the steps in the wizard.
7. The policy takes effect when the user reconnects the ICA session. Though not required, you can run **gpupdate /force** to pull the policy setting to the server, but the user still has to reconnect the ICA session.
8. Start a session from a supported Citrix Receiver to establish a connection using adaptive transport.
9. For secure external access, configure DTLS encryption on NetScaler Unified Gateway. For more information, see Configuring NetScaler Gateway to support Advanced Transport.

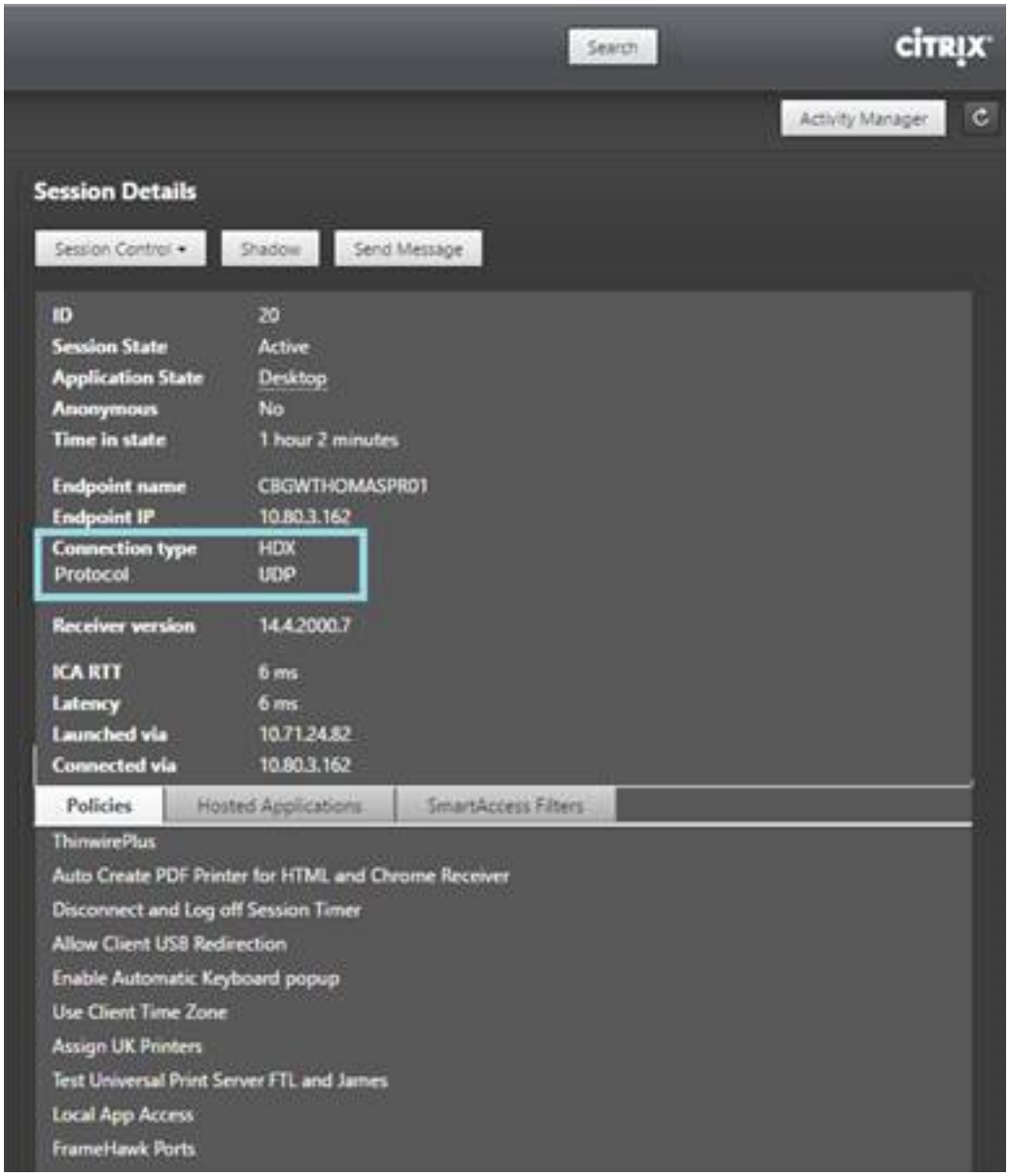
To confirm that the policy setting has taken effect:

- Check that the ICA User Datagram Protocol (UDP) services are enabled on a VDA using netstat -a**
- Check that the virtual channels are running over EDT using **Director** or the **CtxSession.exe** command-line utility available on the VDA.

**Director example:**

In Director, **Session Details > Connection Type** displays the policy settings. Look for Connection type **HDX**. If the protocol is **UDP**, EDT is active for the session. If the protocol is **TCP**, the session is in fallback or default mode. If the Connection type is **RDP**, ICA is not in use and the protocol is **n/a**. For more information, see Monitor sessions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**CtxSession.exe example:**

This example illustrates that EDT over UDP is active for the session. Type CtxSession.exe in the command line.

C:\Program Files (x86)\Citrix\System32>CtxSession

Session 2 Transport Protocols: UDP > CGP > ICA

To see verbose statistics, use the -v switch:

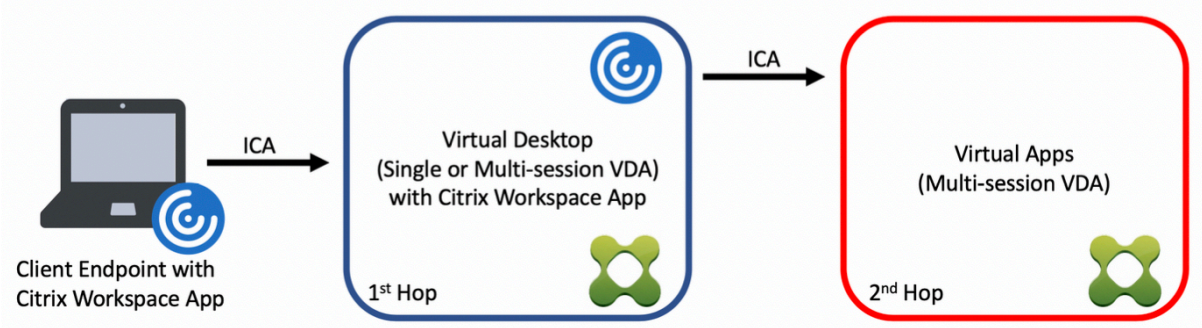
>CtxSession -v

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| First hop (VDI or published desktop) | Second hop (Virtual apps) | Support notes |
|---|---|---|
| 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. |
| 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

August 17, 2018

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 XenApp or XenDesktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 contains complete information about the available VDA installers.)

### Install other 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To enable end users to have greater control over their user accounts, install Self-Service Password Reset. For details, see the Self-Service Password Reset documentation.

Optionally, integrate more Citrix components into your XenApp or XenDesktop deployment.

- Provisioning Services is an optional component of XenApp and XenDesktop that provisions machines by streaming a master image to target devices.
- Citrix NetScaler 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 NetScaler SD-WAN is a set of appliances that optimize WAN performance.

For installation guidance, see the documentation for these components, features, and technologies.

### 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

January 5, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Deploying XenApp and XenDesktop 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 NetScaler. For an introduction to using NetScaler with StoreFront, see Integrate XenApp and XenDesktop with NetScaler Gateway.

### How you can install components

You can use the full-product installer on the XenApp and XenDesktop 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 Provisioning Services (PVS). For details, see Install VDAs using scripts.

As an automated alternative to using the installers, Citrix Smart Tools uses blueprints to create a XenApp and XenDesktop deployment. For details, see Smart Tools product documentation.

### Information to review before installation

- Technical overview: If you're unfamiliar with the product and its components.
- Changes in 7.x: If you are moving from a XenApp 6.x or XenDesktop 5.6 deployment to the current version.
- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 any time 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.

You can install both a Delivery Controller and a VDA for Server 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 Server OS.

Ensure that each operating system has the latest updates. For example, installation of a Controller on Windows Server 2012 R2 or a VDA on Windows 8.1 or 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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp or XenDesktop 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 instructions

### Installation guidance, considerations, and best practice

#### During installation of any component

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.

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 (such as Smart Tools) that collect diagnostics for maintenance and troubleshooting. For information about these programs, see Citrix Insight Services.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### During VDA installation

The Citrix Receiver for Windows is included by default when you install a VDA, except when using the VDAWorkstationCoreSetup.exe installer. You can exclude the Citrix Receiver from the installation. You or your users can download and install (and upgrade) Citrix Receiver and other Citrix Receivers from the Citrix website. Alternatively, you can make those Citrix Receivers available from your StoreFront server.

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 Server 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.

When you install the VDA, a new local user group called Direct Access Users is created automatically. On a VDA for Desktop OS, this group applies only to RDP connections. On a VDA for Server 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.

#### 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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

After each restart, run the installer or command again to continue the VDA installation.

## Installers

### Full-product installer

Using the full-product installer provided in the XenApp and XenDesktop ISO, you can:

- Install, upgrade, or remove core XenApp and XenDesktop components: Delivery Controller, Studio, Director, StoreFront, License Server
- Install or upgrade Windows VDAs for server or desktop operating systems
- Install the Universal Print Server Ups Server component on your print servers
- Install the Federated Authentication Service
- Install the Self-Service Password Reset Service

To deliver a desktop from a Server 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.

**VDAServerSetup.exe** Installs a VDA for Server OS. It supports all the VDA for Server OS options that are available with the full-product installer.

**VDAWorkstationSetup.exe** Installs a VDA for Desktop OS. It supports all the VDA for Desktop OS options that are available with the full-product installer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**VDAWorkstationCoreSetup.exe** Installs a VDA for Desktop 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.

The **VDAWorkstationCoreSetup.exe** installer does not install or contain a Citrix Receiver for Windows.

Using **VDAWorkstationCoreSetup.exe** is equivalent to using the full-product or **VDAWorkstationSetup.exe** installer to install a Desktop OS VDA and either:

- In the graphical interface: Selecting the Remote PC Access option on the **Environment** page and clearing the Citrix Receiver check box on the **Components** page.
- In the command line interface: Specifying the /remotepc and /components vda options.
- 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".

You can install the omitted components/features later by running the full-product installer. That action installs all missing components.

## Microsoft Azure Resource Manager virtualization environments

June 30, 2020

Follow this guidance when using Microsoft Azure Resource Manager to provision virtual machines in your XenApp or XenDesktop deployment.

You can configure XenApp or XenDesktop to provision resources in Azure Resource Manager either when you create the XenApp or XenDesktop Site (which includes creating a connection), or when you create a host connection later (after creating the Site).

You should be familiar with the following:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Azure Active Directory: https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
- Consent framework: https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/
- Service principal: https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

Azure Disk Encryption is not supported when using Machine Creation Services.

This version of XenApp and XenDesktop only supports an Azure unmanaged disk storage system. By default, Azure uses a managed disk storage system. For information about managed and unmanaged Azure storage solutions, refer to Azure managed disks.

### Create a connection to Azure Resource Manager

See the Create a Site and Connections and resources articles for complete information about all pages in the wizards that create a Site or a connection. The following information covers only details specific to Azure Resource Manager connections.

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 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 the 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

5. Click **Accept** to give XenApp or XenDesktop the listed permissions. XenApp or XenDesktop 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. Notice that when you successfully authenticate to Azure, the **Create new** and **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.

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 the 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.

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 below.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To create a service principal:

**Step 1**: Connect to your Azure Resource Manager subscription.

```
Login-AzureRmAccount.
```

**Step 2**: Select the Azure Resource Manager subscription where you want to create the service principal.

```
Select-AzureRmSubscription -SubscriptionID $SubscriptionId;
```

**Step 3**: Create the application in your AD tenant.

```
$AzureADApplication = New-AzureRmADApplication -DisplayName
    $ApplicationName -HomePage "https://localhost/$ApplicationName" -
    IdentifierUris https://$ApplicationName -Password
    $ApplicationPassword
```

**Step 4**: Create a service principal.

```
New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
    ApplicationId
```

**Step 5**: Assign a role to the service principal.

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $AzureADApplication.ApplicationId – scope /
    subscriptions/$SubscriptionId
```

**Step 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 the 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 will be 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.)

Resources comprise the region and the network.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 the 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.

Complete the wizard.

### Create a Machine Catalog using an Azure Resource Manager master image

This information is a supplement to the guidance in the Create Machine Catalogs article.

A master image is the template that will be 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 the Create Machine Catalogs article.
- On the **Master Image** page, select a resource group and then navigate (drill down) 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 of the wizard. 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/windows/disks-types#premium-ssd

  https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 since it waives the price of extra Windows Server licenses from the Azure gallery. You must 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. See https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/.

To check if the provisioned Virtual Machines are successfully utilizing HUB, run the following 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?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json.

- 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.

- The **Network Cards**, **Computer Accounts**, and **Summary** pages do not contain Azure-specific information. Follow the guidance in the Create Machine Catalogs article.

Complete the wizard.

## Microsoft System Center Virtual Machine Manager virtualization environments

June 30, 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 the System requirements article.

You can use Provisioning Services and Machine Creation Services to provision:

- Generation 1 Desktop or Server OS VMs

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Generation 2 Windows Server 2012 R2, Windows Server 2016, and Windows 10 VMs (with or without Secure Boot)

### Upgrade VMM

- Upgrade from VMM 2012 to VMM 2012 SP1 or VMM 2012 R2

  For VMM and Hyper-V Hosts requirements, see https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg610649(v=sc.12)?redirectedfrom=MSDN. For VMM Console requirements, see https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg610640(v=sc.12)?redirectedfrom=MSDN.

  A mixed Hyper-V cluster is not supported. An example of a mixed cluster is one in which half the cluster is running Hyper-V 2008 and the other is running Hyper-V 2012.

- Upgrade from VMM 2008 R2 to VMM 2012 SP1

  If you are upgrading from XenDesktop 5.6 on VMM 2008 R2, follow this sequence to avoid XenDesktop downtime.

  1. Upgrade VMM to 2012 (now running XenDesktop 5.6 and VMM 2012)
  2. Upgrade XenDesktop to the latest version (now running the latest XenDesktop and VMM 2012)
  3. Upgrade VMM from 2012 to 2012 SP1 (now running the latest XenDesktop and VMM 2012 SP1)

- Upgrade from VMM 2012 SP1 to VMM 2012 R2

  If you are starting from XenDesktop or XenApp 7.x on VMM 2012 SP1, follow this sequence to avoid XenDesktop downtime.

  1. Upgrade XenDesktop or XenApp to the latest version (now running the latest XenDesktop or XenApp, and VMM 2012 SP1)
  2. Upgrade VMM 2012 SP1 to 2012 R2 (now running the latest XenDesktop or XenApp, and VMM 2012 R2)

### Installation and configuration summary

> **Important:**
>
> All Delivery Controllers must be in the same forest as the VMM servers.

1. Install and configure a hypervisor.

   a) Install Microsoft Hyper-V server and VMM on your servers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

b) 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.
c) 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).
     Note: Installing a Controller on a server running Hyper-V is not supported.

2. Create a master VM.
   a) Install a Virtual Delivery Agent on the master VM, and select the option to optimize the desktop. This improves performance.
   b) Take a snapshot of the master VM to use as a backup.
3. Create virtual desktops. If you are using MCS to create VMs, when creating a Site or a connection,
   a) Select the Microsoft virtualization host type.
   b) Enter the address as the fully qualified domain name of the host server.
   c) Enter the credentials for the administrator account you set up earlier that has permissions to create new VMs.
   d) In the Host Details dialog box, select the cluster or standalone host to use when creating new VMs.
      Important: 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, make sure 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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
  ```

- **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
  ```

- **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.

  1. The HCL uploads the Identity to the Hyper-V machine through the administrator share.
  2. The Hyper-V machine copies the disk to the SMB storage through a PowerShell script running in the PowerShell remote session. A folder is created on the Hyper-V machine and the permissions on that folder are locked for the VMM user only (through the remote PowerShell connection).
  3. The HCL deletes the file from the administrator share.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. When the HCL completes the identity disk upload to the Hyper-V machine, the remote PowerShell session copies the identity disks to SMB storage and then deletes it from the Hyper-V machine.

   The identity disk folder is recreated if 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.

  1. The HyperV machine copies the disk from the SMB storage to local Hyper-V storage through a PowerShell script running in the PowerShell V3 remote session.
  2. HCL reads the disk from the Hyper-V machine's administrator share into memory.
  3. HCL deletes the file from the administrator share.

- **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.

## Microsoft System Center Configuration Manager environments

August 21, 2018

Sites that use Microsoft System Center Configuration Manager (Configuration Manager) to manage access to applications and desktops on physical devices can extend that use to XenApp or XenDesktop through these integration options.

- **Citrix Connector 7.5 for Configuration Manager 2012**—Citrix Connector provides a bridge between Configuration Manager and XenApp or XenDesktop. The Connector enables you to unify day-to-day operations across the physical environments you manage with Configuration Manager and the virtual environments you manage with XenApp or XenDesktop. For information about the Connector, see Citrix Connector 7.5 for System Center Configuration Manager 2012.
- **Configuration Manager Wake Proxy feature**—The Remote PC Access Wake on LAN feature requires Configuration Manager. For more information, see below.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **XenApp and XenDesktop properties**—XenApp and XenDesktop properties enable you to identify Citrix virtual desktops for management through Configuration Manager. These properties are automatically used by the Citrix Connector but can also be manually configured, as described in the following section.

### 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, User (which 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 may want to install applications on the master 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 a master image (this value is set during installation based on a selection); **Cleared** on a VM that is provisioned from that image. |
| IsVirtualMachine | True for a virtual machine, false for a physical machine. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Property | Description |
| --- | --- |
| 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 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 may include spaces or vary slightly from the property names. For example, **BrokerSiteName** may 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.

### Configuration Manager and Remote PC Access Wake on LAN

To configure the Remote PC Access Wake on LAN feature, complete the following before installing a VDA on the office PCs and using Studio to create or update the Remote PC Access deployment:

- Configure ConfigMgr 2012, 2012 R2, or 2016 within the organization. Then deploy the Config-Mgr client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run (or force one manually, if required). The access credentials you specify in Studio to configure the connection to ConfigMgr must include collections in the scope and the Remote Tools Operator role.
- For Intel Active Management Technology (AMT) support:
  - The minimum supported version on the PC must be AMT 3.2.1.
  - Provision the PC for AMT use with certificates and associated provisioning processes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - Only ConfigMgr 2012 and 2012 R2 can be used, not ConfigMgr 2016.

- For ConfigMgr Wake Proxy and/or magic packet support:

  - Configure Wake on LAN in each PC's BIOS settings.
  - For Wake Proxy support, enable the option in ConfigMgr. For each subnet in the organization that contains PCs that will 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 Remote PC Access deployment in Studio.

- If you enable power management, specify connection details: the ConfigMgr address and access credentials, plus a name.
- 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 and specify the new power management connection.

You can edit a power management connection to configure the use of the ConfigMgr Wake Proxy and magic packets, as well as change the packet transmission method.

For more information, see Remote PC Access.

## VMware virtualization environments

January 4, 2019

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/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=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 of the privileges listed below. Base the roles' creation on the specific level of granularly required over the user's permissions to

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

request the various XenApp or XenDesktop operations at any time. To grant the user specific permissions at any point, associate them with the respective role, at the DataCenter level at a minimum.

The following tables show the mappings between XenApp and XenDesktop operations and the minimum required VMware privileges.

**Add connections and resources**

| SDK | User interface |
|---|---|
| System.Anonymous, System.Read, and System.View | Added automatically. Can use the built-in read-only role. |

**Provision machines (Machine Creation Services)**

| SDK | User interface |
|---|---|
| Datastore.AllocateSpace | Datastore > Allocate space |
| Datastore.Browse | Datastore > Browse datastore |
| Datastore.FileManagement | Datastore > Low level file operations |
| Network.Assign | Network > Assign network |
| Resource.AssignVMToPool | Resource > Assign virtual machine to resource pool |
| VirtualMachine.Config.AddExistingDisk | Virtual machine > Configuration > Add existing disk |
| VirtualMachine.Config.AddNewDisk | Virtual machine > Configuration > Add new disk |
| VirtualMachine.Config.AdvancedConfig | Virtual machine > Configuration > Advanced |
| VirtualMachine.Config.RemoveDisk | Virtual machine > Configuration > Remove disk |
| VirtualMachine.Interact.PowerOff | Virtual machine > Interaction > Power Off |
| VirtualMachine.Interact.PowerOn | Virtual machine > Interaction > Power On |
| VirtualMachine.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 machin |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| SDK | User interface |
| --- | --- |
| VirtualMachine.State.CreateSnapshot | vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Create snapshot<br>vSphere 5.5: Virtual machine > Snapshot management > Create snapshot |

If you want the VMs you create to be tagged, add the following permissions for the user account.

To ensure that you use a clean base image for creating new VMs, tag VMs created with Machine Creation Services to exclude them from the list of VMs available to use as base images.

| SDK | User interface |
| --- | --- |
| Global.ManageCustomFields | Global > Manage custom attributes |
| Global.SetCustomField | Global > Set custom attribute |

**Provision machines (Provisioning Services)**

All privileges from **Provision machines (Machine Creation Services)** and the following.

| SDK | User interface |
| --- | --- |
| VirtualMachine.Config.AddRemoveDevice | Virtual machine > Configuration > Add or remove device |
| VirtualMachine.Config.CPUCount | Virtual machine > Configuration > Change CPU Count |
| VirtualMachine.Config.Memory | Virtual machine > Configuration > Memory |
| VirtualMachine.Config.Settings | Virtual machine > Configuration > Settings |
| VirtualMachine.Provisioning.CloneTemplate | Virtual machine > Provisioning > Clone template |
| VirtualMachine.Provisioning.DeployTemplate | Virtual machine > Provisioning > Deploy template |

**Power management**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 |

**Image update and rollback**

| SDK | User interface |
| --- | --- |
| Datastore.AllocateSpace | Datastore > Allocate space |
| Datastore.Browse | Datastore > Browse datastore |
| Datastore.FileManagement | Datastore > Low level file operations |
| Network.Assign | Network > Assign network |
| Resource.AssignVMToPool | Resource > Assign virtual machine to resource pool |
| VirtualMachine.Config.AddExistingDisk | Virtual machine > Configuration > Add existing disk |
| VirtualMachine.Config.AddNewDisk | Virtual machine > Configuration > Add new disk |
| VirtualMachine.Config.AdvancedConfig | Virtual machine > Configuration > Advanced |
| VirtualMachine.Config.RemoveDisk | Virtual machine > Configuration > Remove disk |
| VirtualMachine.Interact.PowerOff | Virtual machine > Interaction > Power Off |
| VirtualMachine.Interact.PowerOn | Virtual machine > Interaction > Power On |
| VirtualMachine.Interact.Reset | Virtual machine > Interaction > Reset |
| VirtualMachine.Inventory.CreateFromExisting | Virtual machine > Inventory > Create from existing |
| VirtualMachine.Inventory.Create | Virtual machine > Inventory > Create new |
| VirtualMachine.Inventory.Delete | Virtual machine > Inventory > Remove |
| VirtualMachine.Provisioning.Clone | Virtual machine > Provisioning > Clone virtual machine |

**Delete provisioned machines**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 |

#### 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| SDK | User interface |
| --- | --- |
| 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 Controller.

**STEP 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.

**STEP 2.** Obtain the vCenter certificate using any of the following three methods:

**From the vCenter server:**

1. Copy the file rui.crt from the vCenter server to a location accessible on your Delivery Controllers.
2. 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.

1. Open your web browser and make a secure web connection to the vCenter server (for example `https://server1.domain1.com`).
2. Accept the security warnings.
3. Click on the address bar displaying the certificate error.
4. View the certificate and click the Details tab.
5. Select **Copy to file and export in .CER format**, providing a name when prompted to do so.
6. Save the exported certificate.
7. Navigate to the location of the exported certificate and open the .CER file.

**Import directly from Internet Explorer running as an administrator:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Open your web browser and make a secure web connection to the vCenter server (for example `https://server1.domain1.com`).
2. Accept the security warnings.
3. Click on the address bar displaying the certificate error.
4. View the certificate.

**STEP 3**. Import the certificate into the certificate store on each of your Controllers.

1. Click **Install certificate**, select **Local Machine**, and then click **Next**.
2. Select **Place all certificates in the following store**, and then click **Browse**.

On Windows Server 2008 R2: Select the **Show physical stores** check box. Expand **Trusted People**. Select **Local Computer**. Click **Next** and then click **Finish**.

On a later supported version: Select **Trusted People** and then click **OK**. Click **Next** and then click **Finish**.

**Important:**: If you change the name of the vSphere server after installation, you must generate a new self-signed certificate on that server before importing the new certificate.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp or XenDesktop, 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

August 21, 2018

Follow this guidance when using Nutanix Acropolis to provide virtual machines in your XenApp or XenDesktop deployment. The setup process includes the following tasks:

- Install and register the Nutanix plugin in your XenApp or XenDesktop 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 Acropolix MCS Plugin Installation Guide, available at the Nutanix Support Portal: https://portal.nutanix.com.

For support information regarding Nutanix and Provisioning Services, see Knowledge Center article CTX131239.

### Install and register the Nutanix plugin

After you install the XenApp or XenDesktop 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 Service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

5. Run the following PowerShell cmdlets to verify that the Nutanix Acropolis plugin has been registered:

   **Add-PSSnapin Citrix***

   **Get-HypHypervisorPlugin**

### Create a connection to Nutanix

See the Create a Site and Connections and resources articles 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 will be used to create the VMs in the Machine Catalog. Before creating the Machine 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 XenApp and XenDesktop. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Microsoft Azure virtualization environments

June 30, 2020

## 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="https://management.core.windows.net"
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. f 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 a connection.

## 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

- MSDN –Virtual Machine and Cloud Service Sizes for Azure: https://docs.microsoft.com/en-us/previous-versions/azure/dn197896(v=azure.100)?redirectedfrom=MSDN
- Virtual Machine Pricing: https://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 https://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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 40 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://azure.microsoft.com/en-us/documentation/articles/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

June 16, 2020

The core components are the Delivery Controller, Studio, Director, and License Server.

(In versions before 7.15 LTSR CU6, 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.)

**Important:** Before you start an installation, review Prepare to install. Also, review this article before starting an installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

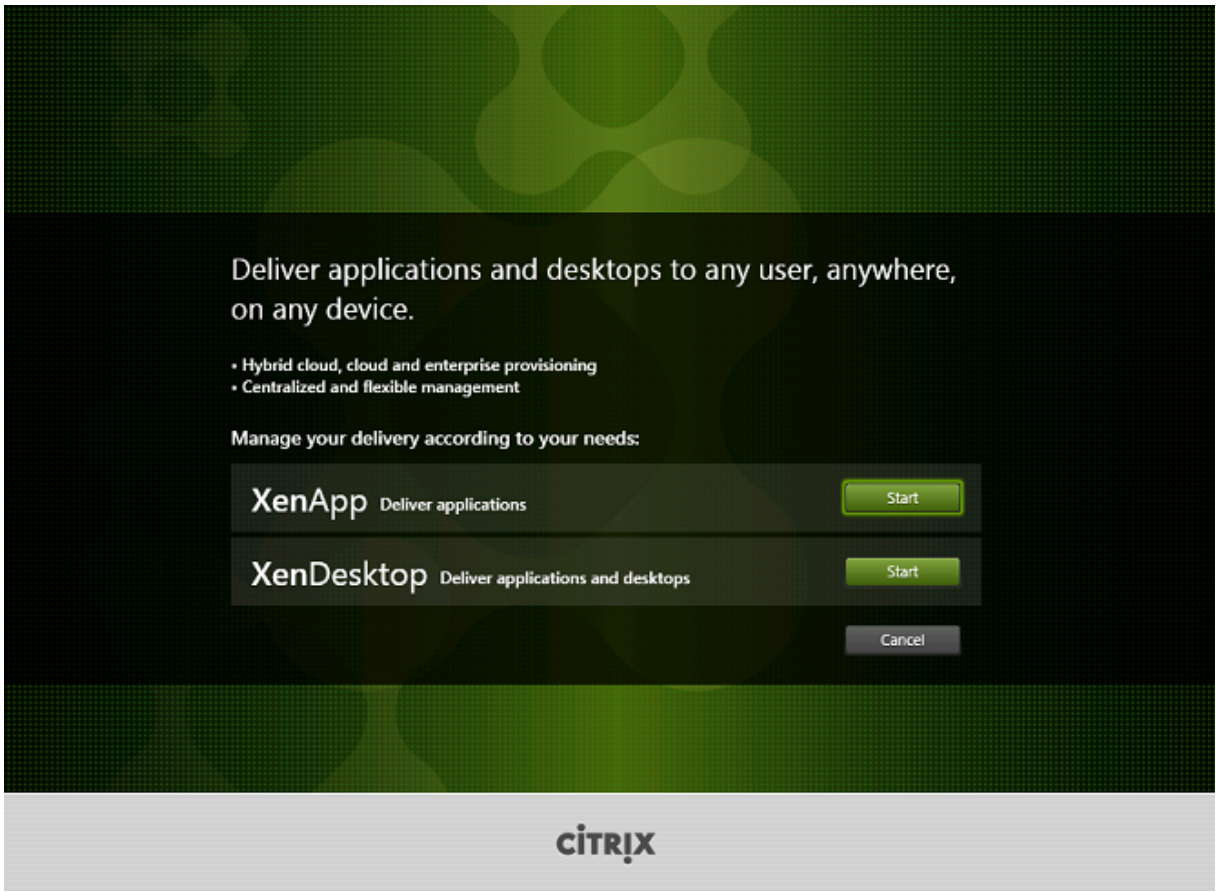
Use your Citrix account credentials to access the XenApp and XenDesktop download page. Download the product ISO file.

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



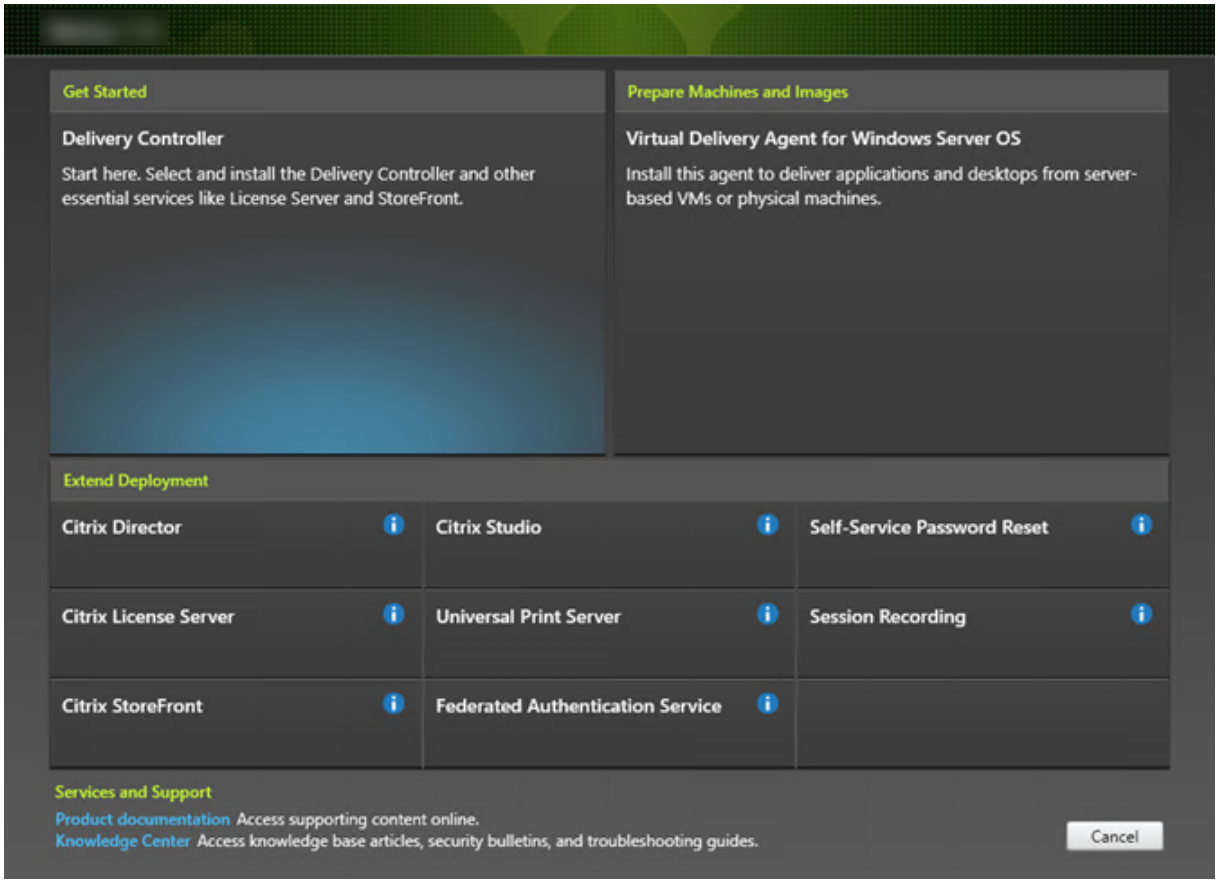

Click **Start** next to the product to install: XenApp or XenDesktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

(If the machine already has XenApp or XenDesktop components installed on it, this page does not appear.)

Command-line option: /xenapp to install XenApp; XenDesktop is installed if option is omitted

### Step 3. Choose what to install



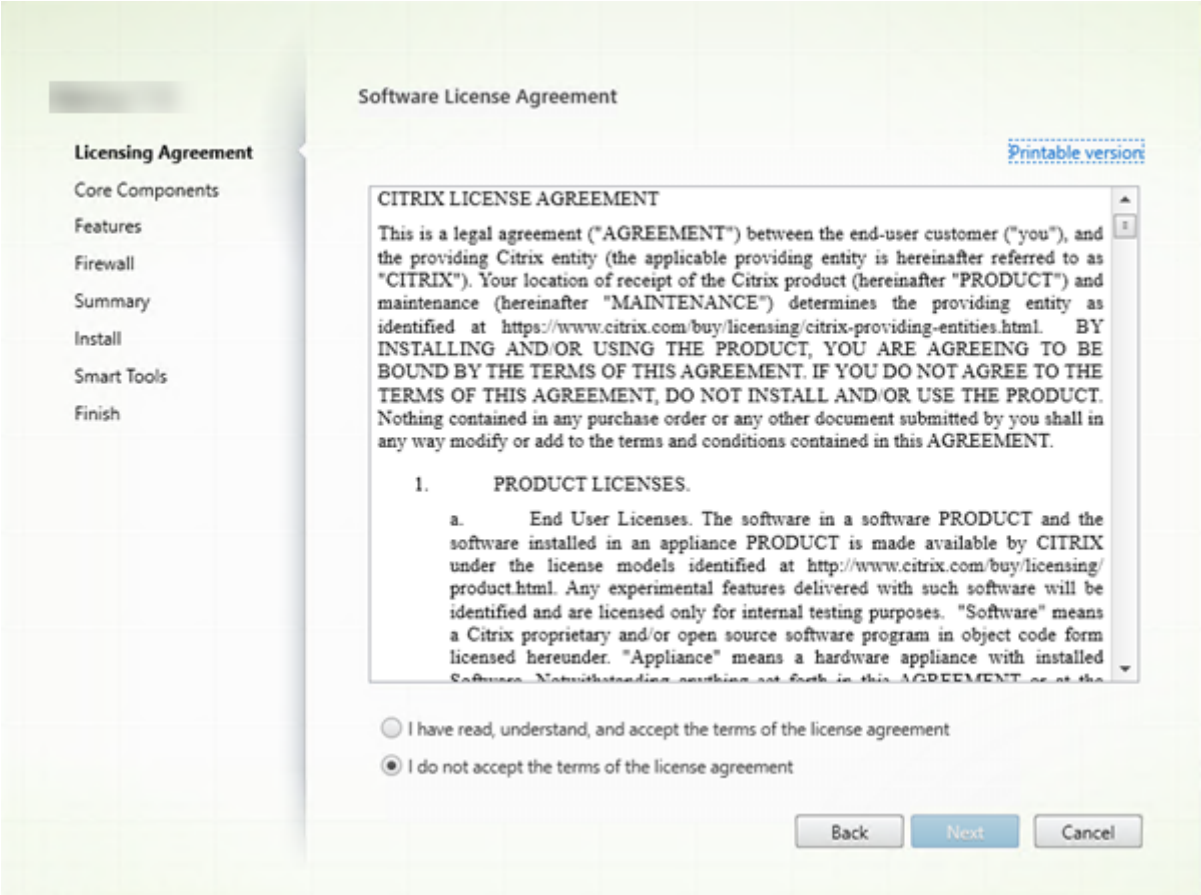

If you're just getting started, select **Delivery Controller**. (On a later page, you select the specific components to install on this machine.)

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

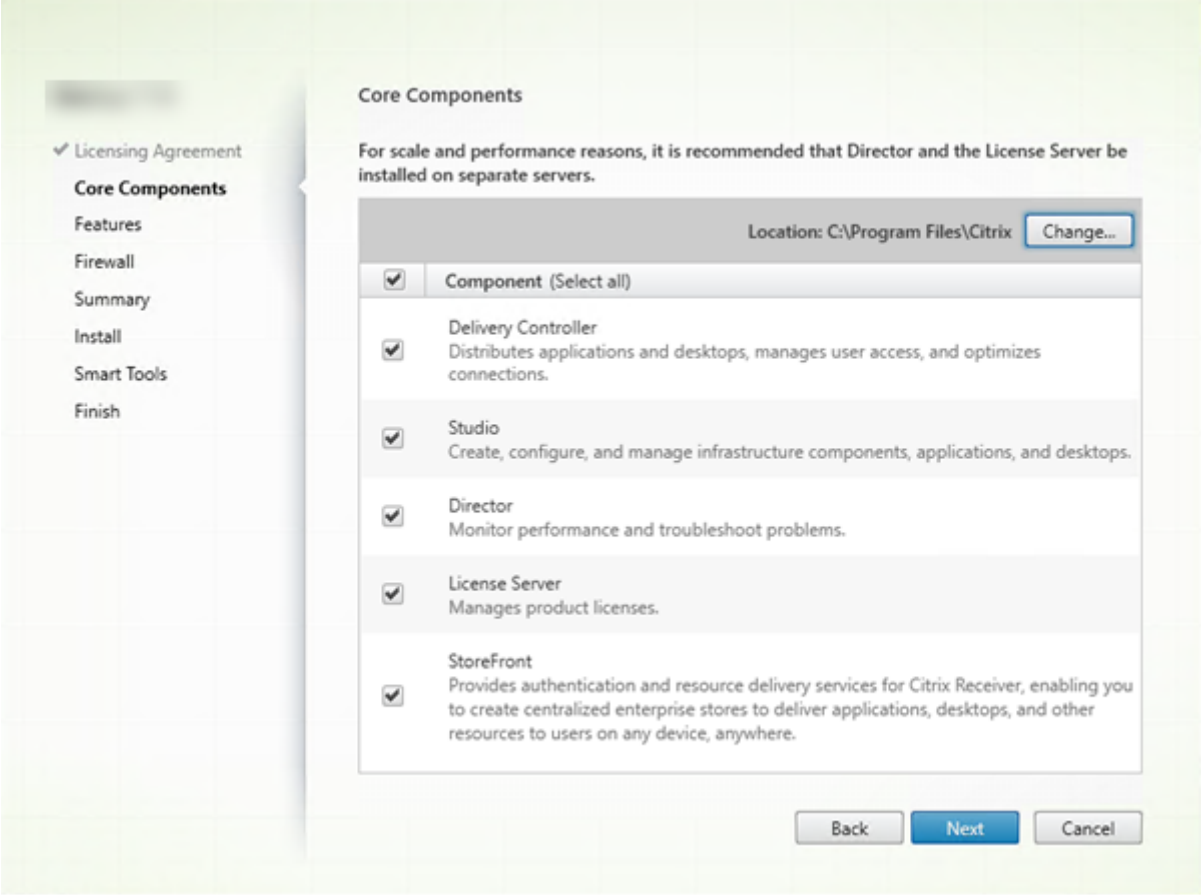
### Step 4. Read and accept the license agreement




On the **Licensing Agreement** page, after you read the license agreement, indicate that you have read and accepted it. Then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 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.

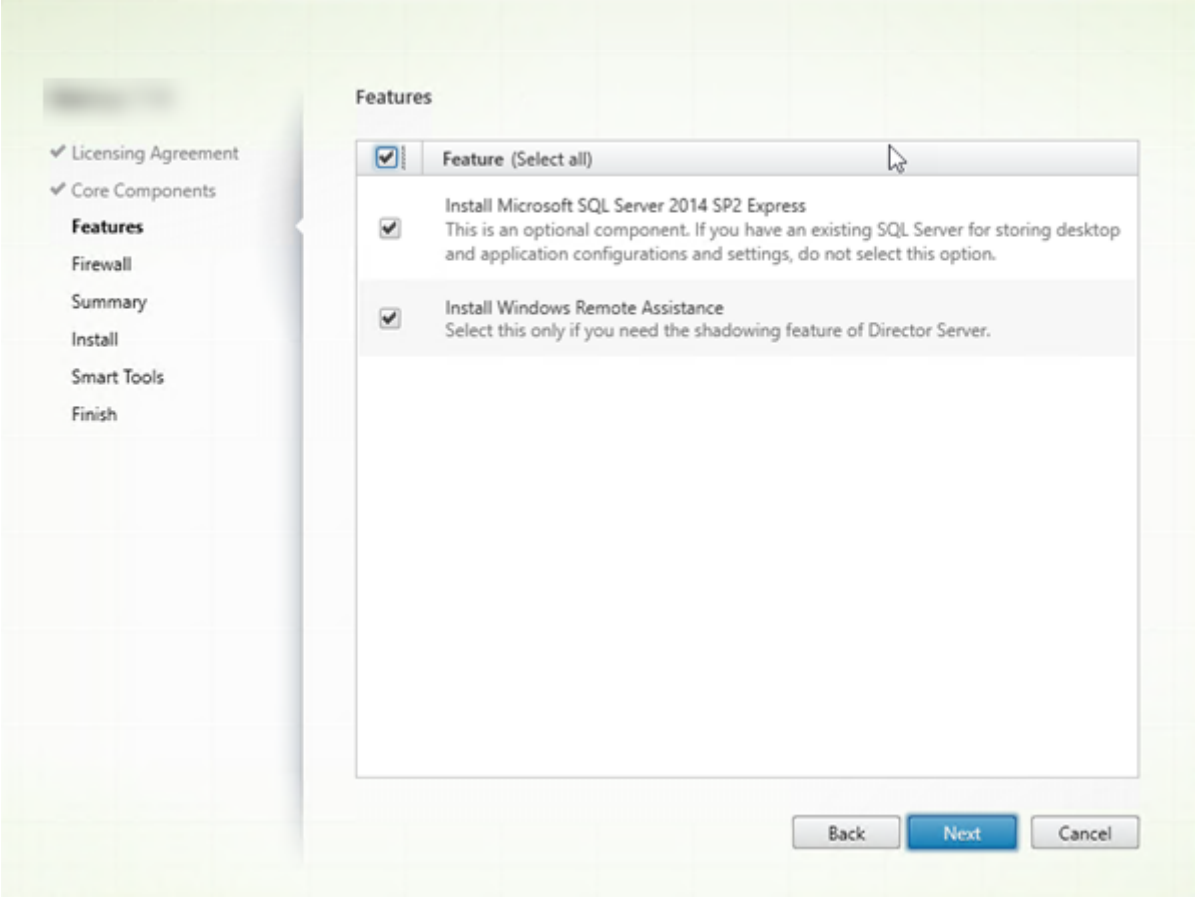
An icon alerts you when you choose not to install a required core component on this machine. That alert reminds you to install that component, although not necessarily on this machine.

Click **Next**.

Command-line options: /installdir, /components, /exclude

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 6. Enable or disable features




On the **Features** page:

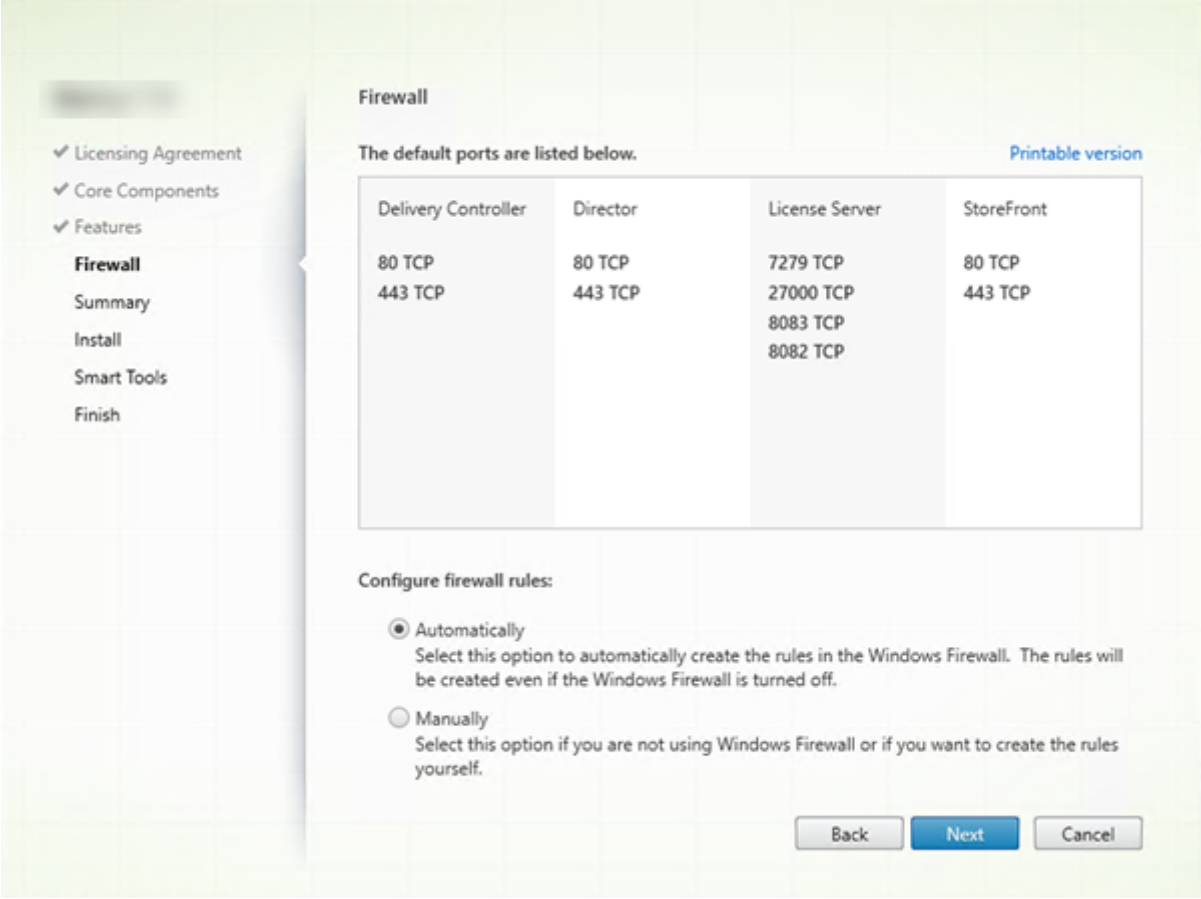
- Choose whether to install Microsoft SQL Server Express for use as the Site database. By default, this selection is enabled. If you're not familiar with the XenApp and XenDesktop databases, review Databases.
- When you install Director, Windows Remote Assistance is installed automatically. You choose 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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 7. Open Windows firewall ports automatically




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.

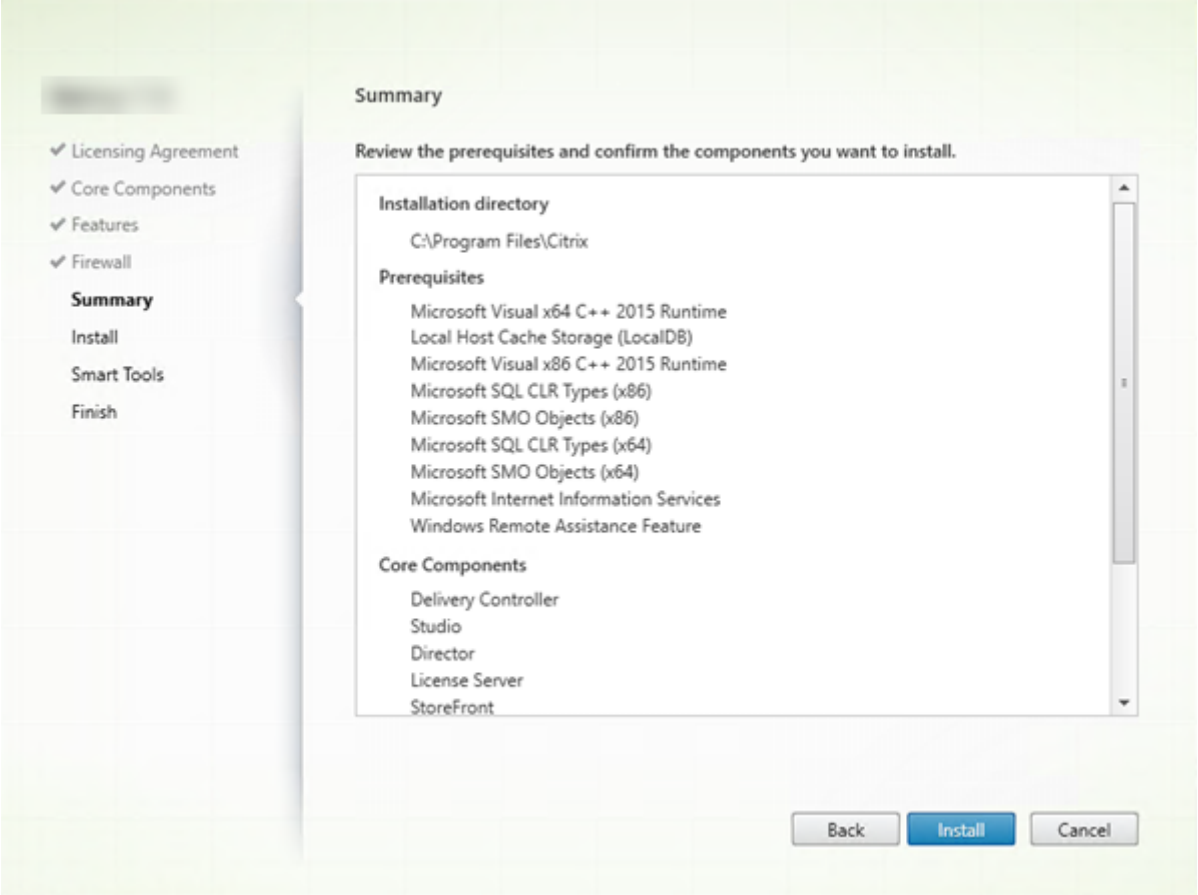
Click **Next**.

(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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 8. Review prerequisites and confirm installation

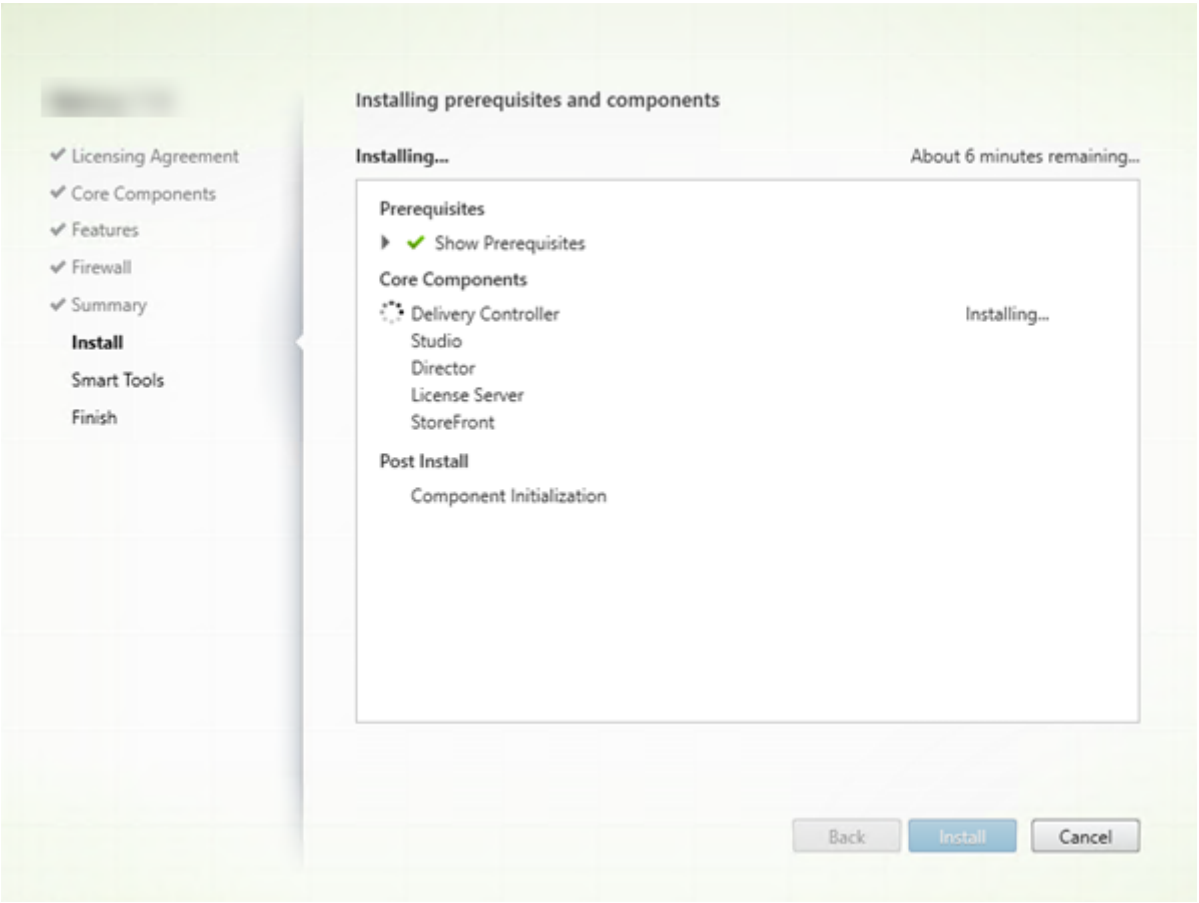



The **Summary** page lists what will be installed. Use the Back button to return to earlier wizard pages and change selections, if needed.

When you're ready, click **Install**.

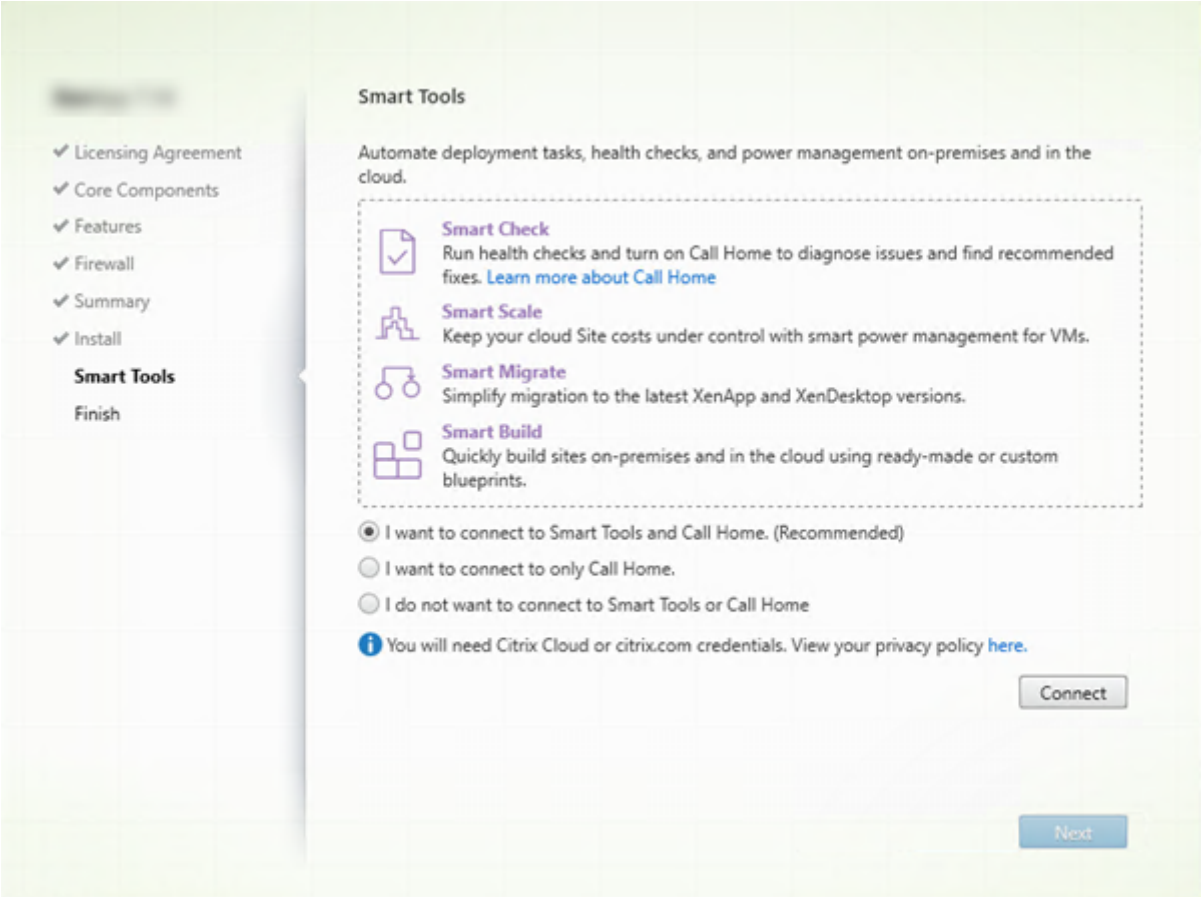
The display shows the progress of the installation:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 9. Connect to Smart Tools and Call Home




When installing or upgrading a Delivery Controller, the Smart Agent page offers several options:

- Enable connections to Smart Tools and Call Home. This is the recommended selection.
- Enable connections to Call Home. During an upgrade, this option does not appear if Call Home is already enabled or if the installer encounters an error related to the Citrix Telemetry Service.
- Do not enable connections to Smart Tools or Call Home.

If you install StoreFront (but not a Controller), the wizard displays the **Smart Tools** page. If you install other core components (but not a Controller or StoreFront), the wizard does not display either the **Smart Tools** or **Call Home** pages.

If you choose an option to enable connections to Smart Tools and/or Call Home:

1. Click **Connect**.
2. Provide your Citrix or Citrix Cloud credentials.
3. After your credentials are validated, the process downloads a Smart Agent certificate. After this completes successfully, a green check mark appears next to the **Connect** button. If an error occurs during this process, change your participation selection (to "**I do not want to ...**"). You can enroll later.

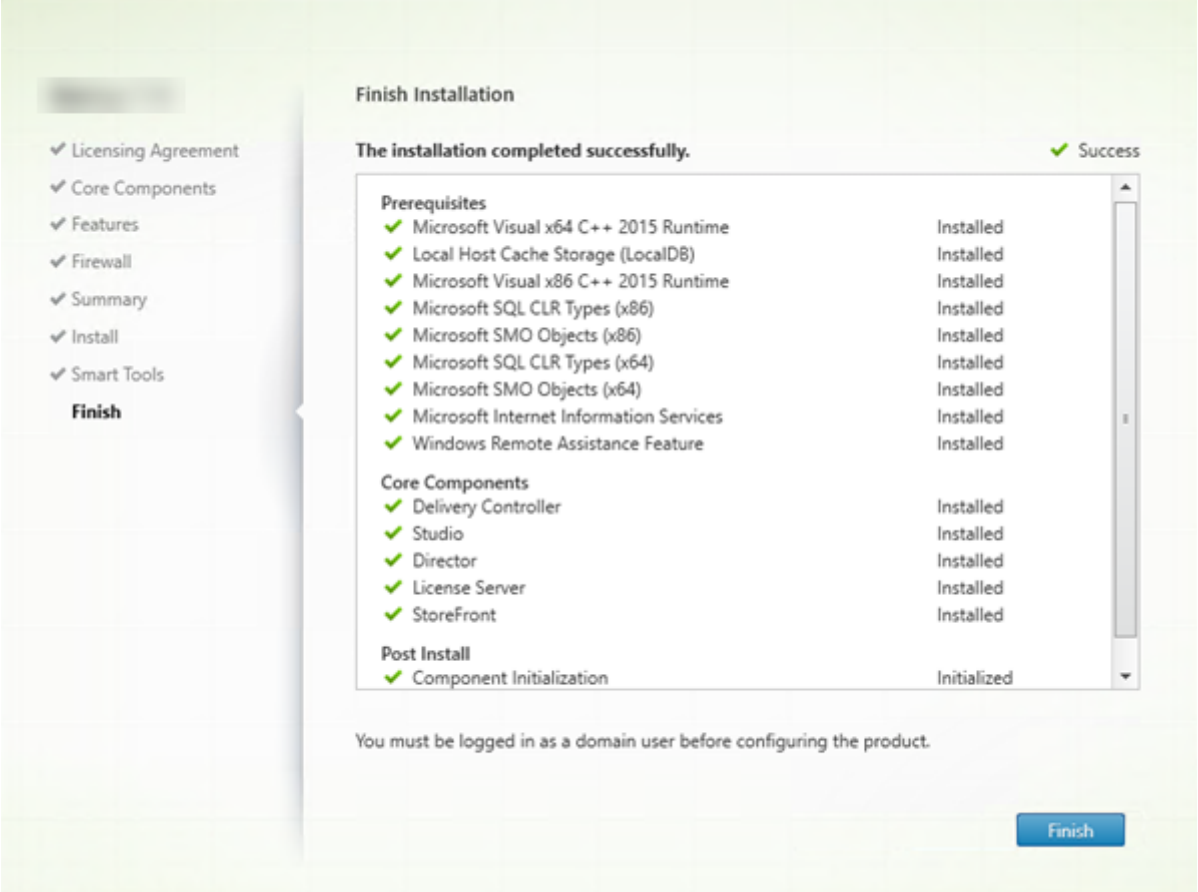
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. Click **Next** to continue with the installation wizard.

If you choose not to participate, click **Next**.

Command-line option: /exclude "Smart Tools Agent"(to prevent installation)

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 the print server. Select **Universal Print Server** in the Extend Deployment section. Accept the license agreement, then proceed to the end of the wizard. There is nothing else to specify or select. To install this component form the command line, see Install using the command line.
- Federated Authentication Service: See Federated Authentication Service.
- Self-Service Password Reset Service: See the Self-Service Password Reset Service documentation.

## Install VDAs

January 5, 2023

There are two types of VDAs for Windows machines: VDA for Server OS and VDA for Desktop OS. (For information about VDAs for Linux machines, see the Linux Virtual Delivery Agent documentation.)

> **Important:**
>
> Before you start an installation, review Prepare to install. For example, the machine should have the latest Windows updates. If required updates are not present (such as KB2919355), installation fails.

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.

If the installation of a VDA or a Delivery Controller 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 1. Download the product software and launch the wizard

If you're using the full-product installer:

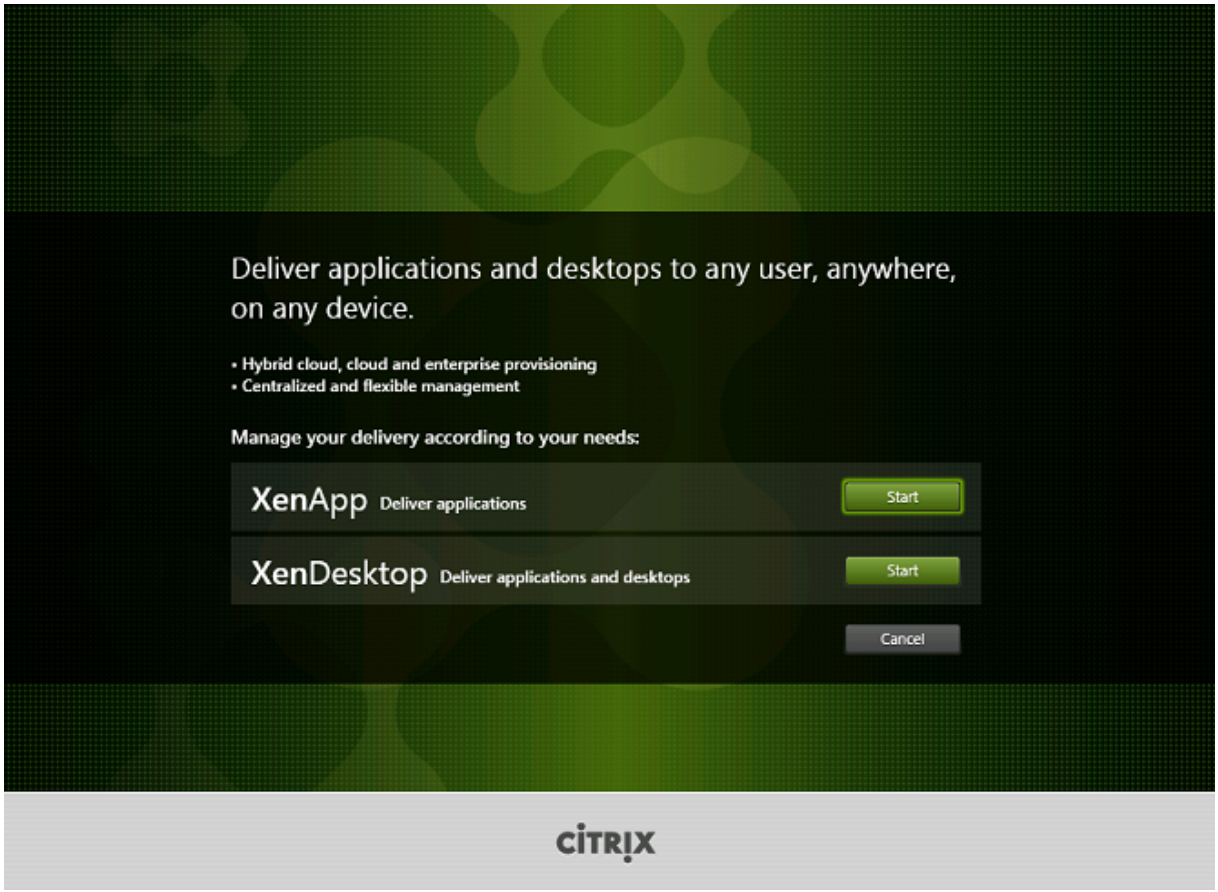
- If you haven't downloaded the XenApp and XenDesktop ISO yet:
  - Use your Citrix account credentials to access the XenApp and XenDesktop download page. Download the product ISO file.
  - Unzip the file. Optionally, burn a DVD of the ISO file.
- Use a local administrator account on the image or machine 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:

- Use your Citrix account credentials to access the XenApp and XenDesktop download page. Download the appropriate package:
  - VDAServerSetup.exe: Server OS VDA <version>
  - VDAWorkstationSetup.exe: Desktop OS VDA <version>
  - VDAWorkstationCoreSetup.exe: Desktop OS Core Services VDA <version>
- Right-click the package and choose **Run as administrator.**
- The installation wizard launches.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 2. Choose which product to install

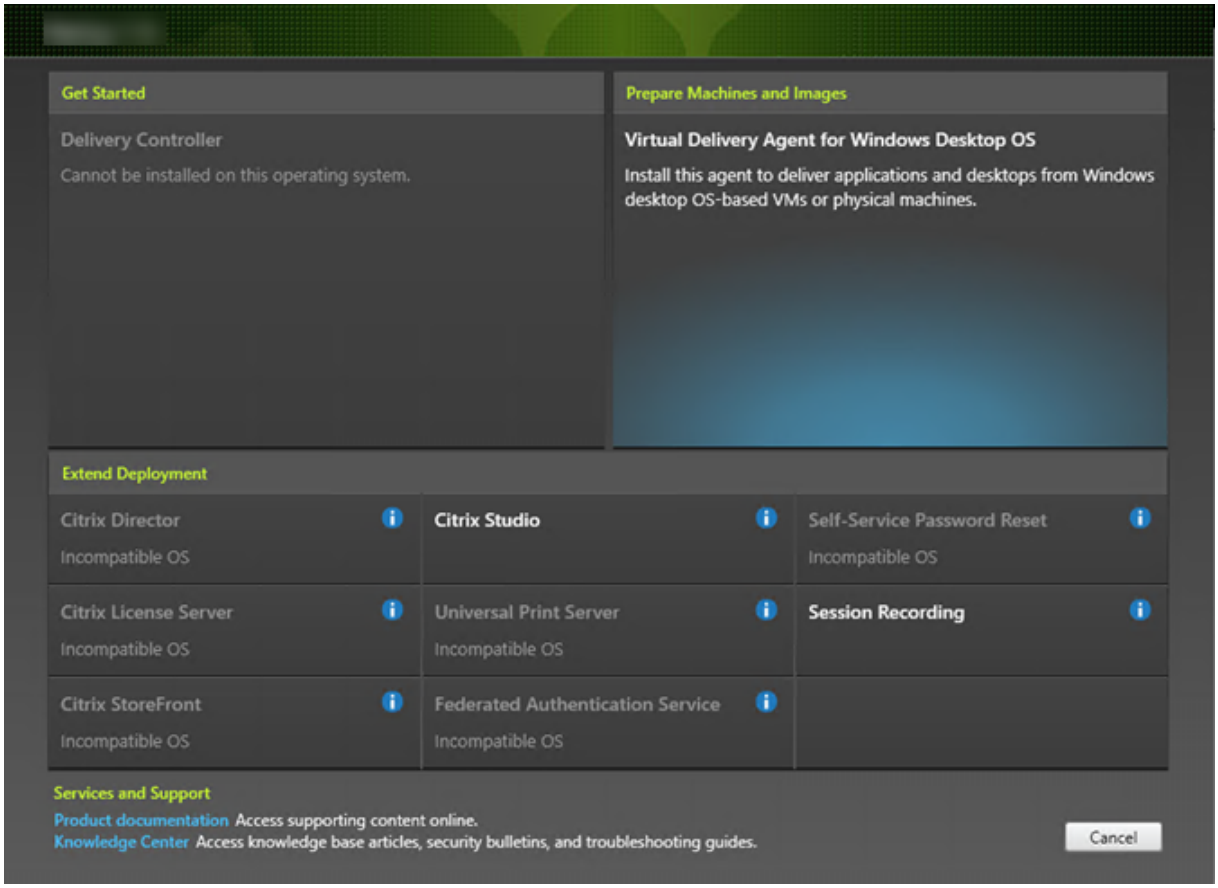



Click **Start** next to the product to install: XenApp or XenDesktop. (If the machine already has a XenApp or XenDesktop component installed, this page does not appear.)

Command-line option: /xenapp to install XenApp; XenDesktop is installed if option is omitted

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 3. Select the VDA

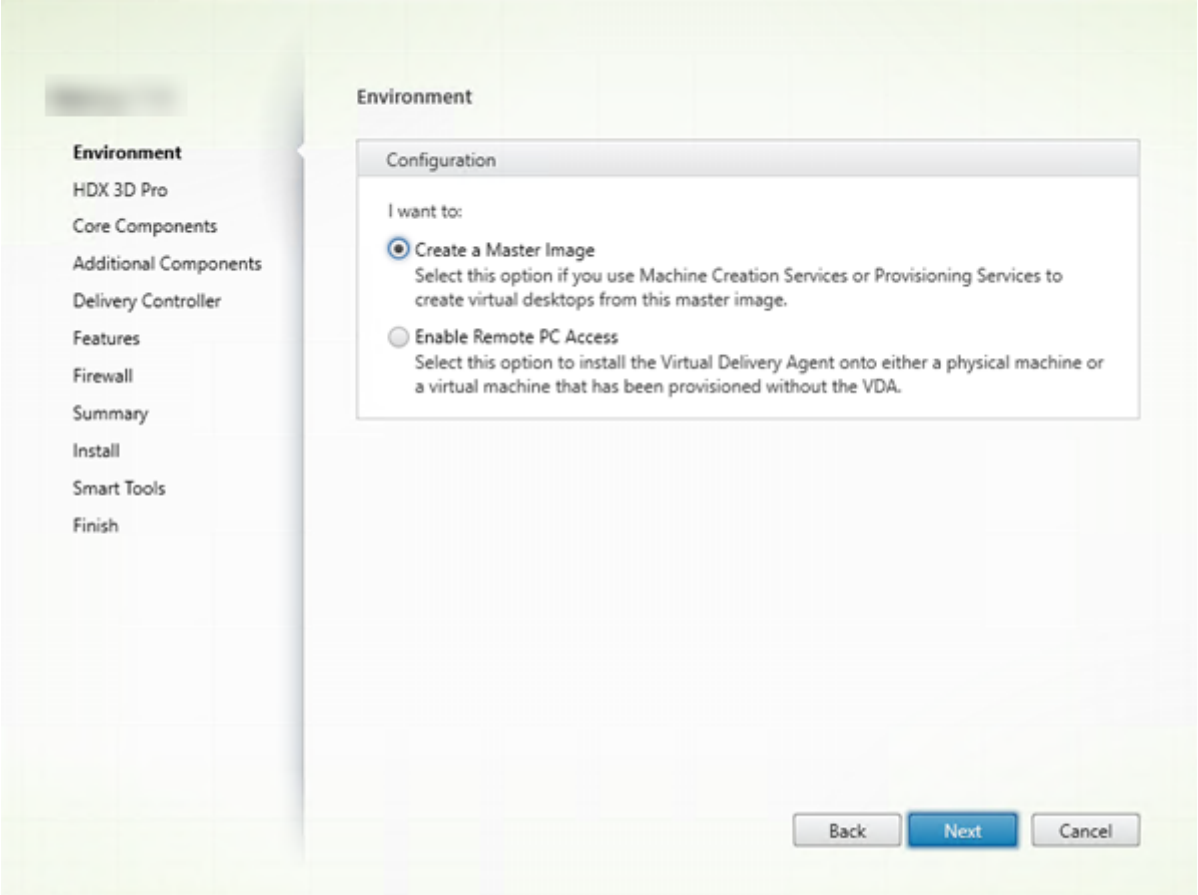



Select the Virtual Delivery Agent entry. The installer knows whether it's running on a Desktop or Server OS, so it offers only the appropriate VDA type.

For example, when you run the installer on a Windows 10 machine, the VDA for Desktop OS option is available. The VDA for Server OS option is not offered.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 4. Specify how the VDA will be used




On the **Environment** page, specify how you plan to use the VDA. Choose one of the following:

- **Master image:** (default) You are installing the VDA on a machine image. You plan to use Citrix tools (Machine Creation Services or Provisioning Services) to create VMs from that master image.
- **Enable connections to a server machine** (if installing on a server) or **Remote PC Access** (if installing on a desktop machine): You are installing the VDA on a physical machine or on a VM that was provisioned without a VDA. If you choose the Remote PC Access option, the following components are not installed/enabled:
  - App-V
  - Profile Management
  - Machine Identify Service
  - Personal vDisk

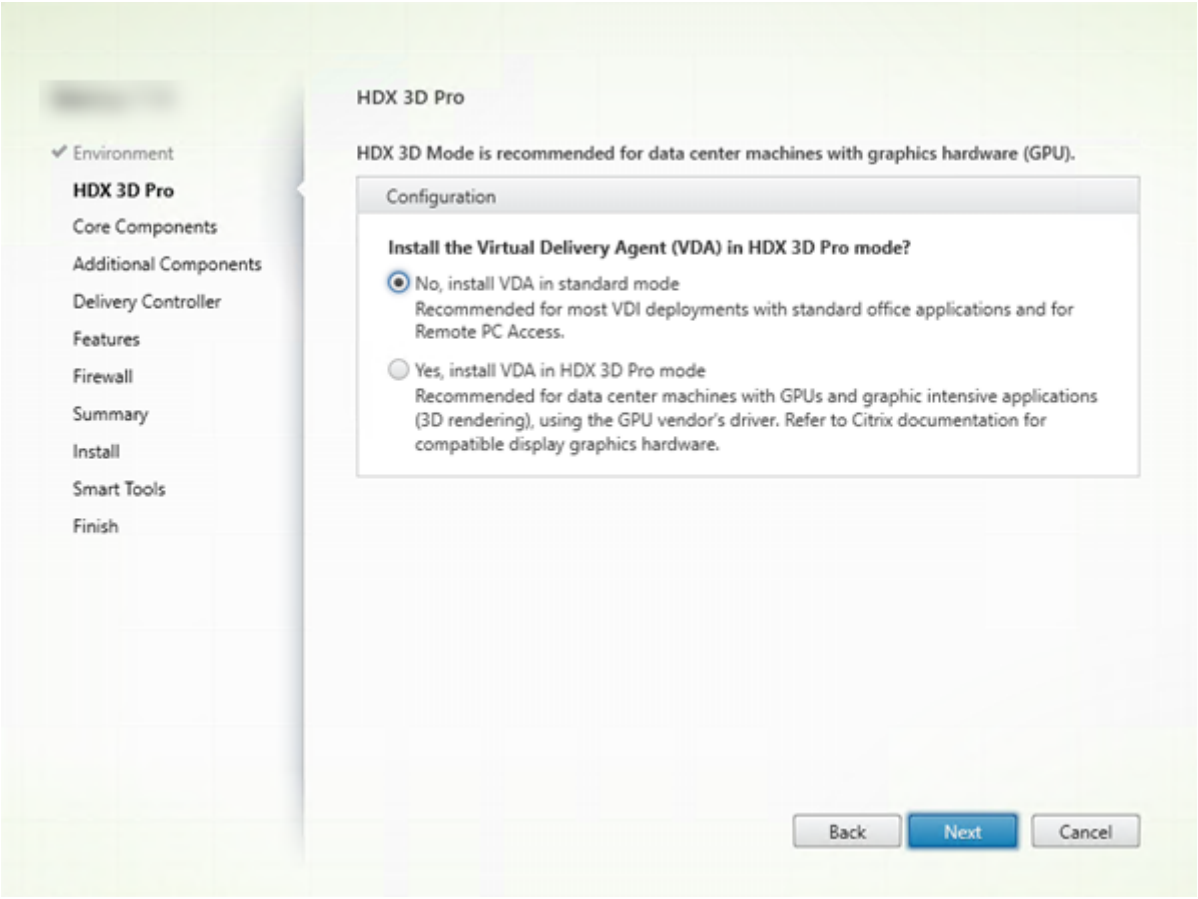
Click **Next**.

Command-line options: /masterimage, /remotepc

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If you are using the VDAWorkstationCoreSetup.exe installer, this page does not appear in the wizard and the command-line options are not valid.

### Step 5. Choose whether to enable HDX 3D Pro mode




The **HDX 3D Pro** page appears only when installing a VDA for Desktop OS.

- The standard VDA mode is recommended for most desktops, including those enabled with Microsoft RemoteFX. The standard VDA mode is the default.
- The HDX 3D Pro VDA mode optimizes the performance of graphics-intensive programs and media-rich applications. HDX 3D Pro VDA mode is recommended if the machine accesses a graphics processor for 3D rendering.
- For Remote PC Access, the VDA is usually configured with the standard VDA mode. For Remote PC Access configured with HDX 3D Pro, monitor blanking is supported with
  - Intel Iris Pro graphics and Intel HD graphics 5300 and above (5th Generation Intel Core Processors and 6th Generation Intel Core i5 Processors)
  - NVIDIA Quadro and NVIDIA GRID GPUs
  - AMD RapidFire

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

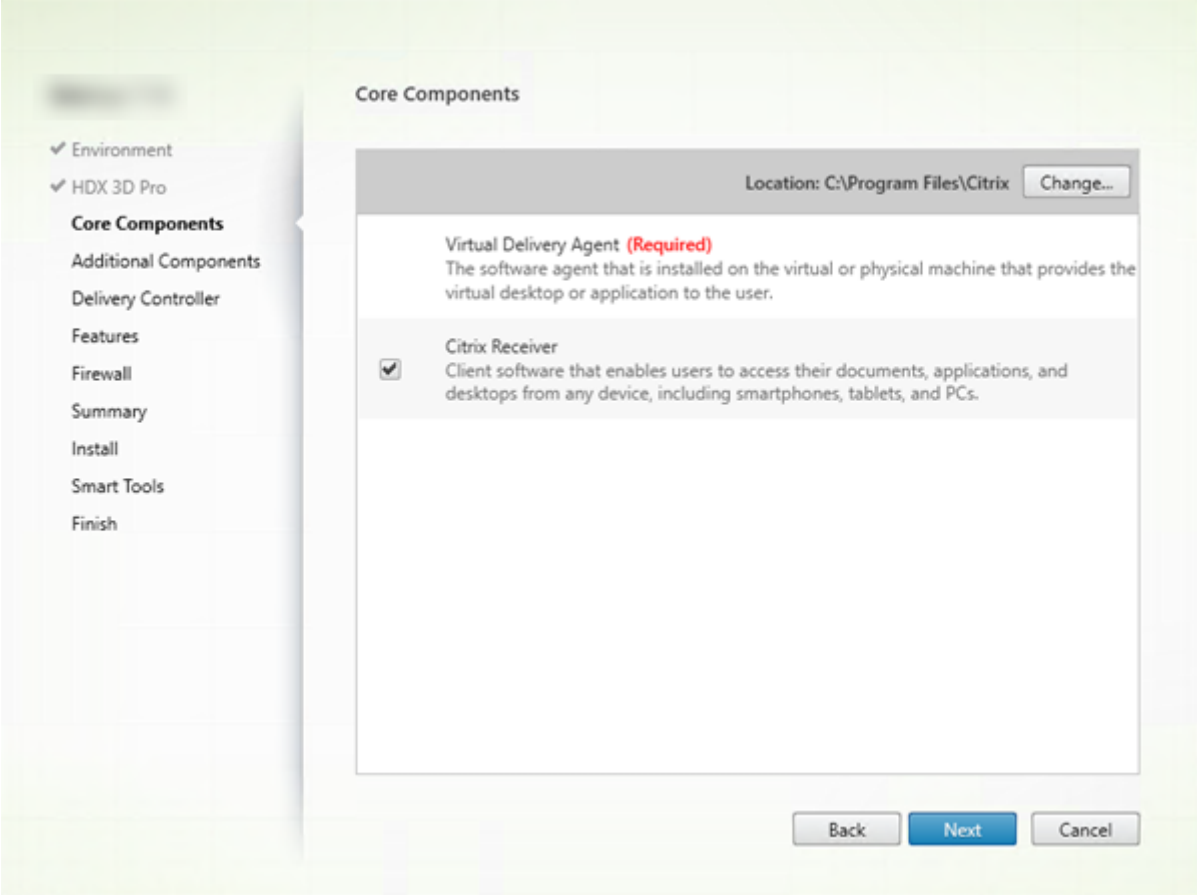
| Standard mode | HDX 3D Pro mode |
| --- | --- |
| Usually best for virtual desktops without graphics hardware acceleration, and for Remote PC Access. | Usually best for data center desktops with graphics hardware acceleration, unless more than four monitors are necessary. |
| Any GPU can be used for Remote PC Access, with some app compatibility limitations: **On Windows 7, 8, and 8.1**, GPU acceleration for DirectX feature levels up to 9.3. Some DirectX 10, 11, 12 applications may not run if they do not tolerate fallback to DirectX 9; **on Windows 10**, GPU acceleration is provided for windowed DirectX 10, 11, and 12 apps. DX 9 apps are rendered by WARP. DX apps cannot be used in full-screen mode; **OpenGL application acceleration** in remote sessions if supported by the GPU vendor (currently only NVIDIA). | Supports GPU acceleration with any GPU. However, console blanking, non-standard screen resolutions and true multi-monitor support require NVIDIA GRID, Intel Iris Pro, or AMD RapidFire graphics. Leverages graphics vendor's driver for broadest application compatibility: **all 3D APIs (DirectX or OpenGL)** that the GPU supports; **full-screen 3D app support** with Intel Iris Pro (Win10 only), NVIDIA GRID, and AMD RapidFire; **support for custom driver extensions and APIs**. For example, CUDA or OpenCL. |
| Arbitrary monitor resolutions (limit determined by Windows OS and performance) and up to eight monitors. | Supports up to four monitors. |
| H.264 hardware encoding available with Intel Iris Pro graphics processors. | H.264 hardware encoding available with Intel Iris Pro graphics processors and NVIDIA cards. |

Click **Next.**

Command-line option: /enable_hdx_3d_pro

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 6. Select the components to install and the installation location




On the **Core components** page:

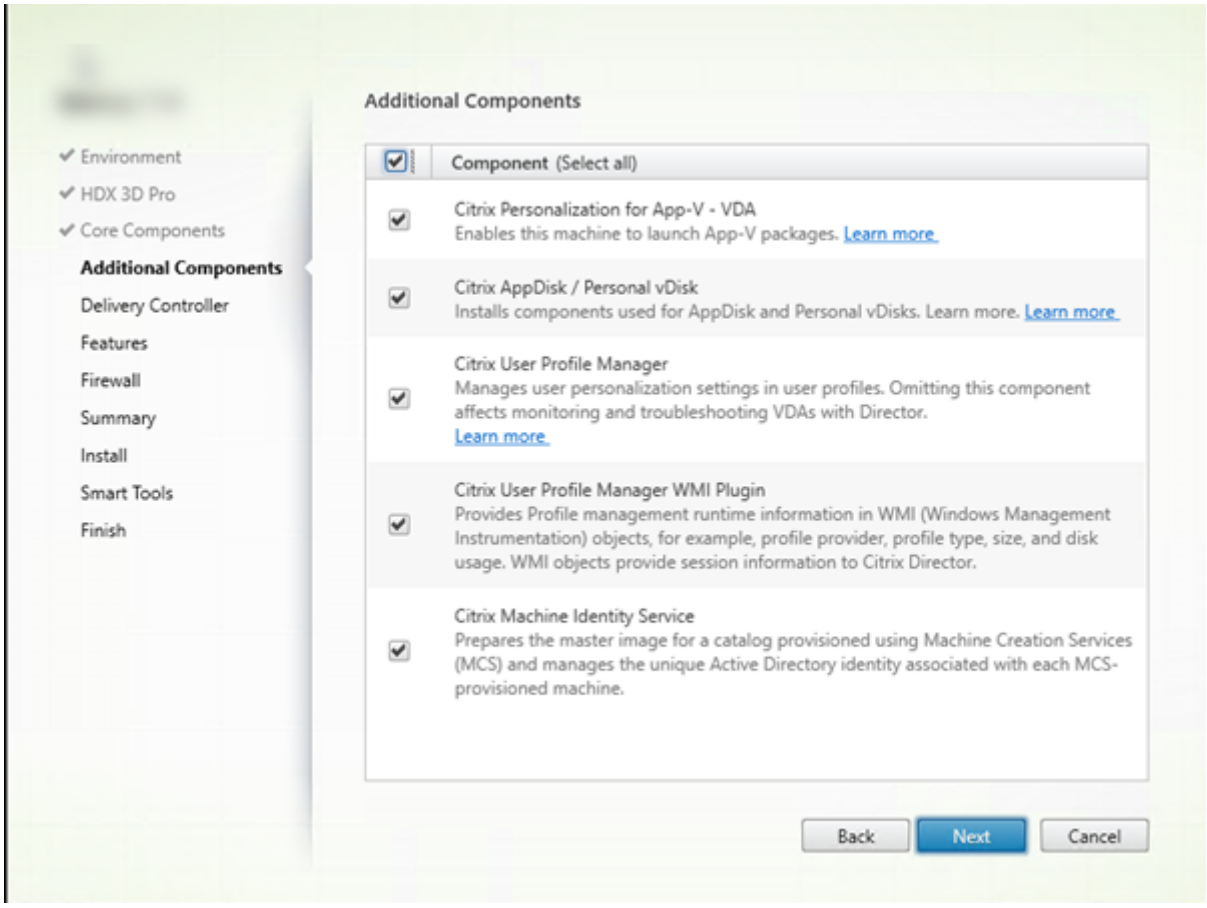
- **Location:** By default, components are installed in C:\Program Files\Citrix. This default is fine for most deployments. If you specify a different location, that location must have execute permissions for network service.
- **Components:** By default, Citrix Receiver for Windows is installed with the VDA (unless you are using the VDAWorkstationCoreSetup.exe installer). Clear the check box if you do not want that Citrix Receiver installed. If you are using the VDAWorkstationCoreSetup.exe installer, Citrix Receiver for Windows is never installed, so this check box is not displayed.

Click **Next**.

Command-line options: /installdir, "/components vda"to prevent Citrix Receiver for Windows installation

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 7. Install additional components




The **Additional Components** page contains check boxes to enable or disable installation of other features and technologies with the VDA. 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.)

**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: /exclude “Citrix Personalization for App-V –VDA”to prevent component installation

**Citrix AppDisk / Personal vDisk:**

Valid only when installing a VDA for Desktop OS on a VM. Installs components used for AppDisk and

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Personal vDisk. For more information, see AppDisks and Personal vDisk.

Command-line option: /exclude "Personal vDisk"to prevent AppDisk and Personal vDisk component installation

**Citrix Profile Management:**

This component manages user personalization settings in user profiles. For details, see Profile Management.

Excluding Citrix Profile management from the installation affects the monitoring and troubleshooting of VDAs 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 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: /exclude "Citrix User Profile Manager"to prevent component installation

**Citrix Profile Management 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: /exclude "Citrix User Profile Manager WMI Plugin"to prevent component installation

**Citrix Machine Identity Service:**

This service prepares the master image for a MCS-provisioned catalog. The service also manages each provisioned machine's unique Active Directory identity.

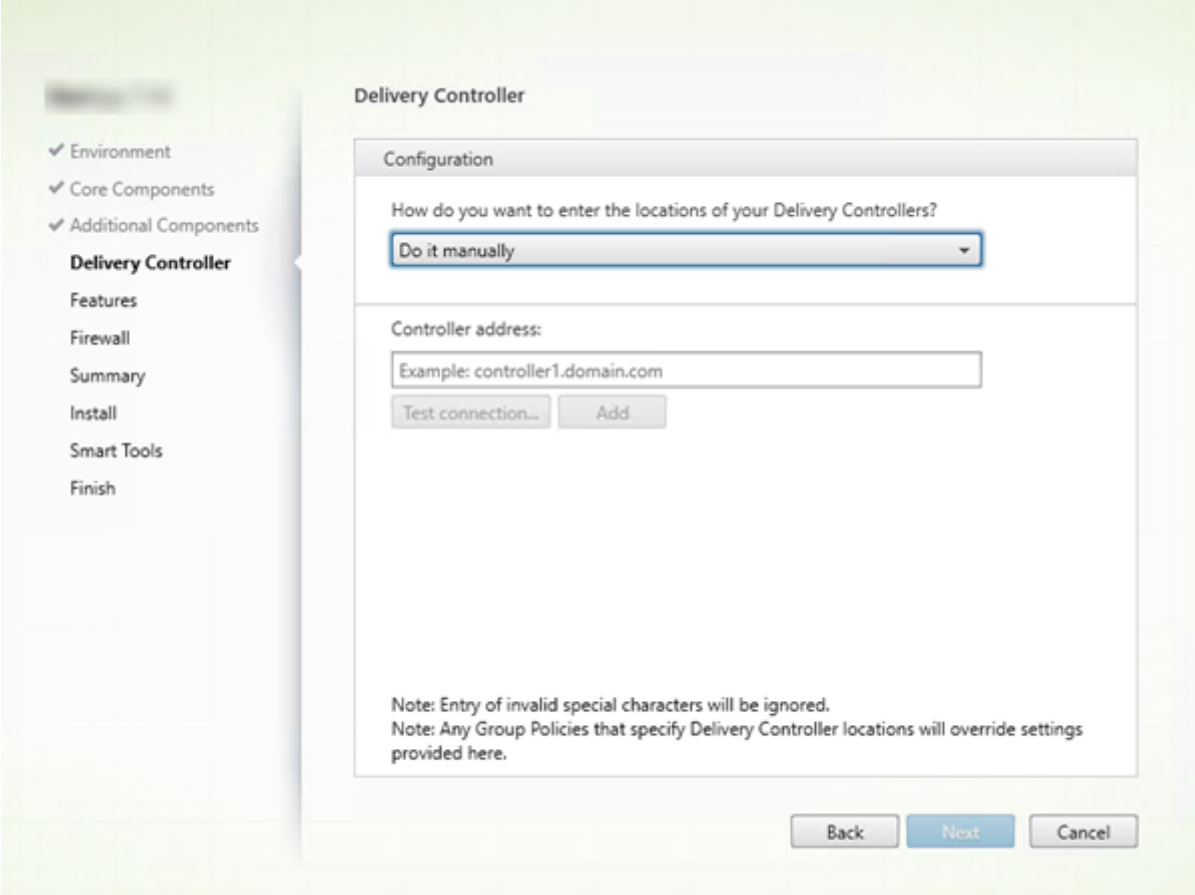
Command-line option: /exclude "Machine Identity Service"to prevent component installation

Default values in the graphical interface:

- If you select "Create a master image"on the **Environment** page (Step 4), items on the **Additional Components** page are enabled by default.
- If you select "Enable Remote PC Access"or "Enable connections to a server machine"on the **Environment** page, items on the **Additional Components** page are disabled by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 8. 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.

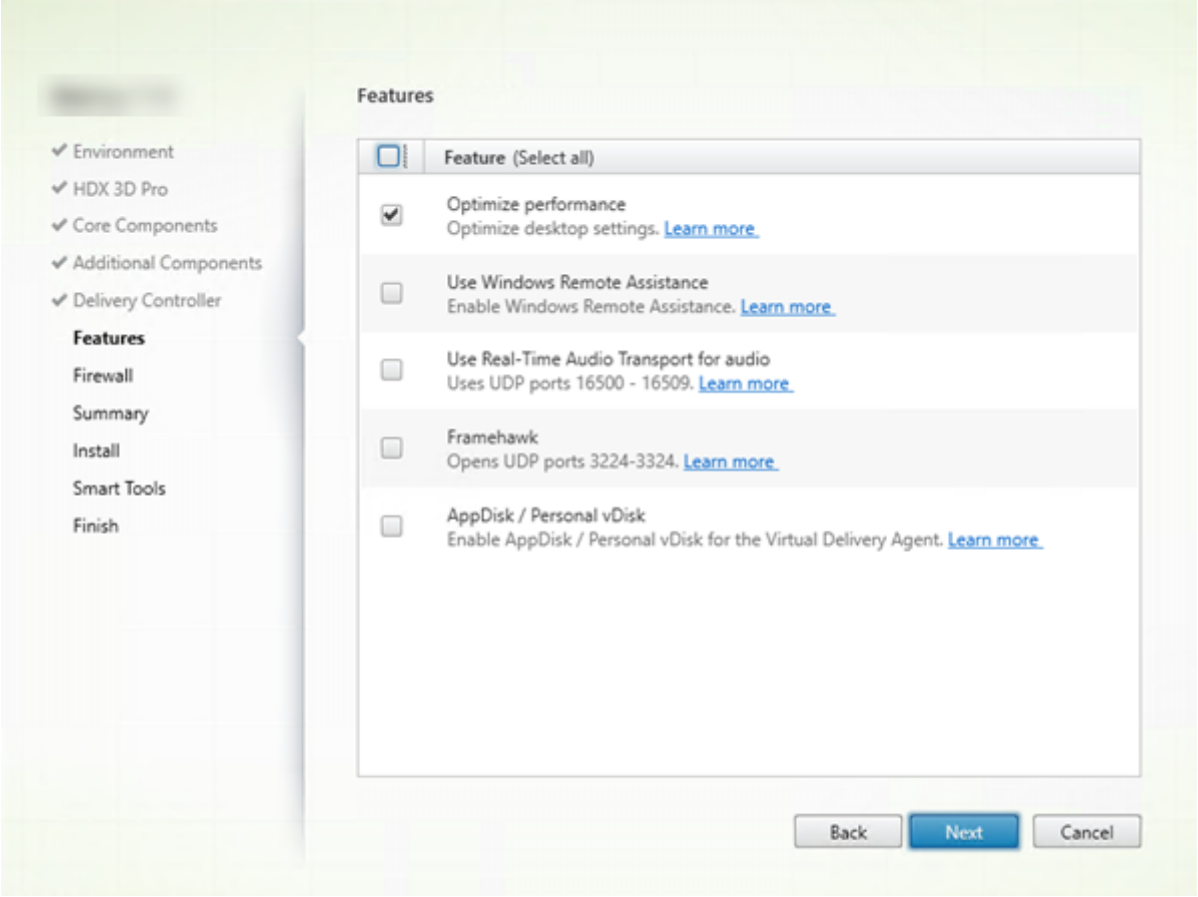
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Other considerations:

- The address cannot contain the 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 Delivery Controllers.

Command-line option: /controllers

### Step 9. Enable or disable features




On the **Features** page, use the check boxes to enable or disable features you want to use.

**Optimize performance:**

Valid only when installing a VDA on a VM, not a physical machine. When this feature is enabled (default), the optimization tool is used for VDAs running in a VM on a hypervisor. VM optimization includes

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

disabling offline files, disabling background defragmentation, and reducing event log size. For details, see CTX224676.

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

**Framehawk:**

When this feature is enabled, bidirectional UDP ports 3224-3324 are opened. (Default = disabled)

You can change the port range later with the "Framehawk display channel port range"Citrix policy setting. You must then open local firewall ports. A UDP network path must be open on any internal (VDA to Citrix Receiver or NetScaler Gateway) and external (NetScaler Gateway to Citrix Receiver) firewalls. If NetScaler Gateway is deployed, Framehawk datagrams are encrypted using DTLS (default UDP port 443). For details, see the Framehawk article.

Command-line option: /enable_framehawk_port

**AppDisk / Personal vDisk**:

Valid only when installing a VDA for Desktop OS on a VM. This check box is available only if the Citrix AppDisk / Personal vDisk check box is selected on the **Additional Components** page. When this check box is enabled, AppDisks and Personal vDisks can be used. For details, see AppDisks and Personal vDisks.

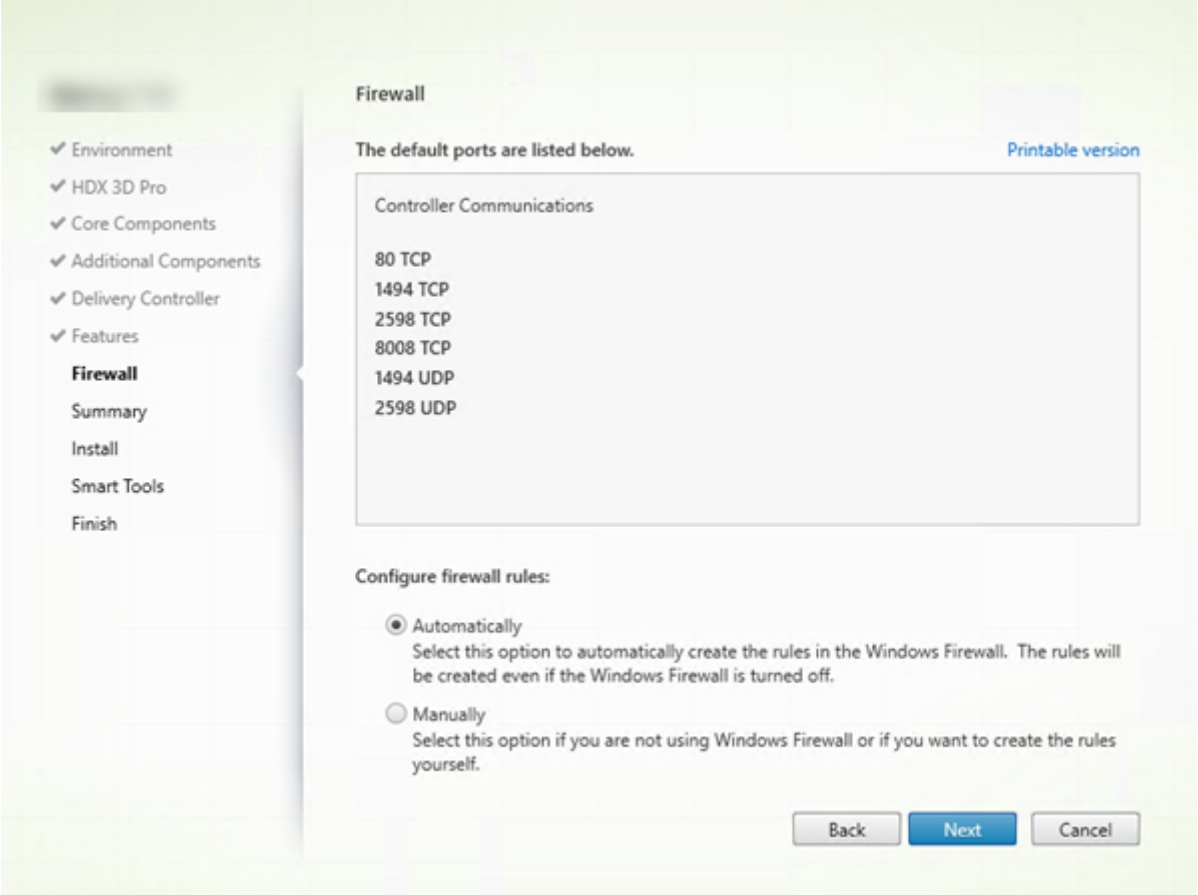
Command-line option: /baseimage

If you are using the VDAWorkstationCoreSetup.exe installer, this feature does not appear in the wizard and the command-line option is not valid.

Click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 10. Firewall ports



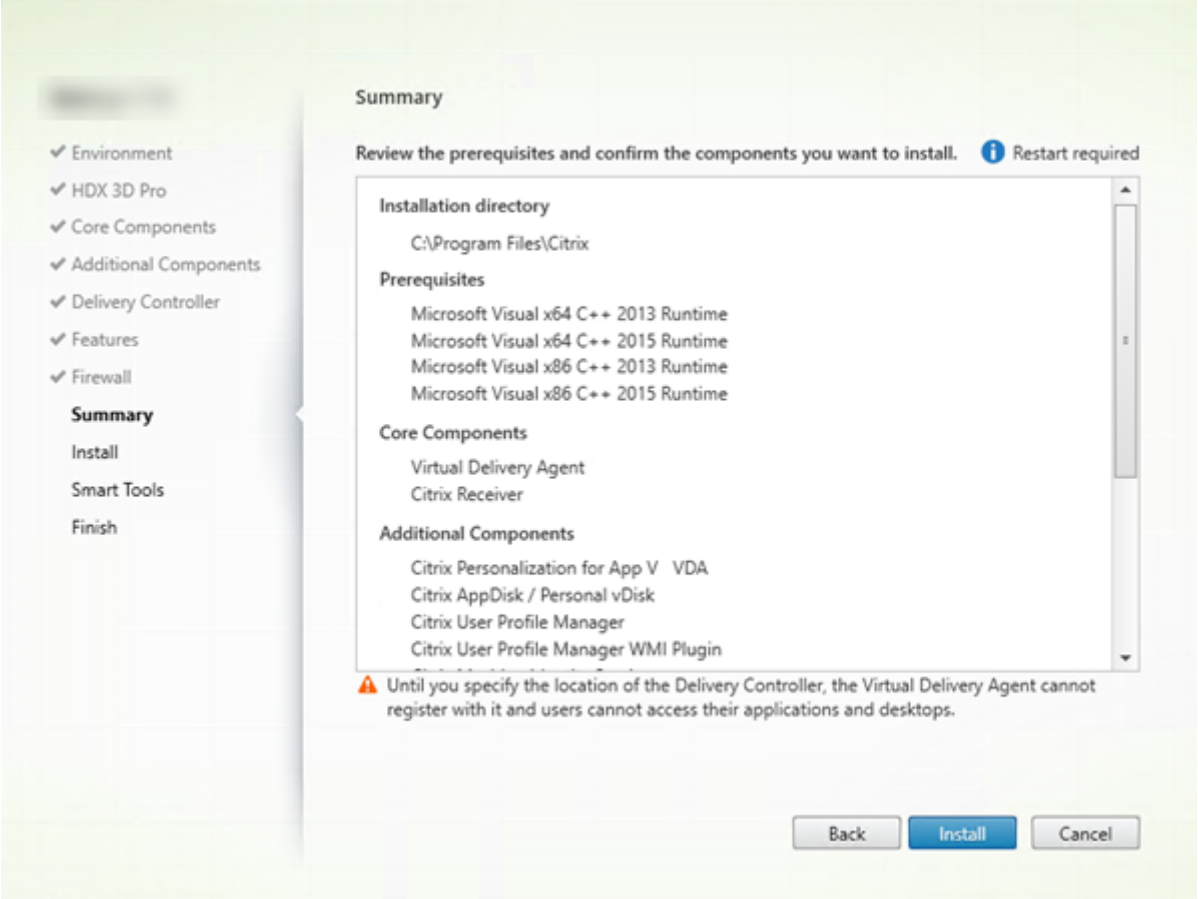

On the **Firewall** page, by default, the ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. This default setting is fine for most deployments. For port information, see Network ports.

Click **Next**.

Command-line option: /enable_hdx_ports

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 11. Review prerequisites and confirm installation



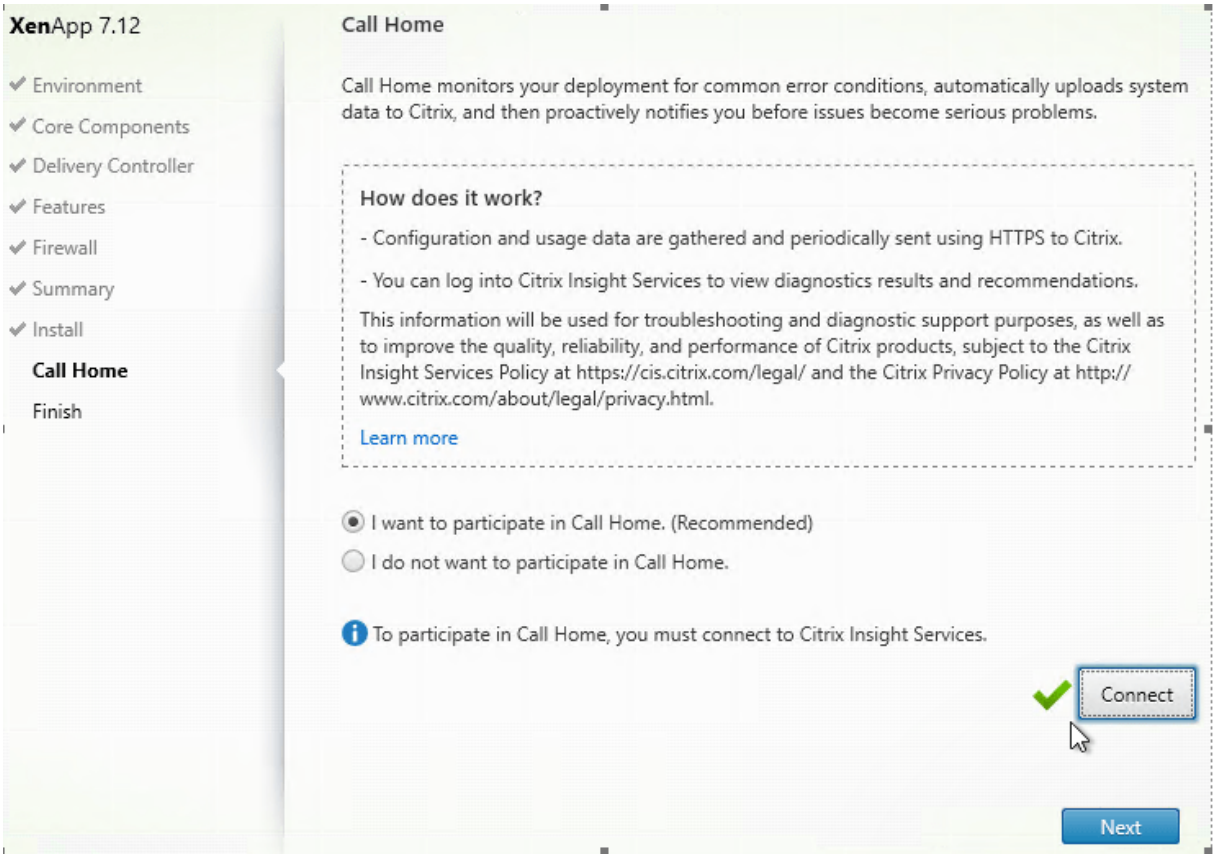

The **Summary** page lists what will be installed. Use the Back button to return to earlier wizard pages and change selections.

When you're ready, click **Install**.

If prerequisites aren't already installed/enabled, the machine may restart once or twice. See Prepare to install.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 12. Participate in Call Home

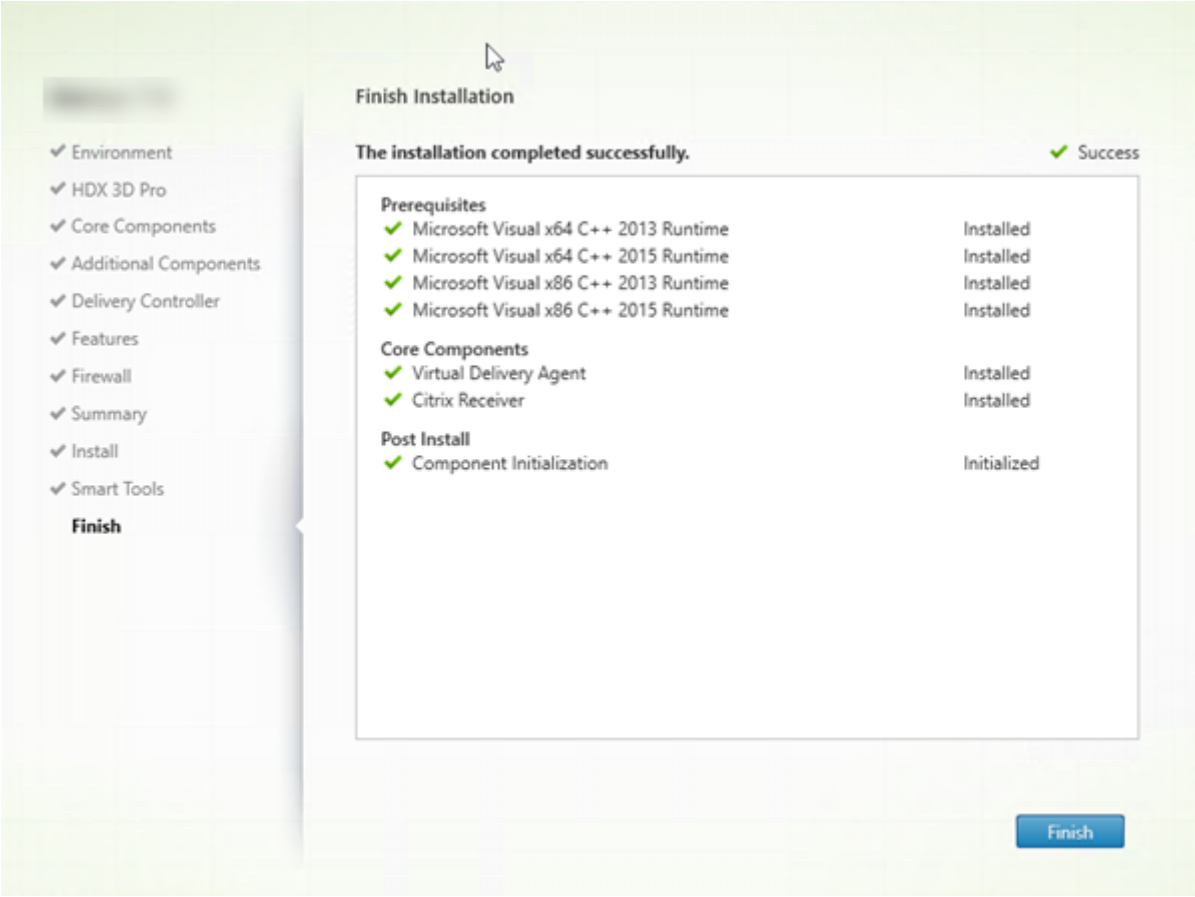



On the **Call Home** page, choose whether to participate in Call Home. If you choose to participate (the default), click **Connect**. When prompted, enter your Citrix account credentials.

After your credentials are validated (or if you choose not to participate), click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 13. 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: Install other VDAs and continue configuration

Repeat the steps 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

Later, if you want to customize an installed VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

If your deployment uses Microsoft System Center Configuration Manager, a VDA installation might appear to fail with exit code 3, even though the VDA installed successfully. To avoid the misleading message, you can wrap your installation in a CMD script or change the success codes in your Configuration Manager package. For more information, see the forum discussion at https://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

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 1, 2020

This article applies to installing components on machines with Windows operating systems. For information about VDAs for Linux operating systems, see the Linux Virtual Delivery Agent documentation.

> **Important:**
>
> 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 VDAs machines in Active Directory. For details, see Install VDAs using scripts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 the `XenDesktopServerSetup.exe` command, with the options listed in Command-line options for installing core components.

#### To install a VDA

Run the `XenDesktopVDASetup.exe` command with the options listed in Command-line options for installing a VDA.

#### To install the Universal Print Server

Follow the guidance in Install the Universal Print Server using the command line.

#### To install the Federated Authentication Service

Citrix recommends using the graphical interface.

#### To install the Self-Service Password Reset Service

Follow the guidance in the Self-Service Password Reset Service documentation.

### 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Download the appropriate package from Citrix:

| Component name on download page | Installer file name |
|---|---|
| Server OS Virtual Delivery Agent <*version*> | VDAServerSetup.exe |
| Desktop OS Virtual Delivery Agent <*version*> | VDAWorkstationSetup.exe |
| Desktop OS Core Services Virtual Delivery Agent <*version*> | VDAWorkstationCoreSetup.exe |

- Either extract the files from the package to an existing directory first and then run the installation command, or just 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 `XenDesktopVdaSetup.exe` from the directory containing the extracted content (in the preceding example, `CitrixVDAInstallMedia`). Use the valid options in Command-line options for installing a VDA.

To run the downloaded package, just run its name: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`. Use the valid options in Command-line options for installing a VDA.

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 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

`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 7.15 LTSR CU6, valid values included StoreFront. For version 7.15 LTSR CU6 and later, use the dedicated StoreFront installation command noted in Install StoreFront).

#### /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

Prevents installation of one or more comma-separated features, services, or technologies, 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.

`Smart Tools Agent`: Prevents installation of the Citrix Smart Tools agent.

> **Note:**
>
> As of CU4, Smart Tools is no longer included in the installer. Instances of Smart Tools present from earlier installations remain untouched.

#### /help or /h

Displays command help.

#### /installdir <*directory*>

Existing empty directory where components will be installed. Default = `c:\Program Files\Citrix`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**/logpath <*path*>**

Log file location. The specified folder must exist. The installer does not create it. Default = `"%TEMP%\Citrix\XenDesktop Installer"`

**/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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### /tempdir <*directory*>

Directory that holds temporary files during installation. Default = c:\Windows\Temp.

#### /xenapp

Installs XenApp. If this option is omitted, XenDesktop is installed.

### Examples: Install core components

The following command installs a XenDesktop 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 XenApp 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
```

### Command-line options for installing a VDA

The following options are valid with one or more of the following commands: `XenDesktopVDASetup.exe`, `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`.

#### /baseimage

Valid only when installing a VDA for Desktop OS on a VM. Enables the use of Personal vDisks with a master image. For details, see Personal vDisk.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

`PLUGINS`: Citrix Receiver for Windows (`CitrixReceiver.exe`)

For example, to install the VDA but not Citrix Receiver, specify `/components vda`.

If this option is omitted, all components are installed.

This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer cannot install a Citrix Receiver.

#### /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_framehawk_port

Opens the UDP ports used by Framehawk. Default = false

#### /enable_hdx_3d_pro

Installs the VDA in HDX 3D Pro mode.

#### /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 and the `/enable_hdx_ports` option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### /enable_hdx_udp_ports

Opens UDP ports in the Windows firewall that are required by HDX adaptive transport, 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 other ports that the VDA uses, specify the `/enable_hdx_ports` option and the `/enable_hdx_udp_ports` option.

#### /enable_real_time_transport

Enables or disables use of UDP for audio packets (Real-Time 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, 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 Personal vDisk or Machine Identity Service components. Valid values are:

- `Personal vDisk`
- `Machine Identity Service`
- `Citrix User Profile Manager`
- `Citrix User Profile Manager WMI Plugin`
- `Citrix Universal Print Client`
- `Citrix Telemetry Service`
- `Citrix Personalization for App-V - VDA`

Excluding Citrix Profile Management from the installation (using the `/exclude "Citrix User Profile Manager"` option) 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

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.

#### /hdxflashv2only

Prevents installation of Flash redirection legacy binaries, for enhanced security.

This option is not available in the graphical interface.

#### /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"`

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 not valid when using the `VDAWorkstationCoreSetup.exe` installer.

#### /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 for N editions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### /nocitrixwddm

Valid only on Windows 7 machines that do not include a WDDM driver. Disables installation of the Citrix WDDM driver.

This option is not available in the graphical interface.

#### /nodesktopexperience

Valid only when installing a VDA for Server 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 remount the media or want to capture information during an automated installation.

#### /optimize

Valid only when installing a VDA on a VM. Enables optimization for VDAs running in a VM on a hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. Do not specify this option for Remote PC Access deployments. For more information, see CTX224676.

#### /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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### /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. Excludes installation of the following components on a Desktop OS:

- Citrix Personalization for App-V
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Machine Identity Service
- Personal vDisk

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), the analytics are collected locally, but not sent automatically.

#### /servervdi

Installs a VDA for Desktop OS on a supported Windows server. Omit this option when installing a VDA for Server OS on a Windows server. Before using this option, see Server VDI.

Use this option only with the full-product VDA installer. This option is not available in the graphical interface.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### /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: Install a VDA

#### Install a VDA with the full-product installer

The following command installs a VDA for Desktop OS and Citrix Receiver to the default location on a VM. This VDA will be used as a master image. The VDA will register initially with the Controller on the server named 'Contr-Main'in the domain 'mydomain.'The VDA will use Personal vDisks, the optimization feature, and Windows Remote Assistance.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /
optimize /masterimage /baseimage /enable_remote_assistance
```

#### Install a Desktop OS VDA with the VDAWorkstationCoreSetup standalone installer

The following command installs a Core Services VDA on a Desktop OS for use in a Remote PC Access or VDI deployment. Citrix Receiver 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Customize a VDA using the command line

After you install a VDA, you can customize several settings. From the `\x64\XenDesktop Setup` directory on the product media, run the `XenDesktopVdaSetup.exe` command, 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`

### Install the Universal Print Server using the command line

Run one of the following commands on each print server:

- On a supported 32-bit operating system: From the `\x86\Universal Print Server\` directory on the Citrix installation media, run `UpsServer_x86.msi`.
- On a supported 64-bit operating system: From the `\x64\Universal Print Server\` directory on the Citrix installation media, run `UpsServer_x64.msi`.

After you install the Universal Print Server component on your print servers, configure it using the guidance in Provision printers.

## Install VDAs using scripts

August 2, 2018

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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

> **Important:**
>
> 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 (such as 7.0.0.3018). 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 with SCCM

March 27, 2020

### Overview

VDA installation has two phases:

- Install prerequisites
- Install the VDA

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To successfully deploy the VDA using Microsoft System Center Configuration Manager (SCCM) or similar software distribution tools, Citrix recommends addressing the phases separately. In other words, instead of using the VDA installer to install both the prerequisites and the VDA, we recommend that you first install the prerequisites using the prerequisites' installers, and then install the VDA using a VDA installer.

### Identify requirements and task sequence

Prerequisites must be installed on the machine before the VDA is installed. VDA prerequisites vary, depending on the VDA version. For guidance, see the system requirements for the VDA version you're installing:

- Citrix Virtual Apps and Desktops Current Release
- Citrix Virtual Apps and Desktops 1912 LTSR
- XenApp and XenDesktop 7.15 LTSR

Similarly, the need to install these prerequisites can vary between environments (for example, based on the target machines' operating system, and what the machines already have installed). Before creating scripts or task sequences, it is important to understand your environment's specific requirements (such as which prerequisites need to be installed). Then, you can properly define the task sequence.

**Tip:** A good way to collect this information is by manually installing the VDA in one of the machines in the environment. This process reveals which prerequisites are identified as needed and installed throughout the VDA installation process.

The installation files for the VDA's prerequisites are included in the installation media for the Citrix Virtual Apps and Desktops (or XenApp and XenDesktop) release under the **Support** folder. Use those files to ensure that you're installing the correct prerequisite versions.

#### Restarts

The required number of restarts during the installation of prerequisites and the VDA depends on the environment. For example, a restart might be required for pending updates or restarts from earlier software installations. Also, files previously locked by other processes might need updates.

- During the manual installation, identify which prerequisites trigger a restart.
- Some optional components in the VDA installer (such as Citrix User Profile Manager, Citrix Files) might require a restart. During the manual installation, identify which component installations trigger a restart.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Define the task sequence

After identifying all prerequisites and restarts, use the SCCM Task Sequencer to complete the following:

1. Create separate SCCM jobs for installing each prerequisite. This helps isolate any issues or failures that occur during the deployment, which facilitates troubleshooting.
2. Create the VDA installation job. Do not execute this job until all prerequisites are successfully installed. This can be accomplished one of two ways:
    - Have the SCCM client monitor the prerequisites' GUIDs to determine whether they are present.
    - Make the VDA installation job dependent on the prerequisites' jobs.

### SCCM installation sequence example

The following is an example SCCM installation sequence. Remember: Your prerequisite versions may differ, depending on which VDA version you're installing.

1. SCCM JOB1: Microsoft .NET Framework 4.8
2. SCCM JOB2: Microsoft Visual C++ 2017 Runtime (32-bit and 64-bit)
3. SCCM JOB3: VDA installation
    a) Use the appropriate VDA installer command, based on requirements. Add the `/quiet`, `/noreboot`, and `/noresume` options. (The `/noresume` option removes the dependency on the interactive login to continue the install, thus allowing SCCM to drive the installation process.)
    b) Watch for return codes.
        - `0`: success, installation complete, restart required.
        - `3`: success, installation is not complete, restart required.
        - `8`: success, installation complete, restart required.
    c) Restart the machine.
    d) If the return code was 3, repeat step 3a.

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. (Links are provided to Citrix Virtual Apps and Desktops Current Release locations. If you're using an LTSR product version, see the equivalent LTSR articles.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Install VDAs
- Install using the command line

#### Installation commands for Remote PC Access

- The following command uses the single-session core VDA installer (standalone VDAWorkstationCoreSet.exe):

```
VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.
com" /enable_hdx_ports /noresume /noreboot
```

- The following command uses the single-session full VDA installer (standalone 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 (standalone VDAWorkstationSetup.exe):

```
VDAWorkstationSetup.exe /quiet /components vda /controllers "
control.domain.com" /enable_hdx_ports /optimize /enable_remote_assistance
 /noresume /noreboot
```

## Create a Site

August 17, 2018

A *Site* is the name you give to a XenApp or XenDesktop 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.

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 https://more.citrix.com/XD-CEIP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The user who creates a Site becomes a full administrator; for more information, see Delegated Administration.

Review this article before you start the Site creation wizard.

### To create a Site

Open Studio if it is not already open. You are automatically guided to the action that starts the Site creation wizard. The wizard pages cover the following configuration:

#### Site type and name

There are two Site types; choose one:

- **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*).

#### 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 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 Controllers to the Site, and have already installed the Controller software on other servers, you can add those Controllers from this page. If you plan to generate scripts that set up the databases, add the Controllers before generating the scripts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Licensing

Consider whether you will use existing licenses or the 30-day free trial that allows you to add license files later. You can also add or download license files from within the Site creation wizard. For details, see the Licensing documentation.

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 in the wizard until a successful connection is made to the License Server.

### Power management (Remote PC Access only)

See Remote PC Access.

### 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.

**Connection page**: See Connection type information sources.

- 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.

**Storage and Network pages**: See Host storage, Storage management, and Storage selection for details about storage types and management methods.

### Additional Features

You can select features to customize your Site. When you select the check box for an item that requires information, a configuration box appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**AppDNA Integration** Valid 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. For more information, see AppDisks.

**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.

#### 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 Microsoft System Center Configuration Manager.

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, credential, 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**.

When you create a Remote PC Access Site, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Summary

The last page of the Site creation wizard summarizes 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.

### 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

November 12, 2019

Collections of physical or virtual machines are managed as a single entity called a machine catalog. All the machines in a catalog have the same type of operating system: server or desktop. A catalog containing Server 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.

### 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 Provisioning Services (PVS). Or, you can use your own

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tools to provide machines.

- If you use PVS to create machines, see the Provisioning Services documentation for instructions.
- If you use MCS to provision VMs, you provide a master image (or snapshot) 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 a snapshot of an image), specify the number of VMs to create in the catalog, and configure additional information.
- If your machines are already available (so you do not need master images), you must still create one or more machine catalogs for those machines.

When using MCS or PVS 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. You can run the tests at any time from Studio.

For on-premises deployments only: When using MCS or PVS 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.

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.

#### 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 a variety of 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 could not

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

be obtained about a machine (perhaps because it had never registered), you might choose to add the machine anyway.

For messages about functional level, see VDA versions and functional levels.

For more information about VDA registration troubleshooting, see CTX136668.

#### MCS catalog creation summary

Here's a brief overview of default MCS actions after you provide information in the catalog creation wizard.

- If you 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 (noted above), which is read-only and shared across the just-created VMs.
  - A unique 16 MB identity disk that gives each VM a unique identity. Each VM gets an identity disk.
  - A unique difference disk to store writes made to the VM. This disk is thin provisioned (if supported by the host storage) and increases to the maximum size of the master image, if necessary. Each VM gets a 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.

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.

### 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- A master image might also be known as a clone image, golden image, base VM, or base image. Host vendors and cloud service providers may use different terms.
- When using PVS, you can use a master image or a physical computer as the master target device. PVS uses different terminology than MCS to refer to images; see the Provisioning Services 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 re-arm Microsoft Windows or Microsoft Office. If your deployment includes a 5.x VDA with a XenServer 6.0.2 host, see CTX128580.
- Install and configure the following software on the master image:
  - Integration tools for your hypervisor (such as XenServer 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 anti-virus 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 PVS or MCS, do not run Sysprep on master images.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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 PVS, create a VHD file for the vDisk from your master target device before you join the master target device to a domain. See the Provisioning Services 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.

**Prepare a master image for GPU-capable machines on XenServer**

When using XenServer for your hosting infrastructure, 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 XenServer 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Create a machine catalog using Studio

Before starting the catalog creation wizard, review this section to learn about the choices you make and information you supply.

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 items described below. The wizard pages you see may differ, depending on the selections you make.

### Operating system

Each catalog contains machines of only one type:

- **Server OS**: A Server OS catalog provides hosted shared desktops and applications. 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.)
- **Desktop OS**: A Desktop OS catalog provides VDI desktops and applications that can be assigned 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 or not machines in the catalog will be 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Services (PVS):** Manages target devices as a device collection. A PVS vDisk imaged from a master target device delivers desktops and applications. This option is not available for cloud deployments.
- **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 Desktop 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 to connect to a static desktop when logging in, the **Device collection** screen appears. When you establish this connection type, the catalog displays the Personal vDisk in the user data field under the machine type.

#### Master image

This page appears only when you are using MCS to create VMs.

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 will be the one you configured when you created the Site.

Remember:

- When you are using MCS or PVS, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 may contain additional pages specific to that host.

For details, see Where to find information about connection types.

#### Device Collection

This page appears only when using PVS to create VMs. It displays the device collections and the devices that have not already been added to catalogs.

Select the device collections to use. See the Provisioning Services documentation for details.

#### 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 to create machines:**

- Specify how many virtual machines to create.
- Choose the amount of memory (in MB) each VM will have.
- **Important:** Each created VM will have 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 should be saved on a separate Personal vDisk, specify the vDisk size in gigabytes 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 PVS to create machines:**

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**When using other tools to provide machines:**

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** wizard 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 wizard page.

**When using PVS or other tools (but not MCS):**

An icon and tooltip for each machine added (or imported, or from a PVS 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 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.

A drop-down near the bottom of the **Machines** (or **Devices**) page allows you to select the minimum VDA level that will successfully register; 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 XenApp and XenDesktop 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 XenApp and XenDesktop

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

7.15 LTSR contains a 7.15 VDA, the default functional level ("7.9 .or later") remains the most current. Therefore, after installing or upgrading components from 7.9-7.14 to 7.15 LTSR, 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, but be aware that 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; however, that will prevent 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 Desktop OS catalog, or adding a Desktop OS machine originally created for random allocation to a catalog of static machines.

### 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.

To enable the caching of temporary data, the VDA on each machine in the catalog must be minimum version 7.9.

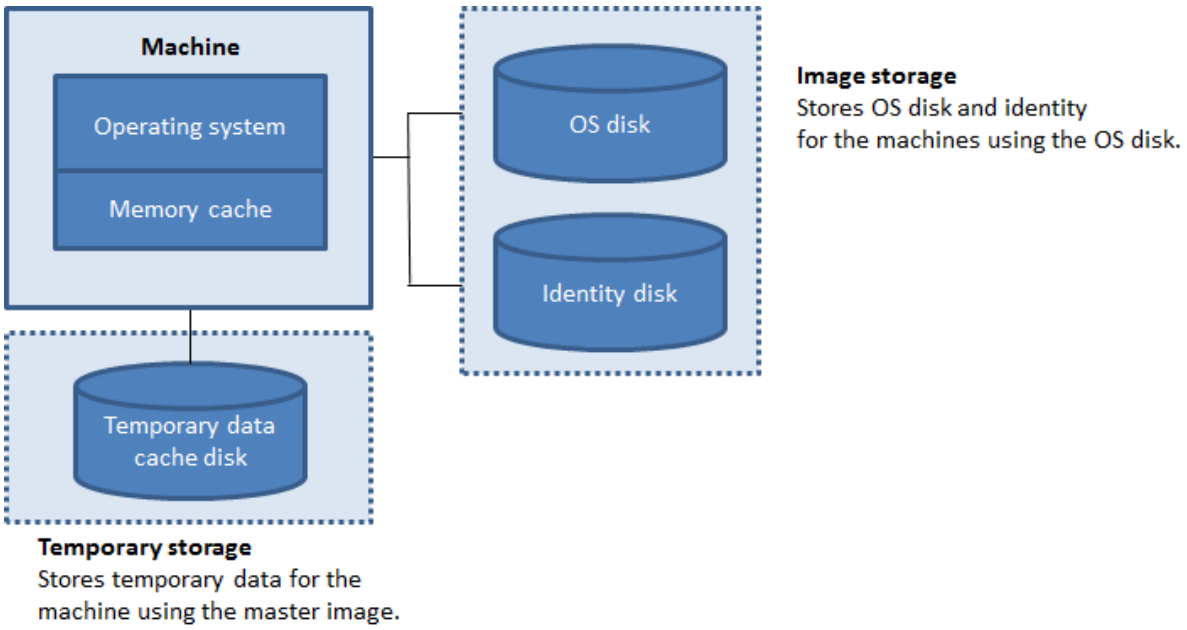
You specify whether temporary data uses shared or local storage when you create the connection that the catalog uses; for details, see Connections and resources. Enabling and configuring the temporary cache in the catalog includes two check boxes and values: **Memory allocated to cache (MB)** and **Disk cache size (GB)**. The default values differ according to the connection type. 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 may be created or copied by a session user or any applications users may install inside the session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Windows will not allow a session to use an amount of cache disk that is significantly 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.

If you enable the **Disk cache size** 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.




The memory cache is part of the total amount of memory on each machine; therefore, if you enable the **Memory allocated to cache** check box, consider increasing the total amount of memory on each machine.

If you clear the **Memory allocated to cache** check box and leave the **Disk cache size** check box enabled, temporary data is written directly to the cache disk, using a minimal amount of memory cache.

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.

> **Important:**
>
> If the disk cache runs out of space, the user's session becomes unusable.

If you clear the **Disk cache size** check box, no cache disk will be created. In this case, specify a **Memory allocated to cache** value that is large enough to hold all of the temporary data; this is feasible only if large amounts of RAM are available for allocation to each VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If you clear both check boxes, temporary data is not cached; it is written to the difference disk (located in the OS storage) for each VM. (This is the provisioning action in releases earlier than 7.9.)

Do not enable caching if you intend to use this catalog to create AppDisks.

This feature is not available when using a Nutanix host connection.

You cannot change the cache values in a machine catalog after it is created.

#### Network Interface Cards (NICs)

This page does not appear when you are creating Remote PC Access catalogs.

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.

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. Indicate whether to create new accounts or use existing accounts, and the location for those accounts.

- If you create new accounts, you must have access to a domain administrator account for the domain where the machines will reside.

Specify the account naming scheme for the machines that will be created, using hash marks to indicate where sequential numbers or letters will 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 PVS, computer accounts for target devices are managed differently; see the Provisioning Services documentation.

#### Summary, name, and description

On the **Summary** page of the wizard, review the settings you specified. Enter a name and description for the catalog; this information appears in Studio.

After reviewing the information you specified, click **Finish** to start the catalog creation.

### Troubleshoot

Citrix recommends collecting logs to help the Support team provide solutions. Use the following procedure to generate log files when using PVS:

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 new snapshot.
3. On the Delivery Controller, run the following command:

   ```
   Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
    -Value $True
   ```

4. Create a new 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:\ drive:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Image-prep.log
- PvsVmAgentLog.txt

6. Shut the machine down, 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_NoAutoShutdo
```

## Manage machine catalogs

March 23, 2021

### Introduction

You can add or remove machines from a machine catalog, in addition to 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.

- For catalogs containing pooled random machines created using Machine Creation Services (MCS), maintain machines by updating the master image used in the catalog. Once the master images are updated, update the machines. This process enables you to efficiently update large numbers of user machines. For machines created using Provisioning Services, updates to machines are propagated through the vDisk. See the Provisioning Services documentation for details.
- Catalogs containing static, permanently assigned machines, and for Remote PC Access Machine catalogs, you manage updates to users' machines outside of Studio, 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.

#### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

instance. To ensure this, the master image must be updated using PowerShell commands. For more information, see Knowledge Center article CTX129205.

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 machine 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 machine 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.

### Change a machine 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 machine 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Move a machine 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 machine 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 machine catalog

To manage Active Directory accounts in a machine catalog, you can:

- Free unused machine accounts by removing Active Directory computer accounts from Desktop OS and Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 machine 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. You can roll back (revert) machines in a catalog to use the previous version of the master image 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 Provisioning Services, you must publish a new vDisk to apply changes to the catalog. For details, see the Provisioning Services documentation.

After a machine is updated, it restarts automatically.

### Update or create a master image

Before you update the 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 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 XenServer XenCenter console.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 will be updated with the new master image: on the next shutdown or immediately. See below for details.
5. Verify the information on the **Summary** page and then click **Finish**. Each machine restarts automatically after it is updated. A VDA in maintenance mode cannot be restarted.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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 machine 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 Provisioning Services, upgrade the VDA version. The provisioning console does not retain the VDA version. Provisioning Services communicates directly with the XenApp and XenDesktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Troubleshoot

For machines with "Power State Unknown"status, see CTX131267 for guidance.

## Create Delivery Groups

October 30, 2019

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 will guide 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

Select a Machine Catalog and select the number of machines you want to use from that catalog.

Good to know:

- At least one machine must remain unused in a selected Machine Catalog.
- A Machine Catalog can be specified in more than one Delivery Group; however, a machine can be used in only one Delivery Group.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Machine Catalogs and Delivery Groups as needed. When creating a Delivery Group, if you select machines that have different VDA versions installed, the Delivery Group will be compatible with the earliest VDA version. (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 Machine 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.

### Step 2. Delivery type

This page appears only if you chose a Machine Catalog containing static (assigned) desktop OS machines. Choose either **Applications** or **Desktops** on the Delivery Type page; 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

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.

AppDisks are deprecated.

### Step 4. Users

Specify the users and user groups who can use the applications and desktops in the Delivery Group.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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 Receiver. (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 Receiver. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 named AnonXYZ, in which XYZ is a unique three-digit value.

Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

The following table describes your choices on the Users page:

| Enable access for | Add/assign users and user groups? | Enable the "Give access to unauthenticated users"check box? |
|---|---|---|
| Only authenticated users | Yes | No |
| Only unauthenticated users | No | Yes |
| Both 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 Receiver.

Click the **Add** dropdown to display the application sources.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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 the App-V article.

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 Machine Catalog.

### Step 6. Desktops (or Desktop Assignment Rules)

The title of this page depends on the Machine Catalog you chose earlier in the wizard:

- If you chose a Machine Catalog containing pooled machines, this page is titled Desktops.
- If you chose a Machine Catalog containing assigned machines and specified "Desktops"on the Delivery Type page, this page is titled Desktop User Assignments.
- If you chose a Machine 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 Receiver.
- To add a tag restriction to a desktop, select **Restrict launches to machines with this tag** and then select the tag from the dropdown. (See the Tags article for more information.)
- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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**.

### Step 7. Summary

Enter a name for the Delivery Group. You can also (optionally) enter a description, which will appear in Receiver 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 30, 2020

### Introduction

This article describes the procedures for managing Delivery Groups. 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.

See Applications for information about managing applications in Delivery Groups, including how to add and remove applications in a Delivery Group, and change application properties.

Managing Delivery Groups requires the Delegated Administration permissions of the Delivery Group Administrator built-in role. See Delegated Administration for details.

### Change user settings in a Delivery Group

The name of this page may appear as either **User Settings** or **Basic Settings**.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Setting | Description |
| --- | --- |
| Description | The text that StoreFront uses and that users see. |
| Enable Delivery Group | Whether or not the Delivery Group is enabled. |
| Time zone | Adjusts time zone. |
| 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 the Users section in the Create Delivery Groups article.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **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**. You can also select/clear the check box that enables or disables 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 Desktop 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 Studio navigation pane.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. Select a Delivery Group, and then select **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.

### 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 a **desktops only** type, delete all applications from the group.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **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 Studio navigation pane.
2. Select a group and then select **Edit Delivery Group** in the Actions pane.
3. On the **StoreFront** page, select or add StoreFront URLs that will be used by the Citrix Receiver that 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 address by selecting **Configuration > StoreFront** in the Studio navigation pane.

### 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 the Tags article.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

5. To change or remove a tag restriction, either select a different tag 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.

### 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 Provisioning Services, upgrade the VDA version in the Provisioning Services console.
- Start the machines containing the upgraded VDA so that they can register with a Delivery Controller. This process tells Studio 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 articles.

To upgrade a Delivery Group:

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **Upgrade Delivery Group** in the Actions pane. The **Upgrade Delivery Group** action appears only if Studio detects upgraded VDAs.

Before starting the upgrade process, Studio tells 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 selecting **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, Studio temporarily assigns the machine 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. You can set this priority value using the PowerShell SDK.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Studio navigation pane.
2. Select a Remote PC Access group.
3. In the Details section, select the **Machine Catalogs** tab and then select a Remote PC Access catalog.
4. To add or restore an association, select **Add Desktops**. To remove an association, select **Remove Association**.

### 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 Studio navigation pane.
2. Select a group and then select **View Machines** in the Actions pane.
3. Select the machine and then select one of the following 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 Desktop 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; see the Connections and resources article.

### Power manage machines in a Delivery Group

You can power manage only virtual Desktop OS machines, not physical ones (including Remote PC Access machines). Desktop OS machines with GPU capabilities cannot be suspended, so power-off

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

operations fail. For Server OS machines, you can create a restart schedule, which is also described in this article.

In Delivery Groups containing pooled machines, virtual Desktop 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 Desktop 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 that 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 examples, machines will suspend automatically outside of office hours if users have been 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To power manage virtual Desktop OS machines:

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group, and then select **Edit Delivery Group** in the Actions pane.
3. On the **Power Management** page, select **Weekdays** in the Power manage machines drop-down. By default, weekdays are Monday to Friday.
4. For random Delivery Groups, in **Machines to be powered on**, select **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 select Suspend. In **During off-peak hours > When disconnected**, specify the delay before turning off any logged-off machine in the Delivery Group, and select **Shutdown**. This timer is not available for Delivery Groups with random machines.
7. Select **Weekend** in the Power manage machines drop-down, 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.

### Create a restart schedule for machines in a Delivery Group

This section describes how to configure a single restart schedule in Studio. Alternatively, you can use PowerShell to configure multiple restart schedules for different subsets of machines in a Delivery Group. See the next section for details.

A restart schedule specifies when to periodically restart all the machines in a Delivery Group.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **Edit Delivery Group** in the Actions pane.
3. On the **Restart Schedule** page, if you do not want to restart machines in the Delivery Group automatically, select the **No** radio button and skip to the last step in this procedure. No restart schedule or rollout strategy will be configured. If a schedule was previously configured, this selection cancels it.
4. If you do want to restart machines in the Delivery Group automatically, select the **Yes** radio button.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

5. For **Restart** frequency, choose either **Daily** or the day of the week the restarts will occur.
6. For **Begin restart at**, using a 24-hour clock, specify the time of day to begin the restart.
7. For **Restart duration**, choose whether all machines should be started at the same time, or the total length of time to begin restarting all machines in the Delivery Group. An internal algorithm determines when each machine is restarted during that interval.
8. In the left **Notification** drop-down, 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 the **Repeat notification** drop-down) to repeat the message every five minutes after the initial message. By default, the message is not repeated.
9. Enter the notification text in the **Notification message** box; 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 will be automatically restarted in %m% minutes.*) If you select a repeat notification interval and your message includes the %m% placeholder, the value decrements by five minutes in each repeated message. Unless you chose to restart all machines at the same time, the notification message displays on each machine in the Delivery Group at the appropriate time before the restart, calculated by the internal algorithm.
10. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

You cannot perform an automated power-on or shutdown from Studio, only a restart.

### Create multiple restart schedules for machines in a Delivery Group

You can use PowerShell cmdlets to create multiple restart schedules for machines in a Delivery Group. Each schedule can be configured to affect only those machines in the group that have a specified tag. This tag restriction functionality allows you to easily create different restart schedules for different subsets of machines in one Delivery Group.

For example, let's say you use one Delivery Group for all machines in the company. You want to restart every machine at least once every week (on Sunday night), but the machines used by the accounting team should be restarted daily. You can set up a weekly schedule for all machines, and a daily schedule for just the machines used by the accounting team.

**Schedule overlap:**

Multiple schedules might overlap. In the example above, the machines used by accounting are affected by both schedules, and might be restarted twice on Sunday.

The scheduling code is designed to avoid restarting the same machine more often than needed, but it cannot be guaranteed. If both schedules coincide precisely in start and duration times, it is more likely that the machines will be restarted only once. However, the more the schedules differ in start

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

and/or duration times, the more likely two restarts will occur. Also, the number of machines affected by the schedules can also influence the chances of an overlap. In the example, the weekly schedule that restarts all machines could initiate restarts significantly faster than the daily schedule (depending on the configured duration for each).

**Requirements:**

Support for creating multiple restart schedules and using tag restrictions in a restart schedule is currently available only through the PowerShell command line, using RebootScheduleV2 PowerShell cmdlets that are new in XenApp and XenDesktop 7.12. (These are referred to as the "V2"cmdlets throughout this article.)

Using the V2 cmdlets requires:

- Delivery Controller version 7.12 (minimum).
  - If you use the latest SDK plug-in with a Controller earlier than 7.12, any new schedules you create will not work as intended.
  - In a mixed site (where some, but not all Controllers have been upgraded), the V2 cmdlets will not work until the database is upgraded and at least one Controller has been upgraded and is being used (by specifying the –adminaddress <controller> parameter with the V2 cmdlets).
  - Best practice: Do not create any new schedules until all Controllers in the site are upgraded.
- PowerShell SDK snap-in provided with XenApp and XenDesktop 7.12 (minimum). After you install or upgrade your components and site, run asnp Citrix.* to load the latest cmdlets.

Studio currently uses earlier V1 RebootSchedule PowerShell cmdlets, and will not display schedules that are created with the V2 cmdlets.

After you create a restart schedule that uses a tag restriction, and then later use Studio to remove the tag from an affected machine during a restart interval (cycle) or add the tag to additional machines during a restart cycle, those changes will not take effect until the next restart cycle. (The changes will not affect the current restart cycle.)

**PowerShell cmdlets:**

Use the following RebootScheduleV2 cmdlets from the command line to create multiple schedules and use tag restrictions in the schedules.

- New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
- Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
- Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
- Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
- Rename-BrokerRebootScheduleV2 (new; not a replacement)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For complete cmdlet syntax and parameter descriptions, enter **Get-Help** –**full** <*cmdlet-name*>.

Terminology reminder: In the PowerShell SDK, the DesktopGroup parameter identifies the Delivery Group.

If you're familiar with the Studio interface for creating a restart schedule, all of those parameters are available when using the V2 cmdlet to create or update a schedule. Additionally, you can:

- Restrict the schedule to machines that have a specified tag.
- Specify an interval before sending the first warning message, during which no new sessions will be brokered to the affected machines.

**Configuration:**

If you configure a restart schedule that uses a tag restriction, you must also add (apply) that tag to the machines that you want the schedule to affect. (For more information, see Tags.)

1. From Studio, select **Delivery Groups** in the navigation pane.
2. Select the Delivery Group containing the machines that will be affected by the schedule.
3. Select View Machines and then select the machines where you'll add a tag.
4. Select **Manage Tags** in the Actions pane.
5. If the tag already 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 box.

After creating and adding (applying) tags, use the –RestrictToTag parameter to specify the tag name when creating or editing the schedule with the V2 cmdlet.

**If you created a restart schedule with an earlier XenApp or XenDesktop version:**

Studio currently uses the V1 RebootSchedule cmdlets. If you have a restart schedule that was created before you upgraded to 7.12 (minimum), you can continue to manage it in Studio with V1 cmdlets, but you cannot use Studio to add a tag restriction to that schedule, or to create additional schedules (because Studio does not support the V2 cmdlets). As long as you use the V1 cmdlets for your existing schedule, Studio will display correct information about the restart schedule.

Alternatively, you can edit your existing schedule from the command line, using the new V2 RebootSchedule cmdlets. When using the new V2 cmdlets, you can use the tag restriction parameters in that schedule, and create additional restart schedules. However, after you use V2 cmdlets to change your existing schedule, Studio will not display complete schedule information (because it recognizes only V1 information). You cannot see whether a tag restriction is used, or the schedule's name and description.

```
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
```

### 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 Server OS machine is in maintenance mode, users can connect to existing sessions, but cannot start new sessions.
- When a Desktop 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 Studio navigation pane.
2. Select a group.
3. To turn on maintenance mode for all machines in the Delivery Group, select **Turn On Maintenance Mode** in the Actions pane. To turn on maintenance mode for one machine, select **View Machines** in the Actions pane. Select a machine, and then select **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 select **Turn Off Maintenance Mode** in the Actions pane.

Windows Remote Desktop Connection (RDC) settings also affect whether a Server 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

You can also turn maintenance mode on or off for a connection (which affects the machines that use that connection), or for a machine catalog (which affects the machines in that catalog).

### Change assignments of machines to users in a Delivery Group

You can change the assignments of Desktop OS machines, not Server OS machines or machines created through Provisioning Services.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group.
3. Select **Edit Delivery Group** in the Actions pane. On the **Desktops** or **Desktop Assignment Rules** page (only one of those pages will be available, depending 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

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **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.

### Load manage machines in Delivery Groups

You can load manage Server 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 Server OS machine is considered for load balancing only when maintenance mode is off.

**Server load index**: Determines how likely a server delivering Server 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. You specify the load evaluators in load management policy settings.

You can monitor the load index in Director, Studio search, and the SDK.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

In Studio, the Server Load Index column is hidden by default. To display it, select a machine, right-select a column heading and then choose Select Column. In the Machine category, select Load Index.

In the SDK, use the Get-BrokerMachine cmdlet. For details, see CTX202150.

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.

**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 versions earlier than 7.5.)

If 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.

### Remove a machine from a Delivery Group

Removing a machine deletes it from a Delivery Group but 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.

Keep in mind that machines may contain personal data, so use caution before allocating the machine to another user. You may want to reimage the machine.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and the select **View Machines** in the Actions pane.
3. Make sure that the machine is shut down.
4. Select **Remove from Delivery Group** in the Actions pane.

You can also remove a machine from a Delivery Group through the connection the machine uses. For details, see Connections and resources.

### 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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. See the Delegated Administration article for details.

**Restrict access for users through SmartAccess policy expressions** that filter user connections made through NetScaler Gateway.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select group and then select **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 NetScaler Gateway site, and add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios. For details, see the NetScaler 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** 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 subnet in the corporate network, to prevent access from that lab to a particular Delivery Group, regardless of who is using the machines in the lab, use the following 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 unified Citrix Receiver user experience feature enabled in the store, you cannot use a client name exclusion filter.

### Update a machine in a Delivery Group

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **View Machines** in the Action pane.
3. Select a machine and then select **Update Machines** in the Actions pane.

To choose a different master image, select **Master image**, and then select a snapshot.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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), and whether users will be notified of the restart, plus the message they will receive.

### 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 Desktop OS machines to automatically handle unused sessions. See the Power manage machines section for details.

### 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 on Server OS machines only.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Windows Server OS, minimum version 7.6.
- These features are supported only when using Citrix Receiver for Windows, and also require additional Citrix Receiver configuration. For instructions, search for session prelaunch in the product documentation for your Citrix Receiver for Windows version.
- Note that Citrix Receiver for HTML5 is not supported.
- When using session prelaunch, if a user's machine is put into "suspend" or "hibernate" mode, prelaunch will not work (regardless of session prelaunch settings). Users can lock their machines/sessions, but if a user logs off from Citrix Receiver, 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 license, but only when connected. 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 Receiver.

#### 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 will 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

You cannot disable this timeout from Studio, but you can in the SDK (`New`/`Set-BrokerSessionPreLaun` cmdlet). If you disable the timeout, it will not appear in the Studio 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 server resources are available. Unused prelaunched and lingering sessions will not cause denied connections because they will be ended automatically when resources are needed for new user sessions.

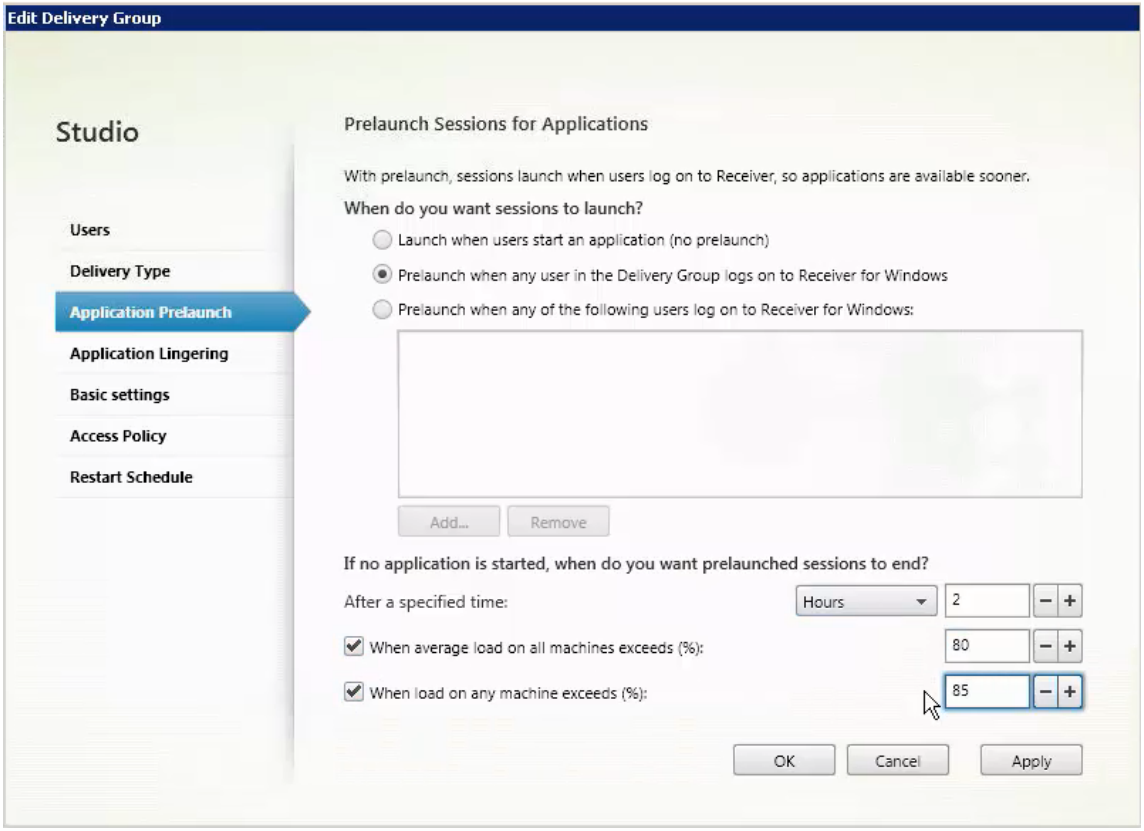
  You can configure two thresholds: the average percentage load of all servers in the Delivery Group, and the maximum percentage load of a single server in the Delivery Group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended, sessions 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 the Controller and servers in maintenance mode are considered fully loaded. An unplanned outage causes prelaunch and lingering sessions end automatically to free capacity.

**To enable session prelaunch**

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a Delivery Group, and then click **Edit Delivery Group** in the Actions pane.
3. On the **Application Prelaunch** page, enable session prelaunch by choosing when sessions should 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 Receiver for Windows.
   - When anyone in a list of users and user groups logs on to Citrix Receiver for Windows. Be sure to also specify users or user groups if you choose this option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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.

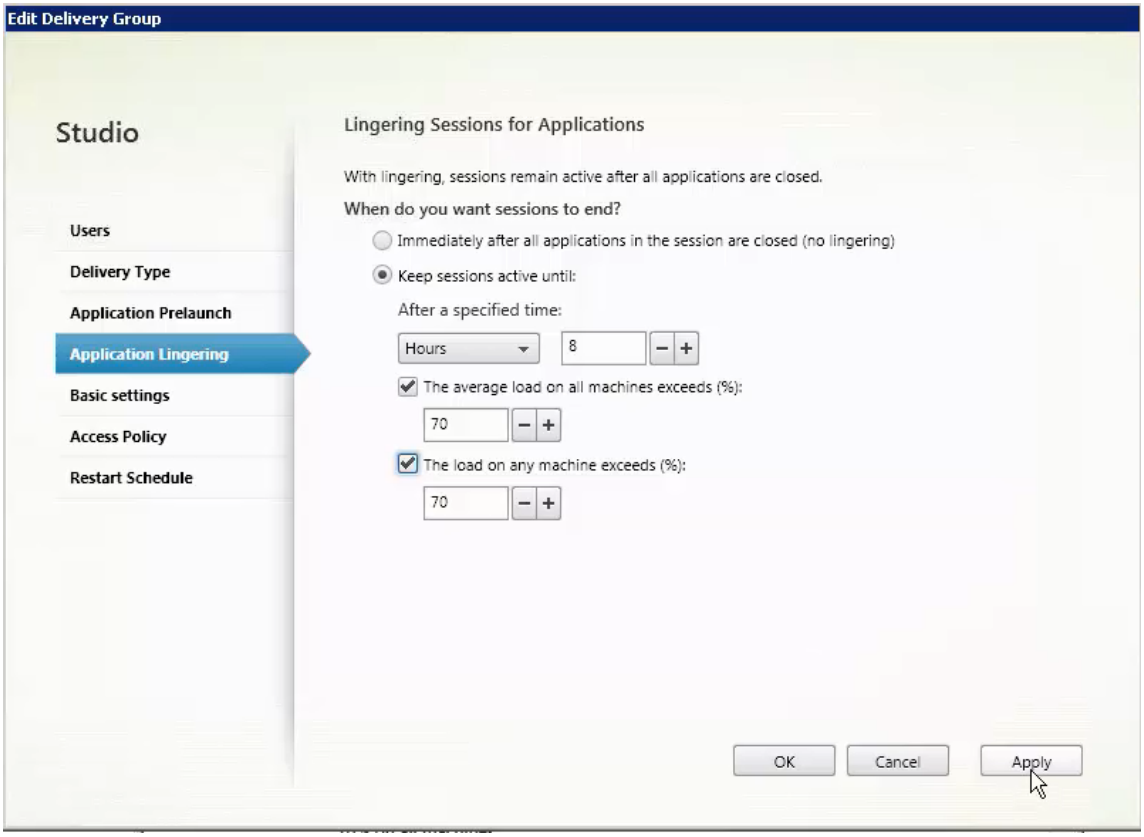
    - When a specified time interval elapses. You can change the time interval (1-99 days, 1-2376 hours, or 1-142,560 minutes).
    - When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99%).
    - When the load on any machine in the Delivery Group exceeds a specified 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 Studio navigation pane.
2. Select a Delivery Group, and then click **Edit Delivery Group** in the Actions pane.
3. On the **Application Lingering** page, enable session linger by selecting the **Keep sessions active until** radio button.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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, which results 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 a catalog to a Delivery Group.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 should 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 should be"machine, review the Troubleshoot tab in the details pane for possible causes and recommended corrective actions.

For messages about functional level, see see VDA versions and functional levels. For more information about VDA registration troubleshooting, see CTX136668.

- In the Studio 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

July 17, 2018

### 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:

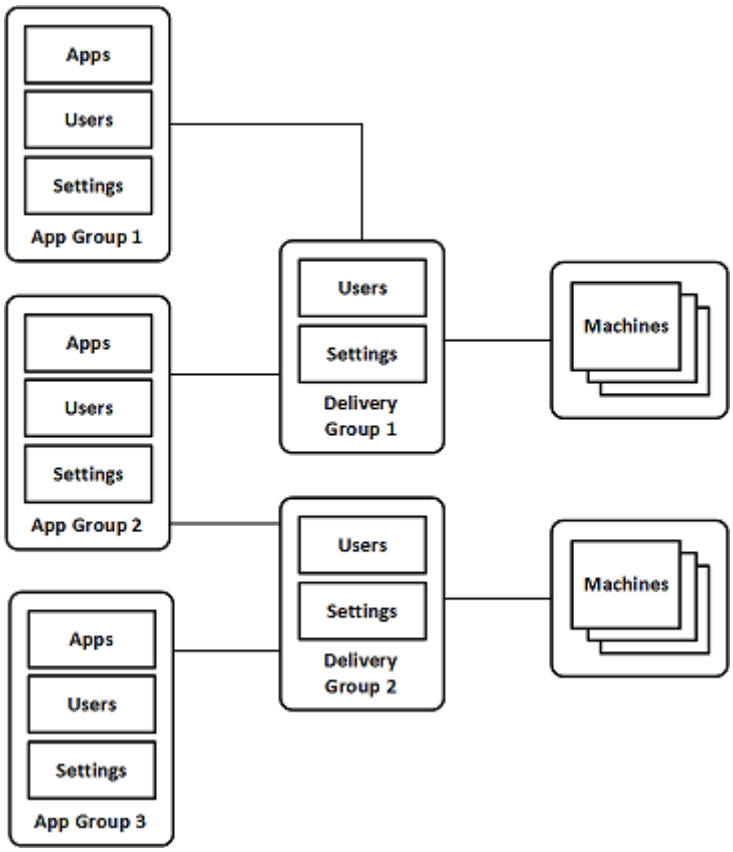
- The logical grouping of applications and their settings lets you manage those applications as a single unit. For example, you don't have to add (publish) the same application to individual Delivery Groups one at a time.
- Session sharing between Application Groups can conserve resource consumption. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp or XenDesktop deployment that includes Application Groups:



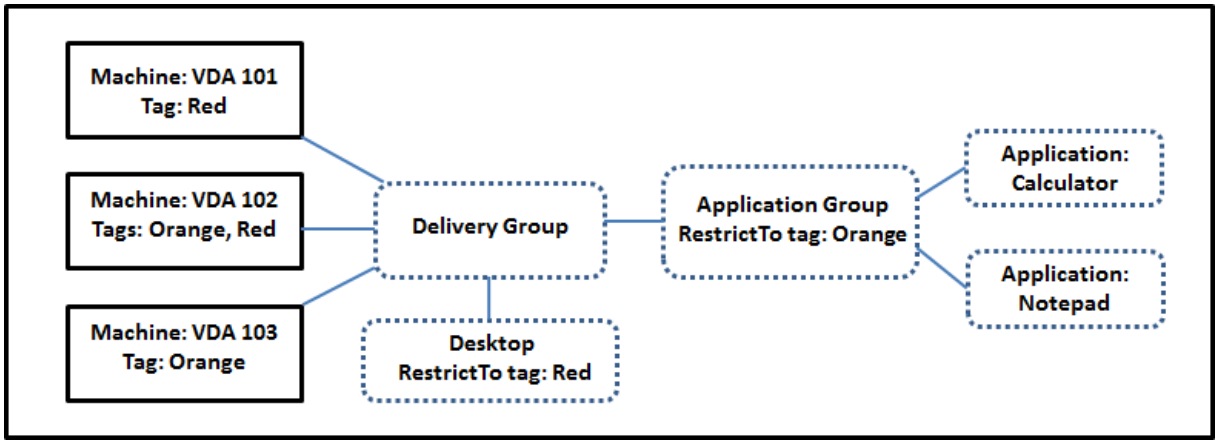

In this configuration, applications are added to the Application Groups, not the Delivery Groups. The Delivery Groups specify which machines will be used. (Although not shown, the machines are in Machine Catalogs.)

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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, then (2) upgrading the machine catalogs containing those machines, and then (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.

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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

Example when disabling session sharing within Application Groups is helpful:

- You want your users to access multiple simultaneous full screen sessions of an application on separate monitors.

  You create an Application Group and add the applications to it. If session sharing is prohibited between applications in that Application Group, when a user specified in it starts one applica-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tion after another they launch in separate sessions, and the user can move each to a separate monitor.

By default, application session sharing is enabled when you create an Application Group; you cannot change this when you create the group. After you create an Application Group, you can edit the group to change this setting. See Manage Application Groups.

### Create an Application Group

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.

#### Delivery Groups

All Delivery Groups are listed, with the number of machines each contains.

- The **Compatible Delivery Groups** list contains Delivery Groups you can select. Compatible Delivery Groups contain random (not permanently or statically assigned) server or desktop OS machines.
- The **Incompatible Delivery Groups** list contains Delivery Groups you cannot select. Each entry explains why it is not compatible, such as containing static assigned machines.

An Application Group can be associated with Delivery Groups containing shared (not private) machines that can deliver applications.

You can also select Delivery Groups containing shared machines that deliver desktops only, if (1) the Delivery Group contains shared machines and was created with an earlier XenDesktop 7.x version, and (2) 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 in use –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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. See Tags for details.

#### 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.

**Where user lists are specified** Active Directory user lists are specified when you create or edit the following:

- The entitlement user list for the delivery group, which is not configured through Studio. By default, the application entitlement policy rule includes everyone; see the PowerShell SDK BrokerAppEntitlementPolicyRule cmdlets for details.
- The Application Group user list.
- The Delivery Group user list.
- The Application visibility property.

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 restricting 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.
- Configure the Application Group user list to allow members of the Administration and Finance business unit to access applications named A through L.
- Configure application A's properties to restrict its visibility to only Accounts Receivable staff in Administration and Finance.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Receiver.
- 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 (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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Scopes

This page appears only if you have previously created a scope. By default, the All scope is selected. For more information, see Delegated Administration.

#### 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

July 4, 2018

### Introduction

This article describes the procedures for managing 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 about application session sharing, see Session sharing between 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 Broker 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 may want users to start non-seamless applications in full-size application windows on separate monitors. For more information about application session sharing, see Session sharing with Application Groups.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

You can use the Broker 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
```

> **Notes:**
>
> - To enable the SingleAppPerSession property you must set 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 only works for applications which 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 having the option set to True, the other set to False) which 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Add, remove, or change 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 desktops only, if (1) the Delivery Group contains shared machines and was created with an earlier XenDesktop 7.x version, and (2) 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

**Important:** Adding, changing, and removing tag restrictions can have unanticipated effects on which machines are considered for application launch. Be sure to review the considerations and cautions in the Tags article.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Add or remove users in an Application Group

For detailed information about users, see the *Users* section in the Create Application Groups article.

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 the Delegated Administration article.

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 your attempt to delete 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, but 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Remote PC Access

August 18, 2021

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 Virtual Delivery Agent (VDA) for Desktop OS and for 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

PC use case.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The PC must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.
- If using Wi-Fi, do the following:

  1. Set the power settings to leave the wireless adapter turned on.
  2. Configure the wireless adapter and network profile to allow automatic connection to the wireless network before the user logs on. Otherwise, the VDA does not register until the user logs on. The PC isn't available for remote access until a user has logged on.
  3. Ensure that the Delivery Controllers or Cloud Connectors can be reached from the Wi-Fi network.

- You can use Remote PC Access on laptop computers. Ensure that the laptop is connected to a power source instead of running on the battery. Configure the laptop power options to match the options of a desktop PC. For example:

  1. Disable the hibernate feature.
  2. Disable the sleep feature.
  3. Set the close lid action to **Do Nothing**.
  4. Set the "press the power button"action to **Shut Down**.
  5. Disable video card and NIC energy-saving features.

- Remote PC Access is supported on Surface Pro devices with Windows 10. Follow the same guidelines for laptops mentioned previously.
- If using a docking station, you can undock and redock laptops. When you undock the laptop, the VDA reregisters with the Delivery Controllers or Cloud Connectors over Wi-Fi. However, when you redock the laptop, the VDA doesn't switch to use the wired connection unless you disconnect the wireless adapter. Some devices provide built-in functionality to disconnect the wireless adapter upon establishing a wired connection. The other devices require custom solutions or third-party utilities to disconnect the wireless adapter. Review the Wi-Fi considerations mentioned previously.

  Do the following to enable docking and undocking for Remote PC Access devices:

  1. In the **Start** menu, select **Settings > System > Power & Sleep**, and set **Sleep** to **Never**.
  2. Under the **Device Manager > Network adapters > Ethernet adapter** go to **Power Management** and clear **Allow the computer to turn off this device to save power**. Ensure that **Allow this device to wake the computer** is checked.

- Multiple users with access to the same office PC see the same icon in Citrix Workspace. When a user logs on to Citrix Workspace, that resource appears as unavailable if already in use by another user.
- Install the Citrix Workspace app on each client device (for example, a home PC) that accesses the office PC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Session management

By default, a remote user's session is automatically disconnected when a local user initiates a session on that machine (by pressing CTRL+ATL+DEL). To prevent this automatic action, add the following registry entry on the office PC, and then restart the machine.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: SasNotification
- Type: DWORD
- Data: 1

By default, the remote user has preference over the local user when the connection message is not acknowledged within the timeout period. To configure the behavior, use this setting:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaMode
- Type: DWORD
- Data:
  - 1 - The remote user always has preference if he or she does not respond to the messaging UI in the specified timeout period. This behavior is the default if this setting is not configured.
  - 2 - The local user has preference.

The timeout for enforcing the Remote PC Access mode is 30 seconds by default. You can configure this timeout but do not set it lower than 30 seconds. To configure the timeout, use this registry setting:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaTimeout
- Type: DWORD
- Data: number of seconds for timeout in decimal values

When a user wants to forcibly get the console access: The local user can press Ctrl+Alt+Del twice in a gap of 10 seconds to get local control over a remote session and force a disconnect event.

After the registry change and machine restart, if a local user presses Ctrl+Alt+Del to log on to that PC while it is in use by a remote user, the remote user receives a prompt. The prompt asks whether to allow or deny the local user's connection. Allowing the connection disconnects the remote user's session.

### Wake on LAN

Integrated Wake on LAN is available only in on-premises Citrix Virtual Apps and Desktops and requires Microsoft System Center Configuration Manager (SCCM).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Troubleshoot

#### Diagnostic Information

Diagnostic information about Remote PC Access is written to the Windows Application Event log. Informational messages are not throttled. Error messages are throttled by discarding duplicate messages.

- 3300 (informational): Machine added to catalog
- 3301 (informational): Machine added to delivery group
- 3302 (informational): Machine assigned to user
- 3303 (error): Exception

#### Power management

If power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method. Ensure that those settings are enabled in the advanced properties for the power management connection.

### 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

June 30, 2020

### Using App-V with XenApp and XenDesktop

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 | XenDesktop and XenApp versions | |
|---|---|---|
| | **Delivery Controller** | **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 |
| 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 Receiver
- From the Start menu

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Through the App-V client and Citrix Receiver
- 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.

#### Management methods

You can use App-V packages 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.

- **Network share:** Packages placed on a network share removes Studio's dependence on the App-V server and database infrastructure, thereby lowering overhead. (You still need to install the Microsoft App-V client on each VDA.)

  This is called the *single admin* management method because App-V package and application use requires only 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.

  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.

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 and/or on a network share.

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 in the package.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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.

#### 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.

### Setup

The following table summarizes the sequence of setup tasks for using App-V in XenApp and XenDesktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 |
| 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/?redirectedfrom=MSDN.

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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 installed and enabled by default when you install a VDA.

You can control this default action during VDA installation. In the graphical interface, clear the **Citrix Personalization for App-V - VDA** check box on the **Additional Components** page. In the command line interface, include the **/exclude "Citrix Personalization for App-V - VDA"** option.

If you expressly disable installation of 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 are not using a publishing server, but have packages on the VDA managed by another mechanism (such as SCCM, custom scripting, or a third party App-V management solution), the clean-up routines may remove packages which are still required. In this scenario, add a dummy App-V Management server registration to the VDA to prevent clean up being attempted.

### 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)?redirectedfrom=MSDN.
- 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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

specifying the credentials of the user who has administrator privileges on the App-V server. For guidance, see https://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 will display: "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)?redirectedfrom=MSDN.
- Do packages have the appropriate security permissions for the Studio administrator to access?

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 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

August 12, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## 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 XenApp and XenDesktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 up-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

grade 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 XenApp and XenDesktop 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, XenApp and XenDesktop coordinate with the AppLibrary, then interact with Creation Services (MCS) or Provisioning Services (PVS), 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 the System requirements article.

The AppDisks feature is supported only in deployments containing (at minimum) versions of the Delivery Controller and Studio provided in the XenApp and XenDesktop 7.8 download, including the prerequisites that the installer automatically deploys (such as .NET 4.5.2).

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 the Create Delivery Groups article.

To provision VMs that will be used to create AppDisks, you can use:

- MCS provided with the 7.8 Controller (minimum).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- PVS version provided on the download page with your XenApp and XenDesktop 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 XenApp and XenDesktop.

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 XenApp and XenDesktop 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 XenApp or XenDesktop 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

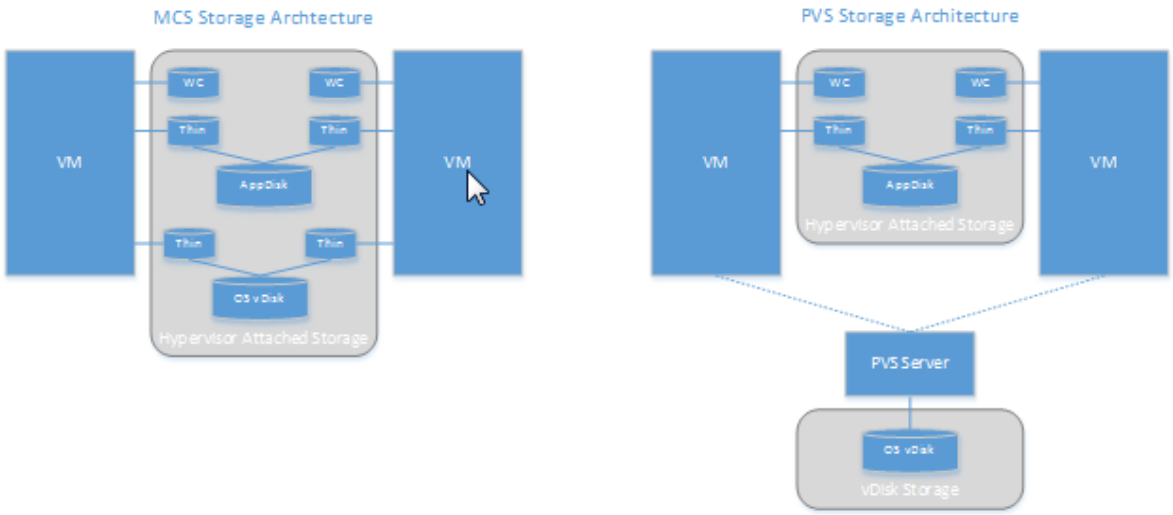
- There is a dependency between Studio and AppDNA server versions.
  - From version 7.12, Studio must be the same, or a higher version than the AppDNA server.
  - For versions 7.9 and 7.11, Studio and AppDNA server versions must match.
  - The following table summarizes which versions work together (Yes = versions work together, –= versions do not 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 PVS 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 PVS environments:

- You must allow for the increased capacity and IOPS as applications move from AppDisk storage to the hypervisor-attached storage.
- With PVS, 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 PVS environments to accommodate those changes.
- AppDisks in the hypervisor-attached storage require more IOPS while the OS vDisks require fewer.
- Write cache: PVS 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

In either MCS or PVS 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 PVS, applications are not located on the OS vDisk, so fewer requests are made to the PVS server. With the resulting lighter load on each target device, the PVS server can stream to more targets. However, be aware that the increased target-server density might negatively affect boot storm performance.

### Create an AppDisk

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.
- If you use AppDNA, following the guidance in the Requirements section above. 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."

#### PVS 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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 PVS, follow the guidance in the PVS considerations section above.

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

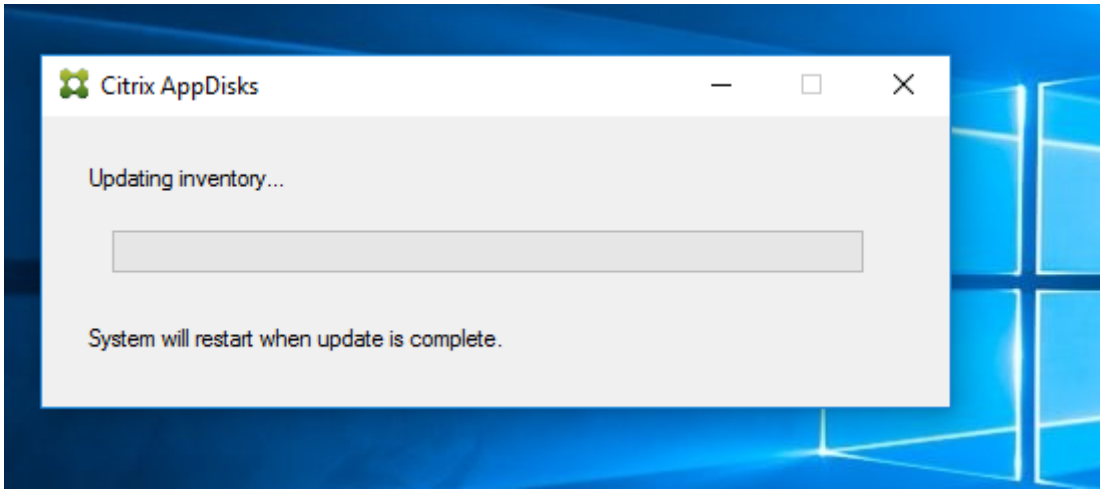
1. Select **AppDisks** in the Studio navigation pane.
2. Select the AppDisk you created, and then select **Seal AppDisk** in the Actions pane.

After you create the AppDisk, install applications on it, and then seal it, assign it to a Delivery Group.

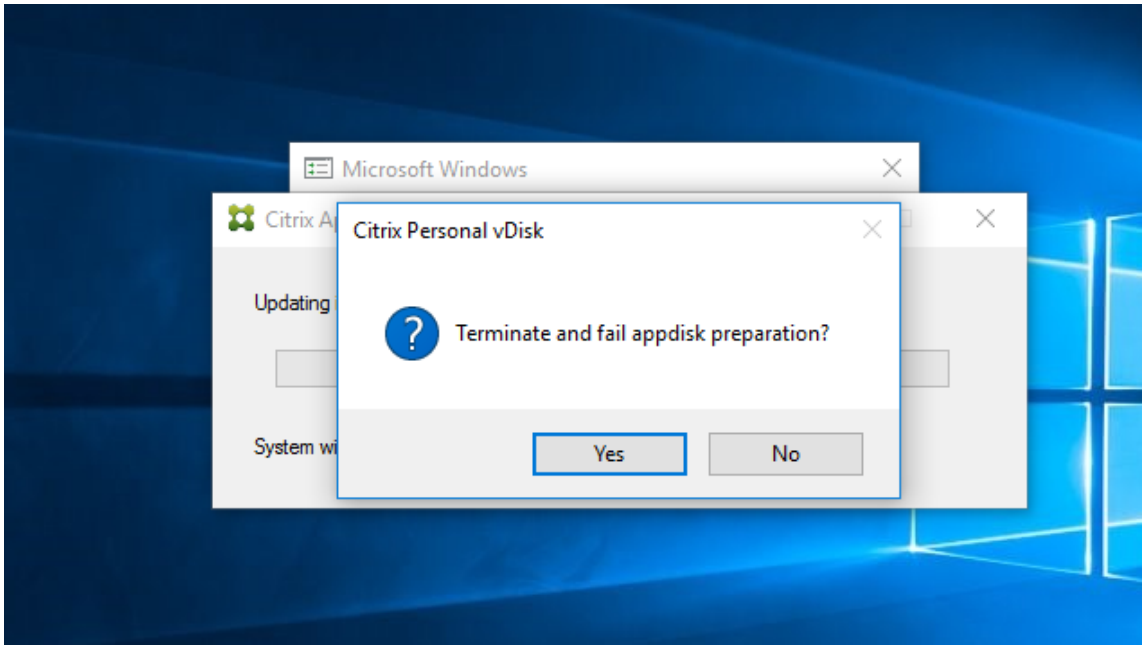
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Canceling 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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 the Create Delivery Groups article.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. On the **Rollout Strategy** page, follow the guidance in Create a restart schedule.

#### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Managing 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:**
>
> 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.

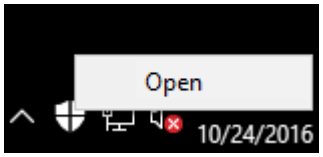
This section provides information about adding exceptions for the following antivirus applications:

- 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:

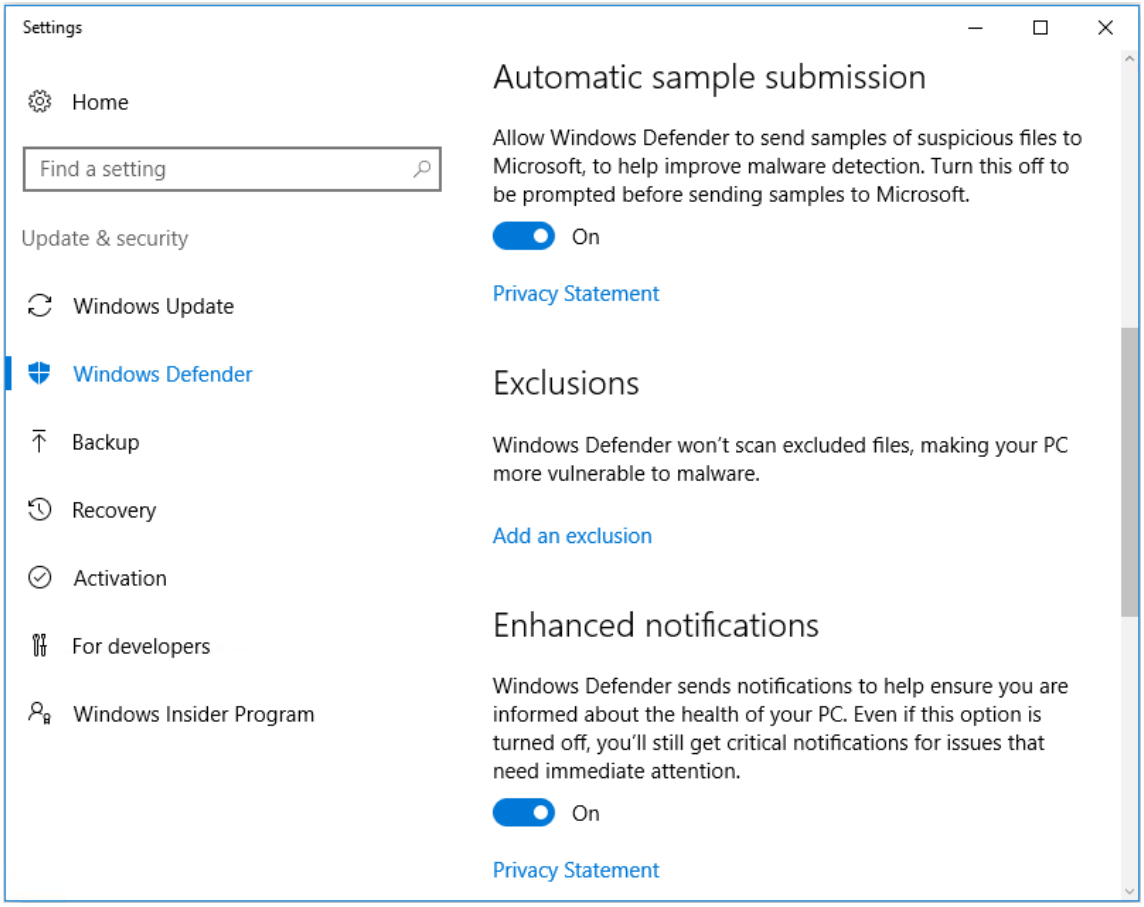



© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. In the Windows Defender console, select **Settings** in the upper right portion of the interface:

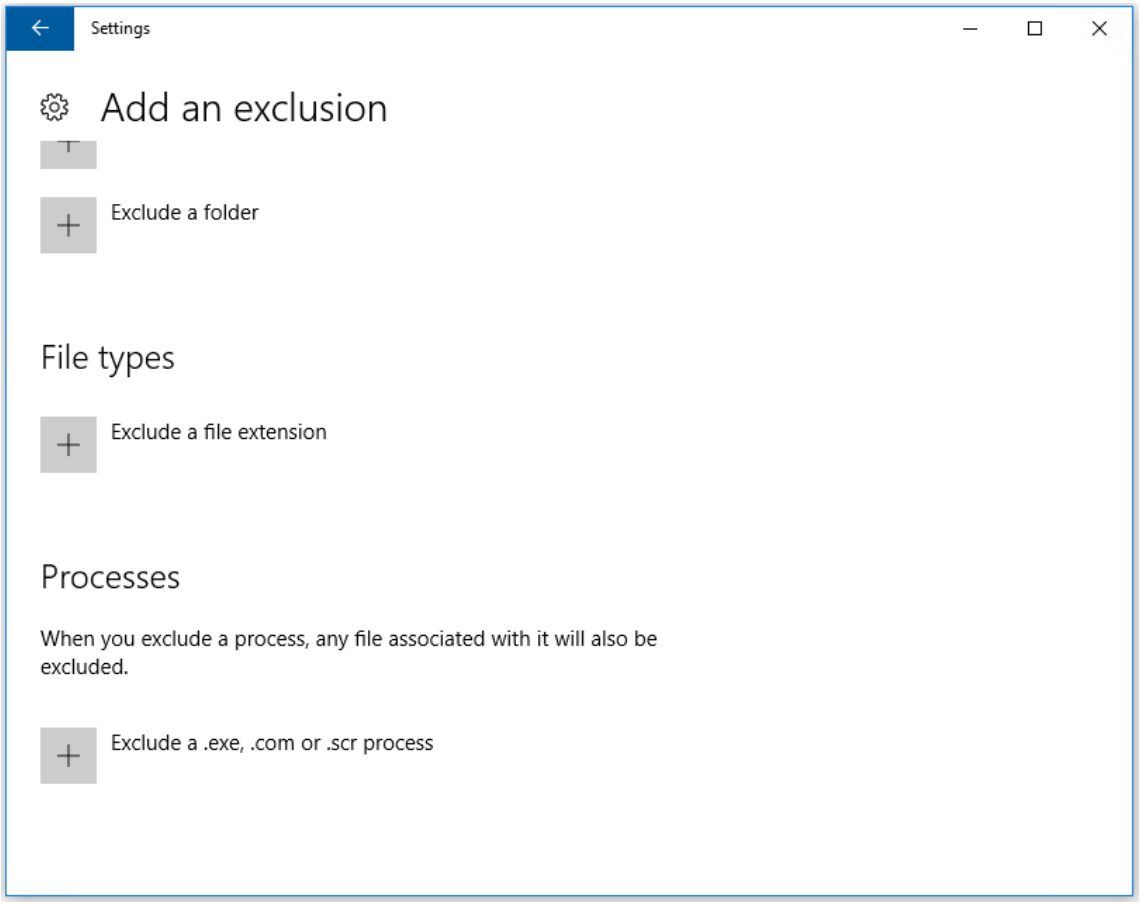
   localized image](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-main-page.png)

4. In the **Exclusions** portion of the Settings screen, click **Add an exclusion**:

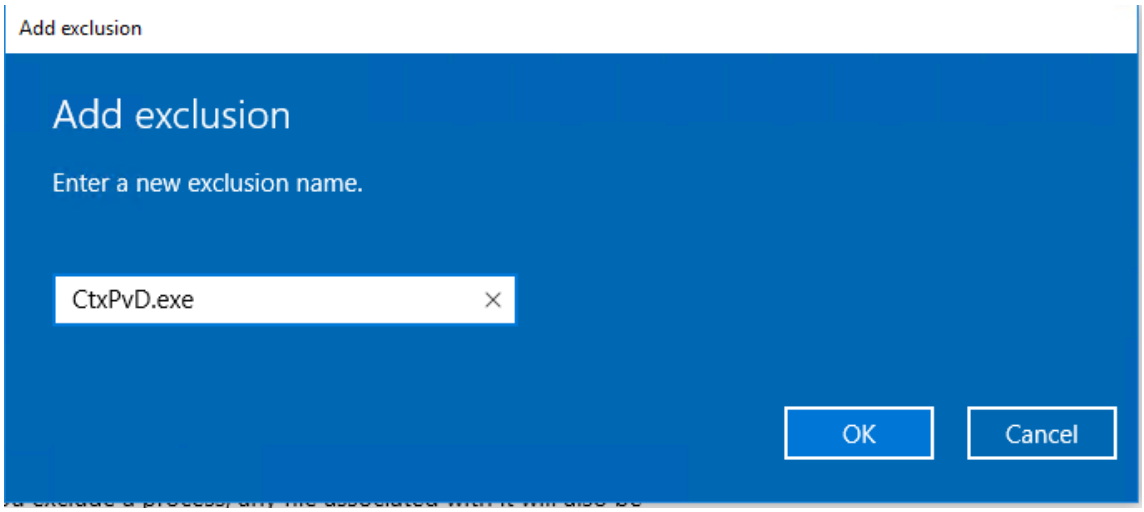



5. In the **Add an exclusion** screen, select **Exclude a .exe, .com, or .scr process**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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:

```
1 ![localized image](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-
```

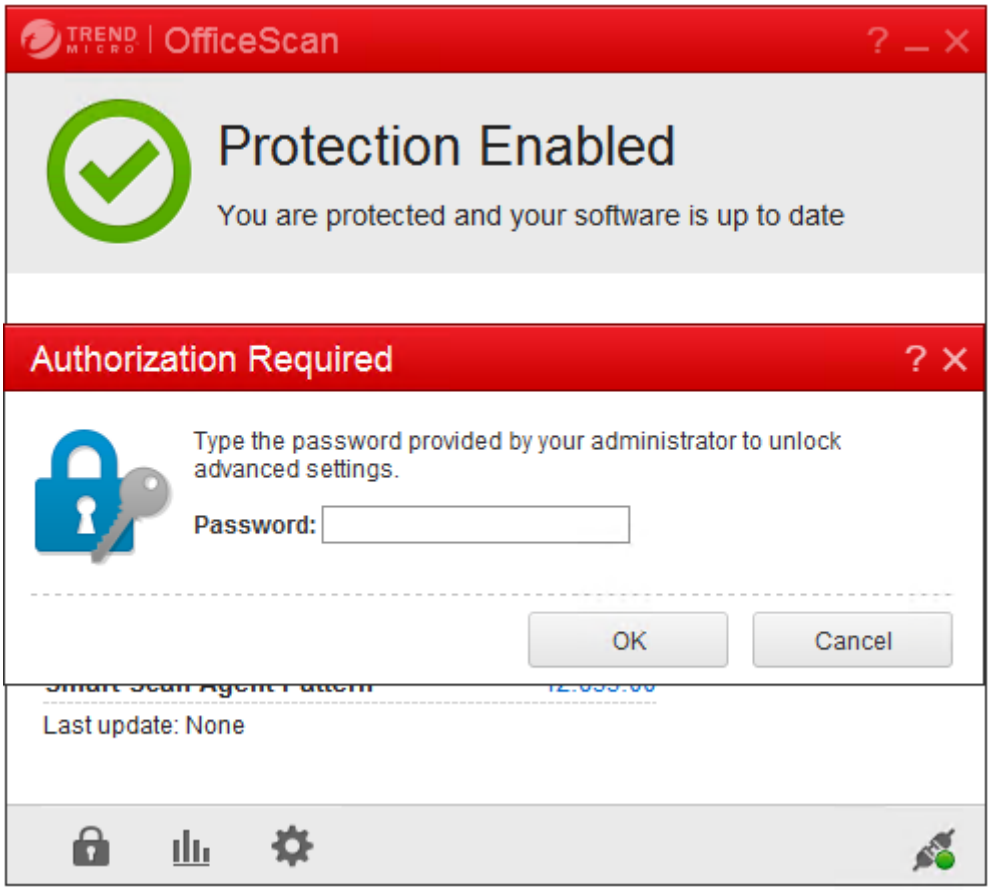
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
        process-added.png)
```

#### OfficeScan

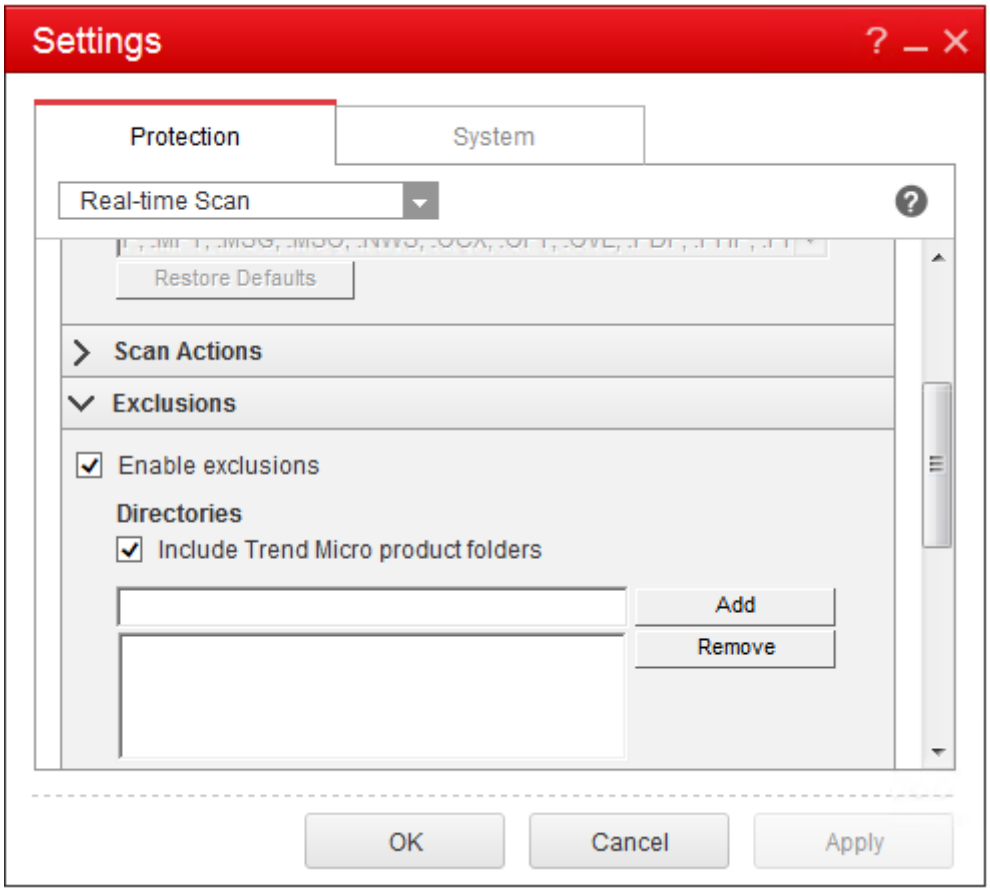
If your base VM uses OfficeScan (version 11):

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.

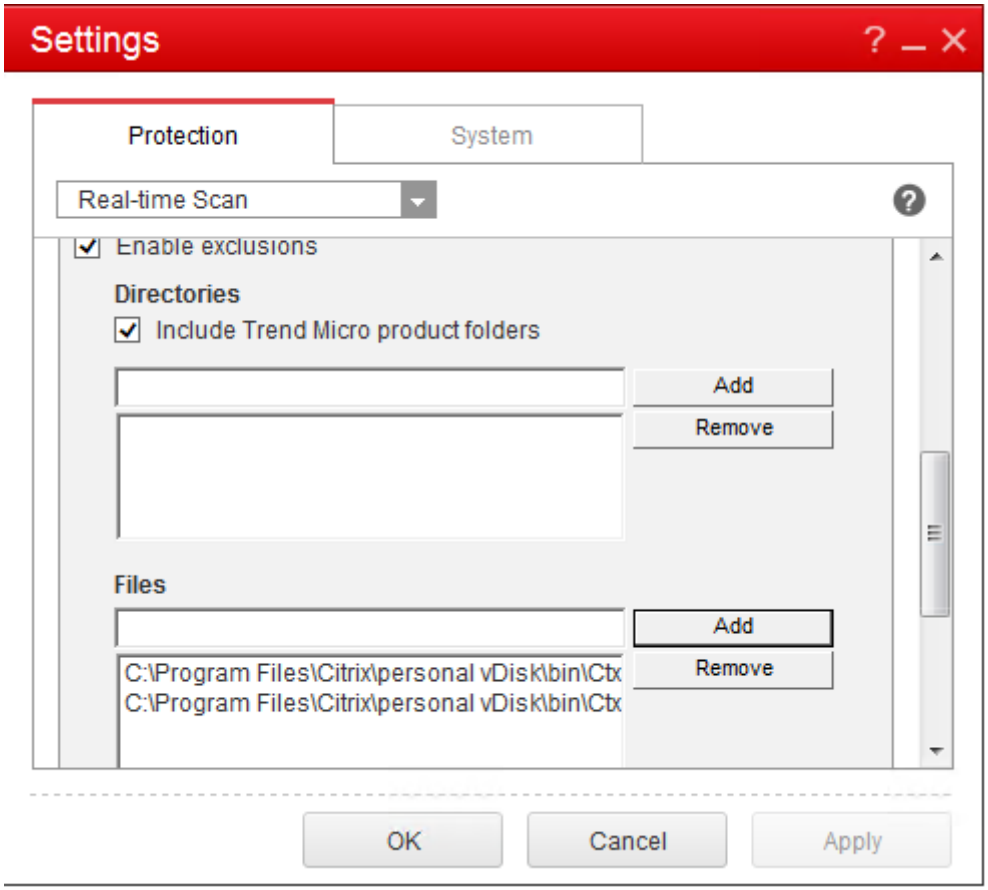
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



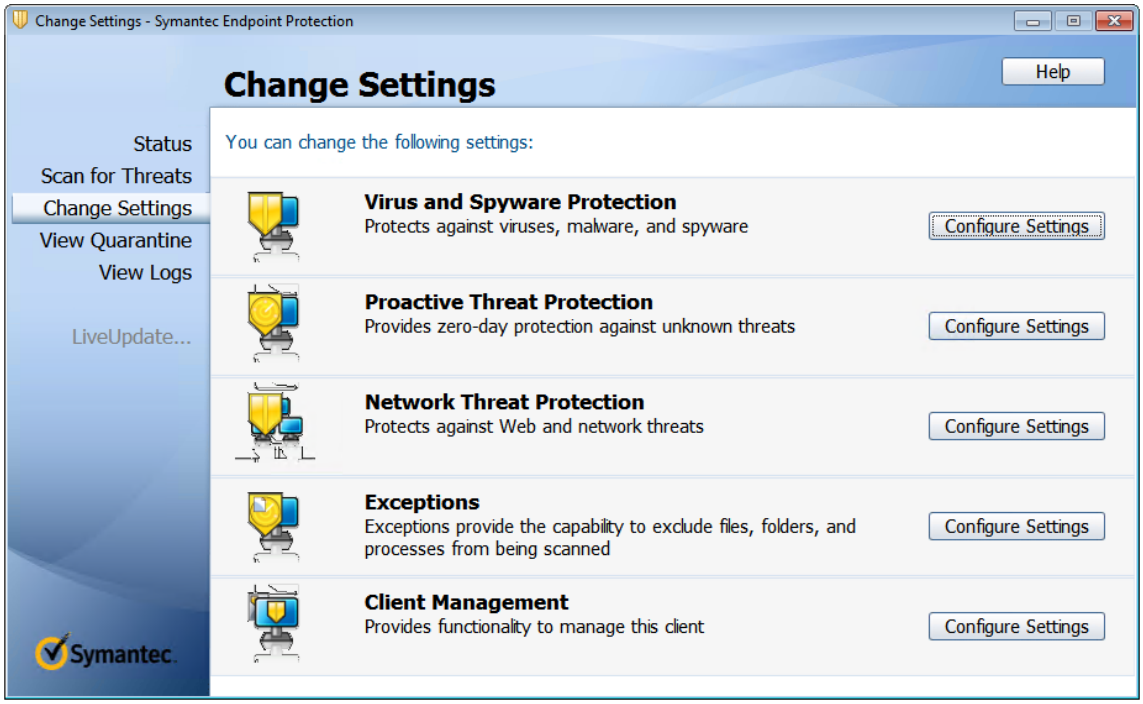

Click **Apply**, then **OK** to add the exclusions.

#### Symantec

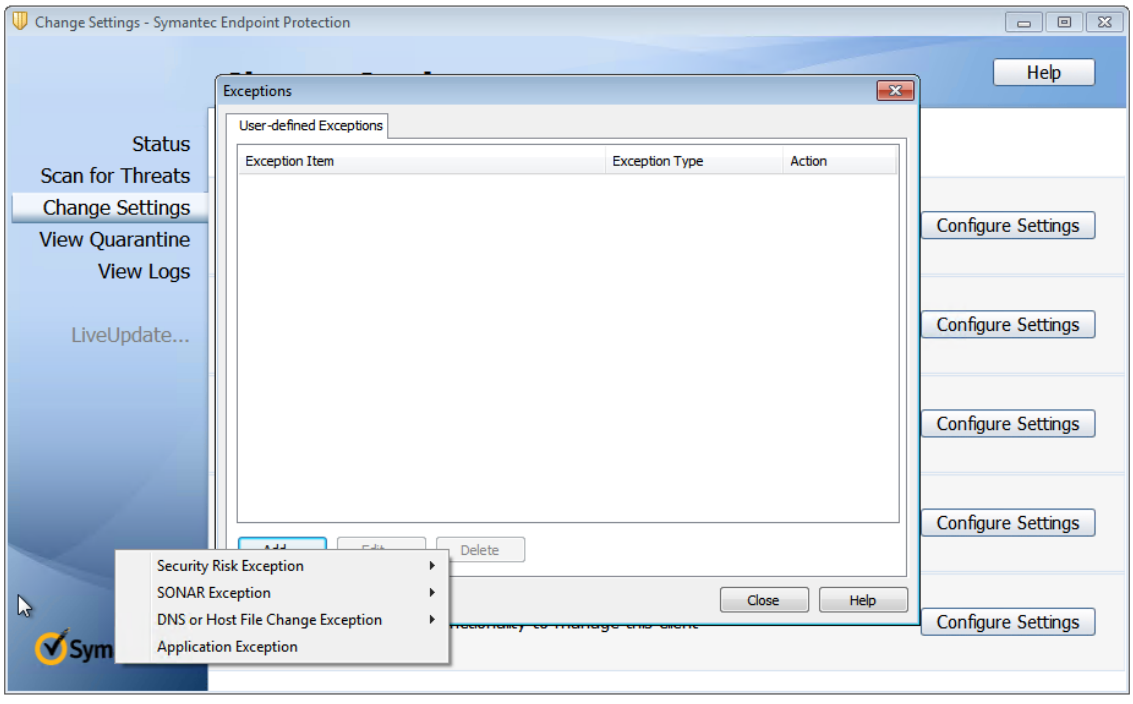
If your base VM uses Symantec (version 12.1.16):

1. Launch the Symantec console.
2. Click **Change Settings**.
3. In the **Exceptions** section, click **Configure Settings**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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**:

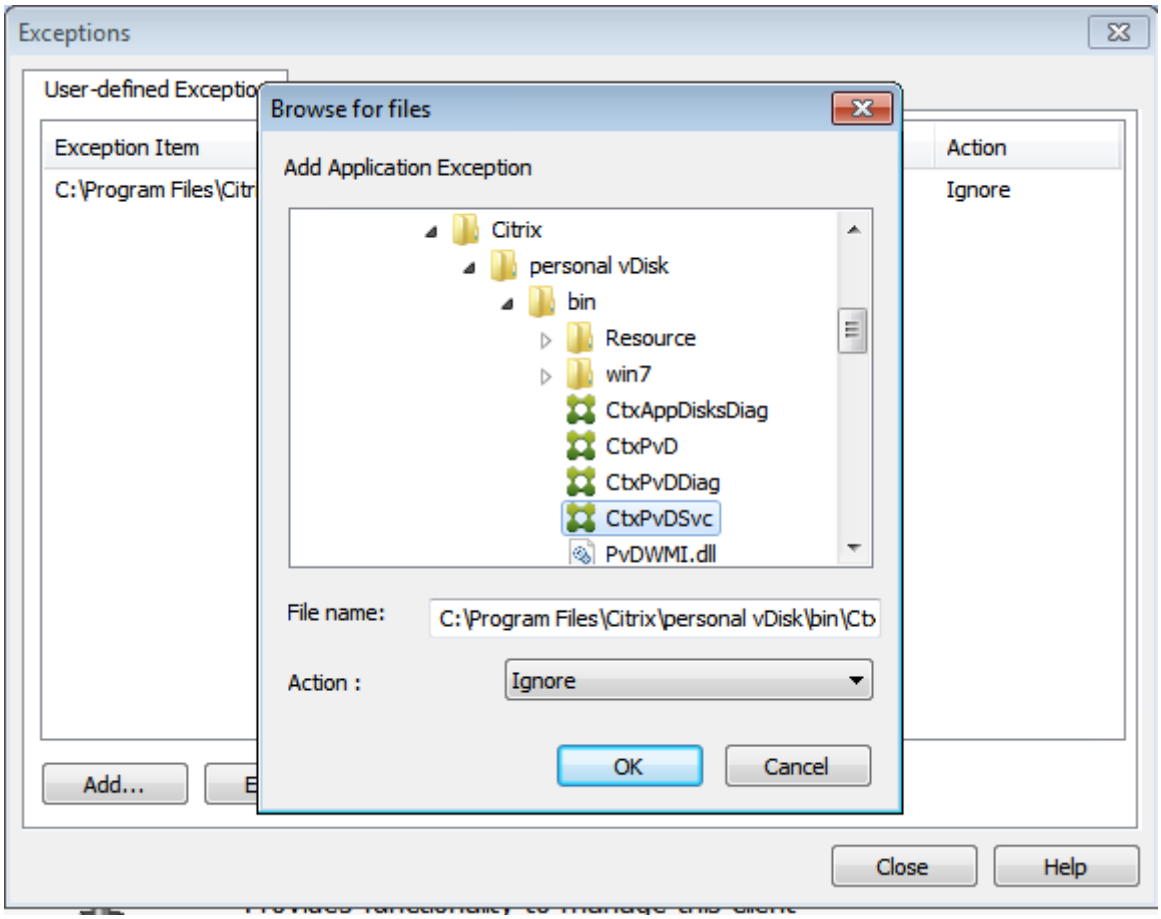



6. In the Exceptions screen, enter the following AppDisk file paths and set the action to **Ignore**:

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
```

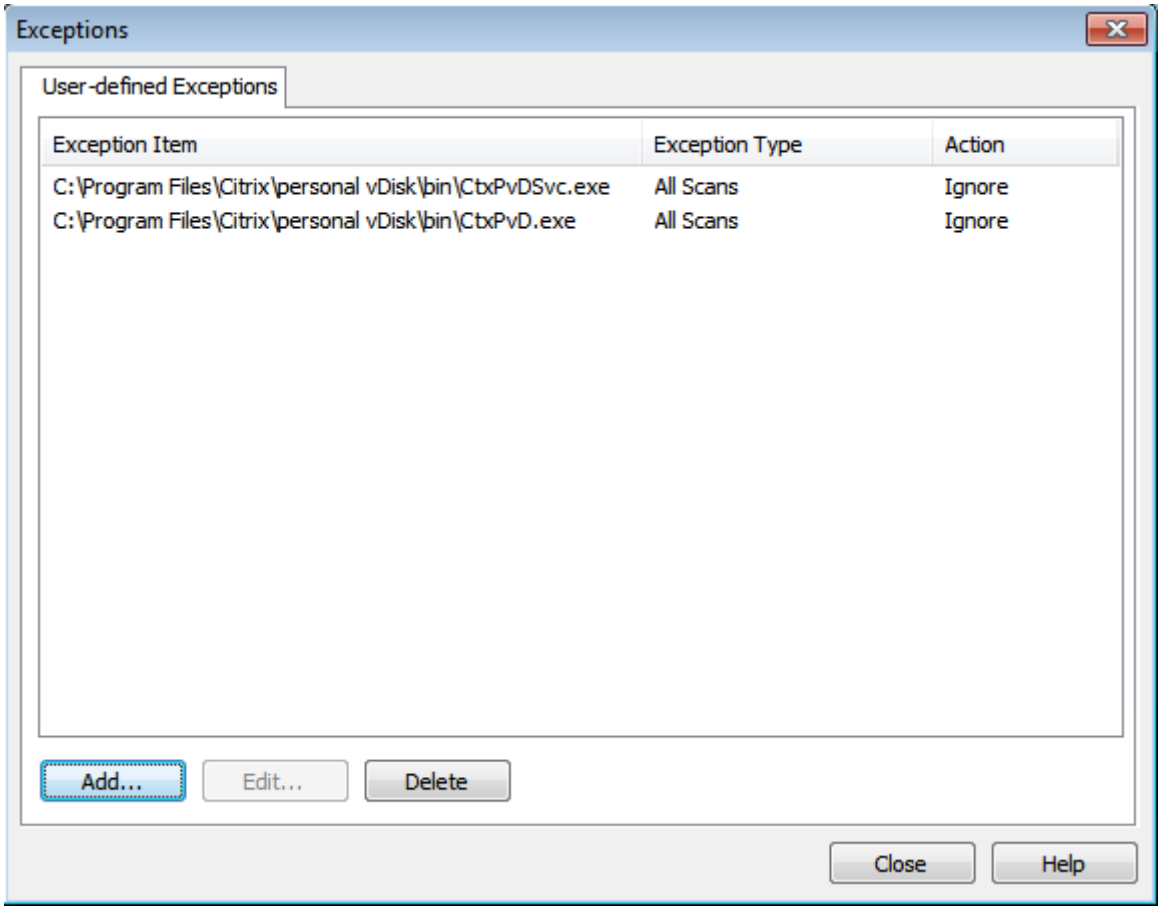
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```




The noted exceptions are added to the list. Close the window to apply your changes:

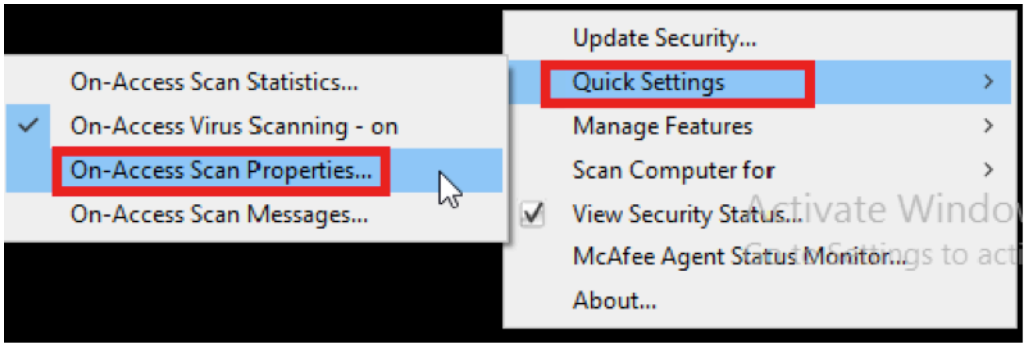
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**McAfee**

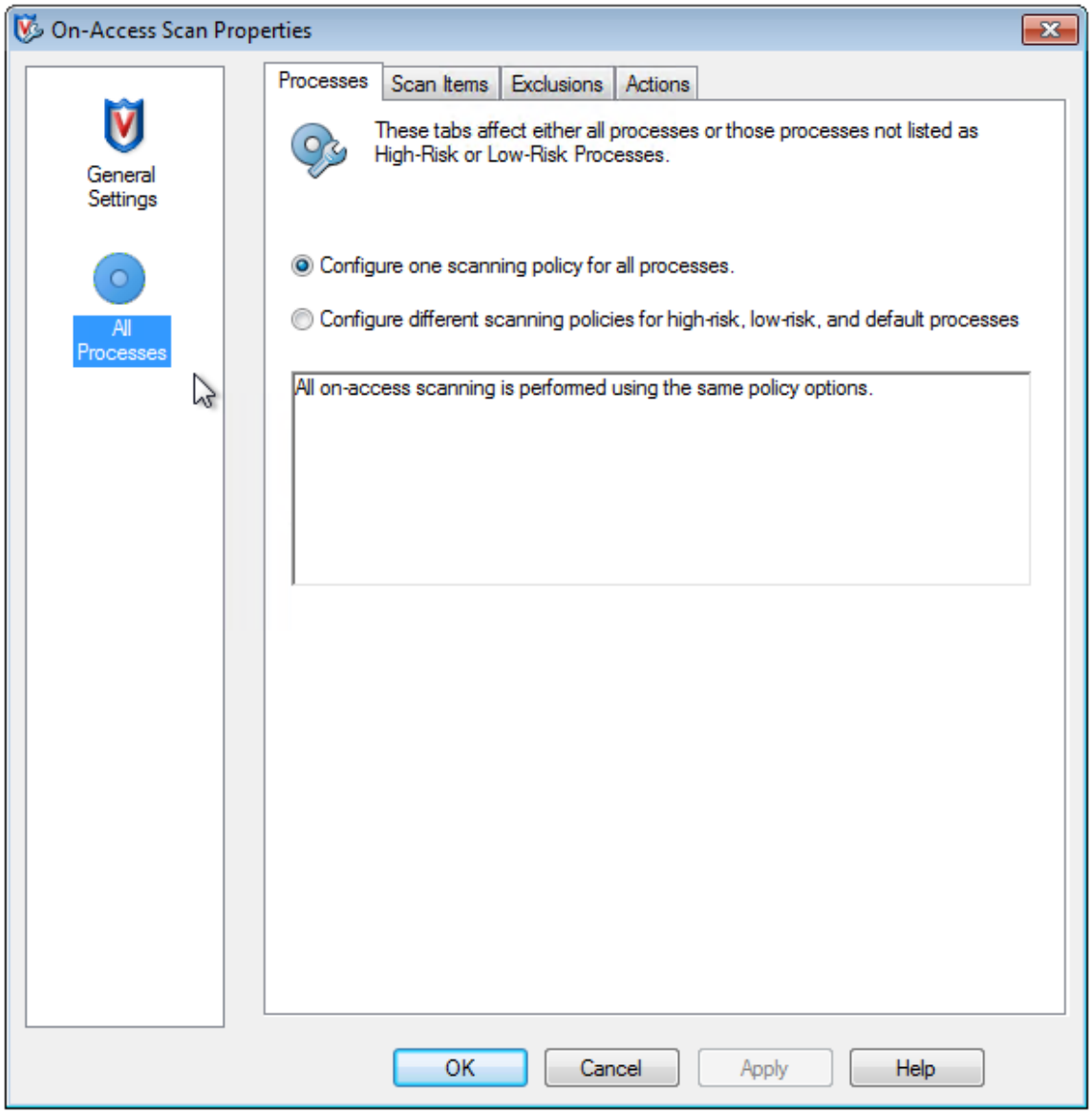
If your base VM uses McAfee (verson 4.8):

1. Right click the McAfee icon, and expand the **Quick Settings** option.
2. In the expanded menu, select **On-Access Scan Properties**:



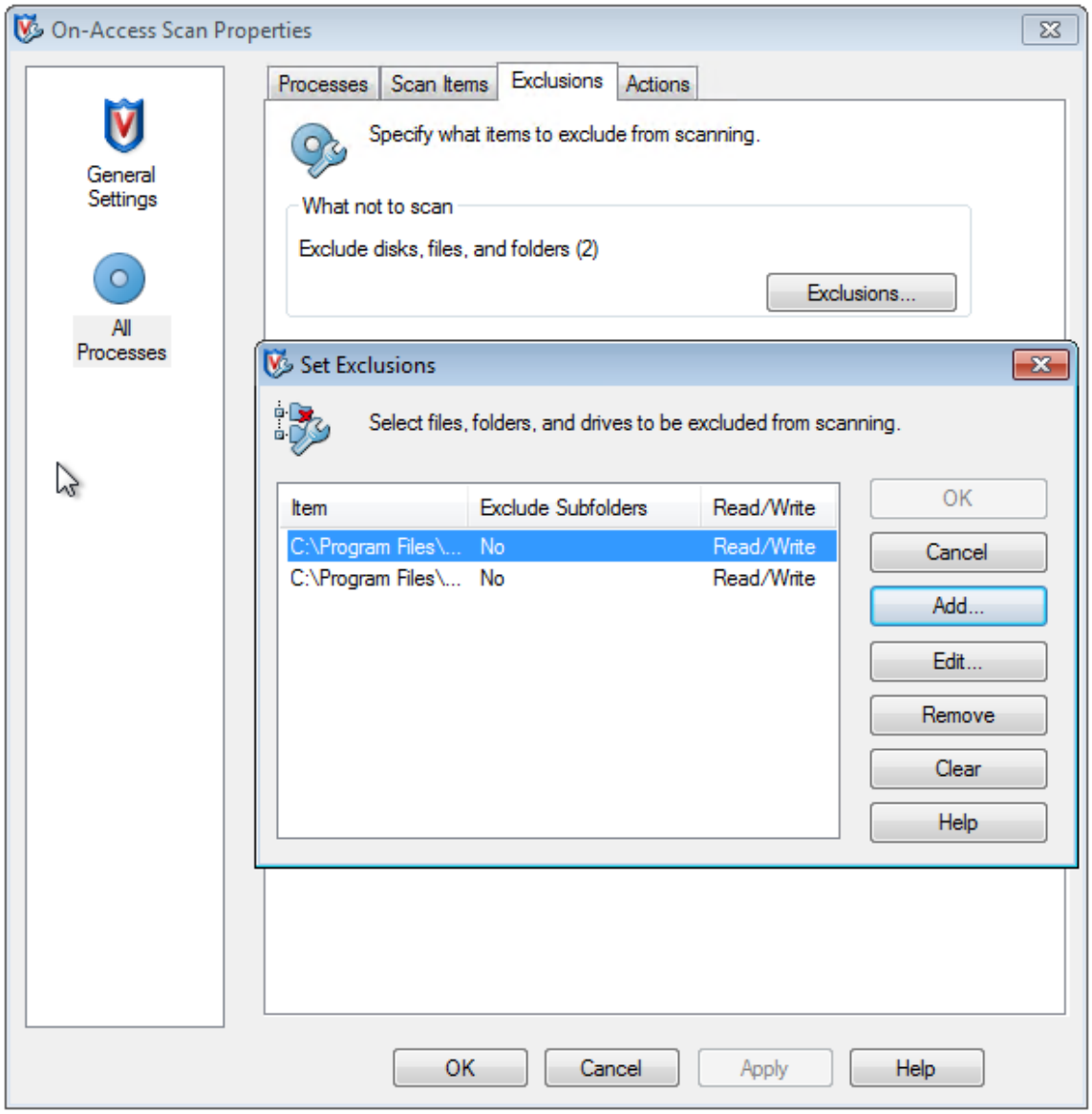

3. In the **On-Access Scan Properties** screen, click **All Processes**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




4. Select the **Exclusions** tab.
5. Click the **Exclusions** button.
6. In the **Set Exclusions** screen, click **Add**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

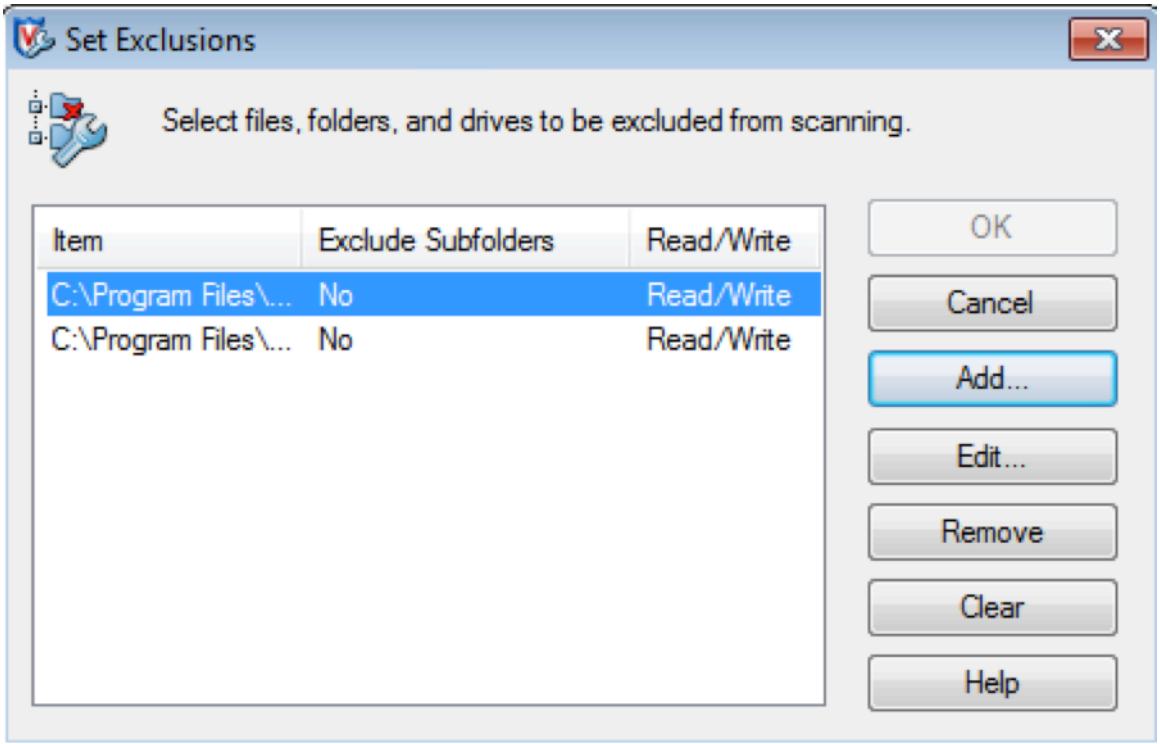



7. In the **Add Exclusion Item** screen, select **By name/location (can include wildcards * or ?)**. Click **Browse** to locate the exclusion executables:

```
    C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
    C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```

Click **OK**. The **Set Exclusions** screen now displays the added exclusions. Click **OK** to apply the changes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




> **Note:**
>
> After configuring these exclusions, create the AppDisk.

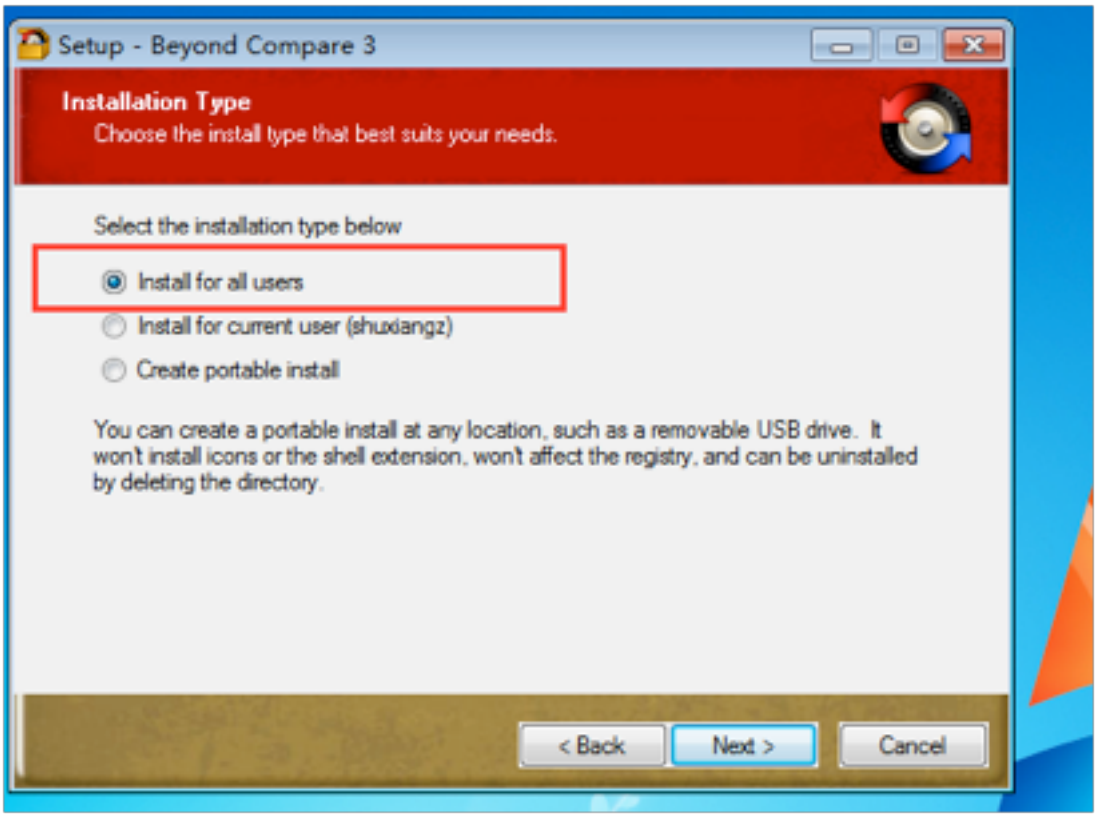
### How applications appear in the Start menu

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.

#### To create a new app and make it available for all users

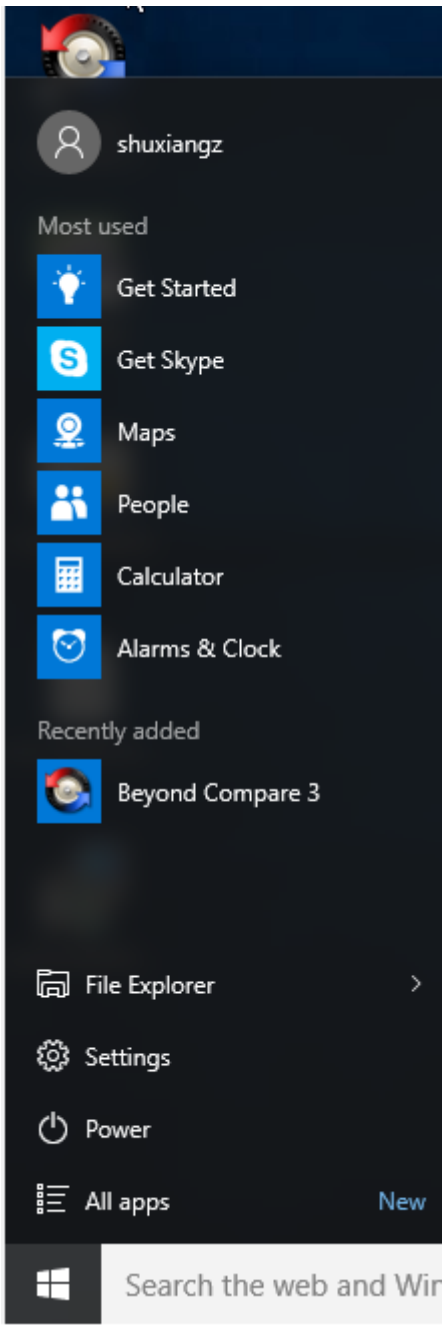
1. Install an app on the AppDisk (for example, *Beyond Compare* is the selected app):

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




2. Attach the disk to the desktop; the shortcut for the newly installed app (*Beyond Compare*) appears in the Start menu:

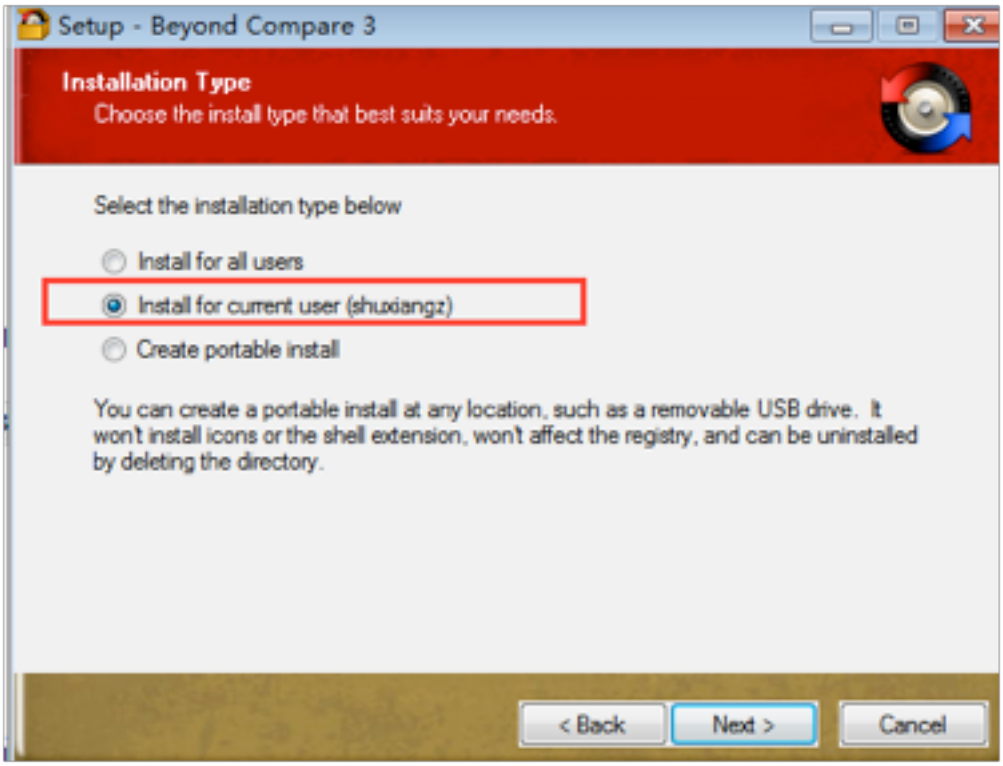
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**To install an app for the current user only**

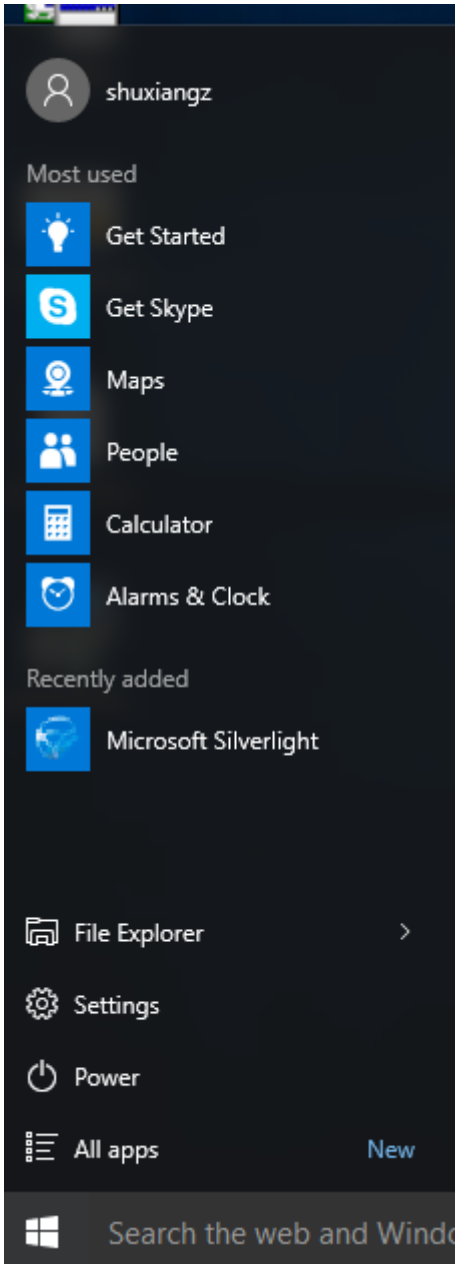
1. Install an app on the AppDisk and make it available for the current user:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




2. Attach the disk to the desktop; note that the shortcut does not appear in the Start menu:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### AppDisk logging updates

This release provides an enhancement to the AppDisk logging and support paradigm. With this update, AppDisk users can now obtain diagnostic information and optionally upload it to the Citrix Insight Services (CIS) website.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**How does it work?**

This new 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 Insight Services (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 new scripts for diagnostic data collection:

- **Upload-AppDDiags.ps1** –performs AppDisk diagnostic data collection
- **Upload-PvDDiags.ps1** –performs PvD diagnostic data collection

> **Note:**
>
> These scripts are added in C:\Program Files\Citrix\personal vDisk\bin\scripts. You must execute these PowerShell scripts as an administrator.

Use **Upload-AppDDiags.ps1** to initiate AppDisk diagnostic data collection and optionally manually upload the data to the CIS website.

```
SYNTAX
    Upload-AppDDiags [[-OutputFile] <string>] [-help] [<
       CommonParameters>]
        -OutputFile
            Local path for zip file instead of uploading to CIS
 EXAMPLES
    Upload-AppDDiags
        Upload diagnostic data to Citrix CIS website using credentials
            entered by interactive user.
    Upload-AppDDiags -OutputFile C:\MyDiags.zip
        Save AppDisk diagnostic data to the specified zip file. You
           can access https://cis.citrix.com/ to upload it later.
```

> **Tip:**
>
> When there is no –**OutputFile** argument, upload occurs. If –**OutputFile** is specified, the script creates a zip file that the you can upload manually at a later time.

Use **Upload-PvDDiags.ps1** to initiate PvD diagnostic data collection and optionally manually upload the data to the CIS website.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
SYNTAX
 Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
     -OutputFile
         Local path for zip file instead of uploading to CIS
 EXAMPLES
     Upload-PvDDiags
         Upload PvD diagnostic data to Citrix CIS website using
            credentials entered by interactive user.
     Upload-PvDDiags -OutputFile C:\MyDiags.zip
         Save PvD diagnostic data to the specified zip file. You can
            access https://cis.citrix.com/ to upload it later.
```

> **Tip:**
>
> When there is no –**OutputFile** argument, upload occurs. If –**OutputFile** is specified, the script creates a zip file that the you can upload manually at a later time.

## Publish content

August 17, 2018

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 Receiver. 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.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
New-BrokerApplication –ApplicationType PublishedContent
\-CommandLineExecutable \<*location*> -Name \<*app-name*>
\-DesktopGroup \<*delivery-group-name*>
```

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, `https://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 XenApp and XenDesktop Service deployments, download and install the XenApp and XenDesktop Remote PowerShell SDK.
- For on-premises XenApp and XenDesktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
Add-PsSnapin Citrix\*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

If you are using the XenApp and XenDesktop Service, authenticate by entering your Citrix Cloud credentials. If there is more than one customer, choose one.

### Publish a URL

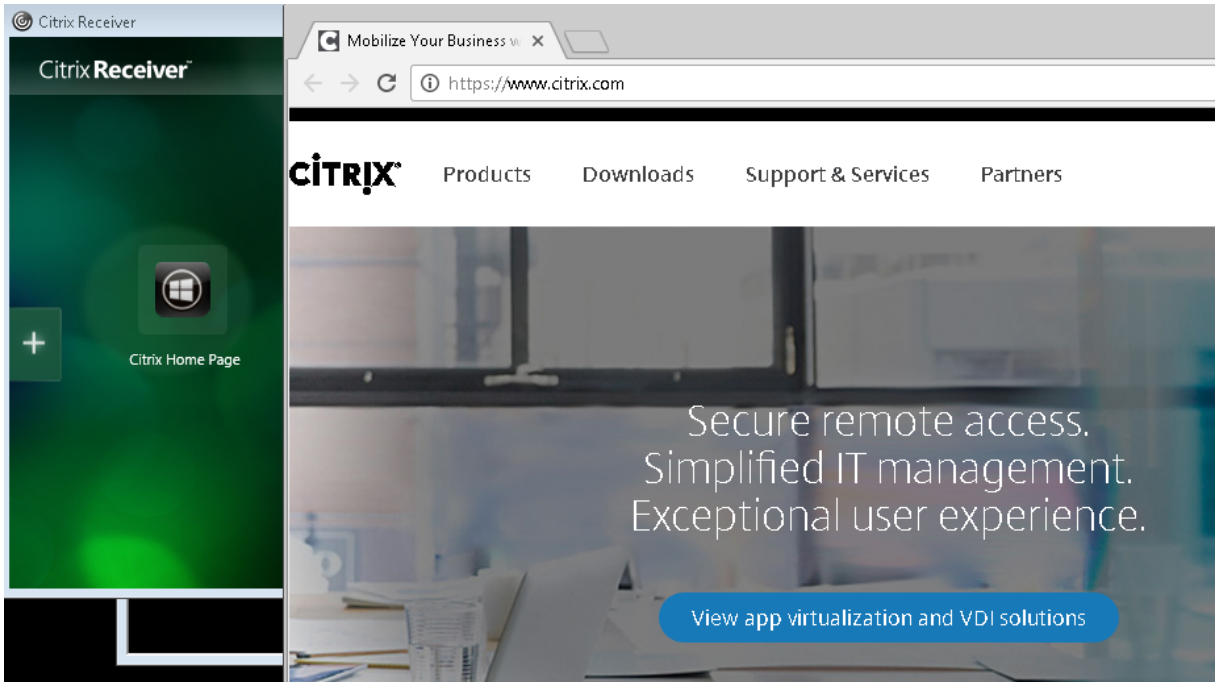
After assigning the location and application name, the following cmdlet publishes the Citrix home page as an application.

```
$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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Publish resources located at UNC paths

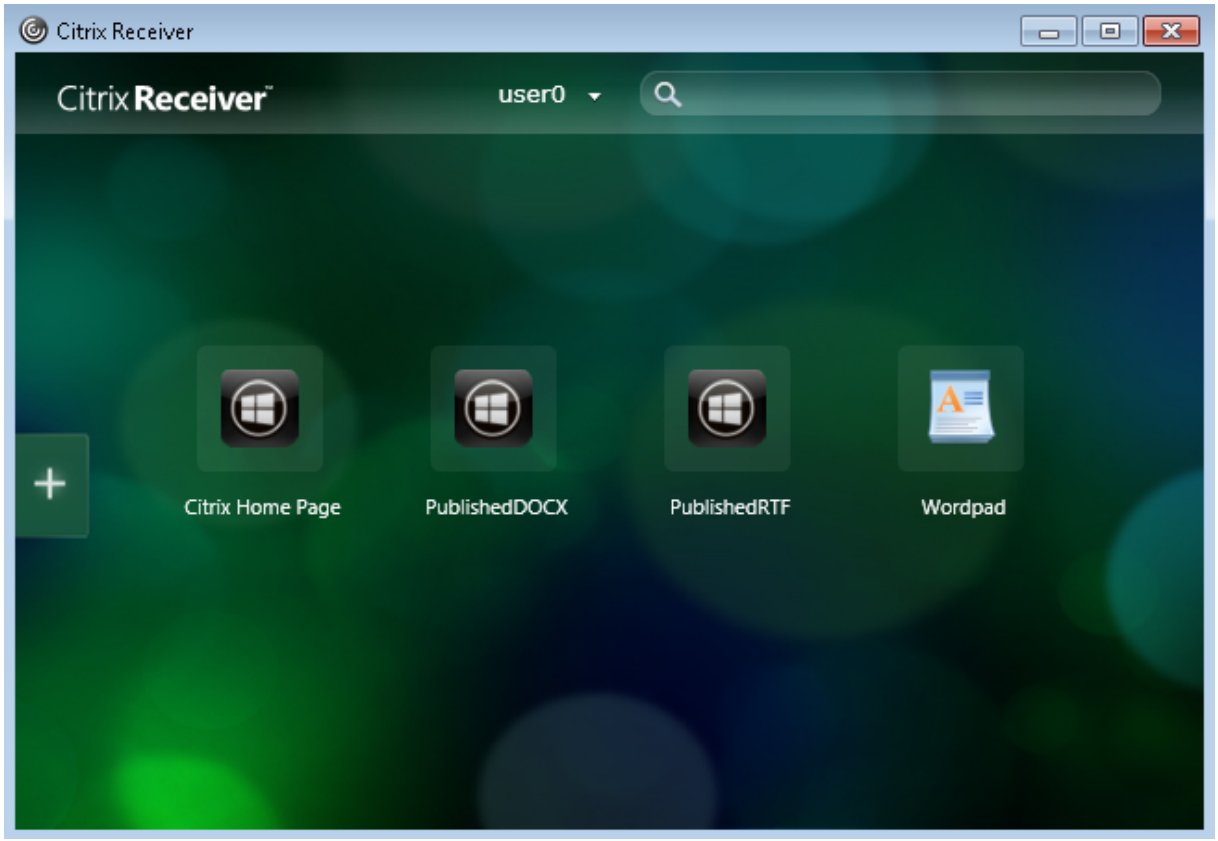
In this example, the administrator has already created a share named PublishedResources. After assigning the locations and application names, the following cmdlets publish an RTF and a DOCX file in that share as a resource.

```
$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-->
```

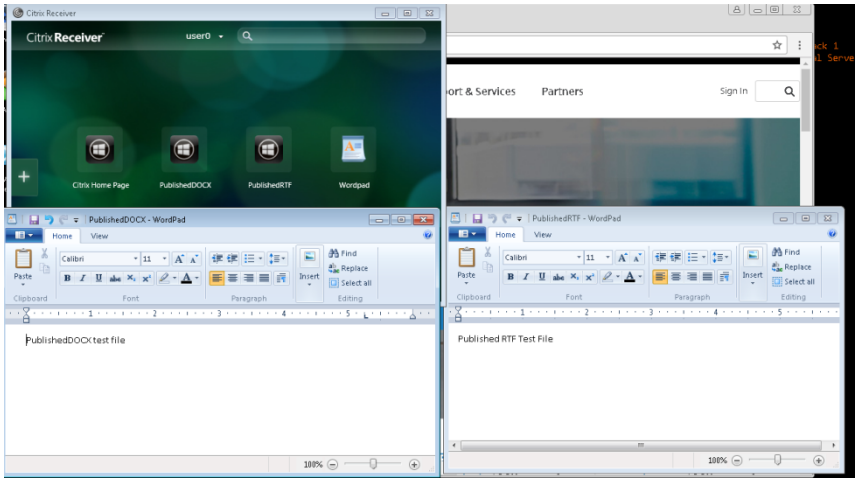
### Verify success

- Refresh your StoreFront window to see the newly published documents.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



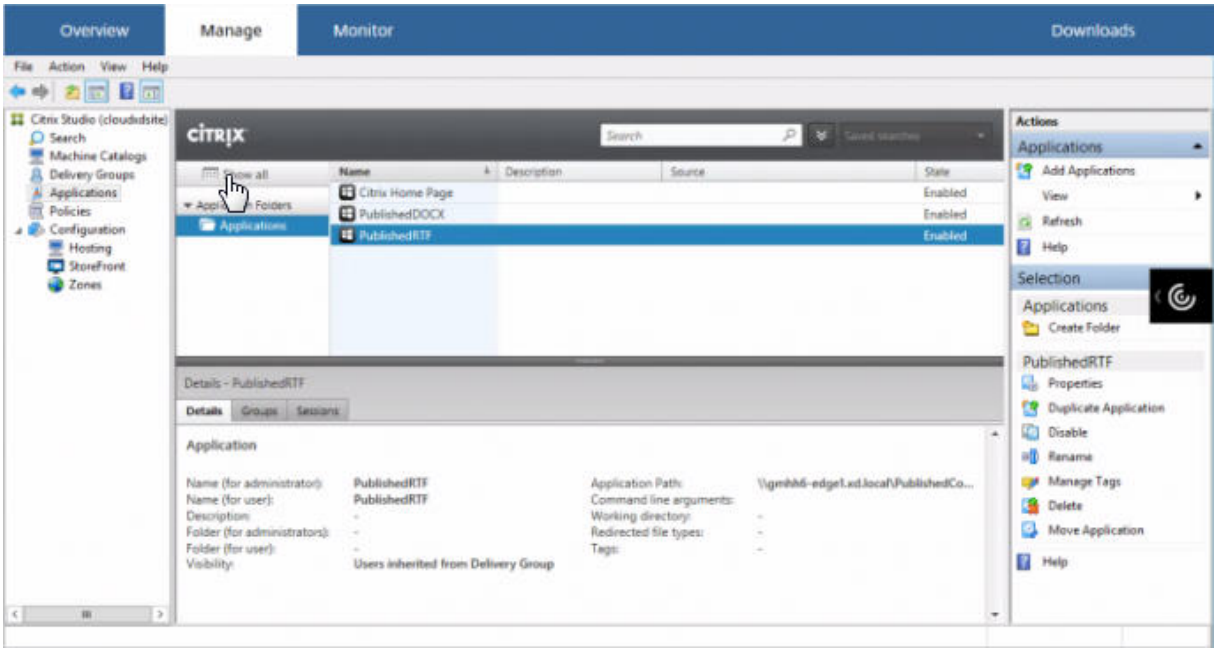

- Click the PublishedRTF and PublishedDOCX applications. Each document opens in a locally running WordPad.



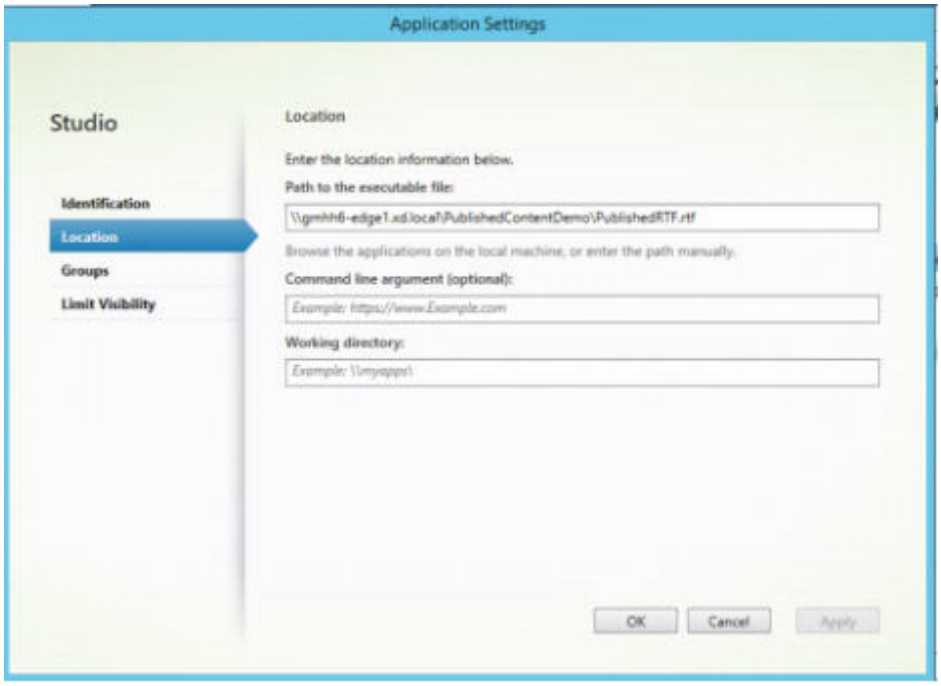
### View and edit PublishedContent applications

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



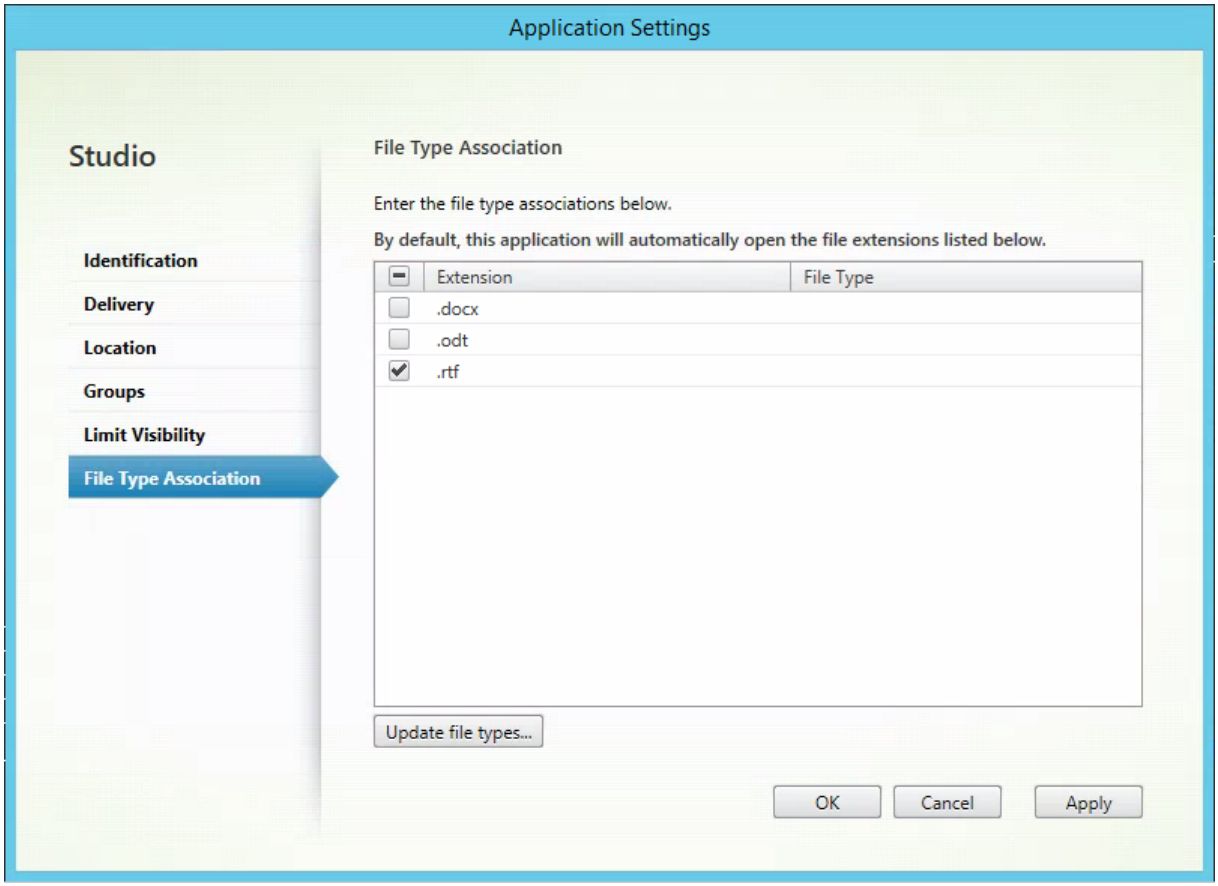

Application properties (such as user visibility, group association, and shortcut) apply to the published content. However, you cannot change the command-line argument or working directory properties on the **Location** page. To change the resource, modify the "Path to the executable file"field on that 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.

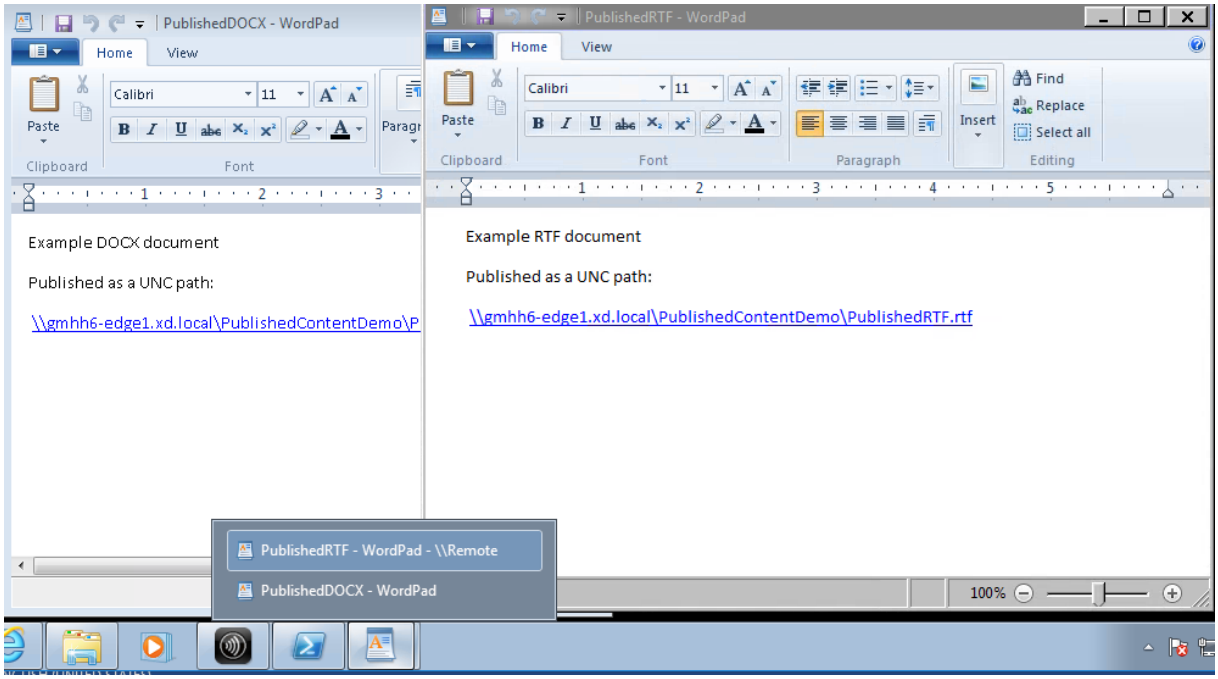
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Important:**
>
> 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### For more information

- Create machine catalogs
- Create Delivery Groups
- Change application properties

## Personal vDisk

July 17, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

> **Note:**
>
> Refer to the Troubleshooting article for information about PvD reports, messages and known issues.

## Install and upgrade

July 4, 2018

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Personal vDisk 7.x is supported on XenDesktop version 5.6 through the current version. The "System requirements"documentation for each XenDesktop version lists the supported operating systems for Virtual Delivery Agents (VDAs), and the supported versions of hosts (virtualization resources), and Provisioning Services. For details about Provisioning Services tasks, see the current Provisioning Services 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 XenApp or XenDesktop 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 Provisioning Services (PVS), 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 XenDesktop version. Then, run the PvD inventory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

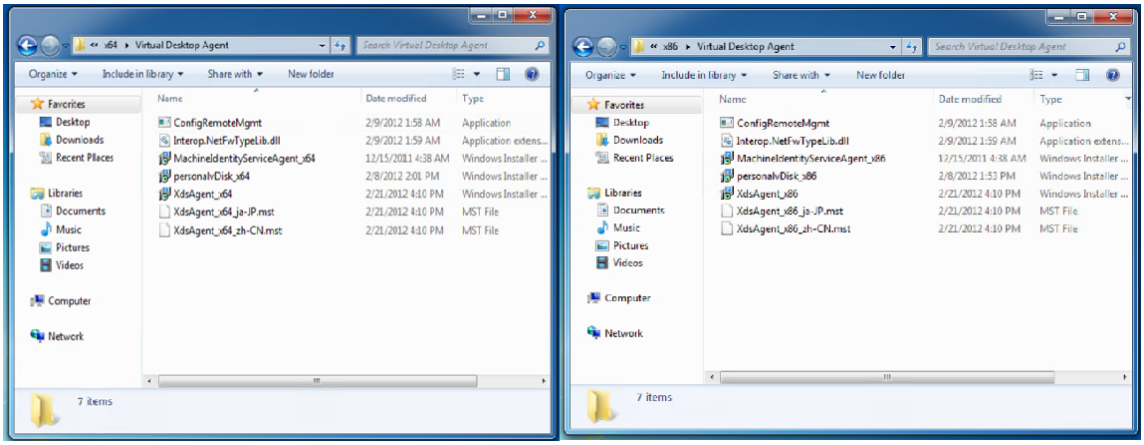
If you uninstall PvD and then want to reinstall the same or a newer version, first back up the registry key HKLM\Software\Citrix\personal vDisk\config, which contains environment configuration settings that might have changed. Then, after installing PvD, reset the registry values that might have changed, by comparing them with the backed-up version.

#### Important considerations when uninstalling PvD

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:

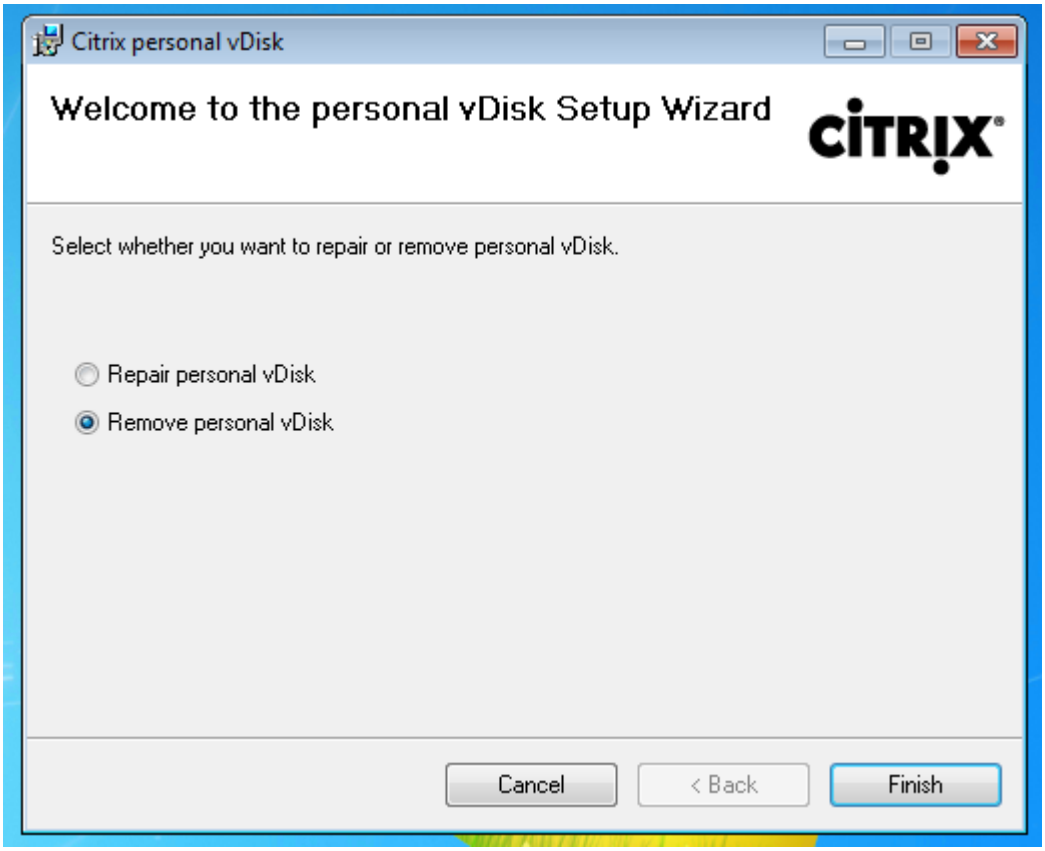
1. Select the appropriate copy of the vDisk installer from the XenApp/XenDesktop media. Locate the latest personal vDisk MSI installer from the XenApp/XenDesktop ISO from one of the following directories (depending on whether the upgraded VM is 32 or 64-bits):

    - 32-bits: XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
    - 64-bits: XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



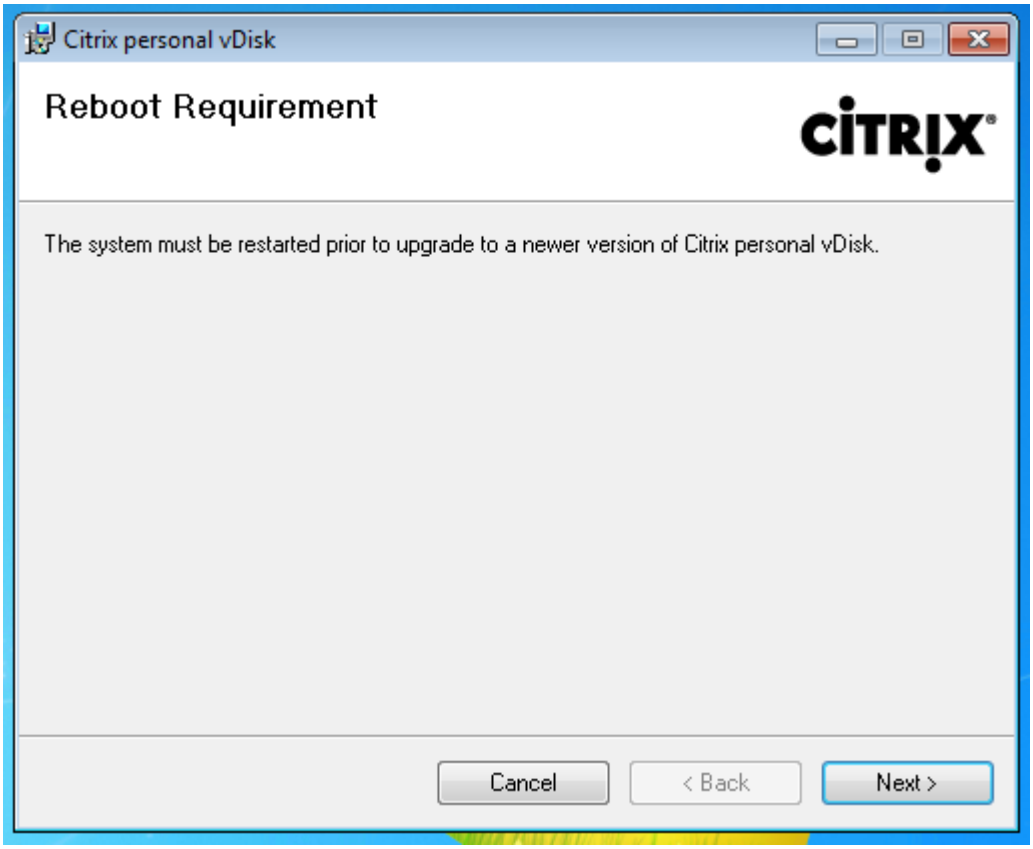

2. Remove the personal vDisk installation. Select the personal vDisk MSI installer package found in step 1. The personal vDisk setup screen appears.
3. Select Remove personal vDisk.
4. Click **Finish**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

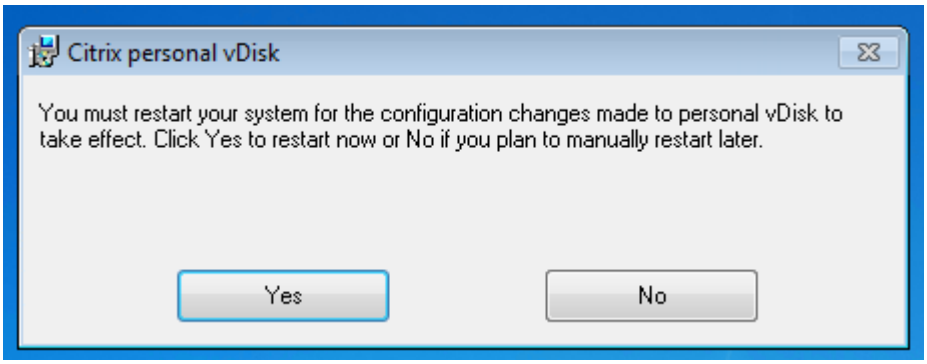



5. The Reboot Requirement page appears. Click **Next**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




6. Click **Yes** to restart the system and to apply your configuration changes:




## Configure and manage

April 23, 2021

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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 XenDesktop 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenDesktop releases use Delegated Administration for this.

Other settings:

- **Windows Update Service**—Ensure that you set Windows updates to Never Check for Update and the Windows update service to Disabled in the master image. In the event Windows Update Service needs to run on the PvD, setting it to Never Check for Update helps prevent the updates from being installed on the associated machines.

  Windows 8 Store needs this service to run to install any Modern-style application.

- **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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Agents and clients (for example, System Center Configuration Manager Agent, App-V client, Citrix Receiver)
- 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: Provisioning Services

When using Provisioning Services 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 Provisioning Services (PVS) vDisk is promoted to production.
- The Provisioning Service 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The personal vDisk size should always be larger than the Provisioning Services write cache disk (otherwise, Provisioning Services 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 PvD Image Update Monitoring Tool or 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 Provisioning Services write cache disk. However, when PvD is not active (such as during image update operations), a small Provisioning Services write cache disk can fill up, resulting in machine crashes.

Citrix recommends that you size Provisioning Services write cache disks according to Provisioning Services best practice and add space equal to twice the size of the template VHD on the master image (to accommodate merge requirements). It is extremely unlikely that a merge operation will require all of this space, but it is possible.

When using Provisioning Services to deploy a catalog with PvD-enabled machines:

- Follow the guidance in the Provisioning Services documentation.
- You can change the power action throttling settings by editing the connection in Studio; see below.
- If you update the Provisioning Services 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 Provisioning Services 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 XenDesktop 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 PvD Image Update Monitoring Tool or 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

April 23, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenDesktop installation media. You can also use the PvD Image Update Monitoring Tool, which is located in the Support\Tools\Scripts\PvdTool folder.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

#### Export

- 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:

#### 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
Importing inventory \share location\ExportedInventory\
    ExportedPvdInventory
...
Successfully added inventory \share location\ExportedInventory\
    ExportedPvdInventory to the
store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
<!--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

July 17, 2018

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The Software.Dat.Report.txt file records the changes made by the user to the HKEY_LOCAL_MACHINE\Software 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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 *\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST\UserData.V2.vhd*. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Error code | Description |
|---|---|
| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Event ID | Description |
|---|---|
| 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. |
| 2 | There is not enough space available on the storage disk to create a Personal vDisk container. |

### Release-independent known issues

The following PvD issues have been identified:

- 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]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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]

## Remove components

July 4, 2018

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. When you remove a Controller, the SQL Server software and the databases are not removed.

Before removing a Controller, remove it from the Site. Before removing Studio or Director, Citrix recommends closing them.

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.

When you remove a VDA, the machine restarts automatically after the removal, by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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, select Citrix XenApp <*version*> or Citrix XenDesktop <*version*>, then right-click and select **Uninstall**. The installer launches, and you can select the components to be removed. Alternatively, you can remove StoreFront by right-clicking **Citrix StoreFront** and selecting **Uninstall**.
- To remove a VDA, select **Citrix Virtual Delivery Agent** <*version*>, then right-click and select **Uninstall**. The installer launches and you can select the components to be removed.
- To remove the Universal Print Server, select **Citrix Universal Print Server**, then right-click and select **Uninstall**.

### Remove 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, 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.

For example, the following command removes Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
   studio
```

### Remove a VDA 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.

For example, the following command removes the VDA and Citrix Receiver.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

To remove VDAs using a script in Active Directory; see Install or remove Virtual Delivery Agents using scripts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Upgrade and migrate

June 7, 2021

## Upgrade

Upgrading changes deployments to the newest component versions without having to set up new machines or Sites. This is known as an in-place upgrade. You can upgrade to the current version from:

- XenDesktop 5.6 *
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

* To upgrade from XenDesktop 5.6, first upgrade to 7.6 LTSR (with the latest CU), and then upgrade to 7.15 LTSR (with the latest CU).

You can also upgrade a XenApp 6.5 worker server to a current VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5. See Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS

To upgrade:

1. Run the installer on the machines where the core components and VDAs 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.

For details, see Upgrade a deployment.

For information about installing Controller hotfixes, see CTX205921.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Migrate

Migrating moves data from an earlier deployment to a newer version. You can migrate from XenApp 6.x to XenApp 7.6. Migrating includes installing current 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 more information about migrating, see Migrate XenApp 6.x.

## Changes in 7.x

March 22, 2021

XenApp and XenDesktop architecture, terminology, and features changed, beginning with the 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* refers to XenApp version 7.5 or later, and XenDesktop version 7 or later.

This article provides an overview. For comprehensive information about moving from pre-7.x to the latest version, see Upgrade to XenApp 7.

### Element differences between XenApp 6 and the current XenApp version

Although they are not exact equivalents, the following table helps map functional elements from XenApp 6.5 and previous versions to XenApp and XenDesktop versions, beginning with 7.x. Descriptions of architectural differences follow.

| Instead of this in XenApp 6.x and earlier | Think of this in version 7.x |
|---|---|
| Independent Management Architecture (IMA) | FlexCast Management Architecture (FMA) |
| Farm | Site |
| Worker Group | Machine catalog, Delivery Group |
| Worker | Virtual Delivery Agent (VDA), Server OS machine, Server OS VDA, Desktop OS machine, Desktop OS VDA |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Instead of this in XenApp 6.x and earlier | Think of this in version 7.x |
|---|---|
| Remote Desktop Services (RDS) or Terminal Services machine | Server OS machine, Server 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, XenApp and XenDesktop are 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 XenApp 7.x and XenDesktop 7.x, 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 XenApp 7.x and XenDesktop 7.x, 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 XenApp 7.x and XenDesktop 7.x, the VDA communicates with Delivery Controllers that manage the user connections.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Delivery Controllers:** In XenApp 6.5 and previous versions there was a zone master responsible for user connection requests and communication with hypervisors. In XenApp 7.x and XenDesktop 7.x, 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 XenApp 7.x and XenDesktop 7.x, the 7.x 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 XenApp 7.x and XenDesktop 7.x, 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:** XenApp 7.x and XenDesktop 7.x 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 XenApp 7.x and XenDesktop 7.x, 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 XenApp 7.x and XenDesktop 7.x, custom 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 7.x |
|---|---|
| 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 XenApp and XenDesktop 7.x, you enable these features for specified users by configuring these settings for existing Delivery groups. |
| 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. |
| 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. |
| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Feature support and changes

The following features are not currently provided, no longer supported, or have changed significantly in XenApp or XenDesktop, beginning with 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. NetScaler 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 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 7.x 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 7.x 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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

- **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 of XenDesktop and XenApp, 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

July 21, 2021

### Introduction

You can upgrade certain deployments to newer versions without having to first set up new machines or Sites. That process is called an in-place upgrade. See Upgrade for a list of the versions you can upgrade.

You can also use the current XenApp installer to upgrade a XenApp 6.5 worker server to a current VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5. See Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS.

To start an upgrade, you run the installer from the new version to upgrade previously installed core components (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server) and VDAs. Then you upgrade the databases and the Site.

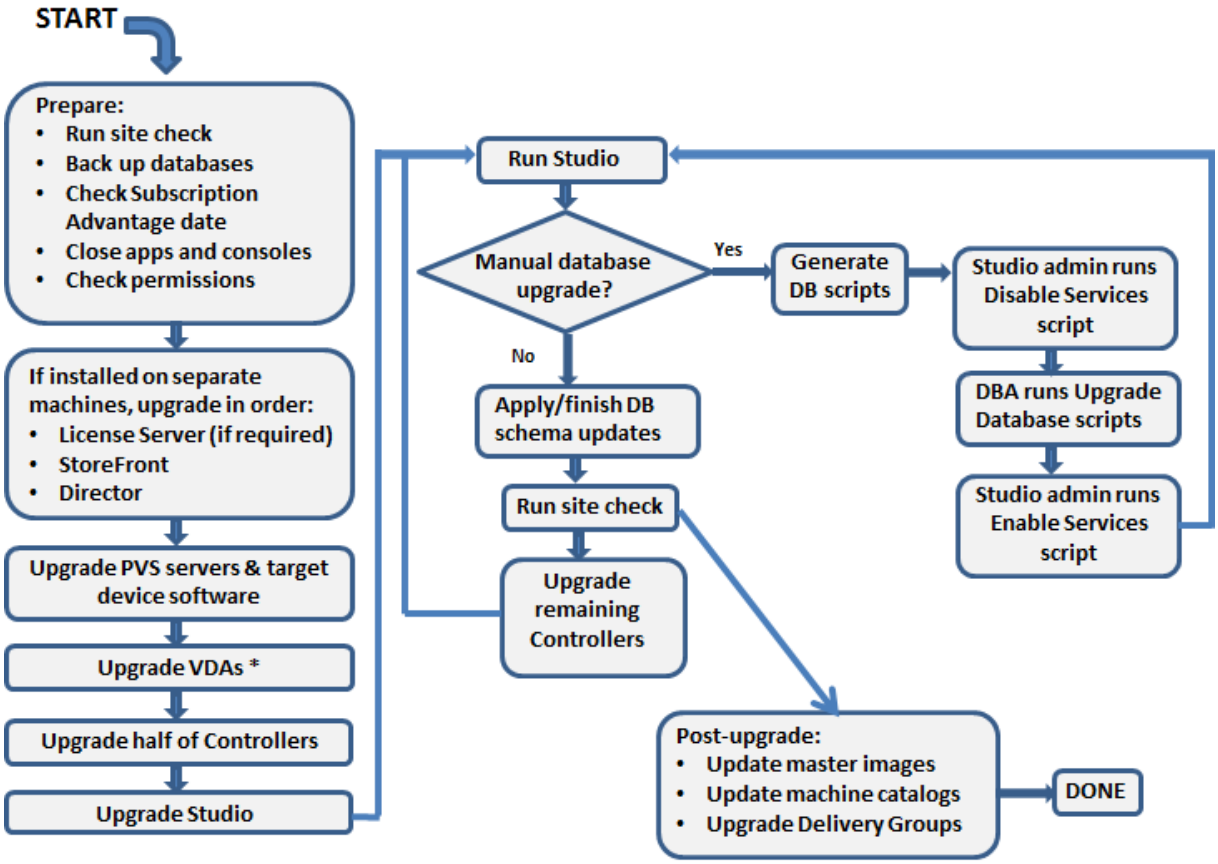
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Be sure to review all the information in this article before beginning the upgrade.

(If you are upgrading to 7.16 or a later release, see the guidance in Upgrade a deployment.)

### Upgrade sequence

The following diagram summarizes the upgrade sequence. Details are provided in Upgrade procedure below. For example, if you have more than one core component installed on a server, running the installer on that machine will upgrade all components that have new versions. You might want to upgrade the VDA used in a master image, and then update the image. Then, update the catalog that uses that image and the Delivery Group that uses that catalog. Details also cover how to upgrade the Site databases and the Site automatically or manually.




### Which product component versions can be upgraded

Using the product installer, you can upgrade:

- Citrix License Server, Studio, and StoreFront

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Delivery Controllers 7.0 and later.
- VDA 5.6 or later
  - Unlike earlier VDA releases, you must use the product installer to upgrade VDAs; you cannot use MSIs.
  - If the installer detects Receiver for Windows (Receiver.exe) on the machine, it is upgraded to the Receiver version included on the product installation media.
  - VDA 5.6 through VDA 7.8: If the installer detects Receiver for Windows Enterprise (CitrixReceiverEnterprise.exe) on the machine, it is upgraded to Receiver for Windows Enterprise 3.4.
- Director 1 or later
- Database: This Studio action upgrades the schema and migrates data for the Site database (plus the Configuration Logging and Monitoring databases, if you're upgrading from an earlier 7.x version)
- Personal vDisk

**Note**: To upgrade from XenDesktop 5.6, first upgrade to 7.6 LTSR (with the latest CU), and then upgrade to this release.

Using the guidance in the feature/product documentation, upgrade the following if needed:

- Provisioning Services (for XenApp 7.x and XenDesktop 7.x, Citrix recommends using the latest released version; the minimum supported version is Provisioning Services 7.0).
  - Upgrade the Provisioning Services server using the server rolling upgrade, and the clients using vDisk versioning. Citrix recommends upgrading servers before target devices. For more information, see Upgrading Provisioning Servers
  - Provisioning Services 7.x does not support creating new desktops with XenDesktop 5 versions. So, although existing desktops will continue to work, you cannot use Provisioning Services 7.x to create new desktops until you upgrade XenDesktop. Therefore, if you plan a mixed environment of XenDesktop 5.6 and 7.x Sites, do not upgrade Provisioning Services to version 7.
- Host hypervisor version.
- StoreFront.
- Profile Management.
- Federated Authentication Service

### Limitations

The following limitations apply to upgrades:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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 will remind 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.

- **XenApp version earlier than 7.5:** You cannot upgrade from a XenApp version earlier than 7.5. You can migrate from XenApp 6.x; see Migrate XenApp 6.x. Although you cannot upgrade a XenApp 6.5 farm, you can replace the XenApp 6.5 software on a Windows Server 2008 R2 machine with a current VDA for Server OS. See Upgrade a XenApp 6.5 worker to a new VDA.
- **XenDesktop version earlier than 5.6:** You cannot upgrade from a XenDesktop version earlier than 5.6.
- **XenDesktop Express Edition:** You cannot upgrade XenDesktop Express edition. Obtain and install a license for a currently supported edition, and then upgrade it.
- **Early Release or Technology Preview versions:** You cannot upgrade from a XenApp or XenDesktop Early Release or Technology Preview version.
- **Windows XP/Vista:** If you have VDAs installed on Windows XP or Windows Vista machines, see VDAs on machines running Windows XP or Windows Vista.
- **Product selection:** When you upgrade from an earlier 7.x version, you do not choose or specify the product (XenApp or XenDesktop) that was set during the initial installation.
- **Mixed environments/sites:** If you must continue to run earlier version Sites and current version Sites, see Mixed environment considerations.

### Preparation

Before beginning an upgrade:

- **Decide which installer and interface to use:** Use the full-product installer from the XenApp or XenDesktop ISO to upgrade core 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.

  You cannot upgrade by importing or migrating data from a version that can be upgraded. (Note: Some much earlier versions must be migrated instead of upgraded; see Upgrade and migrate for a list of which versions can be upgraded.)

  If you originally installed a desktop VDA with the VDAWorkstationCoreSetup.exe installer, Citrix recommends using that installer to upgrade it. If you use the full-product VDA installer or the

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

For example, if you installed a version 7.13 VDA using VDAWorkstationCoreSetup.exe, and then used the full-product installer to upgrade that VDA to version 7.14, the components that were excluded from the original installation (such as Profile management or Personal vDisk) might be installed during the upgrade, if you accept the default settings or do not use the /exclude command-line option.

- **Check your Site's health:** Ensure the Site is in a stable and functional state before starting an upgrade. If a Site has issues, upgrading will not fix them, and can leave the Site in a complex state that is difficult to recover from. To test the Site, select the **Site** entry in the Studio navigation pane. In the Site configuration portion of the middle pane, click **Test site**.
- **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.

  Optionally, back up templates and upgrade hypervisors, if needed.

  Complete any other preparation tasks dictated by your business continuity plan.
- **Ensure your Citrix licensing is up to date:** 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 2017.0801. (This date applies to the 7.15 LTSR release, not to cumulative updates (CUs) that follow.)
- **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 installer on the machine containing the License Server. If an upgrade is needed, the installer initiates it.
  - From the XenDesktop Setup directory on the installation media, run the command: `.\LicServVerify.exe -h \<License-Server-fqdn> -p 27000 –v`. The resulting display indicates whether the License Server is compatible. If the License Server is incompatible, run the installer on that machine to upgrade it.
- **Back up any StoreFront modifications:** 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.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Before starting an upgrade, stop and disable any third-party monitoring agent services.

- **Ensure 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 the Databases article. If the Studio user does not have those permissions, initiating a manual database upgrade will generate 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.

### Mixed environment considerations

When your environment contains Sites/farms with different product versions (a mixed environment), Citrix recommends using StoreFront to aggregate applications and desktops from different product versions (for example, if you have a XenDesktop 7.13 Site and a XenDesktop 7.14 Site). 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.
- If you plan to run XenDesktop 5.6 and 7.x Sites simultaneously and use Provisioning Services for both, either deploy a new Provisioning Services for use with the 7.x Site, or upgrade the current Provisioning Services and be unable to provision new workloads in the XenDesktop 5.6 Site.

Within each Site, Citrix recommends upgrading all components. Although you can use earlier versions of some components, all the features in the latest version might not be available. For example, although you can use current VDAs in deployments containing earlier Controller versions, new features in the current release may not be available. VDA registration issues can also occur when using non-current versions.

- Sites with Controllers at version 5.x and VDAs at version 7.x should remain in that state only temporarily. Ideally, you should complete the upgrade of all components as soon as possible.
- Do not upgrade a standalone Studio version until you are ready to use the new version.

### VDAs on machines running Windows XP or Windows Vista

You cannot upgrade VDAs installed on machines running Windows XP or Windows Vista to a 7.x version. You must use VDA 5.6 FP1 with certain hotfixes; see CTX140941 for instructions. Although earlier-version VDAs will run in a 7.x Site, they cannot use many of its features, including:

- Features noted in Studio that require a newer VDA version.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Configuring App-V applications from Studio.
- Configuring StoreFront addresses from Studio.
- Automatic support for Microsoft Windows KMS licensing when using Machine Creation Services. See CTX128580.
- Information in Director:
  - Logon times and logon end events impacting the logon duration times in the Dashboard, Trends, and User Detail views.
  - Logon duration breakdown details for HDX connection and authentication time, plus duration details for profile load, GPO load, logon script, and interactive session establishment.
  - Several categories of machine and connection failure rates.
  - Activity Manager in the Help Desk and User Details views.

Citrix recommends reimaging Windows XP and Windows Vista machines to a supported operating system version and then installing the latest VDA.

### VDAs on machines running Windows 8.x and Windows 7

To upgrade VDAs installed on machines running Windows 8.x or Window 7 to Windows 10, Citrix recommends reimaging Windows 7 and Windows 8.x machines to Windows 10 and then installing the supported VDA for Windows 10. If reimaging is not an option, uninstall the VDA before upgrading the operating system; otherwise, the VDA will be in an unsupported state.

### Mixed VDA support

When you upgrade the product to a later version, Citrix recommends you upgrade all the core components and VDAs so you can access all the new and enhanced features in your edition.

In some environments, you may not be able to upgrade all VDAs to the most current version. In this scenario, when you create a machine catalog, you can specify the VDA version installed on the machines. By default, this setting specifies the latest recommended VDA version; you need to consider changing this setting only if the machine catalog contains machines with earlier VDA versions. However, mixing VDA versions in a machine catalog is not recommended.

If a machine catalog is created with the default recommended VDA version setting, and any of the machines in the catalog has an earlier VDA version installed, those machines will not be able to register with the Controller and will not work.

For more information, see VDA versions and functional levels.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Controllers on earlier OSs

Citrix recommends that all Delivery 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.
3. Add the new Controllers to the Site.
4. Remove the Controllers that are running on operating systems that are not valid for the newer release.

For information about adding and removing Controllers, see Delivery Controllers.

### Upgrade procedure

To run the product installer 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, see Install using the command line.

1. If more than one core component is installed on the same server (for example, the Controller, Studio, and License Server) and several of those components have new versions available, they will all be upgraded when you run the installer on that server.

   If any core components are installed on machines other than the Controller, run the installer on each of those machines. The recommended order is: License Server, StoreFront, and then Director.

   If you have not yet determined whether your License Server is compatible with the new version (see Preparation), it is essential that you run the installer on the License Server before upgrading any other core components.

   If you wish to preserve manual modifications to StoreFront stores, back up the store files before upgrading StoreFront (see Preparation).

2. If you use Provisioning Services, upgrade the PVS servers and target devices, using the guidance in the Provisioning Services documentation.
3. Run the product installer on machines containing VDAs. (See Step 12 if you use master images and Machine Creation Services.)
4. Run the product installer on half of the Controllers. (This also upgrades any other core components installed on those servers.) 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 may be times when the Site has reduced capacity

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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, the Site is inoperable during the upgrade.

5. If Studio is installed on a different machine than one you've already upgraded, run the installer on the machine where Studio is installed.
6. From the newly upgraded Studio, upgrade the Site database. For details, see Upgrade the databases and the Site.
7. From the newly upgraded Studio, select **Citrix Studio** *site-name* in the navigation pane. Select the **Common Tasks** tab. Select **Upgrade remaining Delivery Controllers**.
8. After completing the upgrade and confirming completion on the remaining Controllers, close and then reopen Studio. Studio might prompt for an additional Site upgrade to register the Controller's services to the Site, or to create a zone ID if it does not yet exist.
9. In the Site Configuration section of the Common Tasks page, select **Perform registration**. Registering the Controllers makes them available to the Site.
10. After you select **Finish** when the upgrade completes, you are offered the opportunity to enroll in the Citrix telemetry programs, which collect information about your deployment. That information is used to improve product quality, reliability, and performance.
11. After upgrading components, the database, and the Site, test the newly-upgraded Site. From Studio, select **Citrix Studio** *site-name* in the navigation pane. Select the **Common Tasks** tab and then select **Test Site**. These tests were run automatically after you upgraded the database, but you can run them again at any time.

    The Test Site functionality might fail for a Controller installed on Windows Server 2016, when a local SQL Server Express is used for the Site database, if the SQL Server Browser service is not started. To avoid this, complete the following tasks.

    a) Enable the SQL Server Browser service (if required) and then start it.

    b) Restart the SQL Server (SQLEXPRESS) service.

12. If you use Machine Creation Services and want to use upgraded VDAs: After you upgrade and test the deployment, update the VDA used in the master images (if you haven't done that already). Update master images that use those VDAs. See Update or create a new master image. Then update machine catalogs that use those master images, and upgrade Delivery Groups that use those catalogs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Upgrade the databases and the Site

After upgrading the core components and VDAs, use the newly upgraded Studio to initiate an automatic or manual database and Site upgrade.

Remember: Check the Preparation section above for permission requirements.

- For an automatic database upgrade, the Studio user's permissions must include the ability to update the SQL Server database schema.
- For a manual upgrade, the Studio user runs some of the generated scripts from Studio. The database administrator runs other scripts, using either the SQLCMD utility or the SQL Server Management Studio in SQLCMD mode. Otherwise, inaccurate errors can result.

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.

After the database upgrade completes and product services are enabled, Studio 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.

**Upgrade the database and site automatically:**

Launch the newly upgraded Studio. After you choose 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. Launch the newly upgraded Studio. Choose to upgrade the site manually. The wizard checks for License Server compatibility and requests confirmation. After you confirm that you have backed up the database, the wizard generates and displays the scripts and a checklist of upgrade steps.
2. Run the following scripts in the order shown.
    - **DisableServices.ps1**: PowerShell script to be run by the Studio user on a Controller to disable product services.
    - **UpgradeSiteDatabase.sql**: SQL script to be run by the database administrator on the server containing the Site database.
    - **UpgradeMonitorDatabase.sql**: SQL script to be run by the database administrator on the server containing the Monitor database.
    - **UpgradeLoggingDatabase.sql**: SQL script to be run by the database administrator on the server containing the Configuration Logging database. Run this script only if this database changes (for example, after applying a hotfix).
    - **EnableServices.ps1**: PowerShell script to be run by the Studio user on a Controller to enable product services.
3. After completing the checklist tasks. click **Finish upgrade.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Dbschema upgrade

When you update your deployment to a new CU, several of your database schemas are upgraded. Consult the following table for information about which database schemas are being upgraded in the process:

| 7.15 DBschema upgrade | 7.15 CU1 | 7.15 CU2 | 7.15 CU3 | 7.15 CU4 | 7.15 CU5 | 7.15 CU6 | 7.15 CU7 | 7.15 CU8 |
|---|---|---|---|---|---|---|---|---|
| 7.15 RTM | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging |
| 7.15 CU1 | | Config | Site; Config | Site; Config | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging |
| 7.15 CU2 | | | Site; Config | Site; Config | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging |
| 7.15 CU3 | | | | Site; Config | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging |
| 7.15 CU4 | | | | | Monitor, Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging | Site; Monitor; Config; Logging |
| 7.15 CU5 | | | | | | Site; Monitor; Config | Site; Monitor; Config | Site; Monitor; Config |
| 7.15 CU6 | | | | | | | Site; Monitor; Config | Site; Monitor; Config |
| 7.15 CU7 | | | | | | | | Site; 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, License Server version, or both are updated in the Configuration table.
- Logging = Logging Datastore; Dbschema update is made to the Logging Datastore.

## Upgrade a XenApp 6.5 worker to a new VDA

August 17, 2018

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 earlier software and then installing a new VDA for Server OS.

**NOTE:** 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, using the instructions in Removing Roles and Components. 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\."

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. 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

### Troubleshooting

Symptoms: 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 Windows Server OS.

## Migrate XenApp 6.x

December 10, 2021

**NOTE:** You cannot use the Citrix Smart Migrate product with this version of XenApp and XenDesktop. However, the Migration Tool is available.

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.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 farm data to XML files.
    c) 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.
2. On the XenApp 7.6 Controller:
    a) Import the PowerShell import modules.
    b) Run the import cmdlets to import policy and farm data (applications), using the XML files as input.
3. 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.

#### New in this release

This December 2014 release (version 20141125) contains the following updates:

- If you encounter issues using the migration tool on a XenApp 6.x farm, report them to https://discussions.citrix.com/forum/1411-xenapp-7x/.
- New packaging - the `XAMigration.zip` file now contains two separate, independent packages: `ReadIMA.zip` and `ImportFMA.zip`. To export from a XenApp 6.x server, you need only `ReadIMA.zip`. To import to a XenApp 7.6 server, you need only `ImportFMA.zip`.
- The `Export-XAFarm` cmdlet supports a new parameter (`EmbedIconData`) that eliminates the need to copy icon data to separate files.
- The `Import-XAFarm` cmdlet supports three new parameters:
    - `MatchServer` - import applications from servers whose names match an expression
    - `NotMatchServer` - import applications from servers whose names do not match an expression
    - `IncludeDisabledApps` - import disabled applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Prelaunched applications are not imported.
- The `Export-Policy` cmdlet works on XenDesktop 7.x.

#### Migration Tool package

The migration tool is available under the XenApp 7.6 Citrix download site. The XAMigration.zip file contains two separate, independent packages:

- `ReadIMA.zip` - 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.zip` - 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Module or file | Description |
| --- | --- |
| 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 and server names, plus other farm, application, and policy configura-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tion 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 might be applied to the policy after the import. The allow and 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, the file is placed in the script's current execution folder. The default log name is `XFarmYYYYMMDDHHmmSS-xxxxxx` where the last six digits are 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 more logging coverage, use the PowerShell logging features. For example, PowerShell transcripts

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 need to understand basic PowerShell concepts. Although extensive scripting expertise is not required, you need understand the cmdlets you run. Use the `Get-Help` cmdlet to review each migration cmdlet's help before running 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 product documentation for your StoreFront or Web Interface release (**Manage > Create a store**).
- 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 run.
- In the step-by-step sections, most `<string>` parameter values show surrounding quotation marks. These are optional for single-word strings.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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 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 contain instructions.
- Do not have any other active user connections during an import. The import scripts create many new objects, and disruptions might 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, without actually importing anything. The logs 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

and the XenApp 7.6 site. Unzip `XAMigration.zip` on the network file share. There are 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 run (for example: `Set-ExecutionPolicy RemoteSigned`).
7. Import the module definition files `ExportPolicy.psd1` and `ExportXAFarm.psd1`:

   ```
   Import-Module .\ExportPolicy.psd1
   ```

   ```
   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, run the `Export-Policy` cmdlet.

| Parameter | Description |
|---|---|
| -XmlOutputFile “.xml” | XML output file name. This file holds 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 “” | 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| -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`.

```
1 Export-Policy -XmlOutputFile ".\MyPolicies.XML" -LogFile ".\
     MyPolicies.Log"
2 <!--NeedCopy-->
```

9. To export farm data, run the `Export-XAFarm` cmdlet, specifying a log file and an XML file.

| Parameter | Description |
| --- | --- |
| -XmlOutputFile “.xml” | XML output file name. This file holds 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| -LogFile “” | 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 parameter 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 for how-to-use information. Default: False. Administrator information is exported. |
| -IgnoreApps | Do not export application information. See Advanced use for how-to-use information. Default: False. Application information is exported. |
| -IgnoreServers | Do not export server information. Default: False. Server information is exported. |
| -IgnoreZones | Do not export zone information. Default: False. Zone information is exported. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| -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. **Note**: This switch allows you to proceed with an export when an error occurs that would not affect the actual data being used for the export or import process. |
| -AppLimit | Number of applications to be exported. See Advanced use for how-to-use information. 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 for details. |
| -SkipApps | Number of applications to skip. See Advanced use for how-to-use information. 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 running the `Import-Policy` or `Import-XAFarm` cmdlet with the `Preview` parameter). You can then 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 `Export-XAFarm`, 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 (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 run (for example: `Set-ExecutionPolicy RemoteSigned`).
7. Import the PowerShell module definition files `ImportPolicy.psd1` and `ImportXAFarm.psd1`:

   ```
   Import-Module .\ImportPolicy.psd1
   ```

   ```
   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, run the `Import-Policy` cmdlet, specifying the XML file containing the exported policy data.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| -XmlInputFile “.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. |
| -XsdFile “” | XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use for how-to-use information. Default: PolicyData.XSD |
| -LogFile “” | 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Example: The following 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"
<!--NeedCopy-->
```

9. To import applications, run the `Import-XAFarm` cmdlet, specifying a log file and the XML file containing the exported farm data.

| Parameter | Description |
| --- | --- |
| -XmlInputFile “.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 “” | XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use for how-to-use information. Default: XAFarmData.XSD |
| -LogFile “” | 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| -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. |
| -DeliveryGroupName “” | Delivery Group name for all imported applications. See Advanced use for how-to-use information. Default: “-Delivery Group” |
| -MatchFolder “” | Import only those applications in folders with names that match the string. See Advanced use for how-to-use information. Default: No matching occurs. |
| -NotMatchFolder “” | Import only those applications in folders with names that do not match the string. See Advanced use for how-to-use information. Default: No matching occurs. |
| -MatchServer “” | Import only those applications from servers whose names match the string. See Advanced use for how-to-use information. |
| -NotMatchServer “” | Import only those applications from servers whose names do not match the string. See Advanced use for how-to-use information. Default: No matching occurs. |
| -MatchWorkerGroup “” | Import only those applications published to worker groups with names that match the string. See Advanced use for how-to-use information. Default: No matching occurs. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| -NotMatchWorkerGroup “” | Import only those applications published to worker groups with names that do not match the string. See Advanced use for how-to-use information. Default: No matching occurs. |
| -MatchAccount “” | Import only those applications published to user accounts with names that match the string. See Advanced use for how-to-use information. Default: No matching occurs. |
| -NotMatchAccount “” | Import only those applications published to user accounts with names that do not match the string. See Advanced use for how-to-use information. Default: No matching occurs. |
| -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"

<!--NeedCopy-->
```

10. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Policies and policy settings

Importing policies is essentially a copy operation, except for 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. Keep the settings values the same (except for deprecated policy settings, as noted in the next step).
    - If you have a few 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 many 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 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 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 might change the effect of filters.

### Filters

Carefully examine the filters for each policy. Changes might be required to ensure they still work in XenApp 7.6 as originally intended in XenApp 6.x.

| Filter | Considerations |
| --- | --- |
| Access Control | Usually, Access Control contains the same values as the original XenApp 6.x filters, and works without requiring changes. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Filter | Considerations |
| --- | --- |
| Citrix CloudBridge | A simple Boolean. Usually works 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 might require changes if different clients connect to the XenApp 7.6 VDA machines. |
| Organizational Unit | Values might be preserved, depending on whether 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 might 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, carefully review the values. |
| User or Group | Values might be preserved, depending on whether 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 might 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Filter | Considerations |
| --- | --- |
| 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, only some accounts might be resolved. While there is only a small chance that different domains and users have the same name, 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 that the basic properties were preserved during the import. Use the information in the Application property mapping section 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 might 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 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 long time, you can 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 not only create the Delivery Group object, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 many 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"
-AppLimit "200"
<!--NeedCopy-->
```

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"
<!--NeedCopy-->
```

#### 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- `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 parameter 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 might 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 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.
  - `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
<!--NeedCopy-->
```

  - `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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile
    XAFarmImport.log -MatchFolder 'Productivity Apps' -
    DeliveryGroupName 'Productivity Apps'
<!--NeedCopy-->
```

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/.*"
<!--NeedCopy-->
```

- `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'
<!--NeedCopy-->
```

- `MatchServer` and `NotMatchServer` - For example, for applications organized on servers, the following cmdlet imports applications associated with the server not named `Current` to a Delivery Group named `Legacy`.

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.
    log -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
<!--NeedCopy-->
```

#### 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 recommends 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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. Unfiltered policies are never imported. The features and components that support these settings have either been replaced by new technologies and components, or the settings do not apply because of architectural and platform changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Log shadow attempts *
- Notify user of pending shadow connections *
- Prelaunch disconnect timer interval, Prelaunch 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 |
| DisplayName | PublishedName |
| Enabled | Enabled |
| StartMenuFolder | StartMenuFolder |
| WaitOnPrinterCreation | WaitForPrinterCreation |
| WorkingDirectory | WorkingDirectory |
| FolderPath | AdminFolderName |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| IMA Property | Comments |
| --- | --- |
| 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. |
| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| IMA Property | Comments |
| --- | --- |
| 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

August 17, 2018

XenApp and XenDesktop offer 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, XenApp and XenDesktop securely separate 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 XenDesktop and XenApp 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

XenApp and XenDesktop 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 XenDesktop and XenApp 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.

XenApp and XenDesktop 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 could 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 XenApp or XenDesktop 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.

XenApp and XenDesktop also support multifactor authentication for Windows or a specific application. Multifactor authentication could also be used to manage all resources delivered by XenApp and XenDesktop. These methods include:

- Tokens
- Smart cards
- RADIUS
- Kerberos
- Biometrics

XenDesktop can be integrated with many third-party security solutions, ranging from identity management to antivirus software. A list of supported products can be found at https://www.citrix.com/ready.

Select releases of XenApp and XenDesktop are certified for Common Criteria standard. For a list of those standards, go to https://www.commoncriteriaportal.org/cc/.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Security considerations and best practices

May 13, 2021

> **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 https://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 such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET) for Windows machines. Some authorities recommend using the latest Microsoft-supported version of EMET within their regulated environments. Note that, according to Microsoft, EMET may not be compatible with some software, so it should be thoroughly tested with your applications before deployment in a production environment. XenApp and XenDesktop have been tested with EMET 5.5 in its default configuration. Currently, EMET is not recommended for use on a machine that has a Virtual Delivery Agent (VDA) installed.

Protect all machines in your environment with perimeter firewalls, including at enclave boundaries as appropriate.

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.

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 configure those firewall ports manually. If you use a different firewall, you must configure the firewall manually.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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 (https://www.iana.org/).

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 Security (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.

#### 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.

When planning for desktop privileges, note:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Change basic settings.
- 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.

Some applications require desktop privileges, even though they are intended for users rather than for administrators. These users may not be as aware of security risks.

Treat these applications as highly-sensitive applications, even if their data is not sensitive. Consider these approaches to reduce security risk:

- Enforce two-factor authentication and disable any single sign-on mechanism for the application
- Enforce contextual access policies
- Publish the application to a dedicated desktop. If the application must be published to a shared hosted desktop, do not publish any other applications to that shared hosted desktop
- Ensure the desktop privileges are only applied to that desktop, and not to other computers
- Enable Session Recording for the application. Also enable other security logging capabilities in the application, and within Windows itself.
- Configure XenApp and XenDesktop to limit features used with the application (for example, clipboard, printer, client drive, and USB redirection)
- Enable any security features of the application. Limit it to match strictly the users' requirements - no more
- Configure security features of Windows to match strictly the users' requirements. This will be a simpler configuration if only that single application is published to the desktop; for example, a restrictive AppLocker configuration can be used. Control access to the file system.
- Plan to reconfigure, upgrade, or replace the application so that desktop privileges are not required in future

These approaches will not remove all security risk from applications that require desktop privileges.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Server 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 XenApp and XenDesktop, including the VDA for Desktop 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 XenApp or XenDesktop deployment, and also offers functionality used by the console to enumerate resources in a hypervisor pool.
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService): Orchestrates the creation of desktop VMs.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Collects metrics for XenApp or XenDesktop, 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 databse 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## Integrate XenApp and XenDesktop with NetScaler Gateway

August 21, 2018

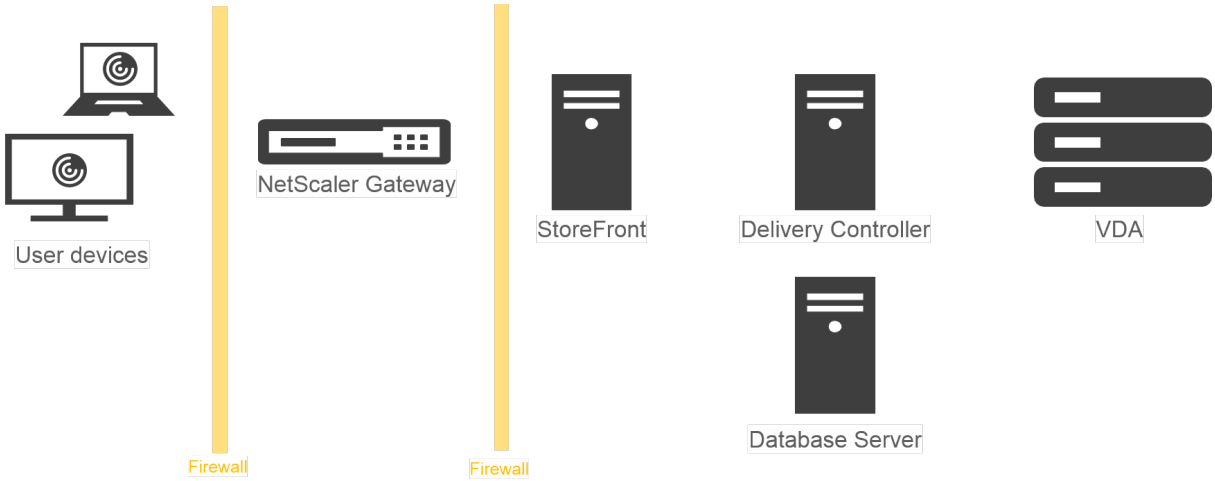
StoreFront servers are deployed and configured to manage access to published resources and data. For remote access, adding NetScaler Gateway in front of StoreFront is recommended.

> **Note:**
>
> For detailed configuration steps on how to integrate XenApp and XenDesktop with NetScaler Gateway, see the StoreFront documentation.

The following diagram illustrates an example of a Citrix simplified Citrix deployment that includes NetScaler Gateway. NetScaler Gateway communicates with StoreFront to protect apps and data de-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

livered by XenApp and XenDesktop. The user devices run Citrix Receiver to create a secure connection and access their apps, desktops, and files.




Users log on and authenticate using NetScaler Gateway. NetScaler 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

November 1, 2018

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 could be a Delivery Group Administrator and a Machine Catalog Administrator. Roles can be built-in or custom.

  The built-in roles are:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 as well as 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, and can also perform session management and machine power management operations for the machines in those Delivery Groups. |
| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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; how-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

ever, 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. Additionally, 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 additional 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 new 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 new administrator now, but that person will not begin 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 will 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

role or the scope, nor does it 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.

- To 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.
- To 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.
- To 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.
- To 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 will result in there being no enabled Full Administrator.

### Create and manage roles

Role names can contain up to 64 Unicode characters; they cannot contain the following characters: \ (backslash), / (forward slash), ; (semicolon), : (colon), # (pound sign) , (comma), * (asterisk), ? (question mark), = (equal sign), < (left arrow), > (right arrow), | (pipe), [ ] (left or right bracket), ( ) (left or right parenthesis), ‘‘(quotation marks), and ‘(apostrophe). 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. Editions that do not support custom roles do not 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.

- To 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.
- To create a custom role, click Create new Role in the Actions pane. Enter a name and description. Select the object types and permissions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- To 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.
- To 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.
- To 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 procedure below. 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; they cannot include the following characters: \ (backslash), / (forward slash), ; (semicolon), : (colon), # (pound sign) , (comma), * (asterisk), ? (question mark), = (equal sign), < (left arrow), > (right arrow), | (pipe), [ ] (left or right bracket), ( ) (left or right parenthesis), "(quotation marks), and '(apostrophe). 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 you make 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.

- To 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).
- To 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.
- To 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- To 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 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 | Where to write the output. Default = stdout |
| -AdminAddress | IP address or host name of the Delivery Controller to connect to. Default = localhost |
| -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. |
| | Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For details, see the Microsoft documentation. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

March 11, 2021

Smart cards and equivalent technologies are supported within the guidelines described in this article. To use smart cards with XenApp or XenDesktop:

- 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 XenApp or XenDesktop 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.

### Types of smart cards

Enterprise and consumer smart cards have the same dimensions, electrical connectors, and fit the same smart card readers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 e-mail. XenApp and XenDesktop 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 XenApp or XenDesktop.

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 Receiver minimum 4.3.
  - Versions of XenApp and XenDesktop earlier than 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 simply stored on the user computer. These digital certificates are not strictly equivalent to smart cards.

XenApp and XenDesktop 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 at https://www.citrix.com/ready/.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

be used. For more information about Citrix-compatible smart cards and middleware, see https://www.citrix.com/ready.

| Middleware | Matching cards |
|---|---|
| ActivClient 7.0 (DoD mode enabled) | DoD CAC card |
| ActivClient 7.0 in PIV mode | NIST PIV card |
| Microsoft mini driver | NIST PIV card |
| GemAlto Mini Driver for .NET card | GemAlto .NET v2+ |
| Microsoft native driver | Virtual Smart Cards (TPM) |

For information about smart card usage with other types of devices, see the Citrix Receiver documentation for that device.

For information about smart card usage with other types of devices, see the Citrix Receiver 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; smart cards are not supported for office PCs running Windows XP.

The following smart cards were tested with Remote PC Access:

| Middleware | Matching cards |
|---|---|
| Gemalto .NET minidriver | Gemalto .NET v2+ |
| ActivIdentity ActivClient 6.2 | NIST PIV |
| ActivIdentity ActivClient 6.2 | CAC |
| Microsoft minidriver | NIST PIV |
| Microsoft native driver | Virtual smart cards |

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receiver you are using. In the Citrix Receiver 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 XenApp and XenDesktop, 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.

If you are using hosted applications running on Windows Server 2008 or 2008 R2 and with smart cards requiring the Microsoft Base Smart Card Cryptographic Service Provider, you might find that if a user

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

runs a smart card transaction, all other users who use a smart card in the logon process are blocked. For further details and a hotfix for this issue, see https://support.microsoft.com/kb/949538.

You can reset PINs using a card management system or vendor utility.

> **Important**
>
> Within a XenApp or XenDesktop 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 XenApp and XenDesktop; 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 https://catalog.update.microsoft.com or from your vendor. Additionally, 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 Receiver 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 NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optional for Remote PC Access): Microsoft Exchange Server

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 NetScaler 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 Receiver 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 Receiver 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 Receiver).

## Smart card deployments

October 29, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Type | StoreFront connectivity |
| --- | --- |
| Local domain-joined computers | Directly connected |
| Remote access from domain-joined computers | Connected through NetScaler Gateway |
| Non-domain-joined computers | Directly connected |
| Remote access from non-domain-joined computers | Connected through NetScaler Gateway |
| Non-domain-joined computers and thin clients accessing the Desktop Appliance site | Connected through Desktop Appliance sites |
| 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 NetScaler Gateway, users log on to their devices and are prompted by Receiver for Windows to authenticate to NetScaler Gateway. This applies to both domain-joined and non-domain-joined devices. Users can log on to NetScaler Gateway using either their smart cards and PINs, or with explicit credentials. This enables you to provide users with bimodal authentication for NetScaler Gateway logons. Configure pass-through authentication from NetScaler Gateway to StoreFront and

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

delegate credential validation to NetScaler 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. |

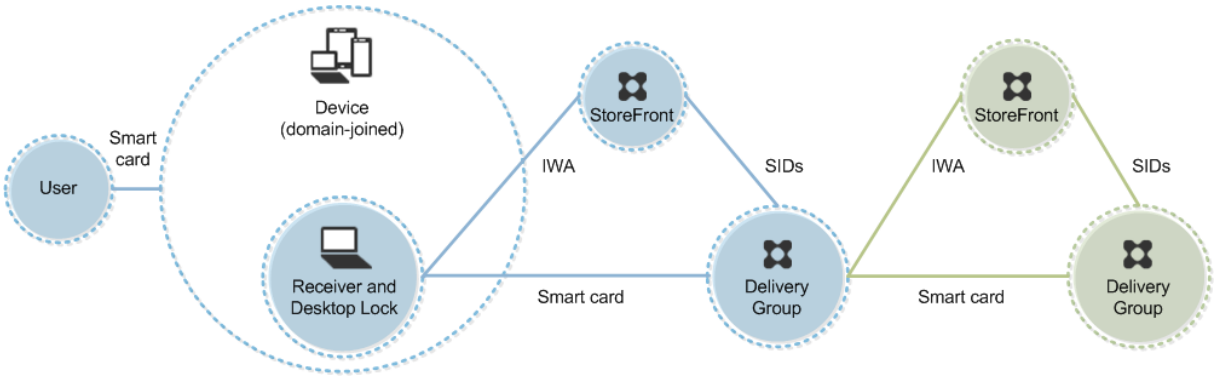
### Certificate revocation checking

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Deployment example: domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.

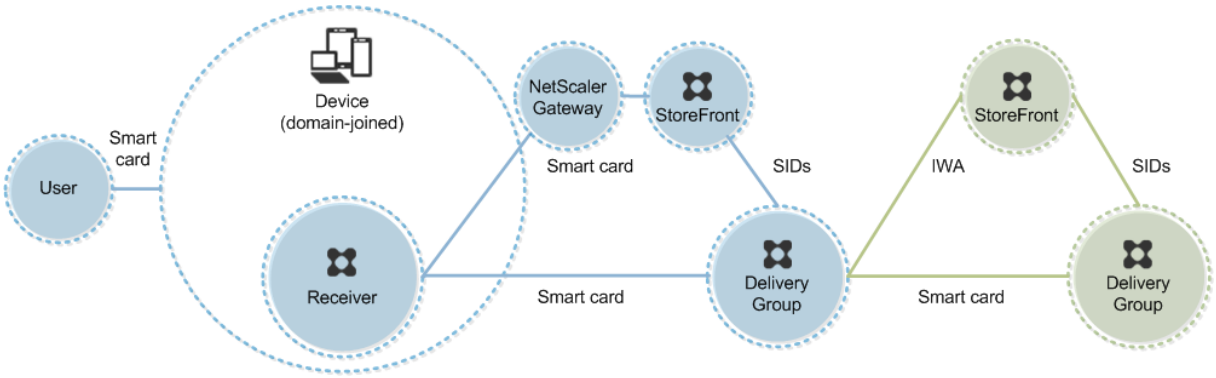



A user logs on to a device using a smart card and PIN. Receiver authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user 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 NetScaler Gateway/Access Gateway.




A user logs on to a device using a smart card and PIN, and then logs on again to NetScaler 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.

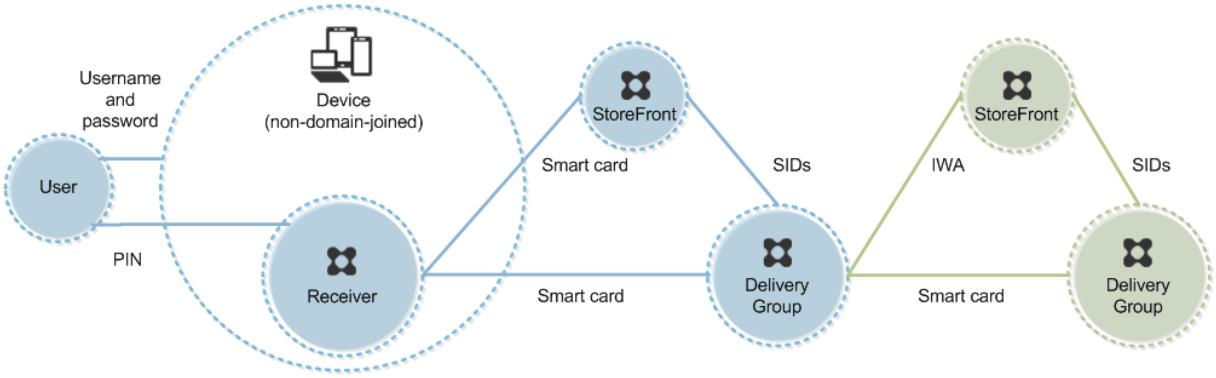
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The user is automatically logged on to StoreFront, which passes the user security identifiers (SIDs) to XenApp or XenDesktop. 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.

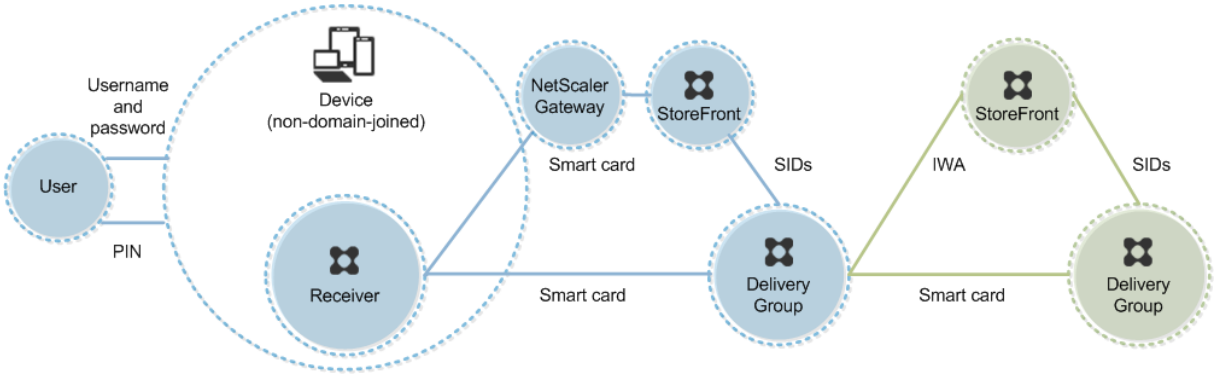
StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 XenApp or XenDesktop. 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.

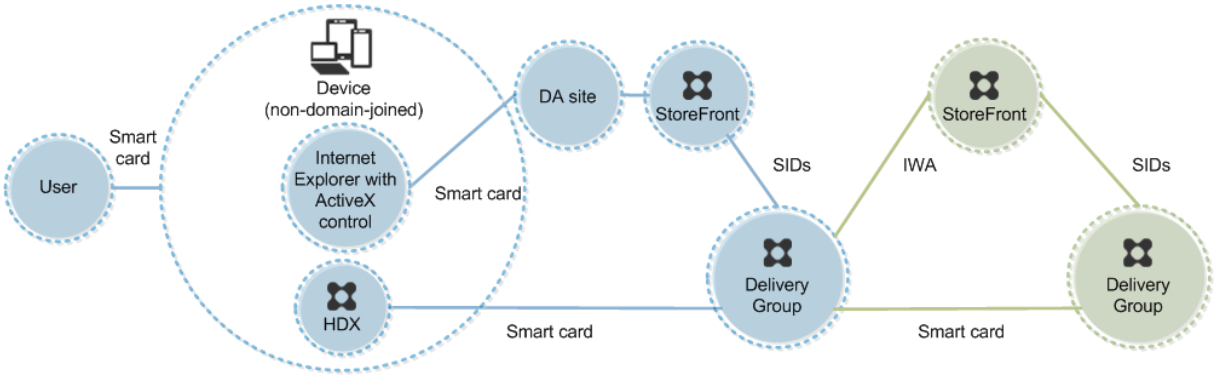
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown 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 XenApp, XenDesktop, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 XenApp or XenDesktop. The first available desktop in the alphabetical list in an assigned Desktop Group starts.

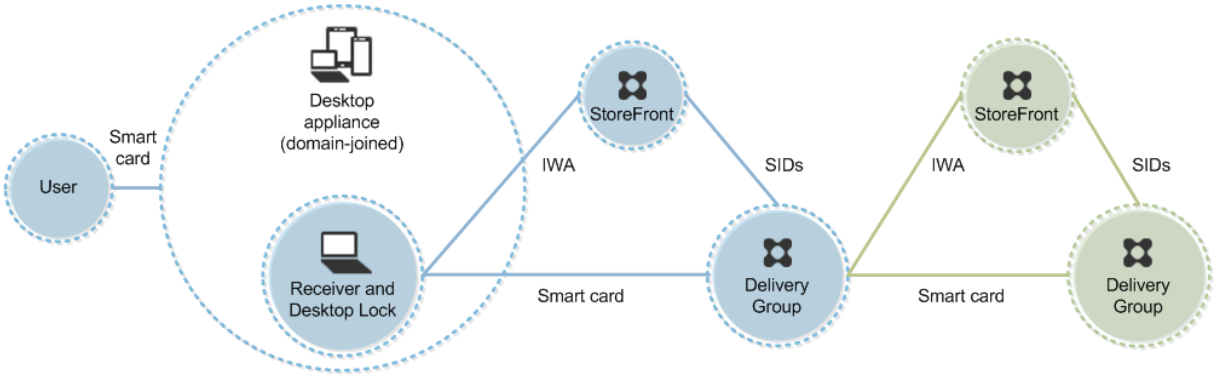
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown 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 XenApp, XenDesktop, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 XenApp or XenDesktop. 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 10, 2022

### 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 NetScaler 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 the 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)

December 20, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Configuring a XenApp or XenDesktop Site to use the Transport Layer Security (TLS) protocol includes the following procedures:

- 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 users 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.") You can use a PowerShell script supplied by Citrix, or configure it manually. For general information, see About TLS settings on VDAs. For details, see Configure TLS on a VDA using the PowerShell script and 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.
  - If you intend to configure TLS on VDAs that have been upgraded from earlier versions, uninstall any SSL relay software on those machines before upgrading them.
  - The PowerShell script configures TLS on static VDAs; it does not configure TLS on pooled VDAs that are provisioned by Machine Creation Services or Provisioning Services, where the machine image resets on each restart.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Note:**
>
> If both TLS and UDT are enabled at the VDA:
>
> - For direct access to the VDA, Citrix Receiver always uses TLS over TCP (not UDP and UDT).
> - For indirect access to the VDA using NetScaler Gateway, Citrix Receiver uses DTLS over UDP for communication with NetScaler Gateway. The communication between NetScaler Gateway and the VDA uses UDP without DTLS. UDT is used.

## 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.

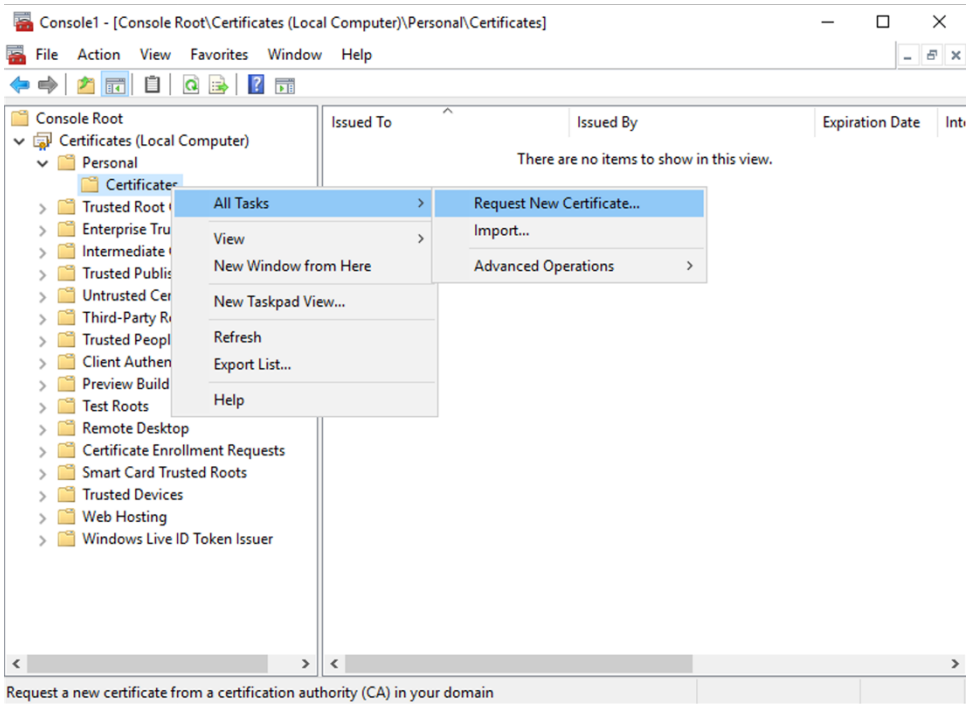
Although there are various different types of certificate authorities and methods of requesting certificate from them, this article describes the Microsoft Certificate Authority. The Microsoft Certificate Authority needs to have a certificate template published with a purpose of Server Authentication.

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.

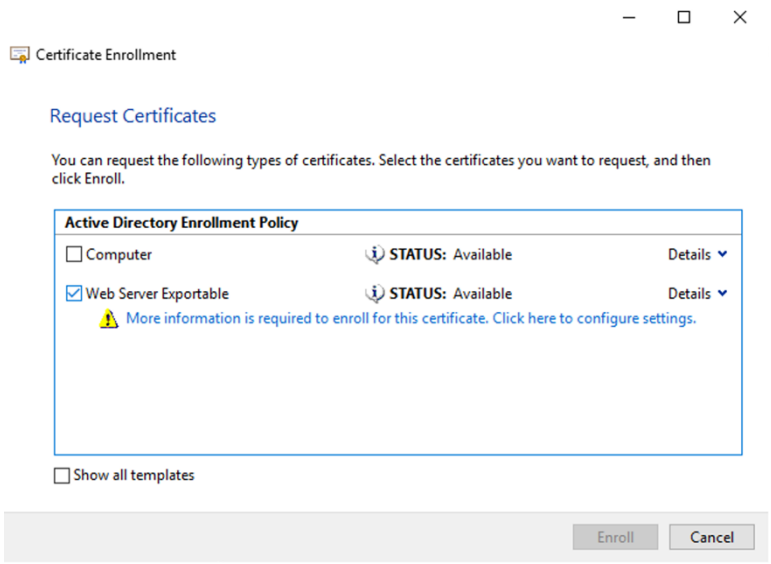
### Requesting and installing a certificate

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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.

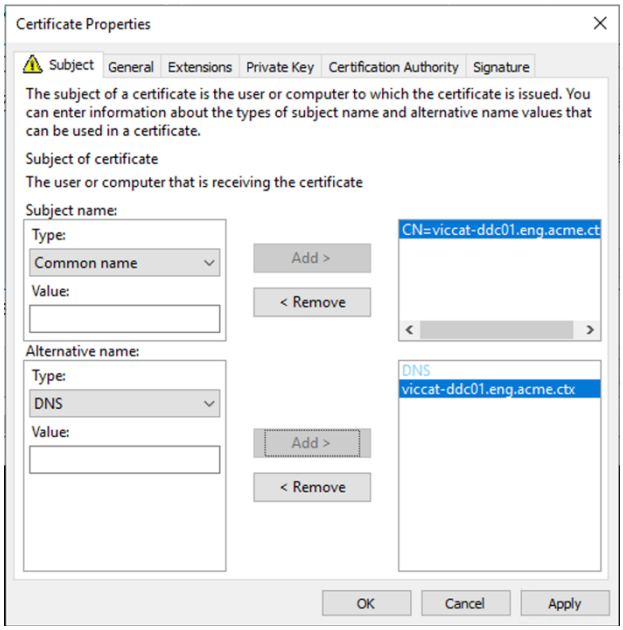



5. To provide more details for the certificate template, click the **Details** arrow button and configure the following:

   **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

The cipher suite order list should include the `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` or `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` cipher suites (or both). These cipher suites must precede any `TLS_DHE_` cipher suites.

> **Note:**
>
> Windows Server 2012 does not support the GCM cipher suites `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3` or `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`.

1. Using the Microsoft Group Policy Editor, browse to **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 ciphersuites 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` 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.

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
```

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### TLS settings on VDAs

A Delivery Group cannot have a mixture of some VDAs with TLS configured and some VDAs without TLS configured. When you configure TLS for a Delivery Group, you should have already configured TLS for all of 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. You 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.

- **Which TLS cipher suites to allow.**

A cipher suite selects the encryption that will be used for a connection. Clients and VDAs can support different sets of cipher suites. When a client (Citrix Receiver 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.

Three sets of cipher suites (also known as compliance modes) are supported by the VDA: GOV(ernment), COM(mercial), and ALL. The acceptable cipher suites also depend on the Windows FIPS mode; see `https://support.microsoft.com/kb/811833` for information about Windows FIPS mode. The following table lists the cipher suites in each set:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| TLS cipher suite | GOV | COM | ALL | GOV | COM | ALL |
|---|---|---|---|---|---|---|
| FIPS mode | Off | Off | Off | On | On | On |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | x | | x | x | | x |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | x | | x | x | | x |
| TLS_RSA_WITH_AES_256_GCM_SHA384 | | | x | x | | x |
| TLS_RSA_WITH_AES_128_GCM_SHA256 | | | x | x | x | x |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | | | x | x | | x |
| TLS_RSA_WITH_AES_256_CBC_SHA | | | x | x | | x |
| TLS_RSA_WITH_AES_128_CBC_SHA | | | x | | x | x |
| TLS_RSA_WITH_RC4_128_SHA | | | x | | | |
| TLS_RSA_WITH_RC4_128_MD5 | | | x | | | |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | | | x | x | | x |

> **Important:**
>
> An extra step is necessary when the VDA is on Windows Server 2012 R2, Windows Server 2016, Windows 10 Anniversary Edition, or a later supported release. This affects connections from Citrix Receiver for Windows (version 4.6 through 4.9), Citrix Receiver for HTML5, and Citrix Receiver for Chrome. This also includes connections via NetScaler Gateway.
>
> This step is also required for all connections using NetScaler Gateway, for all VDA versions, if TLS between the NetScaler Gateway and the VDA is configured. This affects all Citrix Receiver versions.

On the VDA (Windows Server 2016 or Windows 10 Anniversary Edition or later), using the Group Policy Editor, 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_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Note:**
>
> The first four 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 Receiver 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 a VDA using the PowerShell script

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, the script disables all existing Windows Firewall rules for the specified TCP port before adding a new rule that allows the ICA Service to accept incoming connections only on the TLS TCP port. 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; they cannot use ICA/HDX, ICA/HDX with Session Reliability, or HDX over WebSocket, without TLS.

See Network ports.

> **Note:**
>
> For stateless machines, like PVS targets or MCS clones, a FQDN certificate is used by default.

The script contains the following syntax descriptions, plus extra examples; you can use a tool such as Notepad++ to review this information.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **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>"]
<!--NeedCopy-->
```

| 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. |
| 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: “SSL_3.0”, “TLS_1.0”(default), “TLS_1.1”, and “TLS_1.2”. **Important:** Citrix recommends that customers review their usage of SSLv3 and take steps to reconfigure their deployments to remove support for SSLv3 where appropriate. See CTX200238. |
| SSLCipherSuite “” | TLS cipher suite, enclosed in quotation marks. Valid values: “GOV”, “COM”, and “ALL”(default) |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Examples

The following script installs and enables the TLS 1.2 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 TLS certificate's private key for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows Desktop OS, or NT SERVICE\TermService for a VDA for Windows Server OS. On the machine where the VDA is installed:

1. Launch the Microsoft Management Console (MMC): **Start > Run > mmc.exe**.
2. Add the Certificates snap-in to the MMC:
    a) Select **File > Add/Remove Snap-in**.
    b) Select **Certificates** and then click **Add**.
    c) When prompted with **This snap-in will always manage certificates for:**, choose **Computer account** and then click **Next**.
    d) When prompted with **Select the computer you want this snap-in to manage**, choose **Local computer** and then click **Finish**.
3. Under **Certificates (Local Computer) > Personal > Certificates**, right–click the certificate and then select **All Tasks > Manage Private Keys**.
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 Desktop OS, "PORTICASERVICE"
    - For a VDA for Windows Server OS, "TERMSERVICE"

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

5. Double-click the installed TLS certificate. In the certificate dialog, select the **Details** tab and then scroll to the bottom. Click **Thumbprint**.
6. Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
   a) 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).
   b) Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
   c) 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).
7. Ensure the TLS TCP port is open in the Windows Firewall if it is not the default 443. (When you create the inbound rule in Windows Firewall, make sure its properties have the **Allow the connection** and **Enabled** entries selected.)
8. Ensure that no other applications or services (such as IIS) are using the TLS TCP port.
9. For VDAs for Windows Server OS, restart the machine for the changes to take effect. (You do not need to restart machines containing VDAs for Windows Desktop OS.)

### 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 VDA's system event log.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

When using Citrix Receiver for Windows, if you receive a connection error (such as 1030) that indicates an TLS error, disable Desktop Viewer and then try connecting again. Although the connection will still fail, 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.)

### Communication between Controller and VDA

Communication between the Controller and the VDA is secured by Windows Communication Framework (WCF) message-level protection. Additional 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

You can use HTML5 video 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.

For more information on HTML5 video redirection, see Multimedia policy settings.

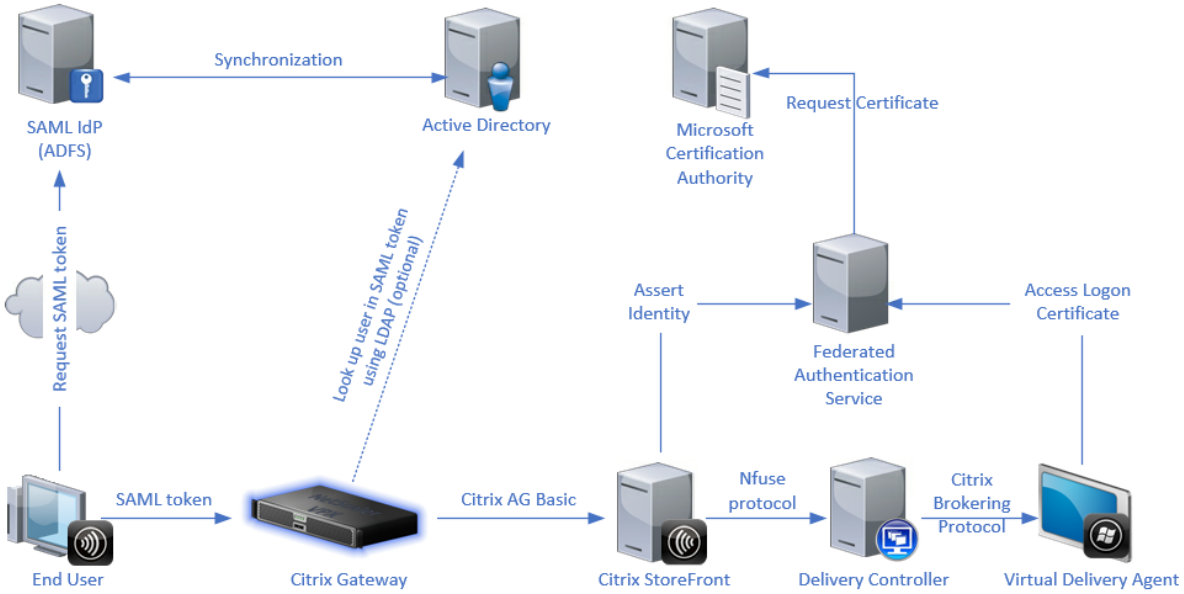
## Federated Authentication Service

December 12, 2023

The Citrix Federated Authentication Service(FAS) is a privileged component designed to integrate with Active Directory Certificate Services. It dynamically issues certificates for users, allowing them to log on to an Active Directory environment as if they had a smart card. FAS allows StoreFront to use a broader range of authentication options, such as SAML (Security Assertion Markup Language) assertions. SAML is commonly used as an alternative to traditional Windows user accounts on the Internet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The following diagram shows the integration of FAS with a certificate authority to provide services to StoreFront and XenApp and XenDesktop Virtual Delivery Agents (VDAs).




Trusted StoreFront servers contact the Federated Authentication Service (FAS) as users request access to the Citrix environment. The FAS grants a ticket that allows a single XenApp or XenDesktop session to authenticate with a certificate for that session. When a VDA needs to authenticate a user, it connects to FAS and redeems the ticket. Only FAS has access to the user certificate's private key. The VDA sends each signing and decryption operation that it requires with the certificate to FAS.

## Requirements

The Federated Authentication Service is supported on Windows servers (Windows Server 2008 R2 or later).

- Citrix recommends installing FAS on a server that does not have other Citrix components.
- The Windows Server must be secured. It has access to a registration authority certificate and the corresponding private key. The server uses these accesses to issue the certificate to domain users. Once issued, the server has access to the user certificates and private keys as well.
- The FAS PowerShell SDK requires Windows PowerShell 64-bit installed on the FAS server.
- A certificate authority such as Microsoft Enterprise or any other certificate authority validated in the Citrix Ready program is required to issue user certificates.
- For certificate authorities other than Microsoft, ensure the following:
  - The certificate authority (CA) is registered in the Active Directory as an enrollment service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - The CA certificate is in the NTAuth store on the Domain Controller. For more information, see How to import third-party certificate authority (CA) certificates into the Enterprise NTAuth store.

In the XenApp or XenDesktop Site:

- The Delivery Controllers must be at least of the version 7.15.
- The VDAs must be at least of the version 7.15. Make sure to apply the FAS Group Policy configuration to the VDAs before creating the Machine Catalog. For more information, see Configure Group Policy.
- The StoreFront server must be at least of the version 3.12 (XenApp and XenDesktop 7.15 ISO supports the 3.12 StoreFront version).

When planning your deployment of this service, review the Security considerations section.

References:

- Active Directory Certificate Services

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)?redirectedfrom=MSDN

- Configuring Windows for Certificate Logon

https://support.citrix.com/article/CTX206156

### Install and setup sequence

1. Install the Federated Authentication Service
2. Enable the Federated Authentication Service plug-in on StoreFront servers
3. Configure Group Policy
4. Use the Federated Authentication Service administration console to: (a) Deploy the provided templates, (b) Set up certificate authorities, and (c) Authorize the Federated Authentication Service to use your certificate authority
5. Configure user rules

### Install the Federated Authentication Service

For security, Citrix recommends installing FAS on a dedicated server, similar to the Domain controller or Certificate Authority. FAS can be installed from the **Federated Authentication Service** button on the autorun splash screen when the ISO is inserted.

This process installs the following components:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Federated Authentication Service
- PowerShell snap-in cmdlets to remotely configure the Federated Authentication Service
- Federated Authentication Service administration console
- Federated Authentication Service Group Policy templates (CitrixFederatedAuthenticationService.admx/adml)
- Certificate template files for simple certificate authority configuration
- Performance counters and event logs

### Enable the Federated Authentication Service plug-in on a StoreFront store

To enable Federated Authentication Service integration on a StoreFront Store, run the following PowerShell cmdlets as an Administrator account. If you have more than one store, or if the store has a different name, the following path text might differ.

```
```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
<!--NeedCopy--> ```
```

To stop using the FAS, use the following PowerShell script:

```
```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
<!--NeedCopy--> ```
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Configure the Delivery Controller

To use FAS, configure the XenApp or XenDesktop Delivery Controller to trust the StoreFront servers that can connect to it: run the **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet.

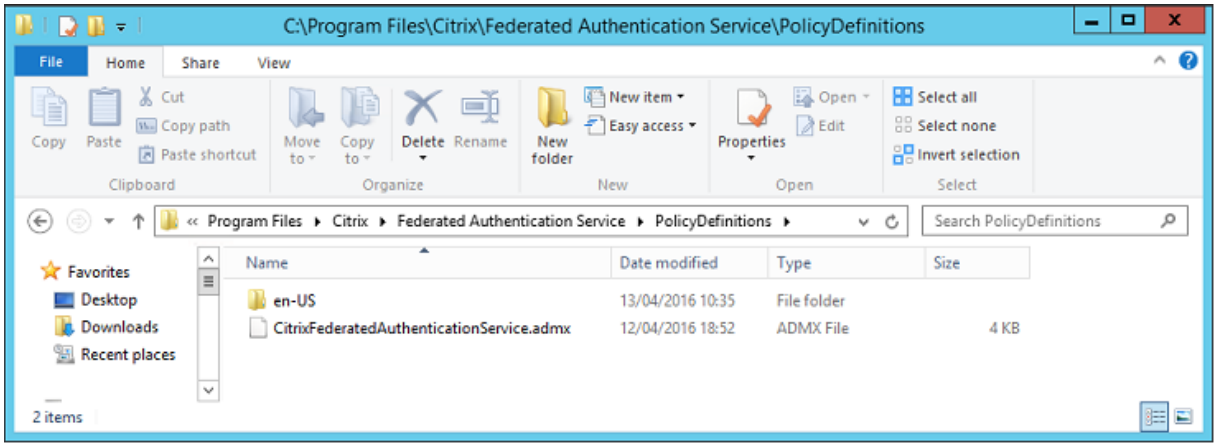
### Configure Group Policy

After you install FAS, specify the full DNS addresses of the FAS servers in the Group Policy using the Group Policy templates which are provided during the installation.

**Important:** Ensure that the StoreFront servers requesting tickets and the VDAs redeeming tickets have identical configuration of DNS addresses, including the automatic server numbering applied by the Group Policy object.

The following examples configure a single policy at the domain level that applies to all machines. However, FAS functions as long as the StoreFront servers, VDAs, and the machine running the FAS administration console see the same list of DNS addresses. The Group Policy object adds an index number to each entry, which must also match if more than one object is used.

**Step 1.** On the server where you installed the FAS, locate the C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx file and the en-US folder.



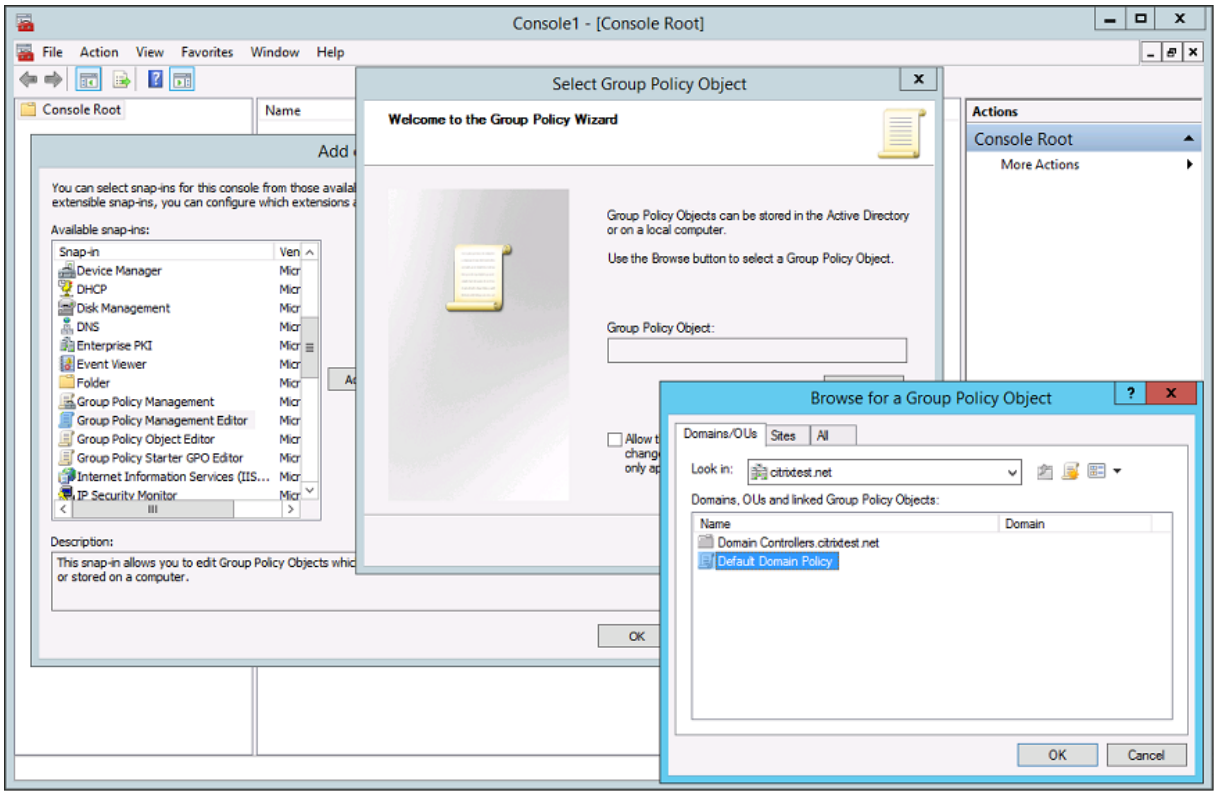

**Step 2.** Copy the files and the folder to your domain controller and place them in the C:\Windows\PolicyDefinitions and en-US subfolder.

**Step 3.** Run the Microsoft Management Console (mmc.exe from the command line). From the menu bar, select **File > Add/Remove Snap-in**. Add the **Group Policy Management Editor**.

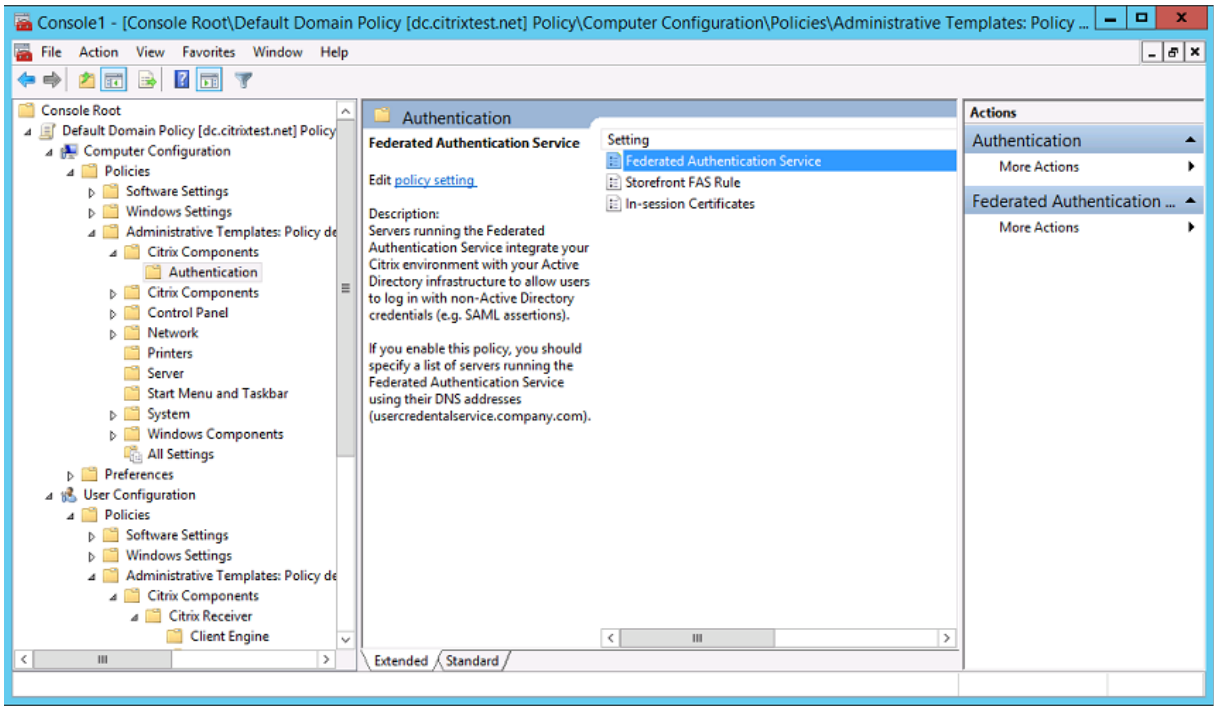
When prompted for a Group Policy Object, select **Browse** and then select **Default Domain Policy**. Also, you can create and select an appropriate policy object for your environment, using the tools

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

of your choice. The policy must be applied to all machines running affected Citrix software (VDAs, StoreFront servers, administration tools).

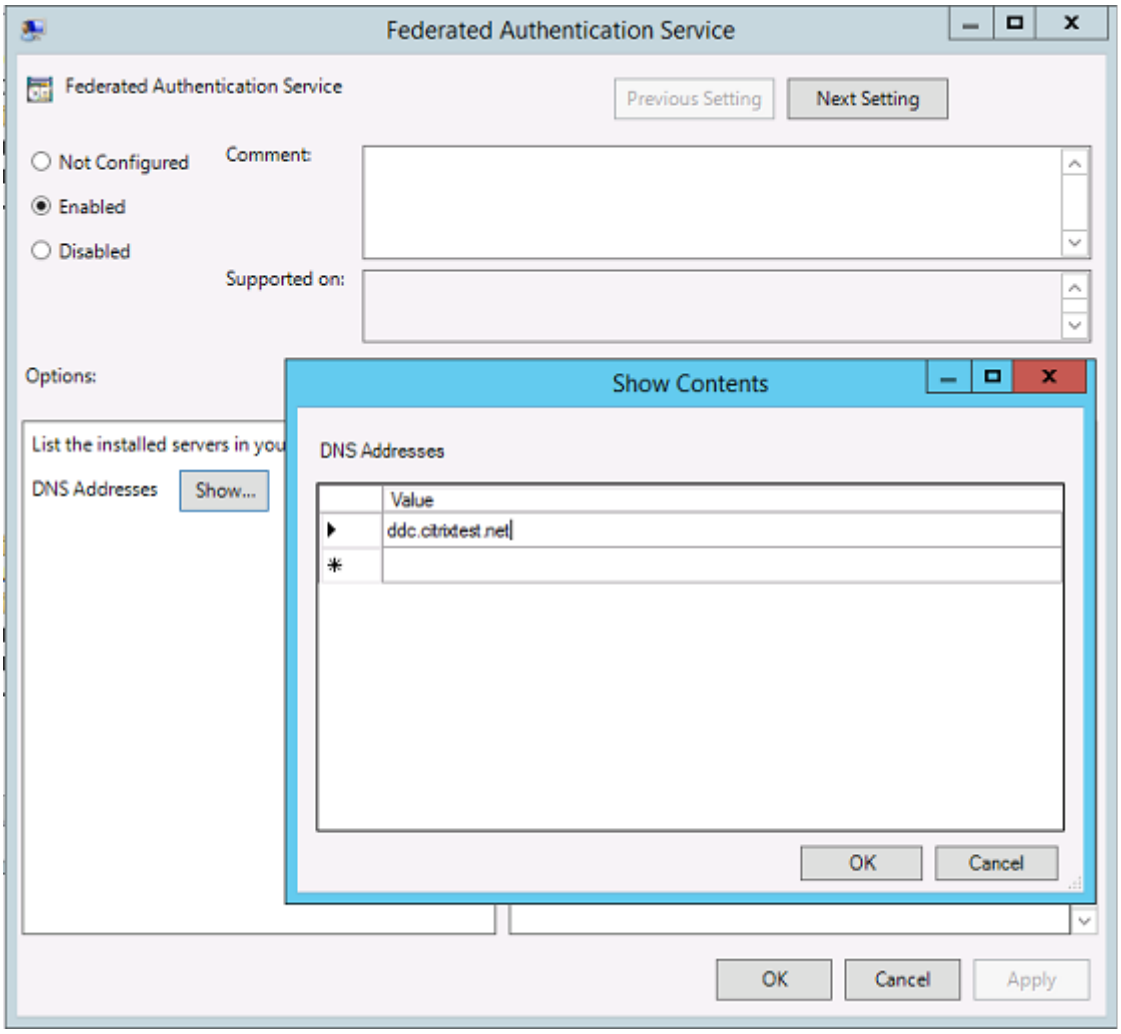



**Step 4.** Navigate to the Federated Authentication Service policy in Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentication.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 5.** Open the Federated Authentication Service policy and select **Enabled**. This option allows you to select the **Show** button, where you configure the DNS addresses of your FAS servers.



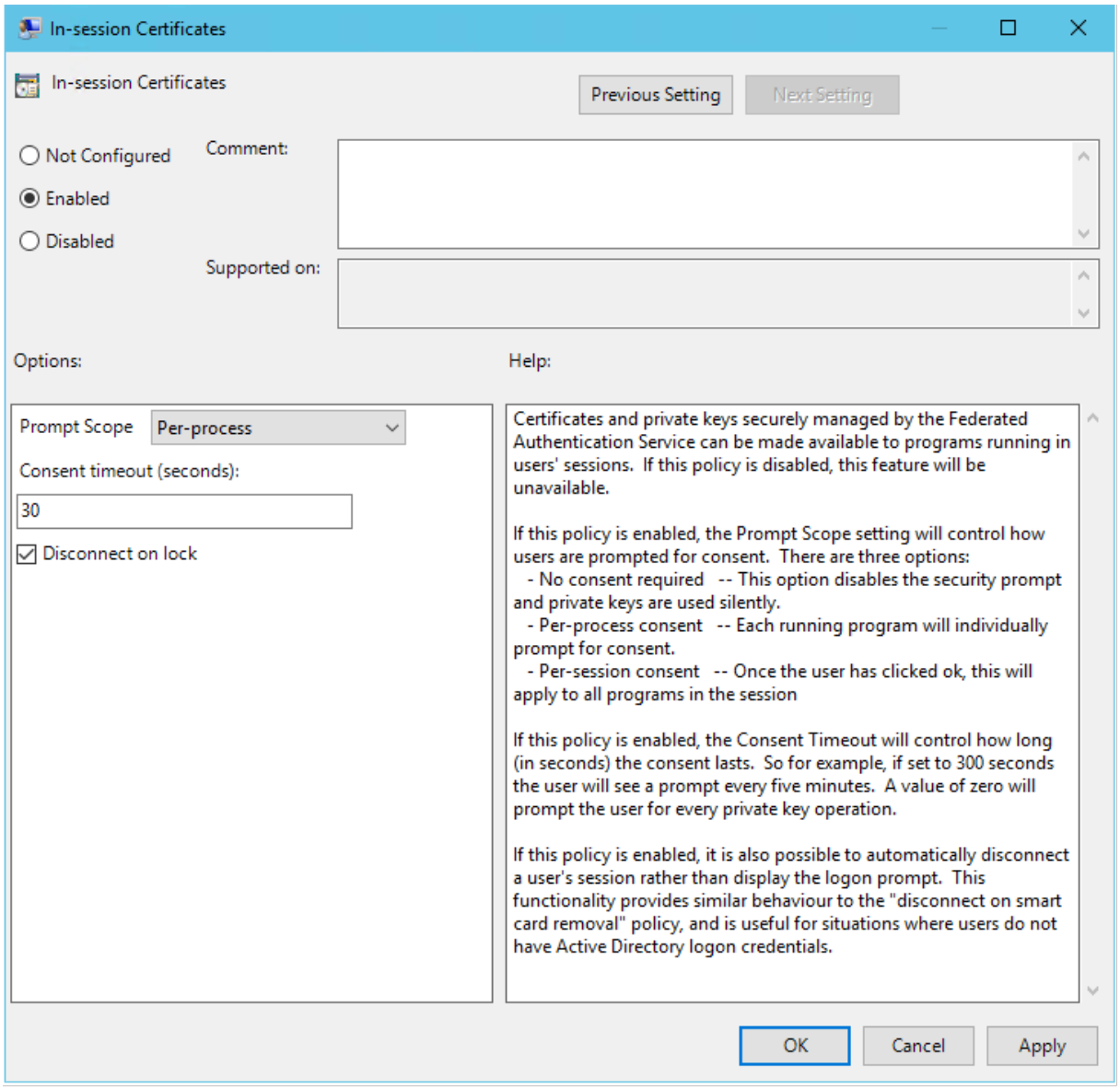

**Step 6.** Enter the DNS addresses of the servers hosting your Federated Authentication Service.

**Remember:** If you enter more than 1 address, the order of the list, including the blank or unused entries, must be consistent between StoreFront servers and VDAs.

**Step 7.** Click **OK** to exit the Group Policy wizard and apply the group policy changes. You might need to restart your machines (or run **gpupdate /force** from the command line) for the change to take effect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Enable in-session certificate support and disconnect on lock**




**In-session certificate support** The Group Policy template includes support for configuring the system for in-session certificates. This places certificates in the user's personal certificate store after logon for application use. For example, if you require TLS authentication to web servers within the VDA session, Internet Explorer can use the certificate. VDAs will not allow access to certificates after logon by default.

**Disconnect on lock** If this policy is enabled the user's session is automatically disconnected when they lock the screen. This behavior is similar to the "disconnect on smart card removal"policy, and is useful when users do not have Active Directory logon credentials.

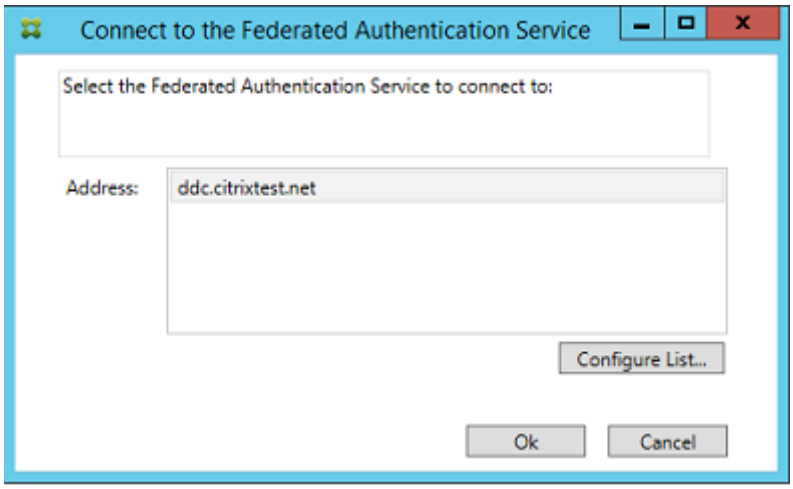
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Note:**
>
> The disconnect on lock policy applies to all sessions on the VDA.

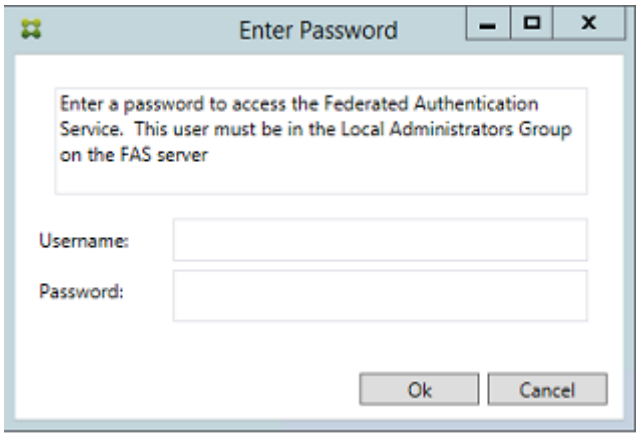
### Using the Federated Authentication Service administration console

The Federated Authentication Service administration console is installed as part of the Federated Authentication Service. An icon (Citrix Federated Authentication Service) is placed in the Start menu.

The console attempts to automatically locate the FAS servers in your environment using the Group Policy configuration. If this process fails, see the Configure Group Policy section.




If your user account is not a member of the Administrators group on the machine running the Federated Authentication Service, you're prompted for credentials.



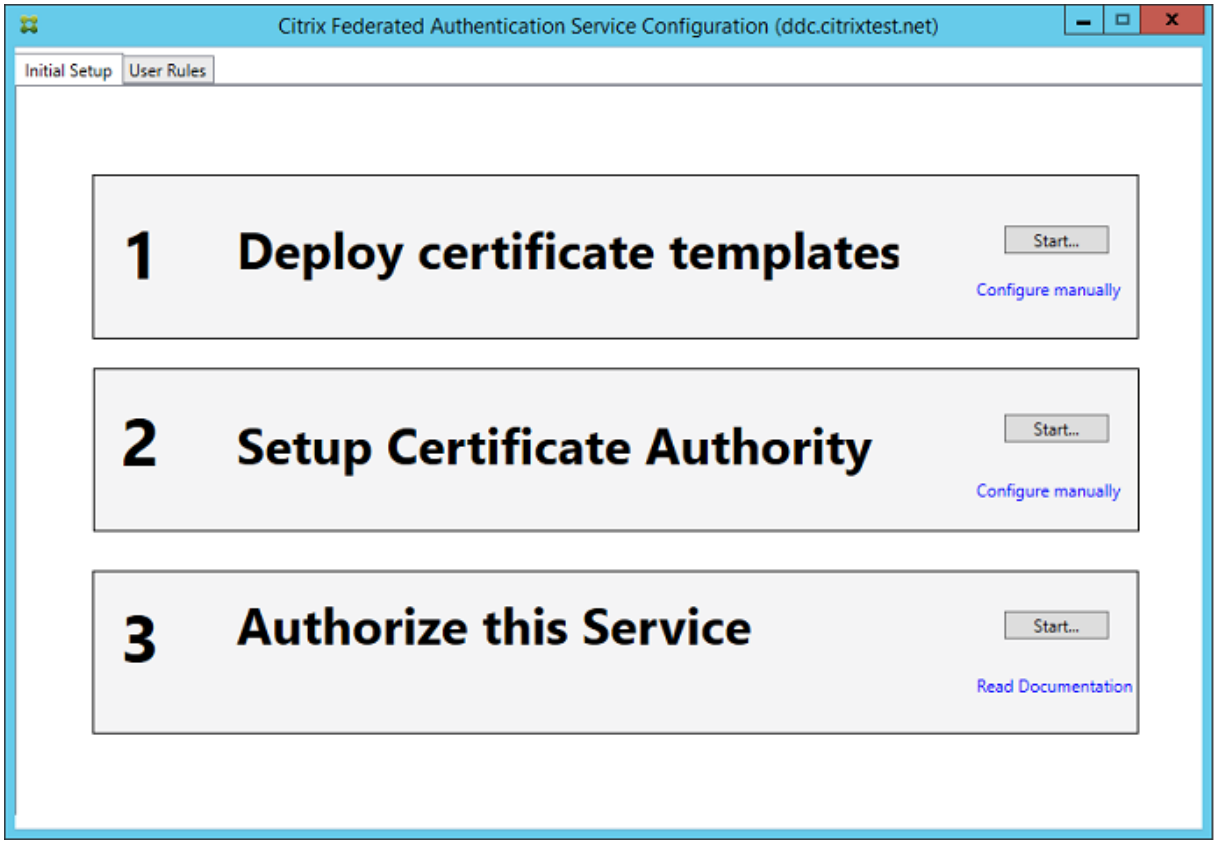

The first time you use the administration console, it guides you through a three-step process that does the following:

- Deploys certificate templates.
- Sets up the certificate authority.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Authorizes the Federated Authentication Service to use the certificate authority.

You can use the OS configuration tools to complete some of the steps manually.



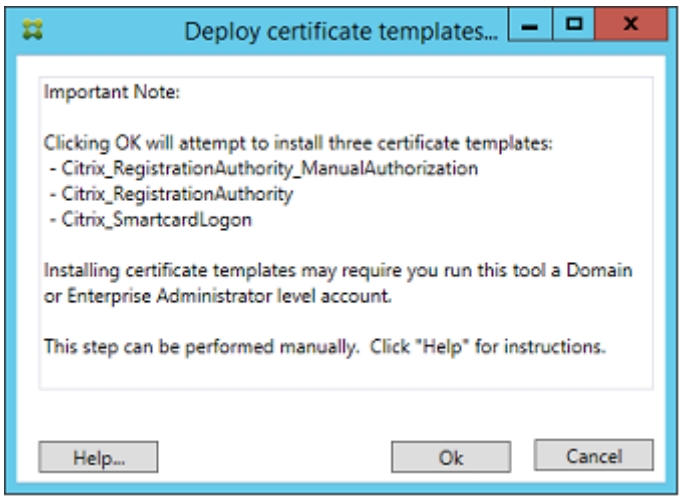

### Deploy certificate templates

To avoid interoperability issues with other software, the Federated Authentication Service provides three Citrix certificate templates for its own use.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

These templates must be registered with an Active Directory. If the console cannot locate them, the **Deploy certificate templates** tool can install them. This tool must be run as an account that has permissions to administer your Enterprise forest.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The configuration of the templates can be found in the XML files with extension .certificatetemplate that are installed with the Federated Authentication Service in:

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

If you do not have permission to install these template files, give them to your Active Directory Administrator.

To manually install the templates, you can use the following PowerShell commands:

```
```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")

 $CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService

 $CertEnrol.InitializeImport($template)

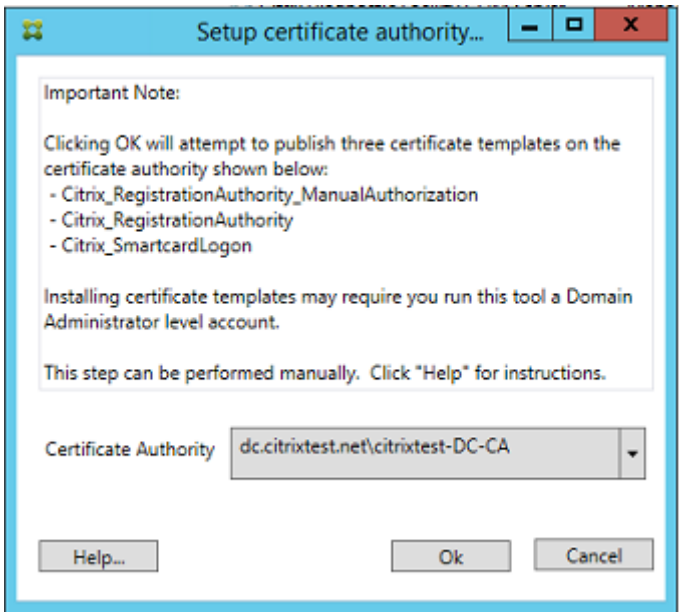
 $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable

 $writabletemplate.Initialize($comtemplate)

 $writabletemplate.Commit(1, $NULL)
 <!--NeedCopy--> ```
```

### Set up Active Directory Certificate Services

After you install the Citrix certificate templates, you must publish them on one or more certificate authority servers. Refer to the Microsoft documentation on how to deploy Active Directory Certificate Services.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 
```

If the templates are not published on at least one server, the **Setup certificate authority** tool offers to publish them. You must run this tool as a user that has permissions to administer the certificate authority.

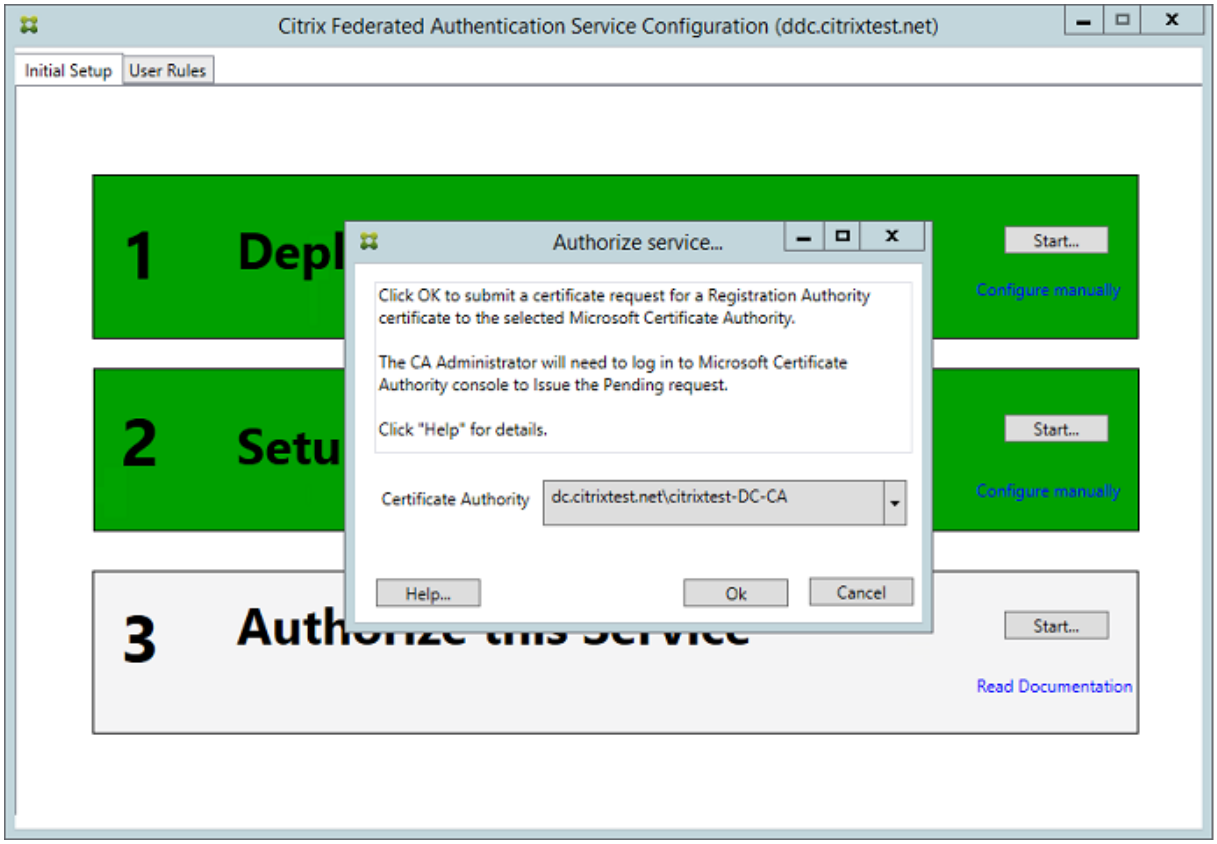
(Certificate templates can also be published using the Microsoft Certification Authority console.)



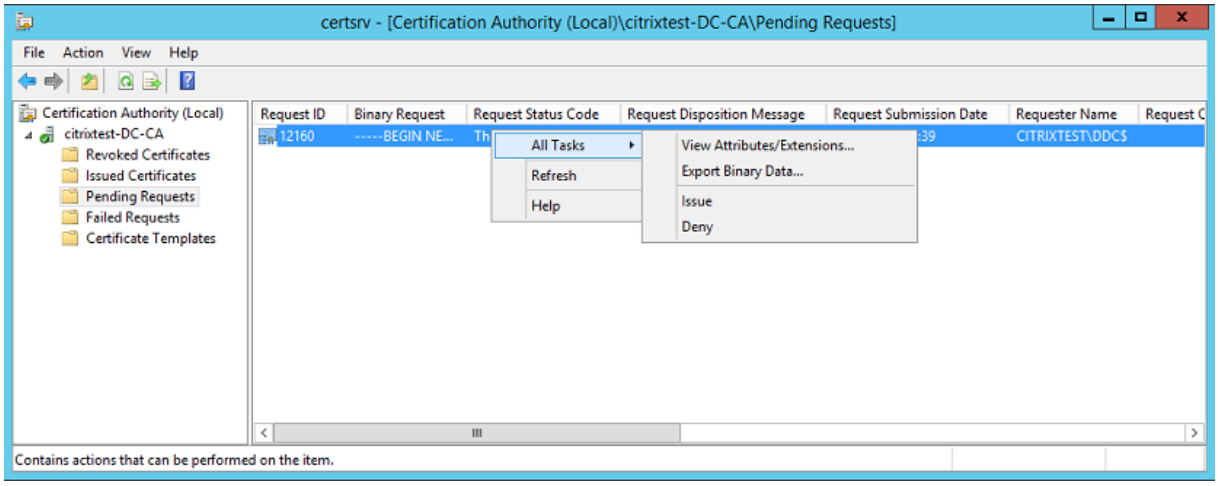

### Authorize the Federated Authentication Service

The final setup step in the console starts the authorization of the Federated Authentication Service. The administration console uses the Citrix_RegistrationAuthority_ManualAuthorization template to generate a certificate request. It then sends the request to one of the certificate authorities that publishes that template.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

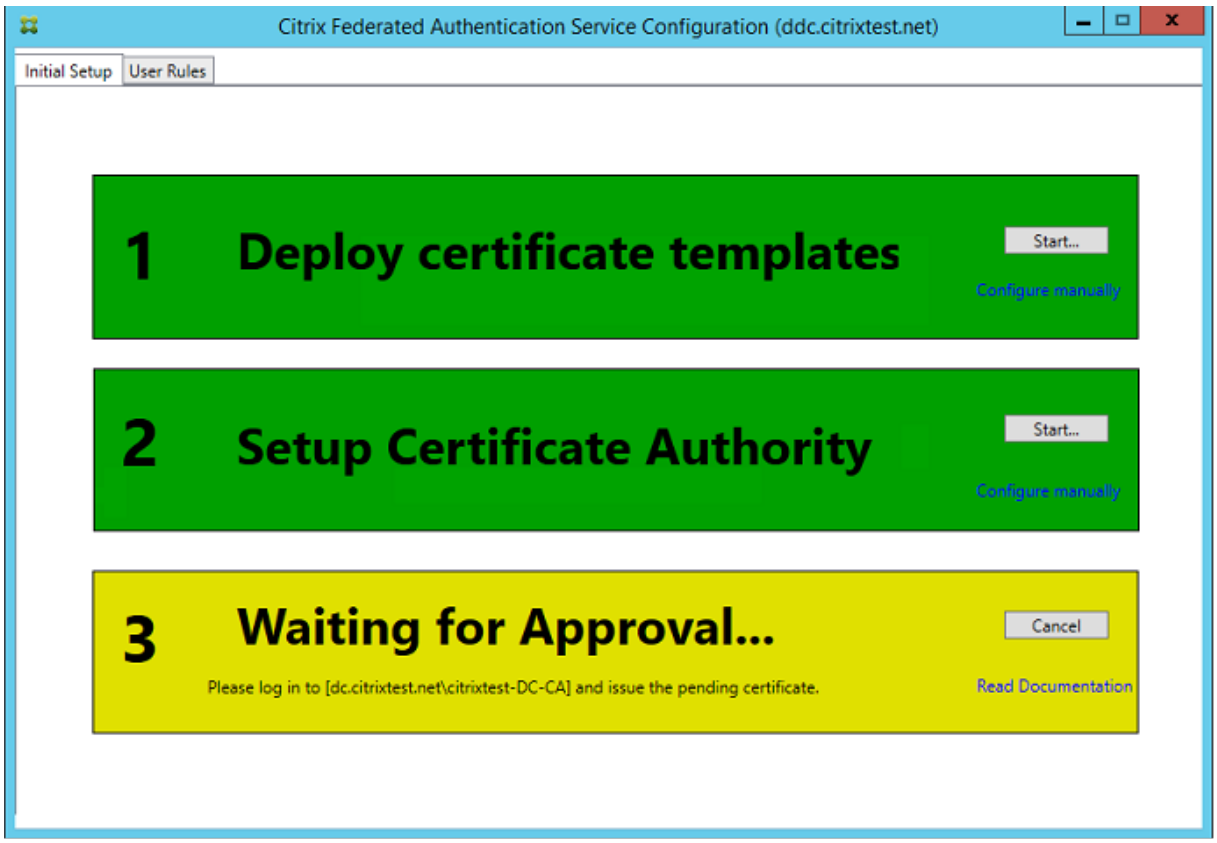



After the request is sent, you can see it in the **Pending Requests** list of the Microsoft Certification Authority console. The certificate authority administrator must choose to **Issue** or **Deny** the request before the configuration of the Federated Authentication Service can continue. The authorization request appears as a **Pending Request** from the FAS machine account.




Right-click **All Tasks** and then select **Issue** or **Deny** for the certificate request. The Federated Authentication Service administration console automatically detects when this process completes. This step can take a couple of minutes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



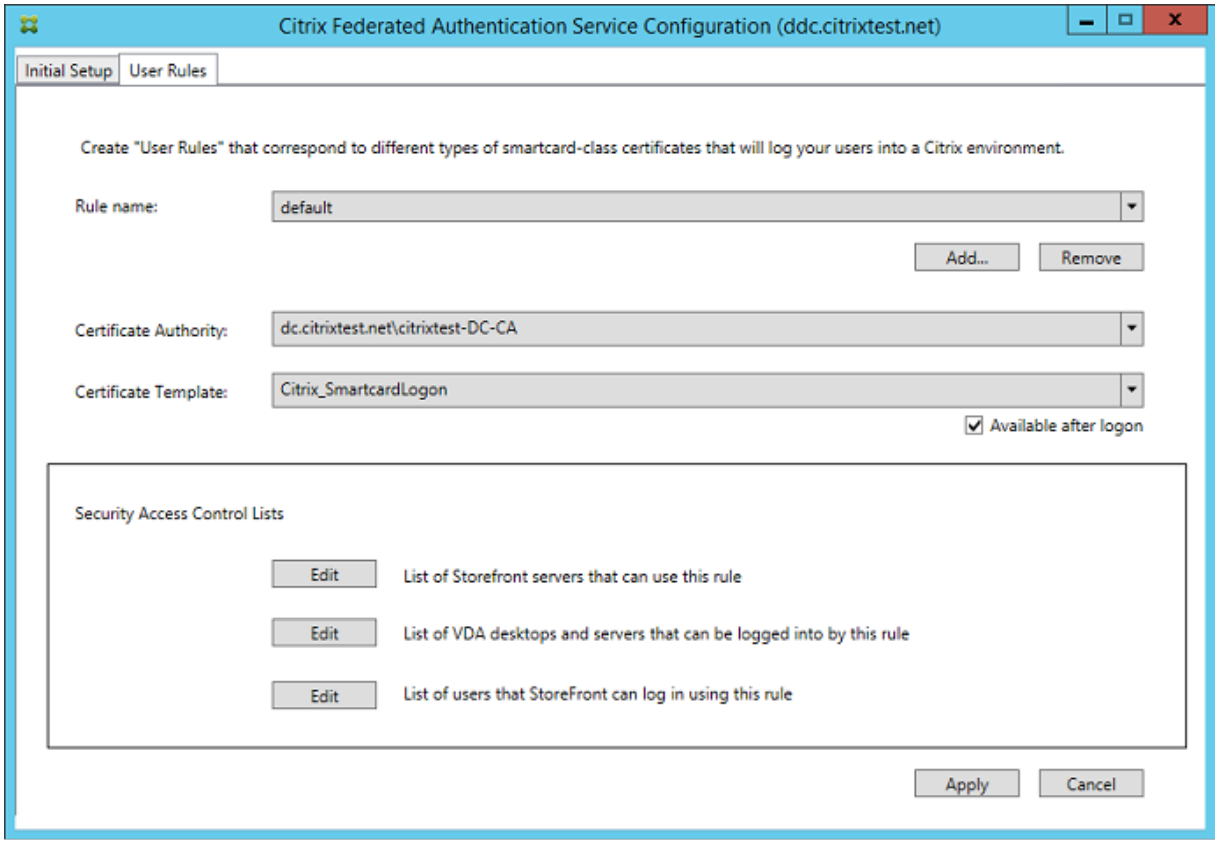

### Configure user rules

A user rule authorizes the issuance of certificates for VDA logon and in-session use, as directed by StoreFront. Each rule specifies the following:

- StoreFront servers that are trusted to request certificates.
- Set of users for whom you can request the certificates.
- Set of VDA machines allowed to use the certificates.

The administrator must define the default rule to complete the setup of the Federated Authentication Service.
To define the default rule, go to the **User Rules** tab of the FAS administration console, select a certificate authority to which the Citrix_SmartcardLogon template is published, and edit the list of StoreFront servers. The list of VDAs defaults to Domain Computers and the list of users defaults to Domain Users; these can be changed if the defaults are inappropriate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Fields:

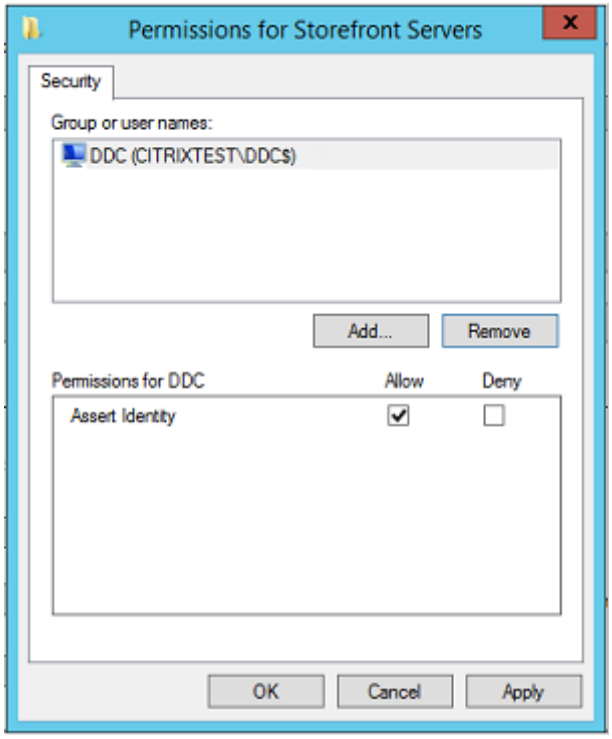
**Certificate Authority and Certificate Template**: The certificate template and certificate authority that is used to issue user certificates. The template must be the Citrix_SmartcardLogon template, or a modified copy of it, on one of the certificate authorities that the template is published to.

The FAS supports adding multiple certificate authorities for failover and load balancing, using PowerShell commands. Similarly, more advanced certificate generation options can be configured using the command line and configuration files. See the PowerShell and Hardware security modules sections.

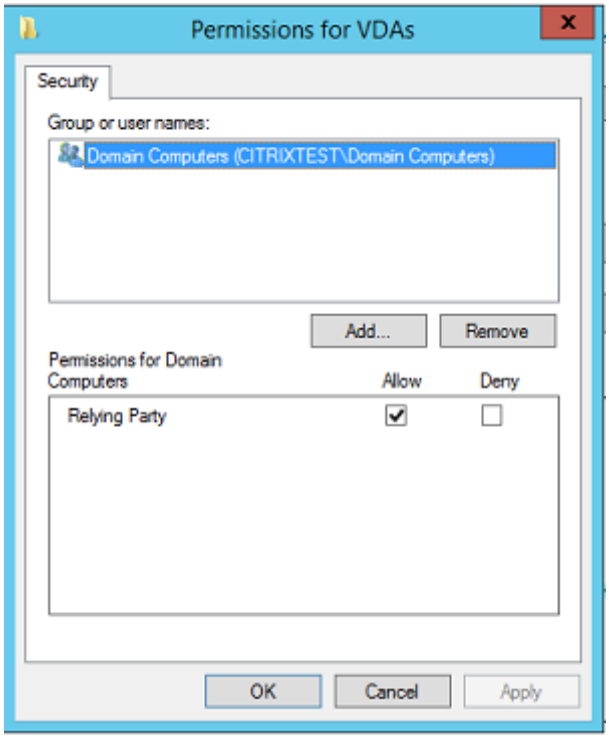
**In-Session Certificates**: The **Available after logon** checkbox controls whether a certificate can also be used as an in-session certificate. If the checkbox is not selected, the certificate is used only for logon or reconnection, and the user will not have access to the certificate after authenticating.

**List of StoreFront servers that can use this rule**: The list of trusted StoreFront server machines that are authorized to request certificates for logon or reconnection of users. This setting is security critical, and must be managed carefully.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

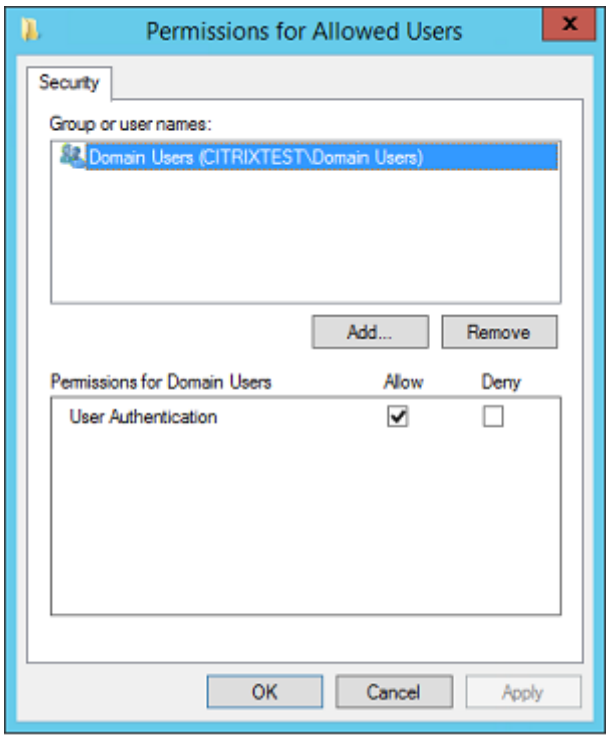



**List of VDA desktops and servers that can be logged into by this rule:** The list of VDA machines that can log users on using the Federated Authentication Service system.




**List of users that StoreFront can log in using this rule:** The list of users who can be issued certificates through the Federated Authentication Service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




#### Advanced use

You can create more rules to reference different certificate templates and authorities, and configure them to have different properties and permissions. You can configure these rules for use by different StoreFront servers. Configure the StoreFront servers to request the custom rule by name using the Group Policy Configuration options.

By default, StoreFront requests **default** when contacting the Federated Authentication Service. This can be changed using the Group Policy Configuration options.

To create a certificate template, duplicate the Citrix_SmartcardLogon template in the Microsoft Certification Authority console, rename it (for example, Citrix_SmartcardLogon2), and modify it as required. Create a user rule by clicking **Add** to reference the new certificate template.

### Upgrade considerations

- All Federated Authentication Service server settings are preserved when you perform an in-place upgrade.
- Upgrade the Federated Authentication Service by running the full-product XenApp and XenDesktop installer.
- Before upgrading the Federated Authentication Service from 7.15 LTSR to 7.15 LTSR CU2 (or a

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

later supported CU), upgrade the Controller and VDAs (and other core components) to the required version.

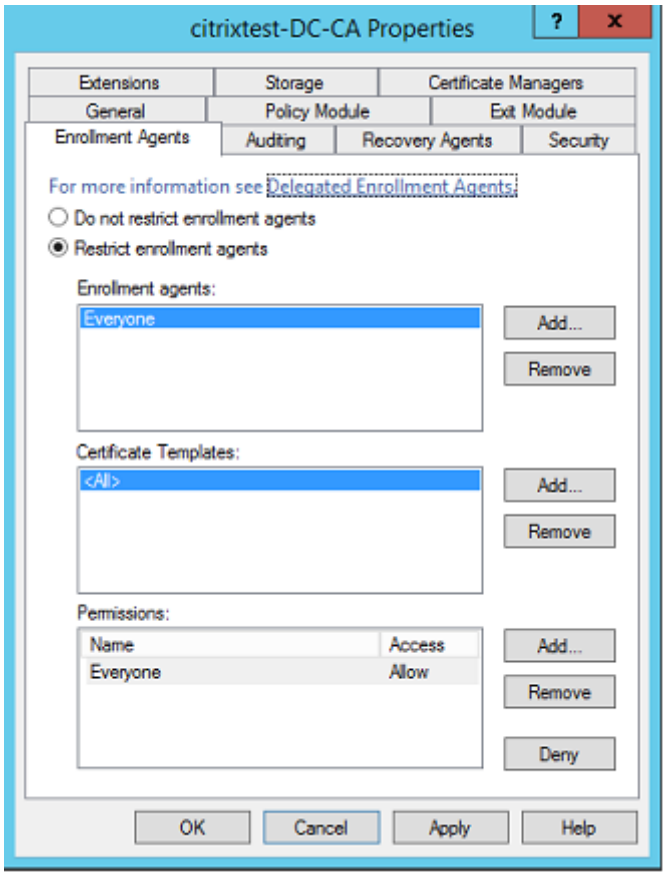
- Ensure that the Federated Authentication Service console is closed before you upgrade the Federated Authentication Service.
- Ensure that at least one Federated Authentication Service server is available always. If no server is reachable by a Federation Authentication Service-enabled StoreFront server, users cannot log on or start applications.

## Security considerations

The Federated Authentication Service has a registration authority certificate that allows it to issue certificates autonomously for your domain users. It is important to develop and implement a security policy to protect the FAS servers, and to constrain their permissions.

### Delegated Enrollment Agents

FAS issues user certificates by acting as an enrollment agent. The Microsoft Certification Authority controls the templates which the FAS server can use. It also determines the users, the FAS server can issue certificates for.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Citrix strongly recommends configuring these options so that the Federated Authentication Service can only issue certificates for the intended users. For example, it is a good practice to prevent the Federated Authentication Service from issuing certificates to users in an Administration or Protected Users group.

#### Access Control List configuration

As described in the Configure user rules section, you must configure a list of StoreFront servers that are trusted to assert user identities to the Federated Authentication Service when certificates are issued. Similarly, you can restrict which users are issued certificates, and which VDA machines they can authenticate to. This step is in addition to any standard Active Directory or certificate authority security features you configure.

#### Firewall settings

All communication to FAS servers uses mutually authenticated Windows Communication Foundation (WCF) Kerberos network connections over port 80.

#### Event log monitoring

The Federated Authentication Service and the VDA write information to the Windows Event Log. This log can be used for monitoring and auditing information. The Event logs section lists event log entries that might be generated.

#### Hardware security modules

All private keys, including user certificates keys issued by the Federated Authentication Service, are stored as non-exportable private keys by the Network Service account. The Federated Authentication Service supports the use of a cryptographic hardware security module, if your security policy requires it.

Low-level cryptographic configuration is available in the FederatedAuthenticationService.exe.config file. These settings apply when private keys are first created. Therefore, different settings can be used for registration authority private keys (for example, 4096 bit, TPM protected) and runtime user certificates.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
|---|---|
| ProviderLegacyCsp | When set to true, FAS uses the Microsoft CryptoAPI (CAPI). Otherwise, FAS uses the Microsoft Cryptography Next Generation API (CNG). |
| ProviderName | Name of the CAPI or CNG provider to use. |
| ProviderType | Refers to Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Must always be 24 unless you are using an HSM with CAPI and the HSM vendor specifies otherwise. |
| KeyProtection | Controls the "Exportable"flag of private keys. Also allows the use of Trusted Platform Module (TPM) key storage, if supported by the hardware. |
| KeyLength | Key length for RSA private keys. Supported values are 1024, 2048 and 4096 (default: 2048). |

### PowerShell SDK

Although the Federated Authentication Service administration console is suitable for simple deployments, the PowerShell interface offers more advanced options. When you are using options that are not available in the console, Citrix recommends using only PowerShell for configuration.

The following command adds the PowerShell cmdlets:

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Use **Get-Help** <*cmdlet name*> to display cmdlet help. The following table lists several commands where * represents a standard PowerShell verb (such as New, Get, Set, Remove).

| Commands | Overview |
|---|---|
| *-FasServer | Lists and reconfigures the FAS servers in the current environment. |
| *-FasAuthorizationCertificate | Manages the Registration Authority certificate. |
| *-FasCertificateDefinition | Controls the parameters that the FAS uses to generate certificates. |
| *-FasRule | Manages User Rules configured on the Federated Authentication Service. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

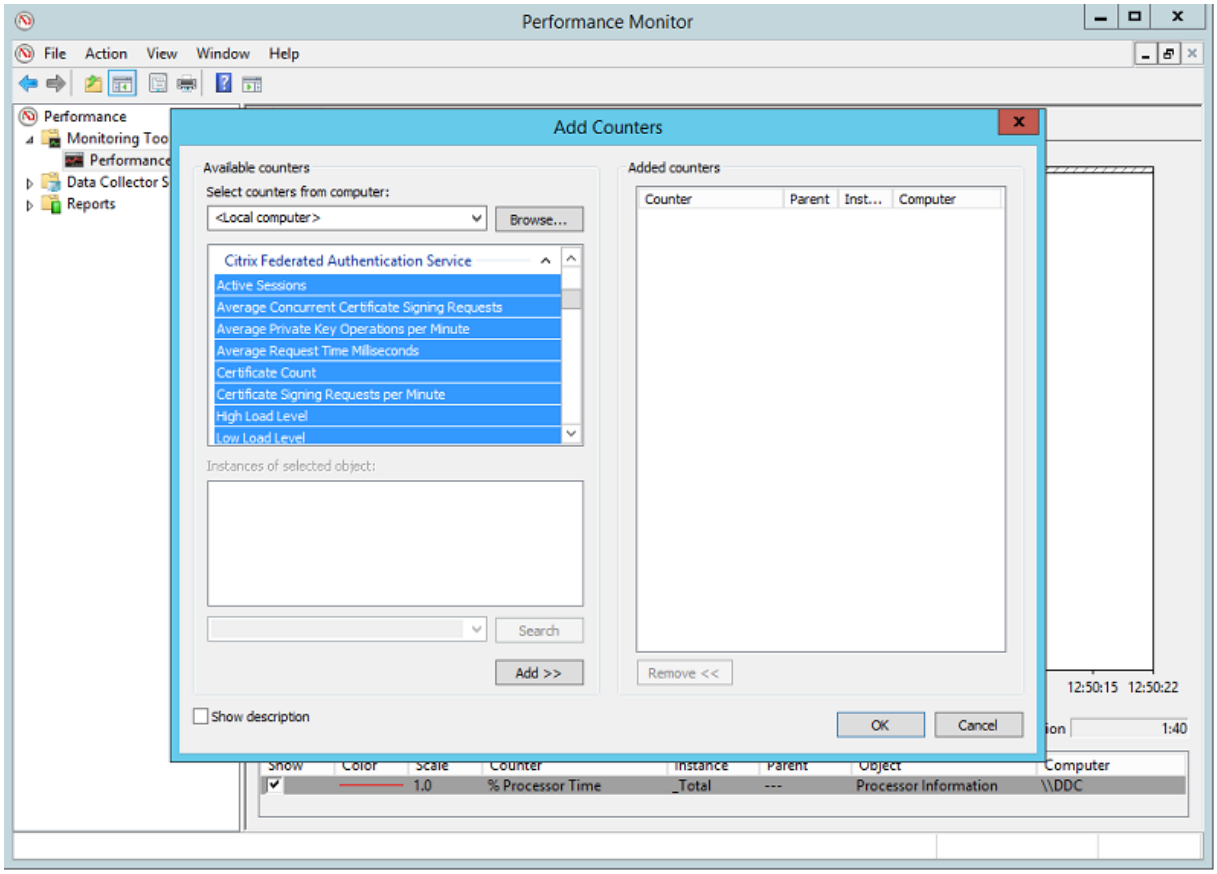
| Commands | Overview |
| --- | --- |
| *-FasUserCertificate | Lists and manages certificates cached by the Federated Authentication Service. |

PowerShell cmdlets can be used remotely by specifying the address of a FAS server.

You can also download a zip file having all the FAS PowerShell cmdlet help files; see the PowerShell SDK article.

### Performance counters

The Federated Authentication Service includes a set of performance counters for load tracking purposes.




The following table lists the available counters. Most counters are rolling averages over five minutes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Description |
| --- | --- |
| Active Sessions | Number of connections tracked by the Federated Authentication Service. |
| Concurrent CSRs | Number of certificate requests processed at the same time. |
| Private Key ops | Number of private key operations performed per minute. |
| Request time | Length of time to generate and sign a certificate. |
| Certificate Count | Number of certificates cached in the Federated Authentication Service. |
| CSR per minute | Number of CSRs processed per minute. |
| Low/Medium/High | Estimates of the load that the Federated Authentication Service can accept in terms of "CSRs per minute". Exceeding the "High Load" threshold might result in session launches failing. |

## Event logs

The following tables list the event log entries generated by the Federated Authentication Service.

### Administration events

[Event Source: Citrix.Authentication.FederatedAuthenticationService]

FAS logs these events in response to the configuration changes on the FAS server.

| Log Codes |
| --- |
| [S001] ACCESS DENIED: User [{0}] is not a member of Administrators group |
| [S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}] |
| [S003] Administrator [{0}] setting Maintenance Mode to [{1}] |
| [S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}] |
| [S005] Administrator [{0}] de-authorizing CA [{1}] |
| [S006] Administrator [{0}] creating new Certificate Definition [{1}] |
| [S007] Administrator [{0}] updating Certificate Definition [{1}] |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Log Codes |
| --- |
| [S008] Administrator [{0}] deleting Certificate Definition [{1}] |
| [S009] Administrator [{0}] creating new Role [{1}] |
| [S010] Administrator [{0}] updating Role [{1}] |
| [S011] Administrator [{0}] deleting Role [{1}] |
| [S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}] |
| [S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}] |

| Log Codes |
| --- |
| [S401] Performing configuration upgrade –[From version {0}][to version {1}] |
| [S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}] |

**Creating identity assertions [Federated Authentication Service]**

These events are logged at runtime on the Federated Authentication Service server when a trusted server asserts a user logon.

| Log Codes |
| --- |
| [S101] Server [{0}] is not authorized to assert identities in role [{1}] |
| [S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3}) |
| [S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3} |
| [S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}]) |
| [S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}] |
| [S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]] |
| [S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2} |
| [S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}]. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Acting as a relying party [Federated Authentication Service]

These events are logged at runtime on the Federated Authentication Service server when a VDA logs on a user.

| Log Codes |
| --- |
| [S201] Relying party [{0}] does not have access to a password. |
| [S202] Relying party [{0}] does not have access to a certificate. |
| [S203] Relying party [{0}] does not have access to the Logon CSP |
| [S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}] |
| [S205] Calling account [{0}] is not a relying party in role [{1}] |
| [S206] Calling account [{0}] is not a relying party |
| [S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}] |
| [S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}]. |

### In-session certificate server [Federated Authentication Service]

These events are logged on the Federated Authentication Service server when a user uses an in-session certificate.

| Log Codes |
| --- |
| [S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card |
| [S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}] |
| [S303] User [{0}] does not match Virtual Smart Card [upn: {1}] |
| [S304] User [{1}] running program [{2}] on computer [{3}] using Virtual Smart Card [upn: {4} role: {5}] for private key operation: [{6}] |
| [S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}]. |

### Log on [VDA]

[Event Source: Citrix.Authentication.IdentityAssertion]

These events are logged on the VDA during the logon stage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Log Codes |
| --- |
| [S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}] |
| [S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}] |
| [S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2} |
| [S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}] |
| [S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}] |
| [S106] Identity Assertion Logon. Logging in [Certificate: {0}] |
| [S107] Identity Assertion Logon failed. [Exception: {1}{2}] |
| [S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}] |

**In-session certificates [VDA]**

These events are logged on the VDA when a user attempts to use an in-session certificate.

| Log Codes |
| --- |
| [S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}] |
| [S202] Virtual Smart Card Subsystem. No smart cards available in session {0} |
| [S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}] |
| [S204] Virtual Smart Card Subsystem. Smart card support disabled. |

**Certificate request and generation codes [Federated Authentication Service]**

[Event Source: Citrix.TrustFabric]

These low-level events are logged when the Federated Authentication Service server performs log-level cryptographic operations.

| Log Codes |
| --- |
| [S0001]TrustArea::TrustArea: Installed certificate chain |
| [S0002]TrustArea::Join: Callback has authorized an untrusted certificate |
| [S0003]TrustArea::Join: Joining to a trusted server |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Log Codes

[S0004]TrustArea::Maintain: Renewed certificate

[S0005]TrustArea::Maintain: Retrieved new certificate chain

[S0006]TrustArea::Export: Exporting private key

[S0007]TrustArea::Import: Importing Trust Area

[S0008]TrustArea::Leave: Leaving Trust Area

[S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor

[S0010]CertificateVerification: Installing new trusted certificate

[S0011]CertificateVerification: Uninstalling expired trusted certificate

[S0012]TrustFabricHttpClient: Attempting single sign-on to {0}

[S0013]TrustFabricHttpClient: Explicit credentials entered for {0}

[S0014]Pkcs10Request::Create: Created PKCS10 request

[S0015]Pkcs10Request::Renew: Created PKCS10 request

[S0016]PrivateKey::Create

[S0017]PrivateKey::Delete

[S0018]TrustArea::TrustArea: Waiting for Approval

[S0019]TrustArea::Join: Delayed Join

[S0020]TrustArea::Join: Delayed Join

[S0021]TrustArea::Maintain: Installed certificate chain

Log Codes

[S0101]TrustAreaServer::Create root certificate

[S0102]TrustAreaServer::Subordinate: Join succeeded

[S0103]TrustAreaServer::PeerJoin: Join succeeded

[S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}

[S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0}

[S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0}

[S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL

[S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0}

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Log Codes |
| --- |
| [S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0} |
| [S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval |
| [S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused |
| [S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate |
| [S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval |
| [S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0} |
| [S0121]NativeCertificateAuthority::SubmitCertificateRequest Error |
| [S0122]NativeCertificateAuthority::RootCARollover New root certificate |
| [S0123]NativeCertificateAuthority::ReissueCertificate New certificate |
| [S0124]NativeCertificateAuthority::RevokeCertificate |
| [S0125]NativeCertificateAuthority::PublishCRL |

### Related information

- The common FAS deployments are summarized in the Federated Authentication Service architectures overview article.
- "How-to"articles are introduced in the Federated Authentication Service configuration and management article.

## Federated Authentication Service architectures overview

October 26, 2022

### Introduction

The Federated Authentication Service (FAS) is a Citrix component that integrates with your Active Directory certificate authority (CA), allowing users to be seamlessly authenticated within a Citrix environment. This document describes the various authentication architectures that are appropriate for your deployment.

When enabled, the FAS delegates user authentication decisions to trusted StoreFront servers. StoreFront has a comprehensive set of built-in authentication options built around modern web technolo-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

gies, and is easily extensible using the StoreFront SDK or third-party IIS plug-ins. The basic design goal is that any authentication technology that can authenticate a user to a website can now be used to log in to a Citrix XenApp or XenDesktop deployment.

This document covers some example top-level deployment architectures, in increasing complexity.

- Internal deployment
- NetScaler Gateway deployment
- ADFS SAML
- B2B account mapping
- Windows 10 Azure AD join

Links are provided to related FAS articles. For all architectures, the Federated Authentication Service article is the primary reference for setting up the FAS.

### How it works

The FAS is authorized to issue smart card class certificates automatically on behalf of Active Directory users authenticated by StoreFront. This uses similar APIs to tools that allow administrators to provision physical smart cards.

When a user is brokered to a Citrix XenApp or XenDesktop Virtual Delivery Agent (VDA), the certificate is attached to the machine, and the Windows domain sees the logon as a standard smart card authentication.

### Internal deployment

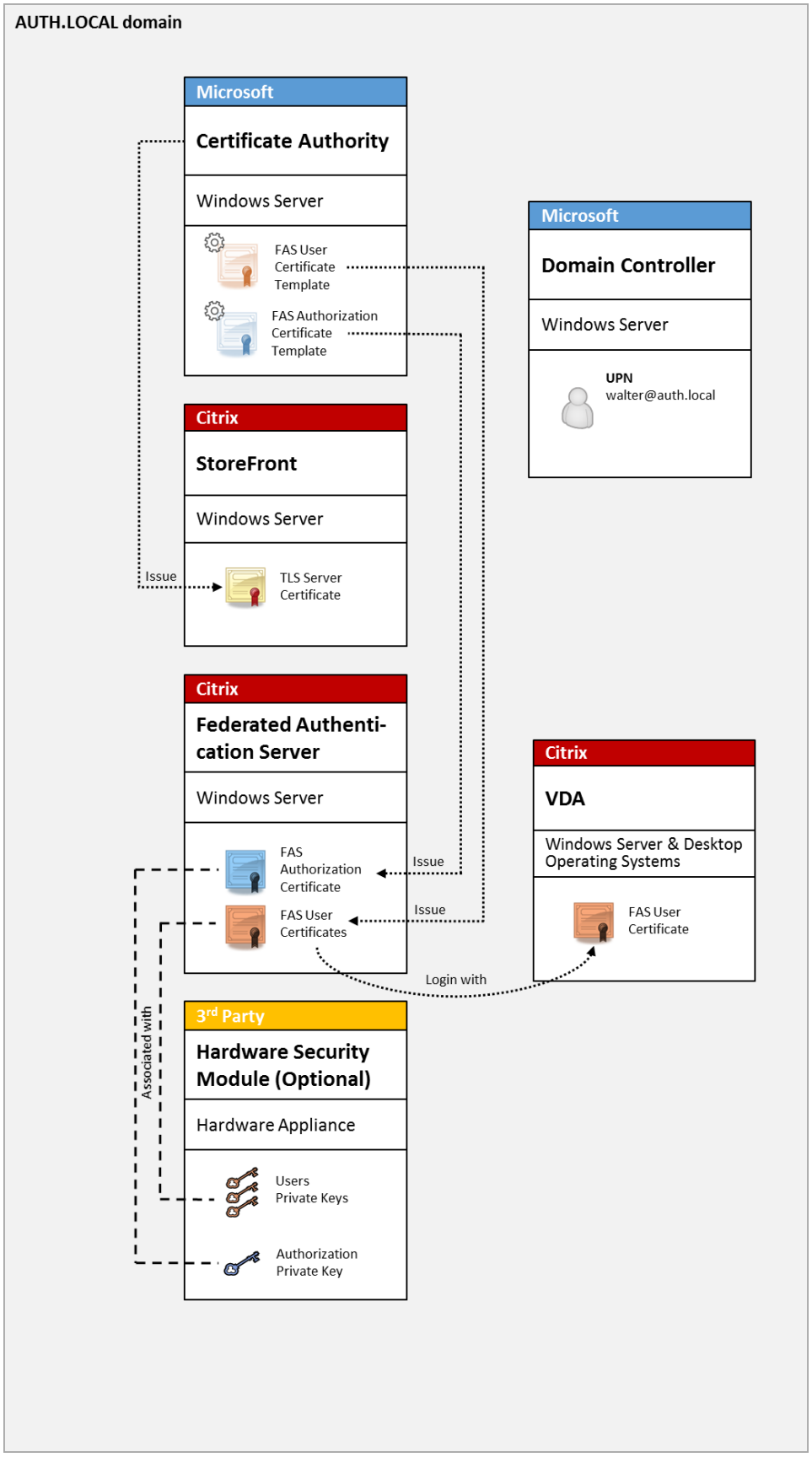
The FAS allows users to securely authenticate to StoreFront using various authentication options, including Kerberos single sign-on (SSO), and connect through to a fully authenticated Citrix HDX session.

This allows Windows authentication without prompts to enter user credentials or smart card PINs, and without using "saved password management"features such as the SSO service. This can be used to replace the Kerberos Constrained Delegation logon features available in earlier versions of XenApp.

All users have access to public key infrastructure (PKI) certificates within their session, regardless of whether they log on to the endpoint devices with a smart card. This allows a smooth migration to two-factor authentication models, even from devices such as smartphones and tablets that do not have a smart card reader.

This deployment adds a server running the FAS, which is authorized to issue smart card class certificates on behalf of users. These certificates are then used to log on to user sessions in a Citrix HDX environment as if a smart card logon was used.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The XenApp or XenDesktop environment must be configured in a similar manner as the smart card logon, which is documented in CTX206156.

In an existing deployment, this usually involves only ensuring that a domain-joined Microsoft certificate authority (CA) is available, and that domain controllers have been assigned domain controller certificates. (See the "Issuing Domain Controller Certificates"section in CTX206156.)

Related information:

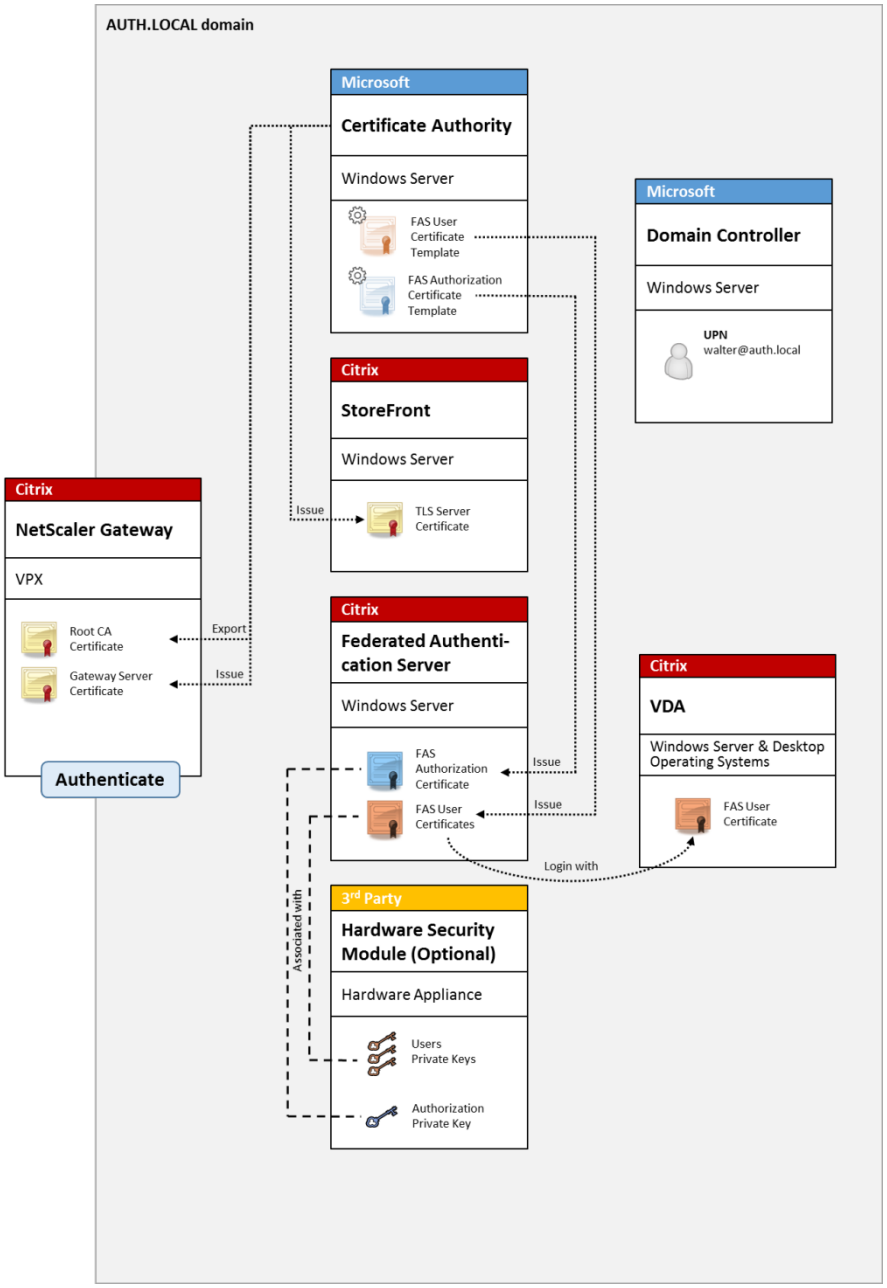
- Keys can be stored in a Hardware Security Module (HSM) or built-in Trusted Platform Module (TPM). For details, see the Federated Authentication Service private key protection article.
- The Federated Authentication Service article describes how to install and configure the FAS.

### NetScaler Gateway deployment

The NetScaler deployment is similar to the internal deployment, but adds Citrix NetScaler Gateway paired with StoreFront, moving the primary point of authentication to NetScaler itself. Citrix NetScaler includes sophisticated authentication and authorization options that can be used to secure remote access to a company's websites.

This deployment can be used to avoid multiple PIN prompts that occur when authenticating first to NetScaler and then logging in to a user session. It also allows the use of advanced NetScaler authentication technologies without requiring AD passwords or smart cards.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




> **Note:**
>
> There are no differences if the back end resource is either Windows VDA or Linux VDA.

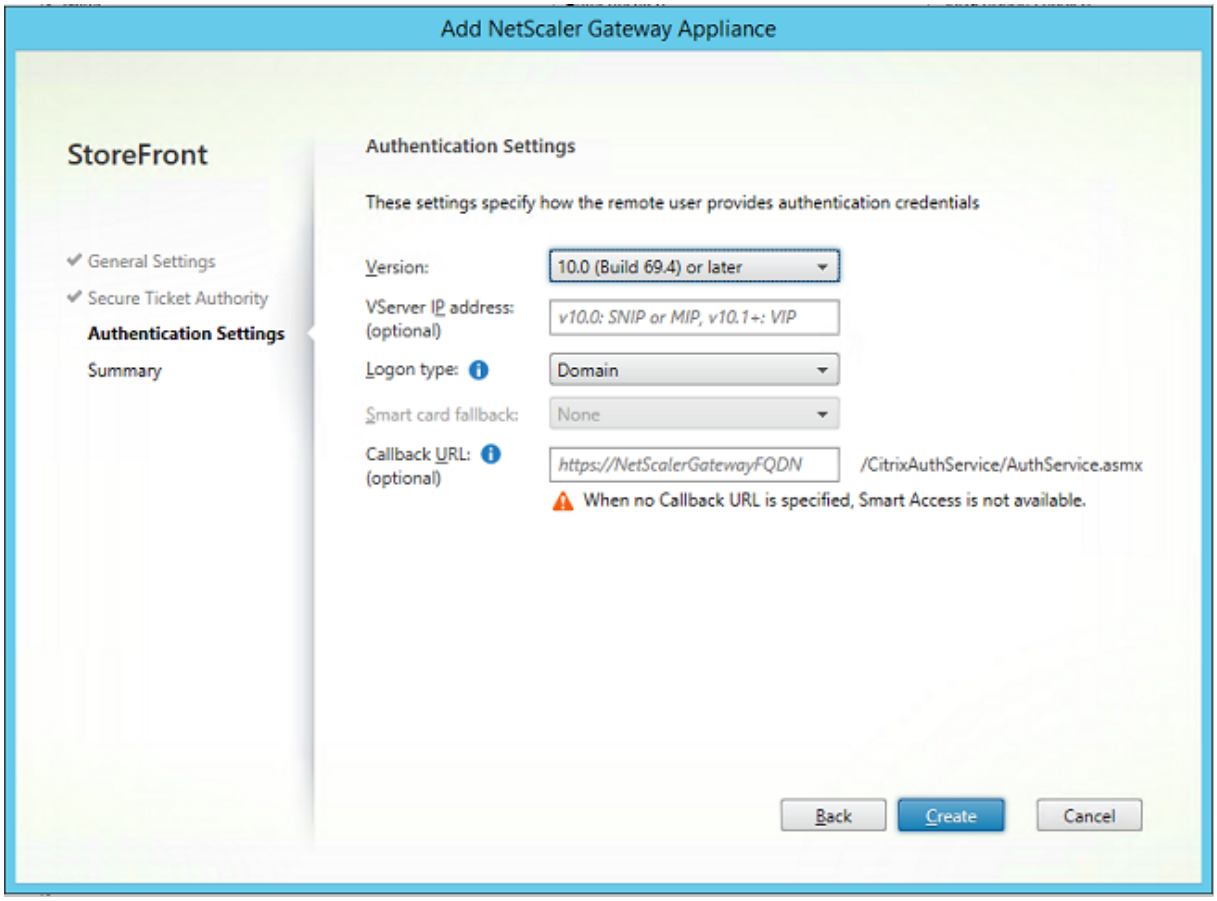
The XenApp or XenDesktop environment must be configured in a similar manner as the smart card logon, which is documented in CTX206156.

In an existing deployment, this usually involves only ensuring that a domain-joined Microsoft certificate authority (CA) is available, and that domain controllers have been assigned Domain Controller certificates. (See the "Issuing Domain Controller Certificates"section in CTX206156).

When configuring NetScaler as the primary authentication system, ensure that all connections be-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tween NetScaler and StoreFront are secured with TLS. In particular, ensure that the Callback Url is correctly configured to point to the NetScaler server, as this can be used to authenticate the NetScaler server in this deployment.



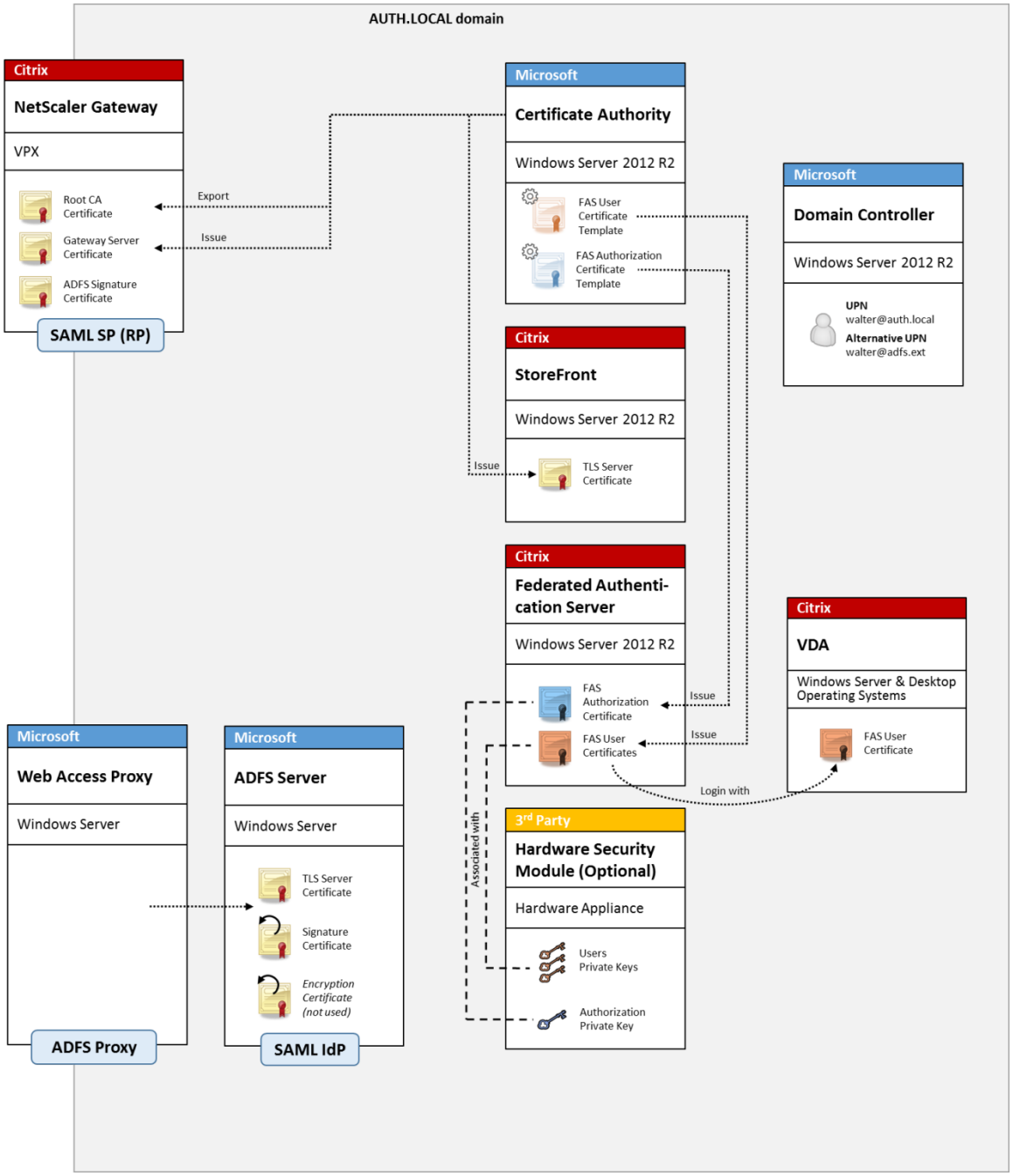

Related information:

- To configure NetScaler Gateway, see How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and XenDesktop 7.6.
- The Federated Authentication Service article describes how to install and configure the FAS.

### ADFS SAML deployment

A key NetScaler authentication technology allows integration with Microsoft ADFS, which can act as a SAML Identity Provider (IdP). A SAML assertion is a cryptographically signed XML block issued by a trusted IdP that authorizes a user to log on to a computer system. It means that the FAS server now allows the authentication of a user to be delegated to the Microsoft ADFS server (or other SAML-aware IdP).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




ADFS is commonly used to securely authenticate users to corporate resources remotely over the Internet. For example, it is often used for Office 365 integration.

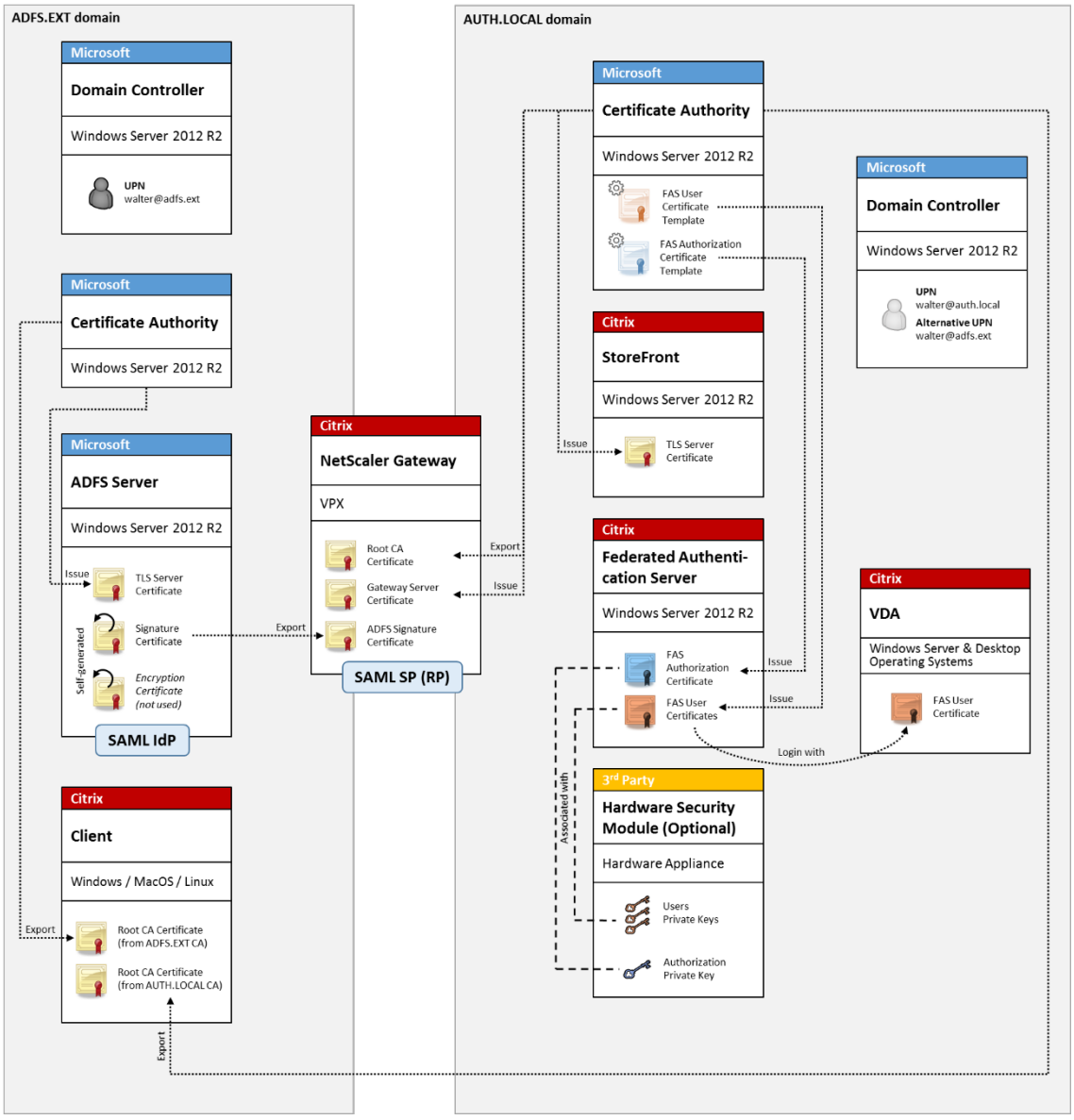
Related information:

- The Federated Authentication Service ADFS deployment article contains details.
- The Federated Authentication Service article describes how to install and configure FAS.
- The NetScaler Gateway deployment section in this article contains configuration considerations.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## B2B account mapping

If two companies want to use each other's computer systems, a common option is to set up an Active Directory Federation Service (ADFS) server with a trust relation. This allows users in one company to seamlessly authenticate into another company's Active Directory (AD) environment. When logging on, each user uses their own company logon credentials. ADFS automatically maps this to a "shadow account" in the peer company's AD environment.



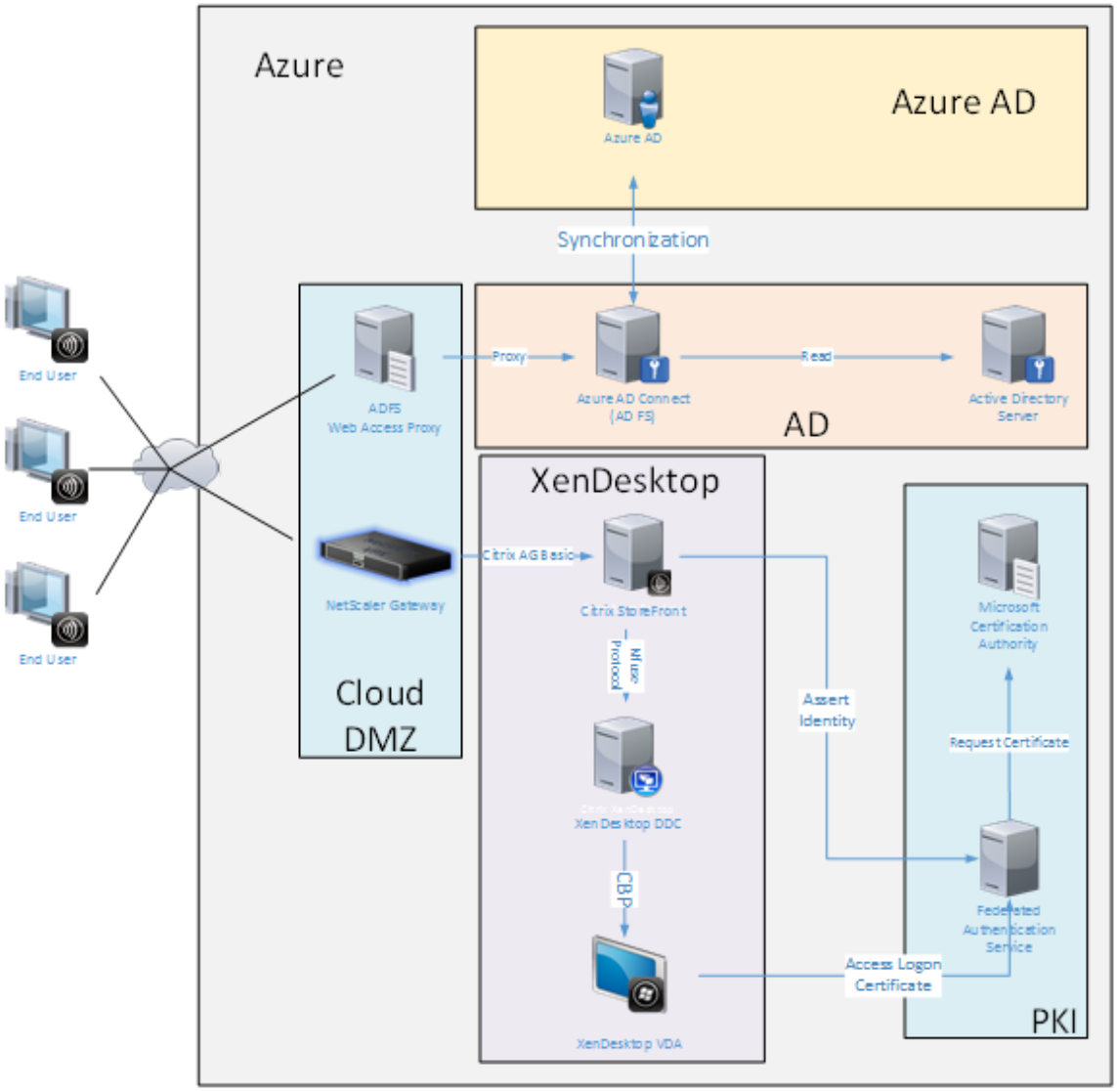

Related information:

- The Federated Authentication Service article describes how to install and configure FAS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Windows 10 Azure AD Join

Windows 10 introduced the concept of "Azure AD Join,"which is conceptually similar to traditional Windows domain join but targeted at "over the internet"scenarios. This works well with laptops and tablets. As with traditional Windows domain join, Azure AD has functionality to allow SSO models for company websites and resources. These are all "Internet aware,"so will work from any Internet connected location, not just the office LAN.




This deployment is an example where there is effectively no concept of "end users in the office."Laptops are enrolled and authenticate entirely over the Internet using modern Azure AD features.

The infrastructure in this deployment can run anywhere an IP address is available: on-premises, hosted provider, Azure, or another cloud provider. The Azure AD Connect synchronizer will automatically connect to Azure AD. The example graphic uses Azure VMs for simplicity.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Related information:

- The Federated Authentication Service article describes how to install and configure FAS.
- The Federated Authentication Service Azure AD integration article contains details.

# Federated Authentication Service ADFS deployment

June 16, 2021

## Introduction

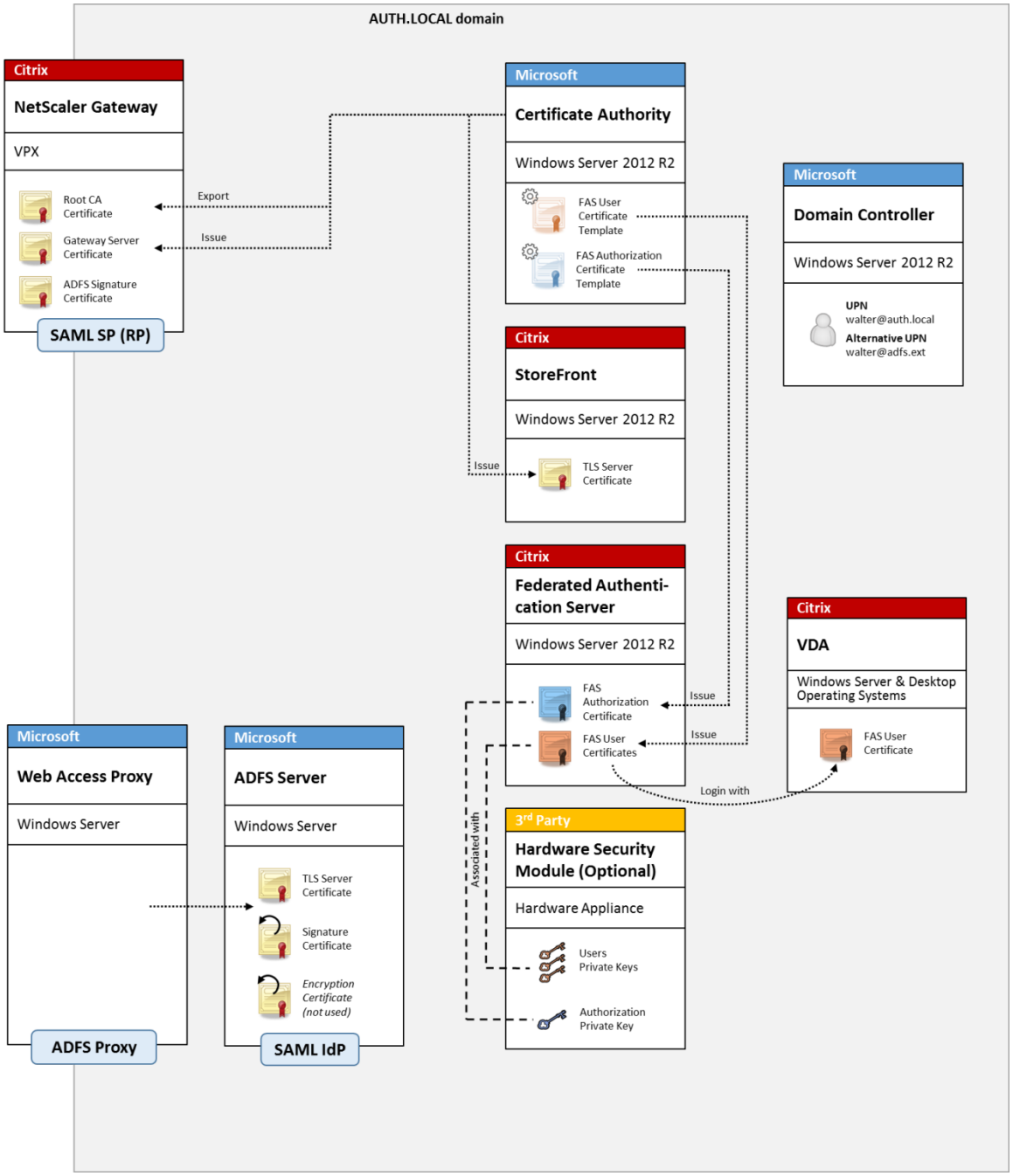
This document describes how to integrate a Citrix environment with Microsoft ADFS.

Many organizations use ADFS to manage secure user access to web sites that require a single point of authentication. For example, a company may have additional content and downloads that are available to employees; those locations need to be protected with standard Windows logon credentials.

The Federated Authentication Service (FAS) also allows Citrix NetScaler and Citrix StoreFront to be integrated with the ADFS logon system, reducing potential confusion for the company's staff.

This deployment integrates NetScaler as a relying party to Microsoft ADFS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




## SAML overview

Security Assertion Markup Language (SAML) is a simple "redirect to a logon page" web browser logon system. Configuration includes the following items:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Redirect URL [Single Sign-on Service Url]

When NetScaler discovers that a user needs to be authenticated, it instructs the user's web browser to do a HTTP POST to a SAML logon webpage on the ADFS server. This is usually an `https://` address of the form: `https://adfs.mycompany.com/adfs/ls`.

This web page POST includes other information, including the "return address" where ADFS will return the user when logon is complete.

#### Identifier [Issuer Name/EntityID]

The EntityId is a unique identifier that NetScaler includes in its POST data to ADFS. This informs ADFS which service the user is trying to log on to, and to apply different authentication policies as appropriate. If issued, the SAML authentication XML will only be suitable for logging on to the service identified by the EntityId.

Usually, the EntityID is the URL of the NetScaler server logon page, but it can generally be anything, as long as NetScaler and ADFS agree on it: `https://ns.mycompany.com/application/logonpage`.

#### Return address [Reply URL]

If authentication is successful, ADFS instructs the user's web browser to POST a SAML authentication XML back to one of the Reply URLs that are configured for the EntityId. This is usually an `https://` address on the original NetScaler server in the form: `https://ns.mycompany.com/cgi/samlauth`.

If there is more than one Reply URL address configured, NetScaler can choose one in its original POST to ADFS.

#### Signing certificate [IDP Certificate]

ADFS cryptographically signs SAML authentication XML blobs using its private key. To validate this signature, NetScaler must be configured to check these signatures using the public key included in a certificate file. The certificate file will usually be a text file obtained from the ADFS server.

#### Single sign-out Url [Single Logout URL]

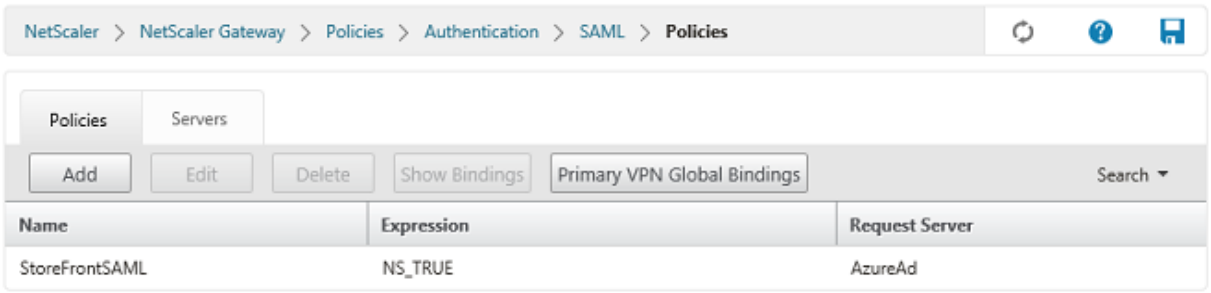
ADFS and NetScaler support a "central logout" system. This is a URL that NetScaler polls occasionally to check that the SAML authentication XML blob still represents a currently logged-on session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

This is an optional feature that does not need to be configured. It is usually an `https://` address in the form `https://adfs.mycompany.com/adfs/logout`. (Note that it can be the same as the Single Logon URL.)

### Configuration

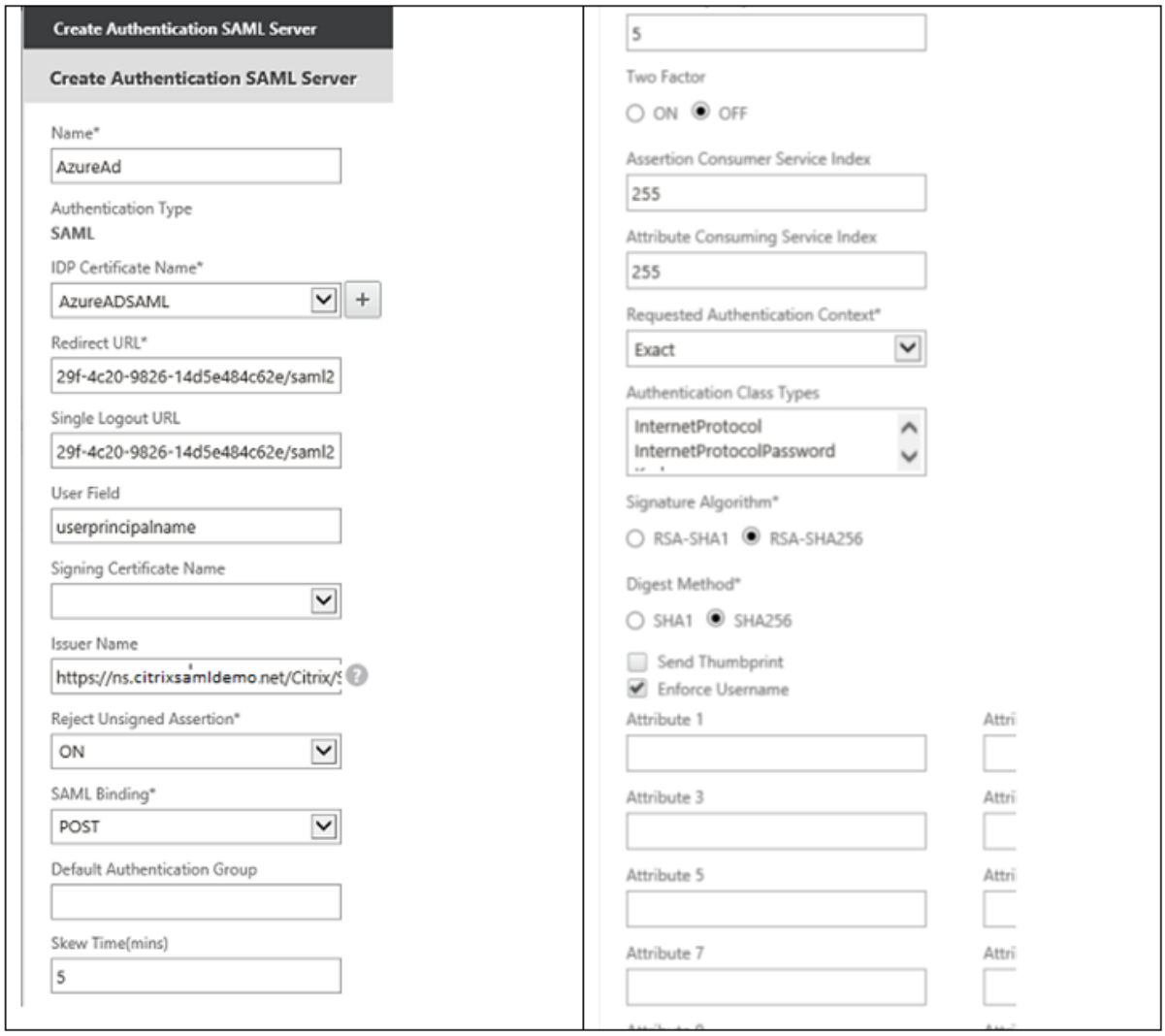
The NetScaler Gateway deployment section in the Federated Authentication Services architectures article describes how to set up NetScaler Gateway to handle standard LDAP authentication options, using the XenApp and XenDesktop NetScaler setup wizard. After that completes successfully, you can create a new authentication policy on NetScaler that allows SAML authentication. This can then replace the default LDAP policy used by the NetScaler setup wizard.




#### Fill in the SAML policy

Configure the new SAML IdP server using information taken from the ADFS management console earlier. When this policy is applied, NetScaler redirects the user to ADFS for logon, and accepts an ADFS-signed SAML authentication token in return.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




## Related information

- The Federated Authentication Service article is the primary reference for FAS installation and configuration.
- The common FAS deployments are summarized in the Federated Authentication Service architectures overview article.
- "How-to"articles are introduced in the Federated Authentication Service configuration and management article.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Federated Authentication Service Azure AD integration

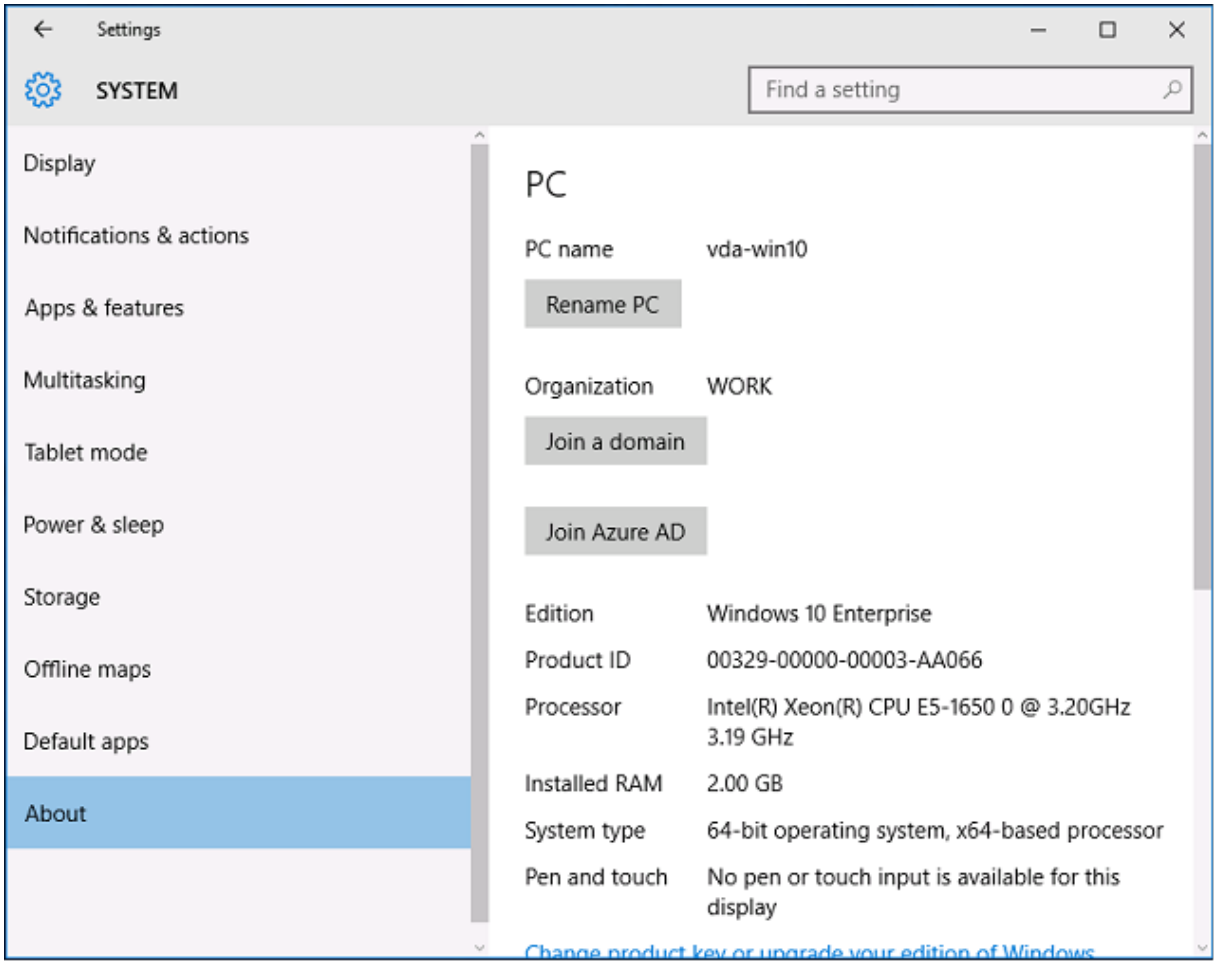
June 16, 2021

## Introduction

This document describes how to integrate a Citrix environment with the Windows 10 Azure AD feature.

Windows 10 introduced Azure AD, which is a new domain join model where roaming laptops can be joined to a corporate domain over the Internet for the purposes of management and single sign-on.

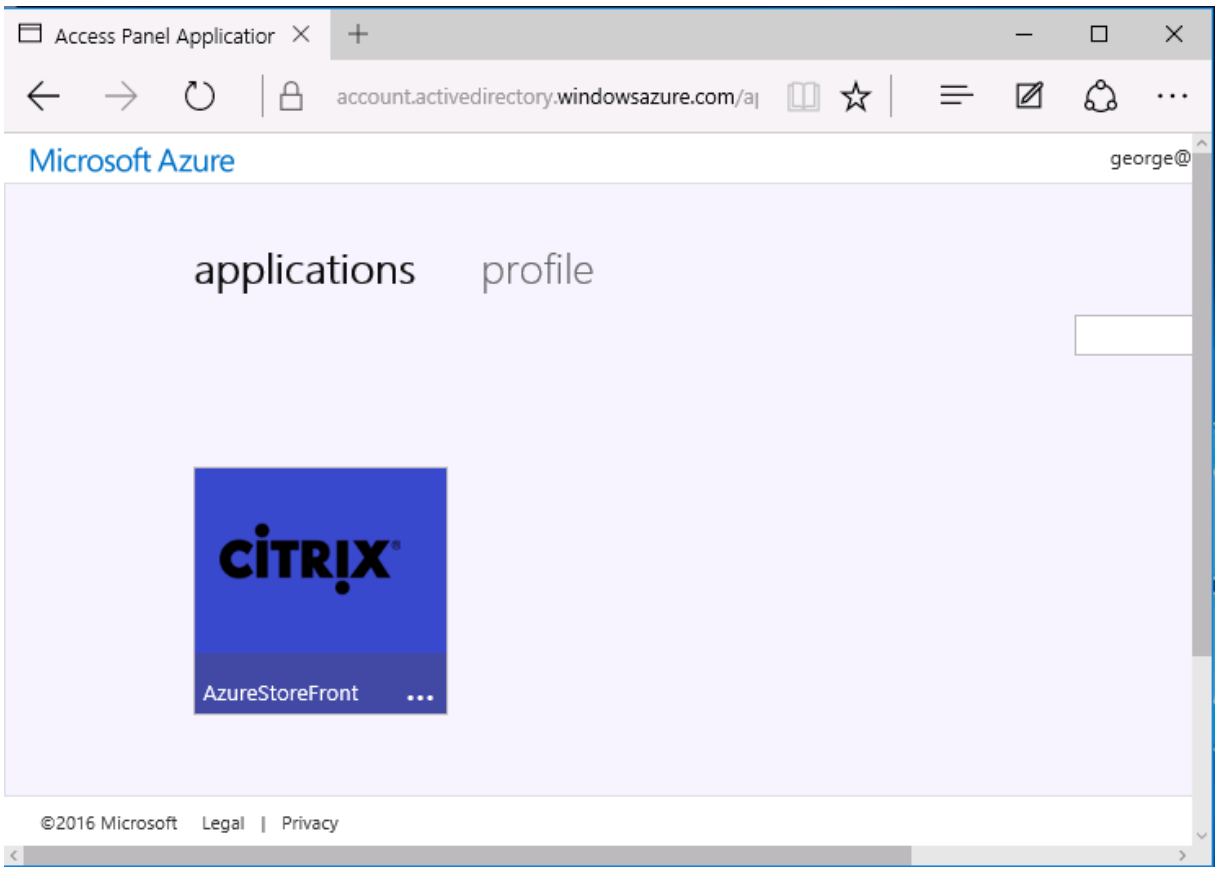
The example deployment in this document describes a system where IT provides new users with a corporate email address and enrollment code for their personal Windows 10 laptops. Users access this code through the **System** > **About** > **Join Azure AD** option in the **Settings** panel.




After the laptop is enrolled, the Microsoft Edge web browser automatically signs on to company web sites and Citrix published applications through the Azure SaaS applications web page, with other

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Azure applications such as Office 365.

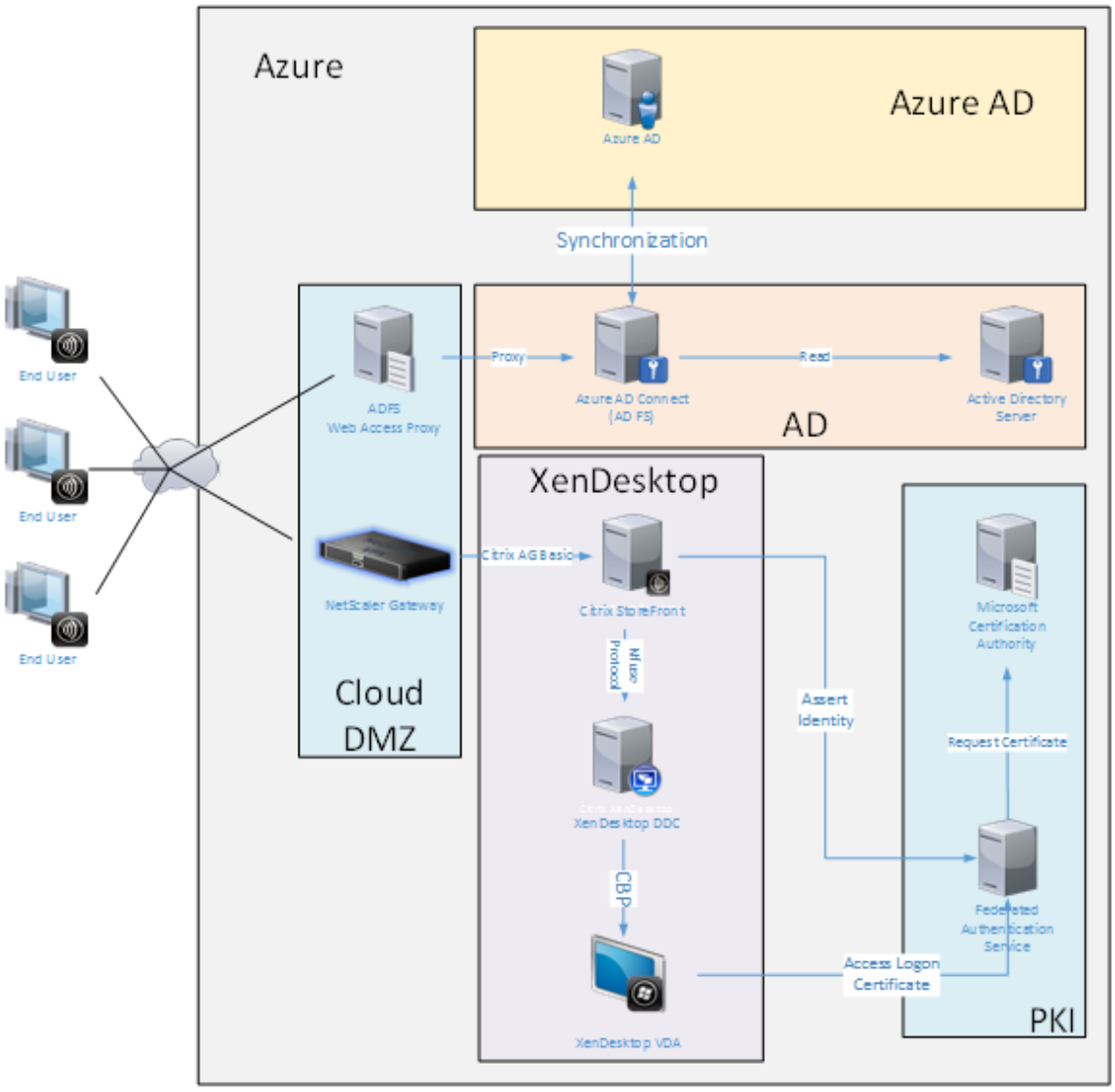



## Architecture

This architecture replicates a traditional company network completely within Azure, integrating with modern cloud technologies such as Azure AD and Office 365. End users are all considered remote workers, with no concept of being on an office intranet.

The model can be applied to companies with existing on premises systems, because the Azure AD Connect Synchronization can bridge to Azure over the Internet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Secure connections and single sign-on, which would traditionally have been firewalled-LAN and Kerberos/NTLM authentication, are replaced in this architecture by TLS connections to Azure and SAML. New services are built as Azure applications joined to Azure AD. Existing applications that require Active Directory (such as a SQL Server database) can be run using a standard Active Directory Server VM in the IAAS portion of the Azure Cloud Service.

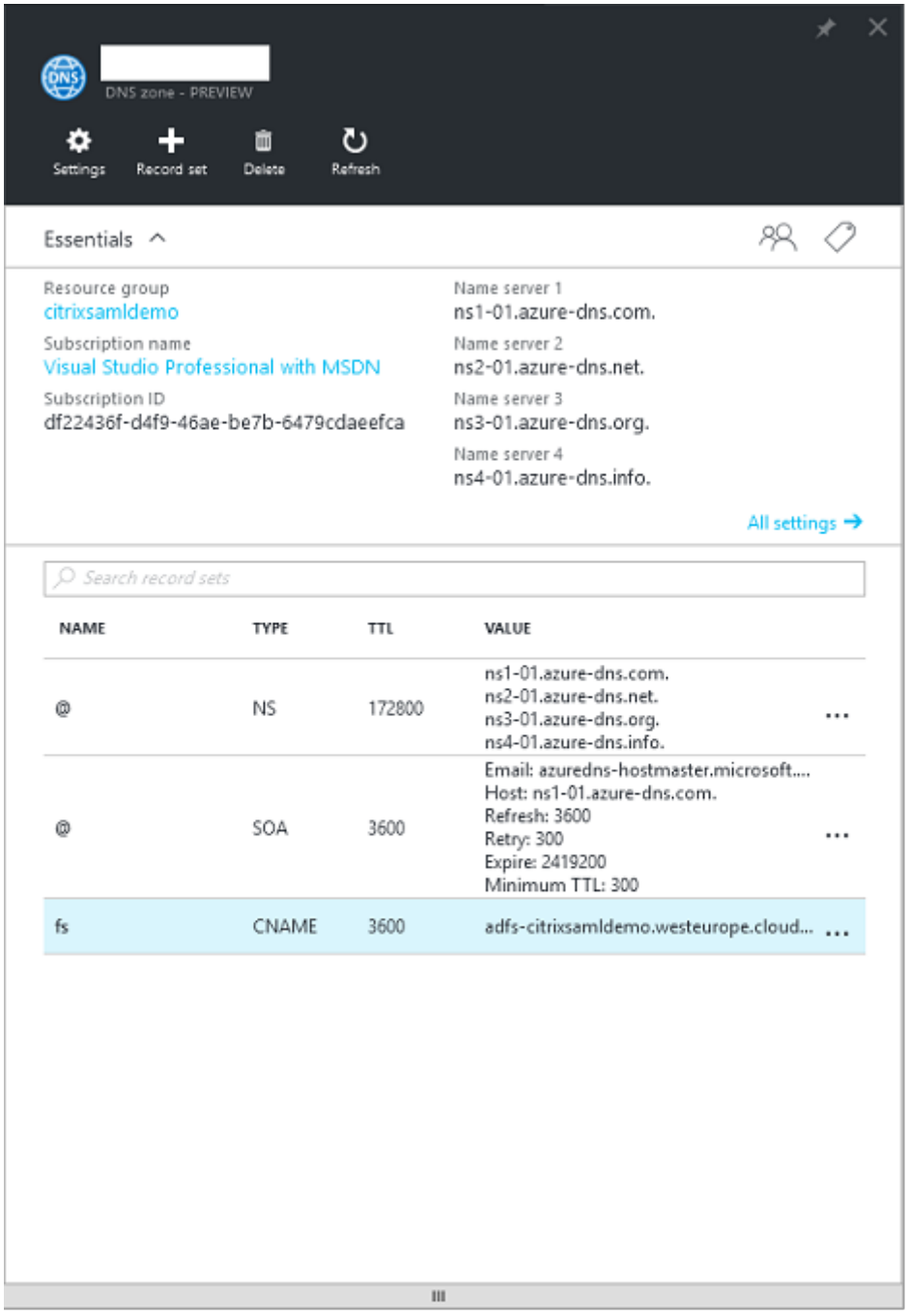
When a user launches a traditional application, they are accessed using XenApp and XenDesktop published applications. The different types of applications are collated through the user's **Azure Applications** page, using the Microsoft Edge Single sign-on features. Microsoft also supplies Android and iOS apps that can enumerate and launch Azure applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Create a DNS zone

Azure AD requires that the administrator has registered a public DNS address and controls the delegation zone for the domain name suffix. To do this, the administrator can use the Azure DNS zone feature.

This example uses the DNS zone name "citrixsamldemo.net."




The console shows the names of the Azure DNS name servers. These should be referenced in the DNS

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

registrar's NS entries for the zone (for example, citrixsamldemo.net. NS n1-01.azure-dns.com)

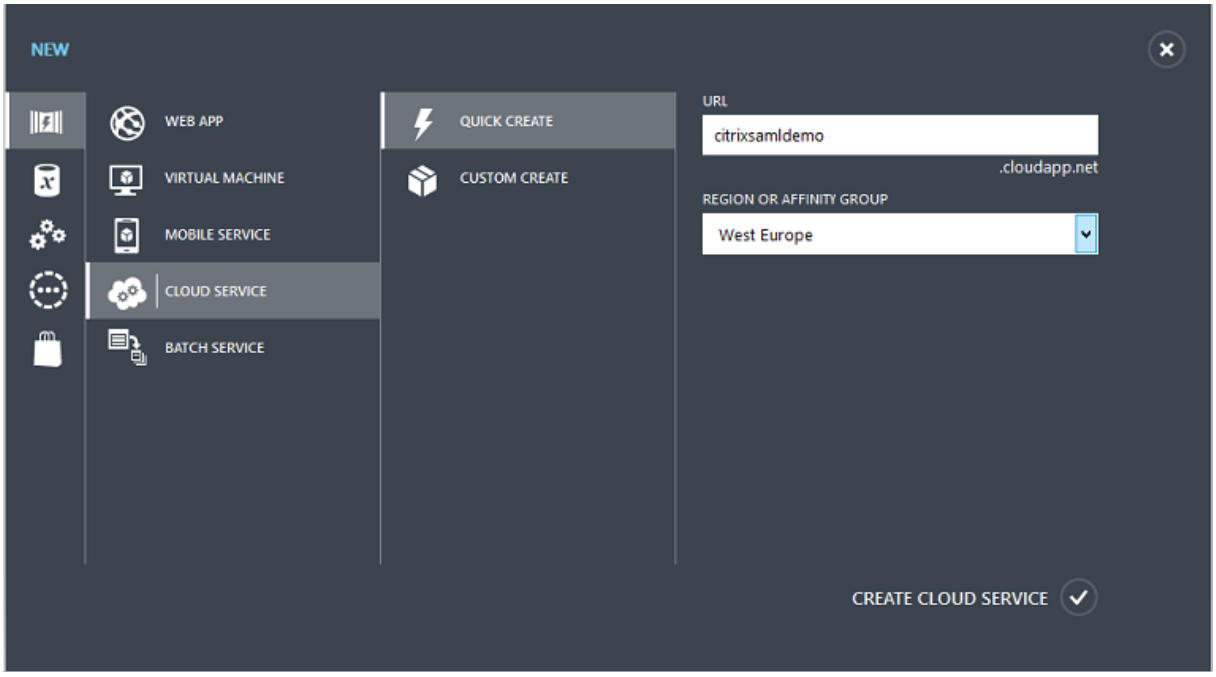
When adding references to VMs running in Azure, it is easiest to use a CNAME pointer to the Azure-managed DNS record for the VM. If the IP address of the VM changes, you will not need to manually update the DNS zone file.

Both internal and external DNS address suffixes will match for this deployment. The domain is citrixsamldemo.net, and uses a split DNS (10.0.0.* internally).

Add an "fs.citrixsamldemo.net"entry that references the Web Application Proxy server. This is the Federation Service for this zone.

### Create a Cloud Service

This example configures a Citrix environment, including an AD environment with an ADFS server running in Azure. A Cloud Service is created, named "citrixsamldemo."



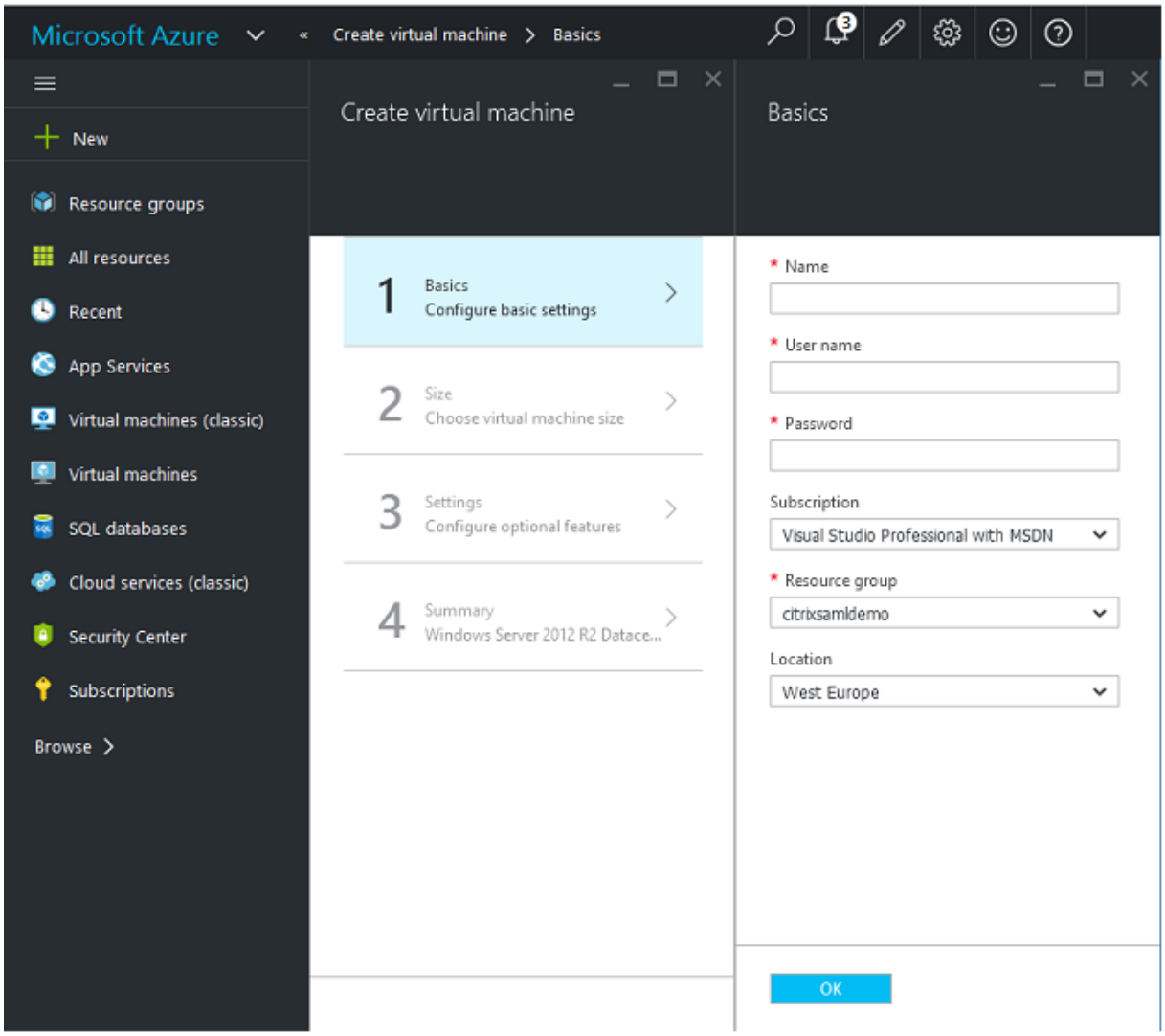

### Create Windows virtual machines

Create five Windows VMs running in the Cloud Service:

- Domain controller (domaincontrol)
- Azure Connect ADFS server (adfs)
- ADFS web access proxy (Web Application Proxy, not domain joined)
- Citrix XenDesktop Delivery Controller (ddc)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Citrix XenDesktop Virtual Delivery Agent (vda)




**Domain Controller**

- Add the **DNS Server** and **Active Directory Domain Services** roles to create a standard Active Directory deployment (in this example, citrixsamldemo. net). After domain promotion completes, add the **Active Directory Certification Services** role.
- Create a normal user account for testing (for example, George@citrixsamldemo.net).
- Since this server will be running internal DNS, all servers should refer to this server for DNS resolution. This can be done through the **Azure DNS settings** page. (For more information, see the Appendix in this document.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### ADFS controller and Web Application Proxy server

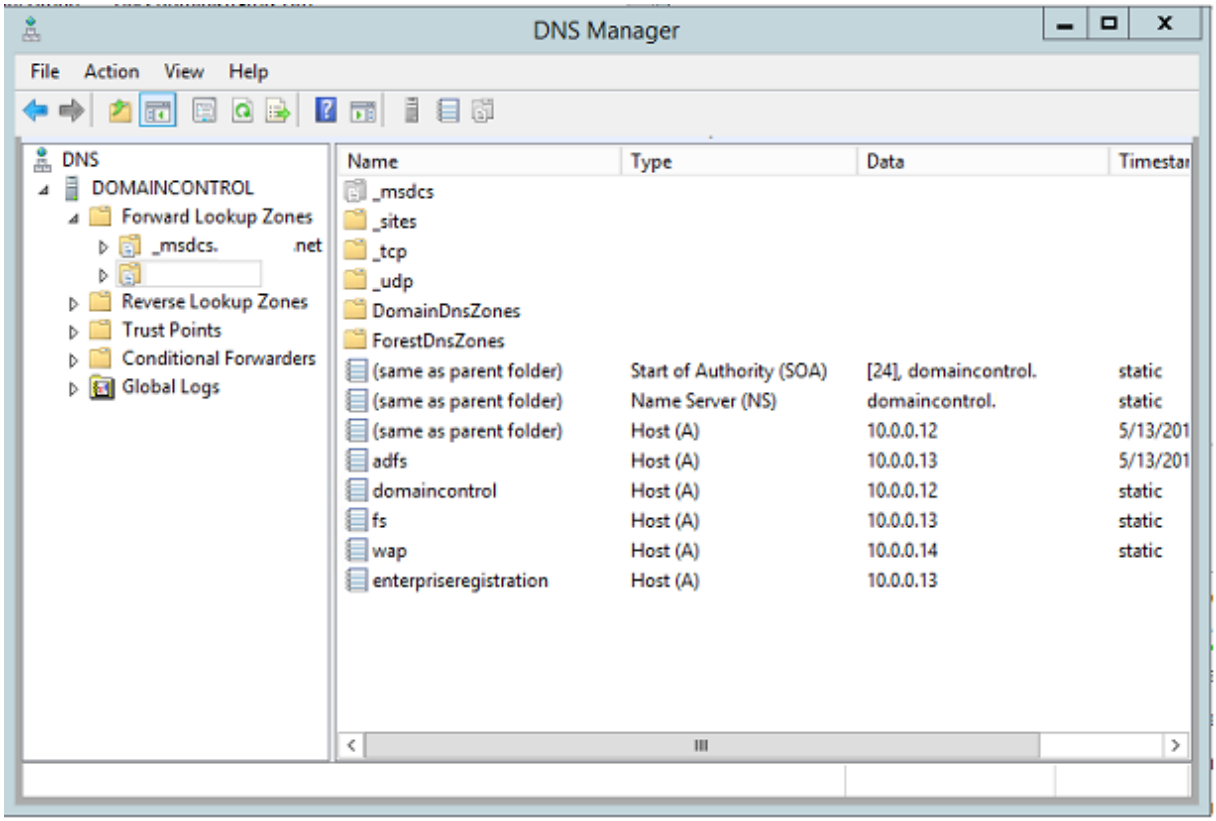
- Join the ADFS server to the citrixsamldemo domain. The Web Application Proxy server should remain in an isolated workgroup, so manually register a DNS address with the AD DNS.
- Run the **Enable-PSRemoting** –**Force** cmdlet on these servers, to allow PS remoting through firewalls from the AzureAD Connect tool.

#### XenDesktop Delivery Controller and VDA

- Install the XenApp or XenDesktop Delivery Controller and VDA on the remaining two Windows servers joined to citrixsamldemo.

### Configure an internal DNS

After the domain controller is installed, configure the DNS server to handle the internal view of citrixsamldemo.net, and act as a forwarder to an external DNS server (for example: 8.8.8.8).



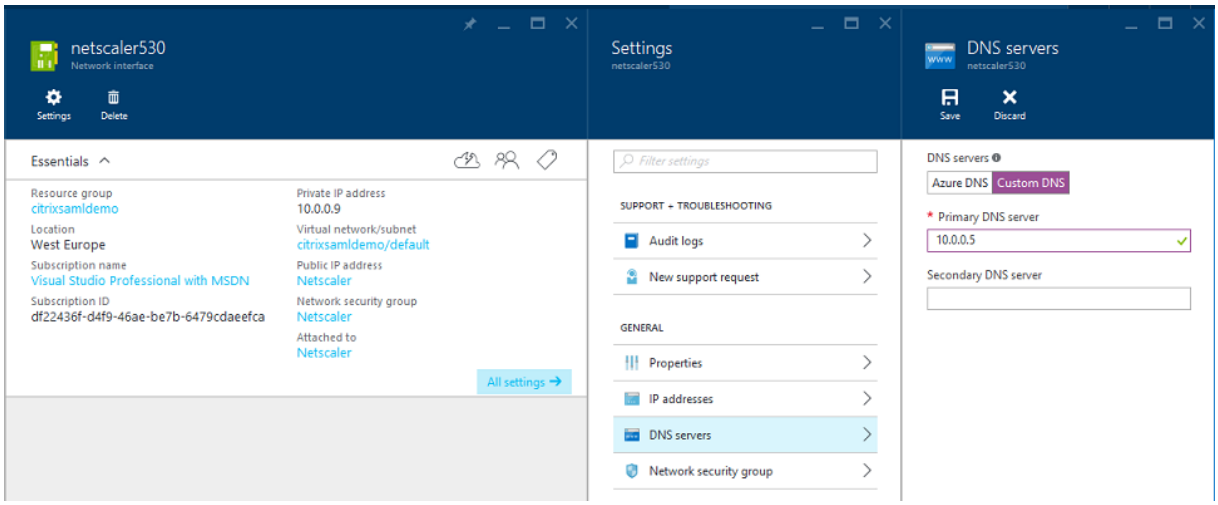

Add a static record for:

- wap.citrixsamldemo.net [the Web Application Proxy VM will not be domain joined]
- fs.citrixsamldemo.net [internal federation server address]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- enterpriseregistration.citrixsaml.net [same as fs.citrixsamldemo.net]

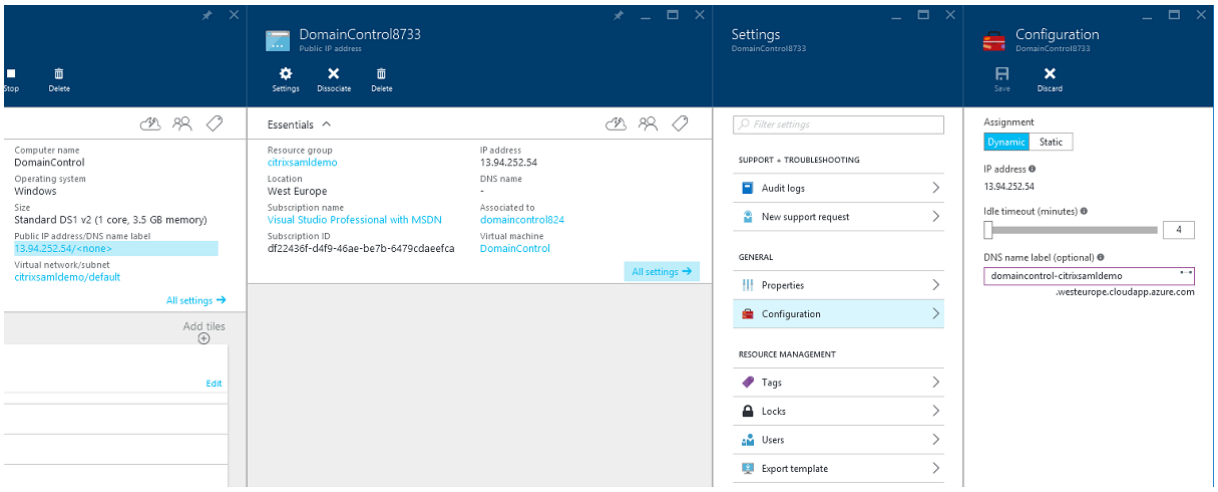
All VMs running in Azure should be configured to use only this DNS server. You can do this through the Network Interface GUI.




By default, the internal IP (10.0.0.9) address is dynamically allocated. You can use the IP addresses setting to permanently assign the IP address. This should be done for the Web Application Proxy server and the domain controller.

### Configure an external DNS address

When a VM is running, Azure maintains its own DNS zone server that points to the current public IP address assigned to the VM. This is a useful feature to enable because Azure assigns IP addresses when each VM starts, by default.



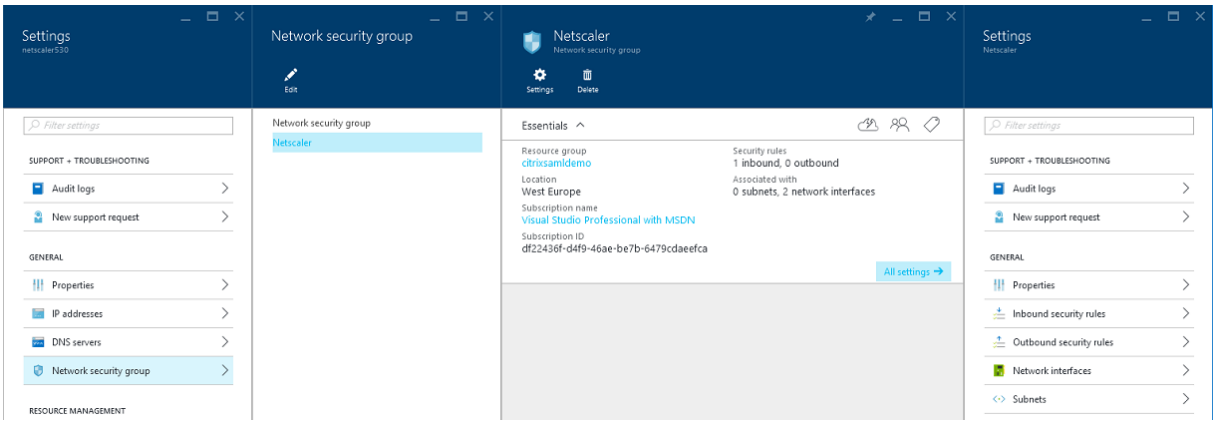

This example assigns a DNS address of domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com to the domain controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Note that when remote configuration is complete, only the Web Application Proxy and NetScaler VMs should have public IP addresses enabled. (During configuration, the public IP address is used for RDP access to the environment).

### Configure security groups

The Azure cloud manages firewall rules for TCP/UDP access into VMs from the Internet using security groups. By default, all VMs allow RDP access. The NetScaler and Web Application Proxy servers should also allow TLS on port 443.



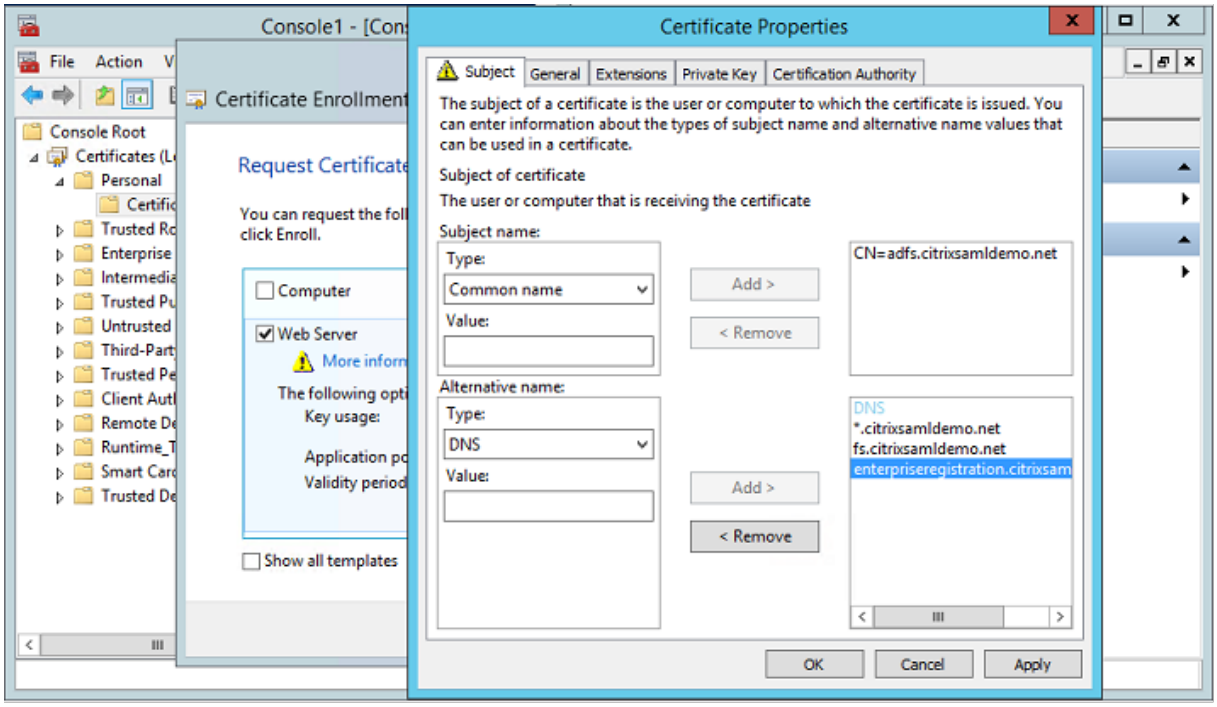

### Create an ADFS certificate

Enable the **Web Server** certificate template on the Microsoft certificate authority (CA). This allows creation of a certificate with custom DNS addresses that can be exported (including private key) to a pfx file. You must install this certificate on both the ADFS and Web Application Proxy servers, so the PFX file is the preferred option.

Issue a Web Server certificate with the following subject names:

- Commonname:
  - adfs.citrixsamldemo.net [name of computer]
- SubjectAltname:
  - *.citrixsamldemo.net [name of zone]
  - fs.citrixsamldemo. net [entry in DNS]
  - enterpriseregistration.citrixsamldemo.net

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Export the certificate to a pfx file, including a password-protected private key.

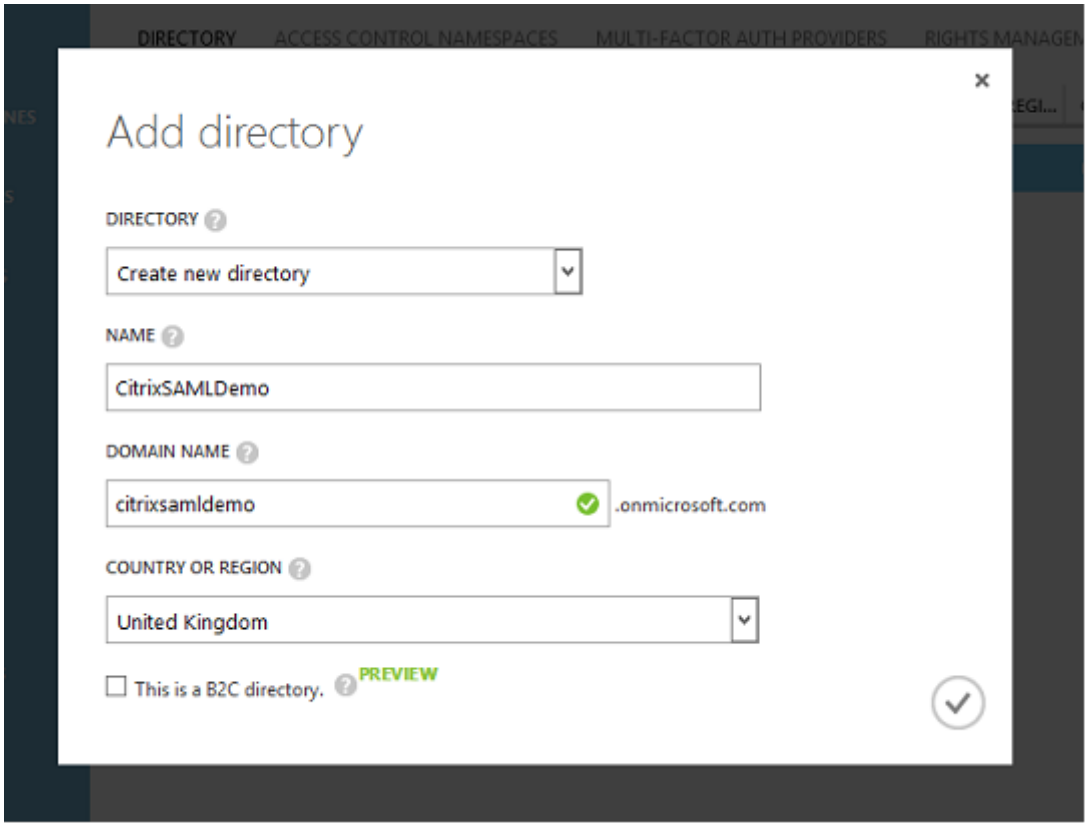
### Set up Azure AD

This section details the process of setting up a new Azure AD instance and creating user identities that can be used to join Windows 10 to Azure AD.

#### Create a new directory

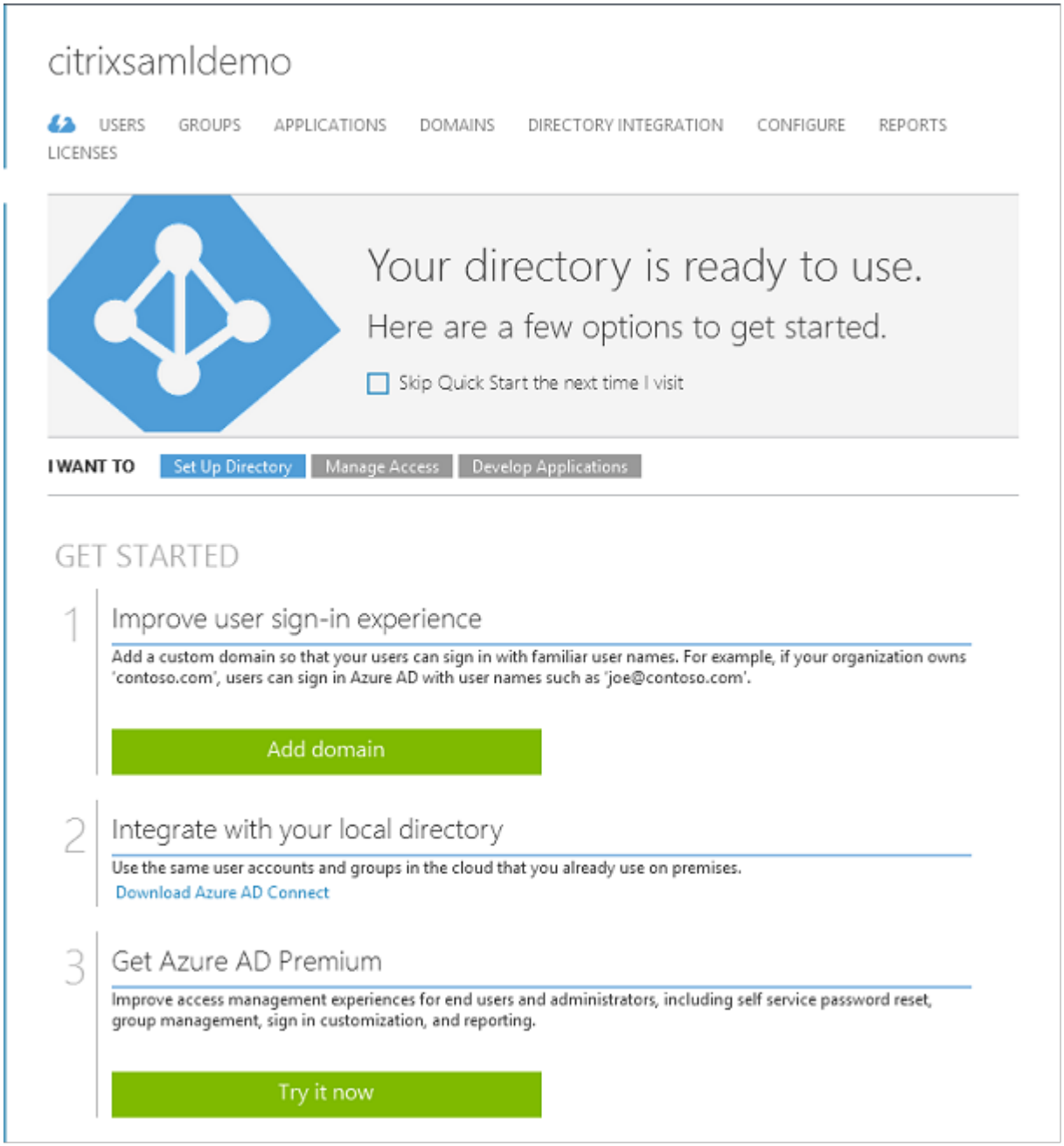
Log on to the classic Azure portal and create a new directory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




When complete, a summary page appears.

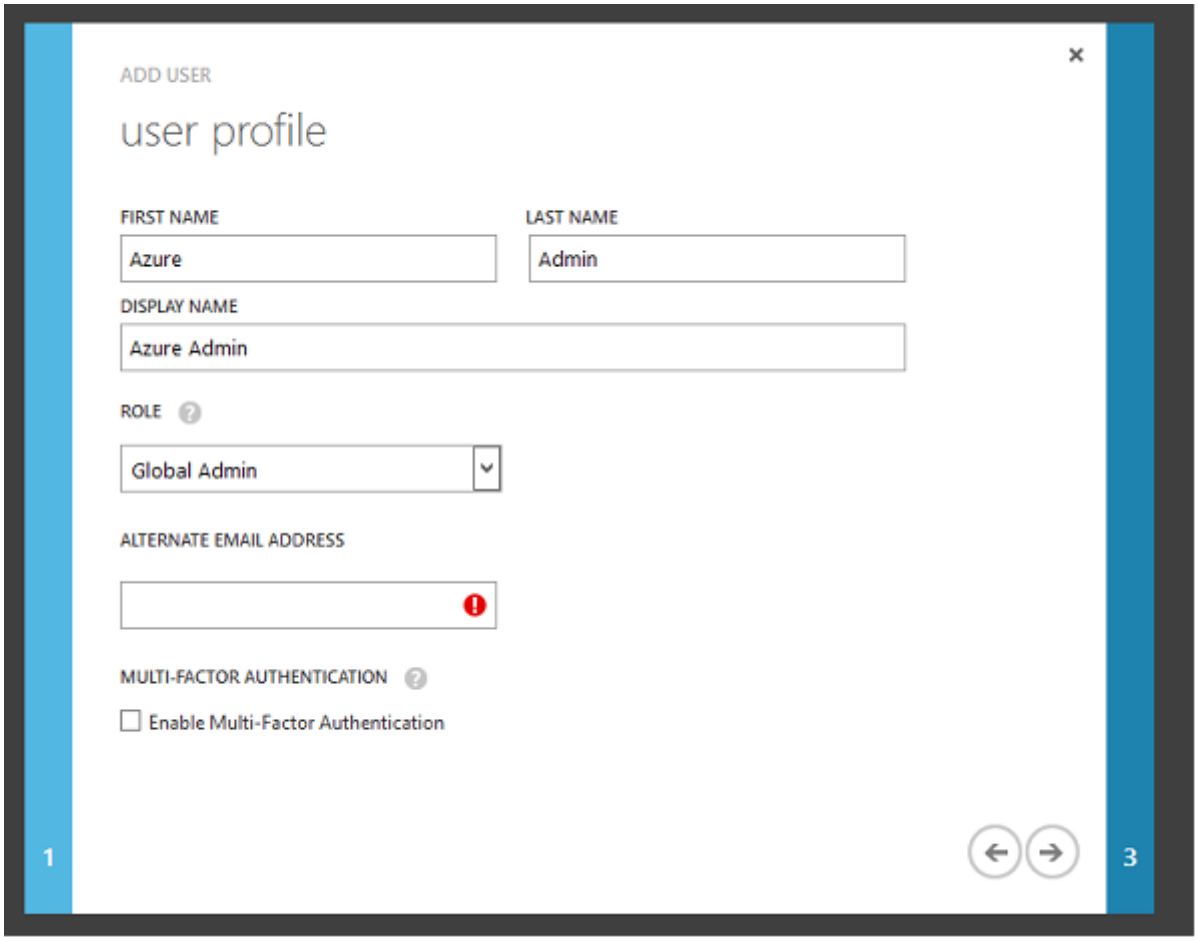
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Create a global administrator user (AzureAdmin)**

Create a global administrator in Azure (in this example, AzureAdmin@citrixsamldemo.onmicrosoft.com) and log on with the new account to set up a password.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Register your domain with Azure AD**

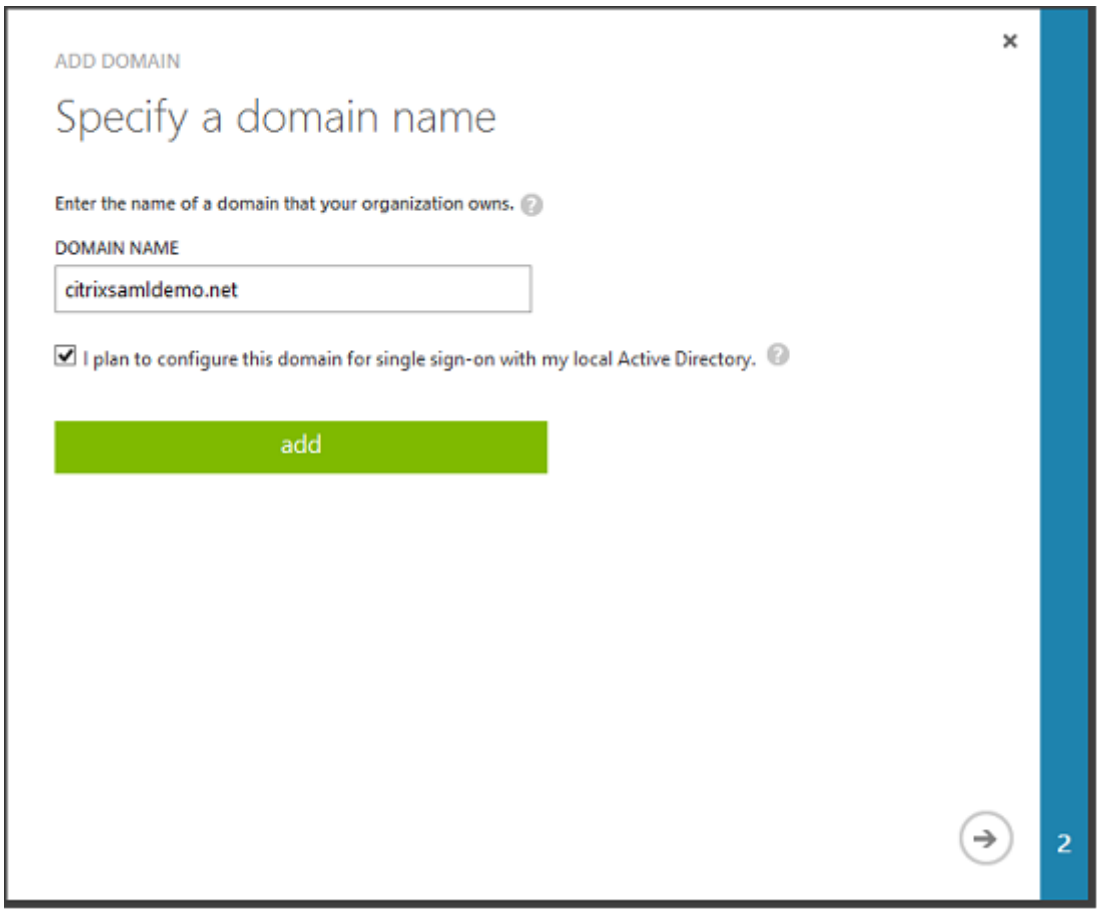
By default, users are identified with an email address in the form: *<user.name>@<company>.onmicrosoft.com.*

Although this works without further configuration, a standard format email address is better, preferably one that matches the email account of the end user: <user.name>@<company>.com

The **Add domain** action configures a redirect from your real company domain. The example uses citrixsamldemo.net.

If you are setting up ADFS for single sign-on, enable the check box.

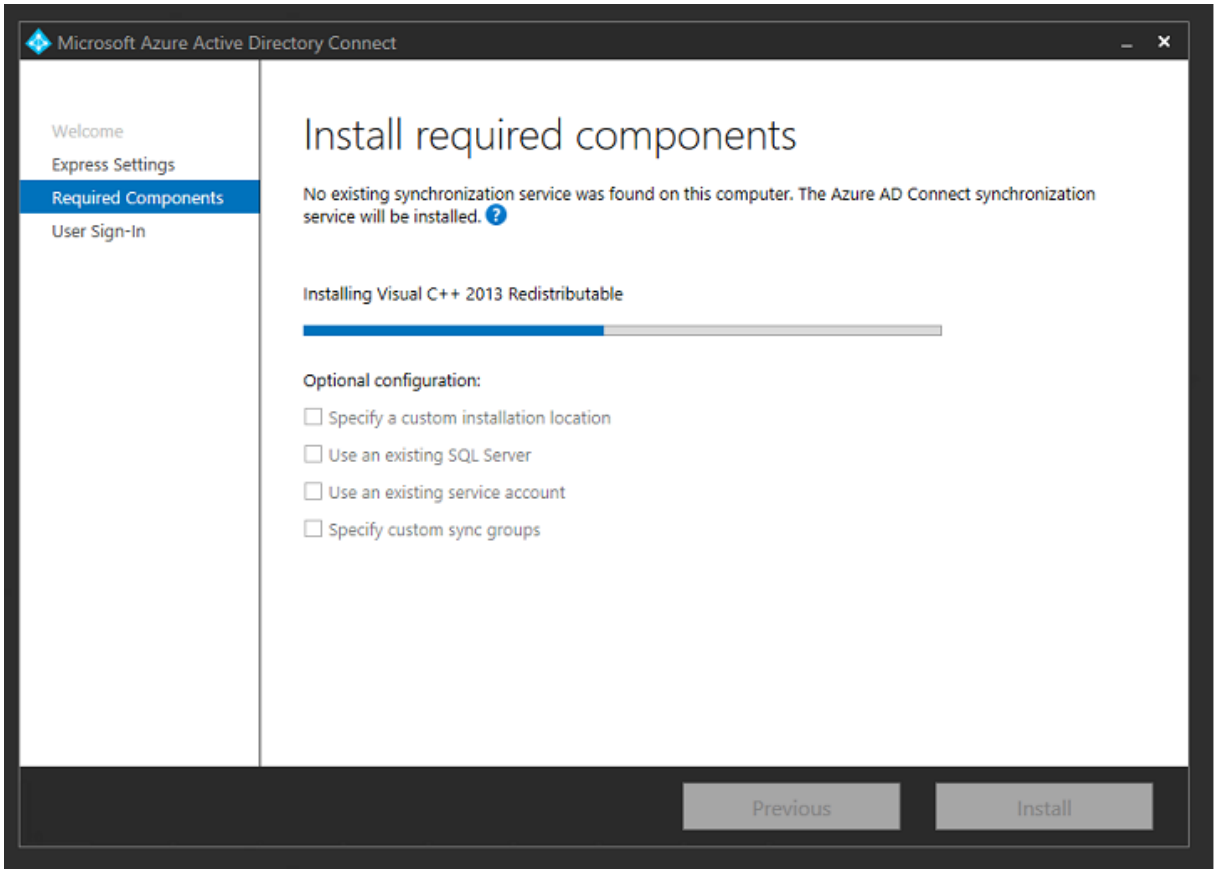
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Install Azure AD Connect**

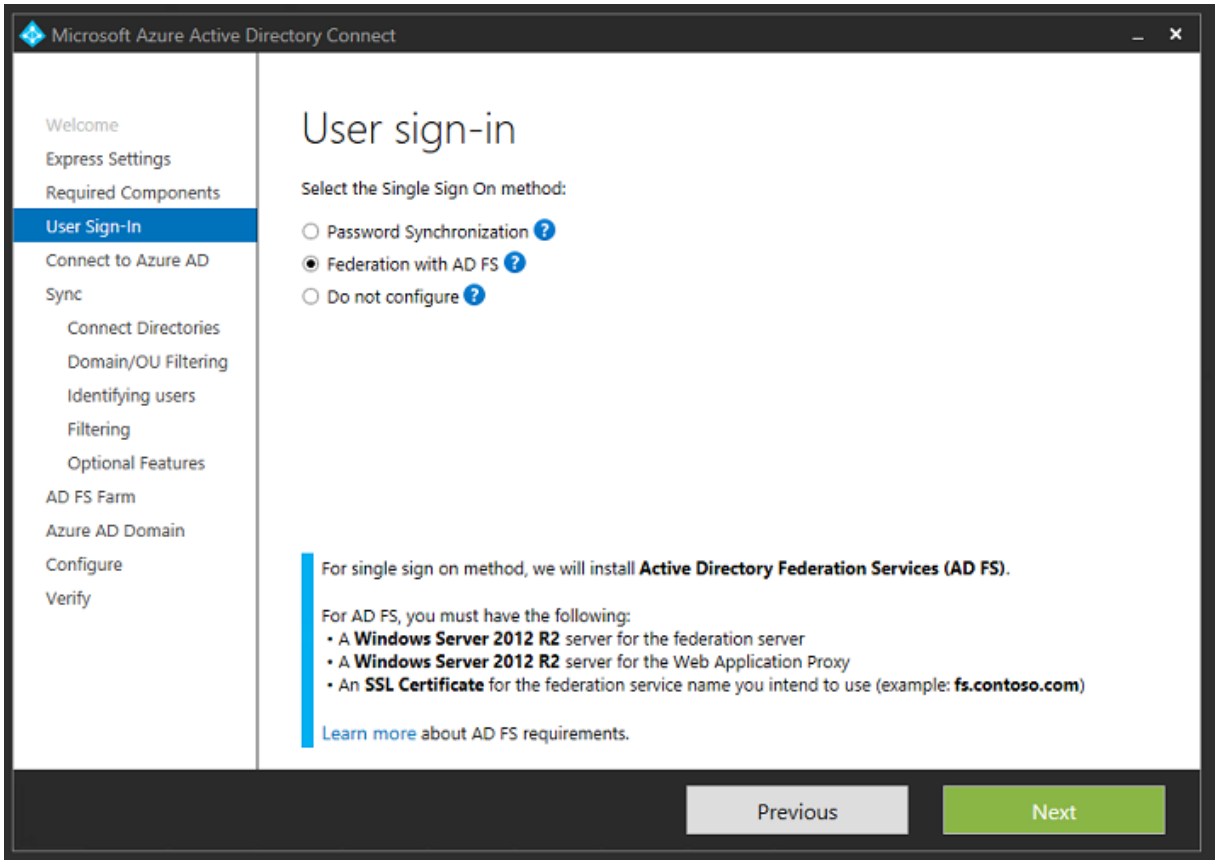
Step 2 of the Azure AD configuration GUI redirects to the Microsoft download page for Azure AD Connect. Install this on the ADFS VM. Use **Custom install**, rather than **Express Settings**, so that ADFS options are available.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



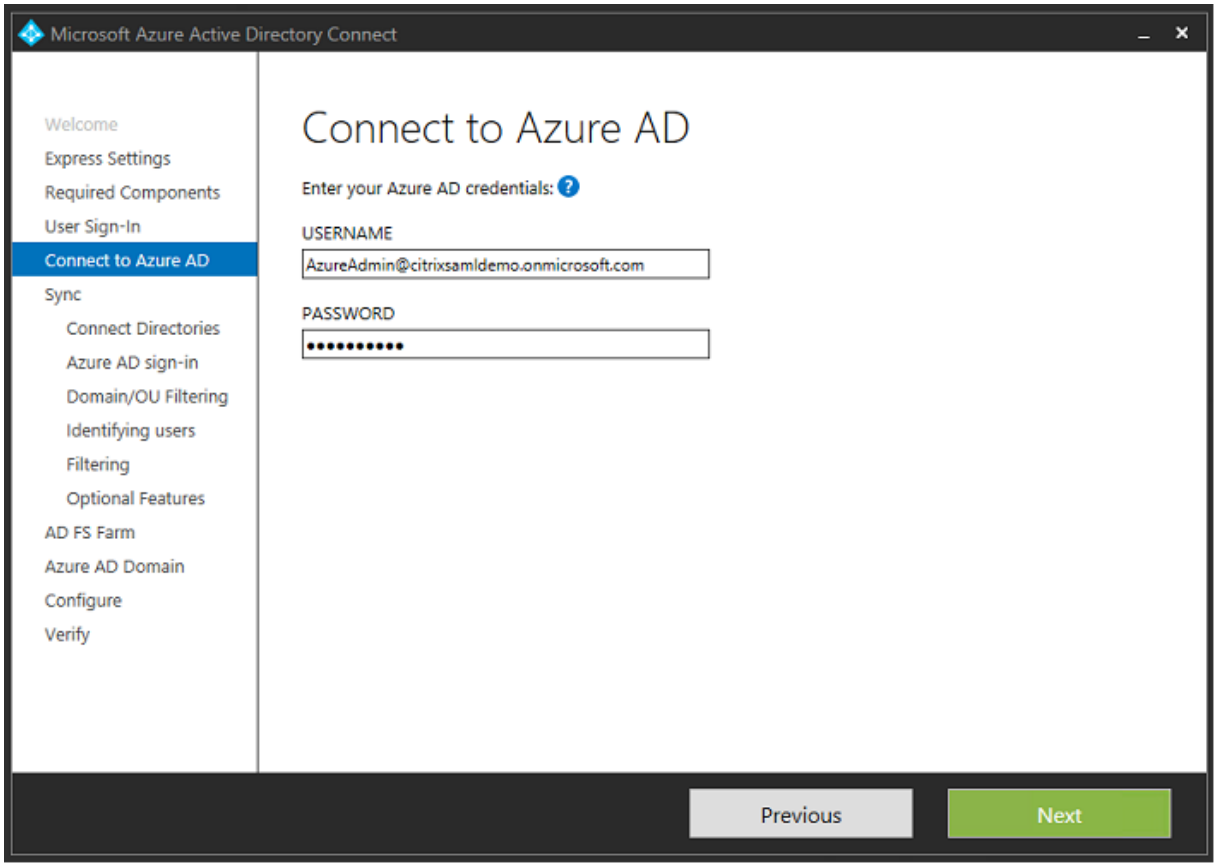

Select the **Federation with AD FS** Single sign-On option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



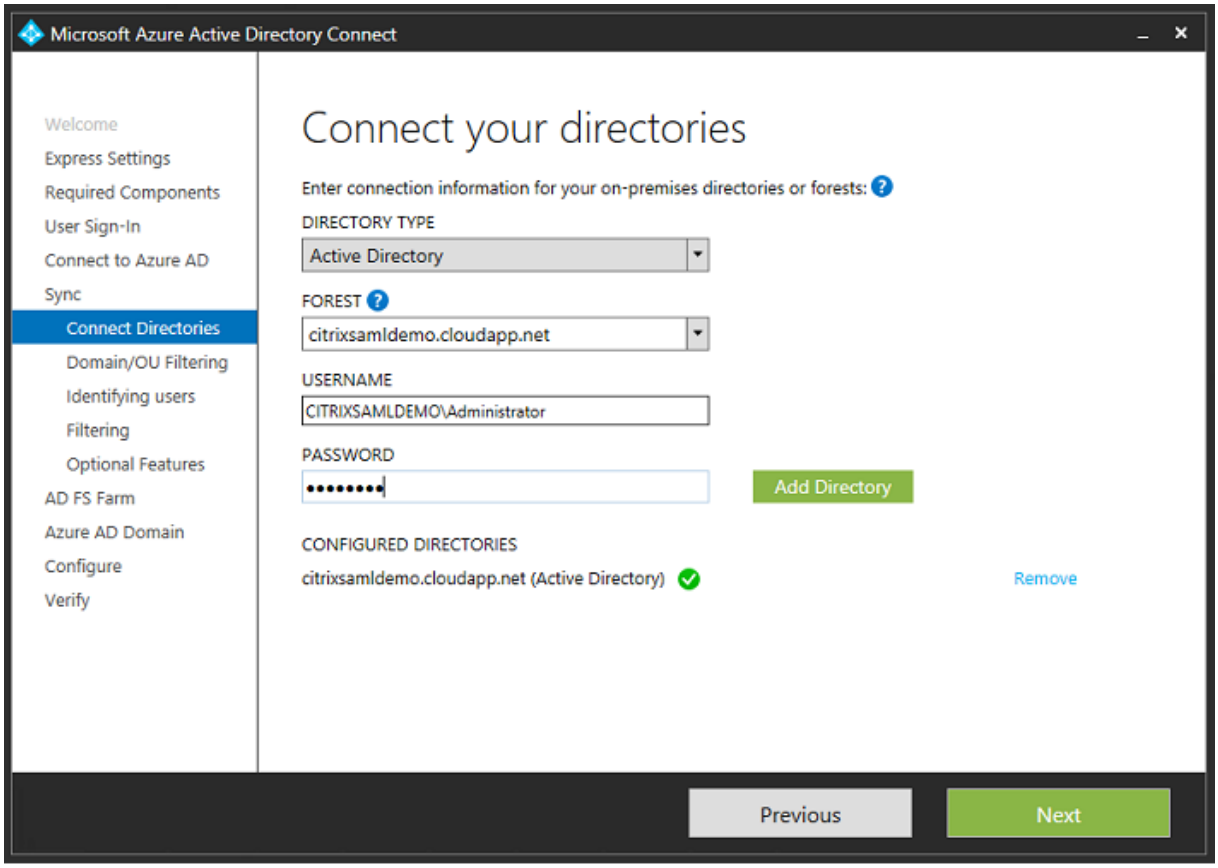

Connect to Azure with the administrator account you created earlier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



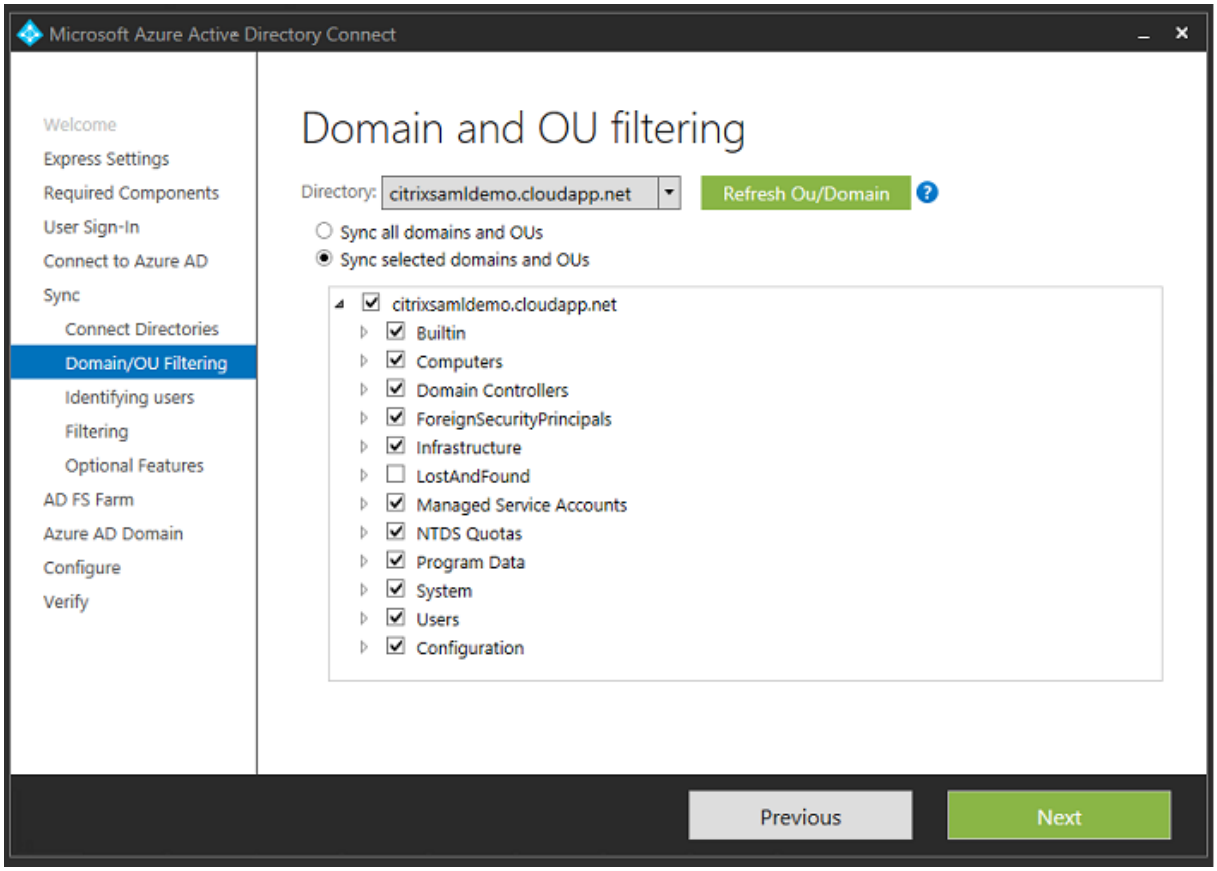

Select the internal AD forest.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



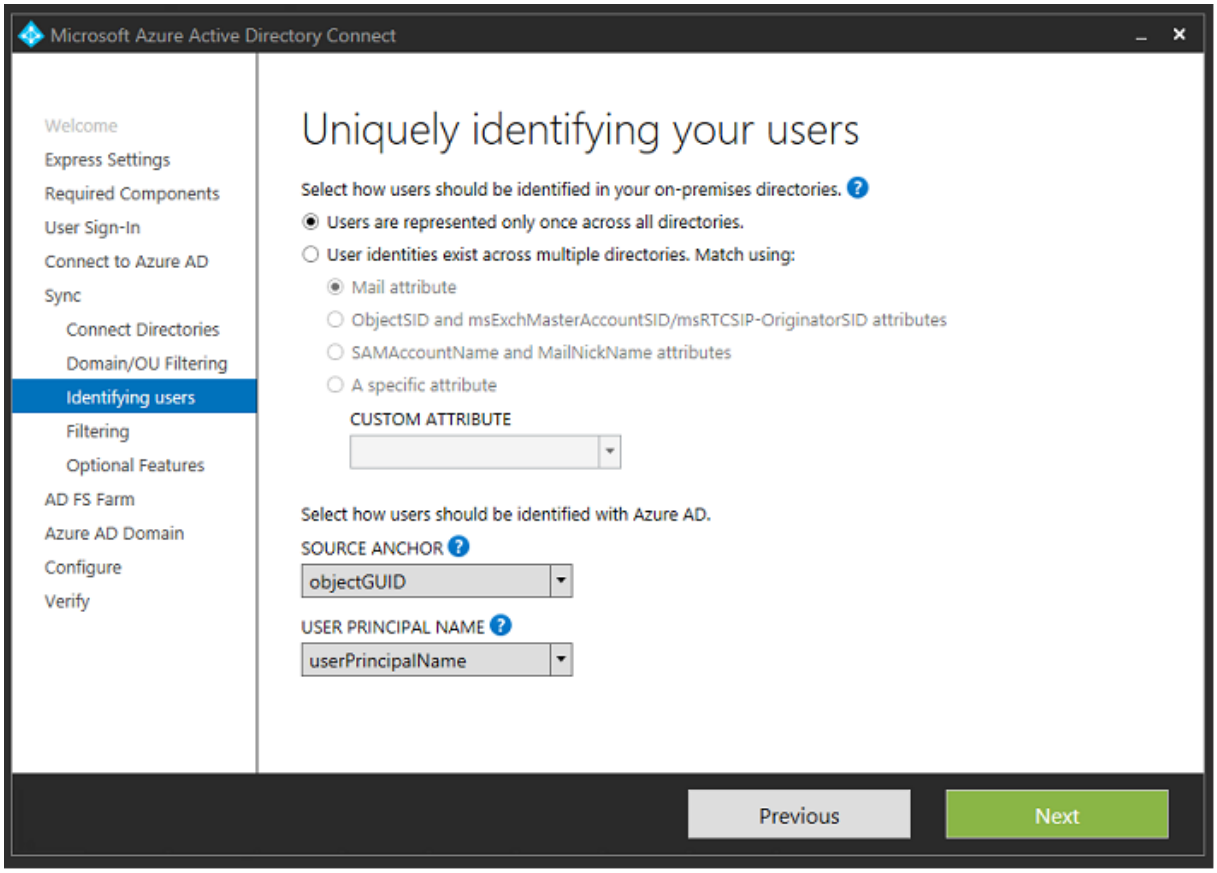

Synchronize all legacy Active Directory objects with Azure AD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



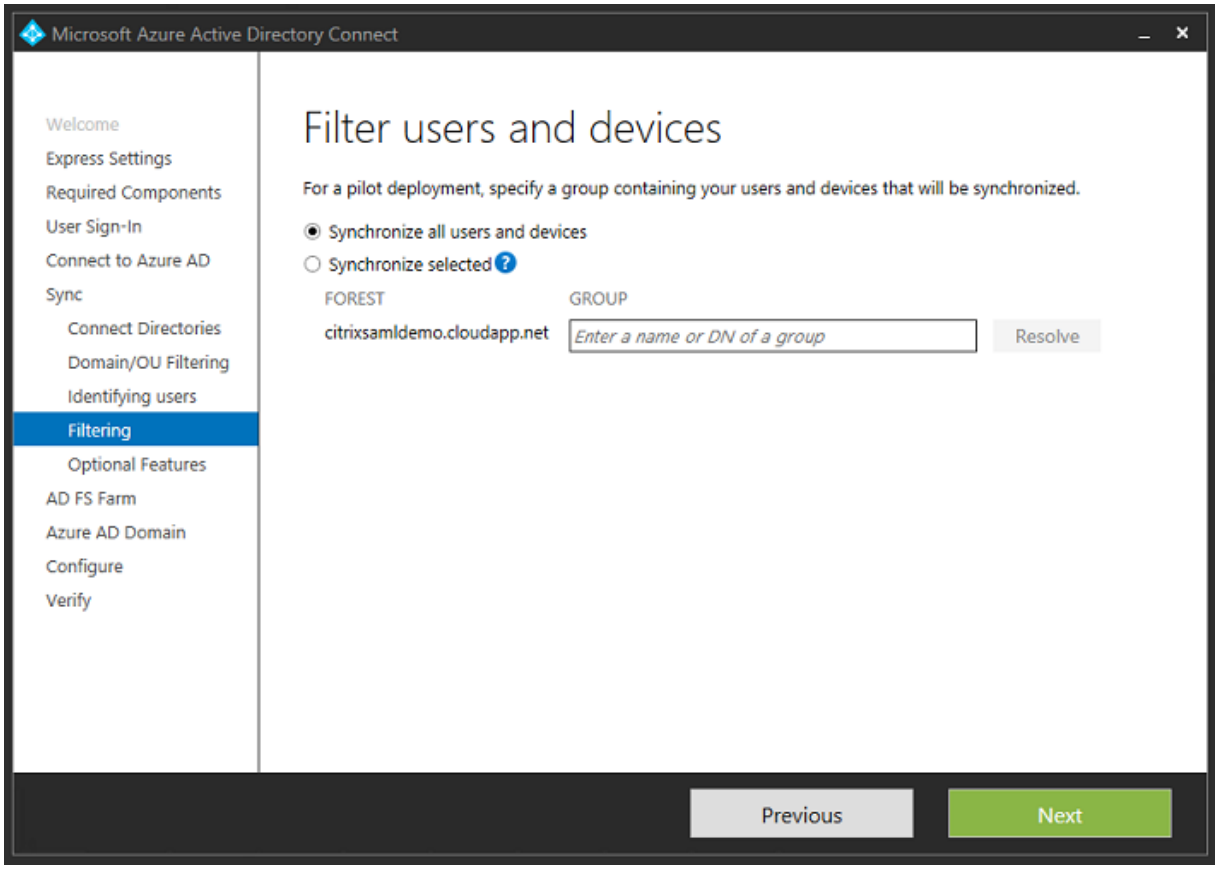

If the directory structure is simple, you can rely on the usernames being sufficiently unique to identify a user who logs on.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



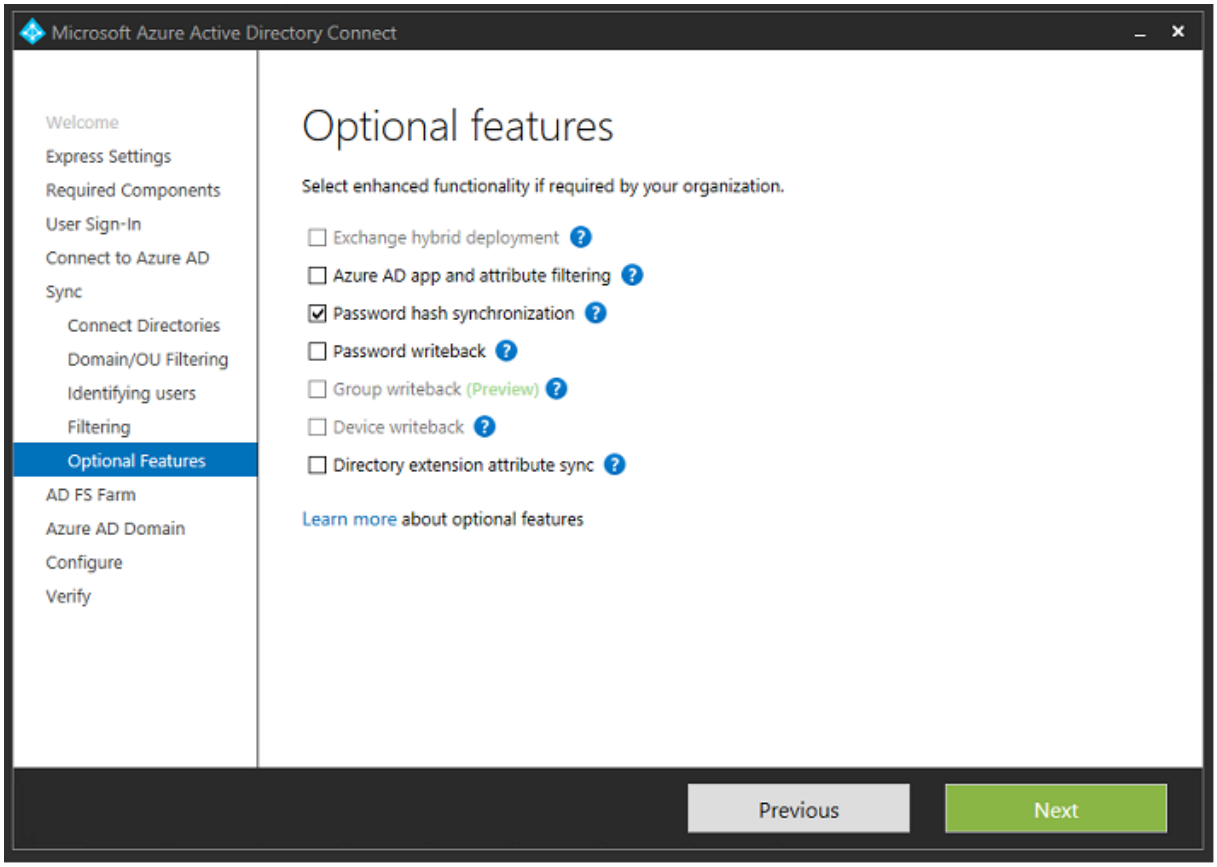

Accept the default filtering options, or restrict users and devices to a particular set of groups.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



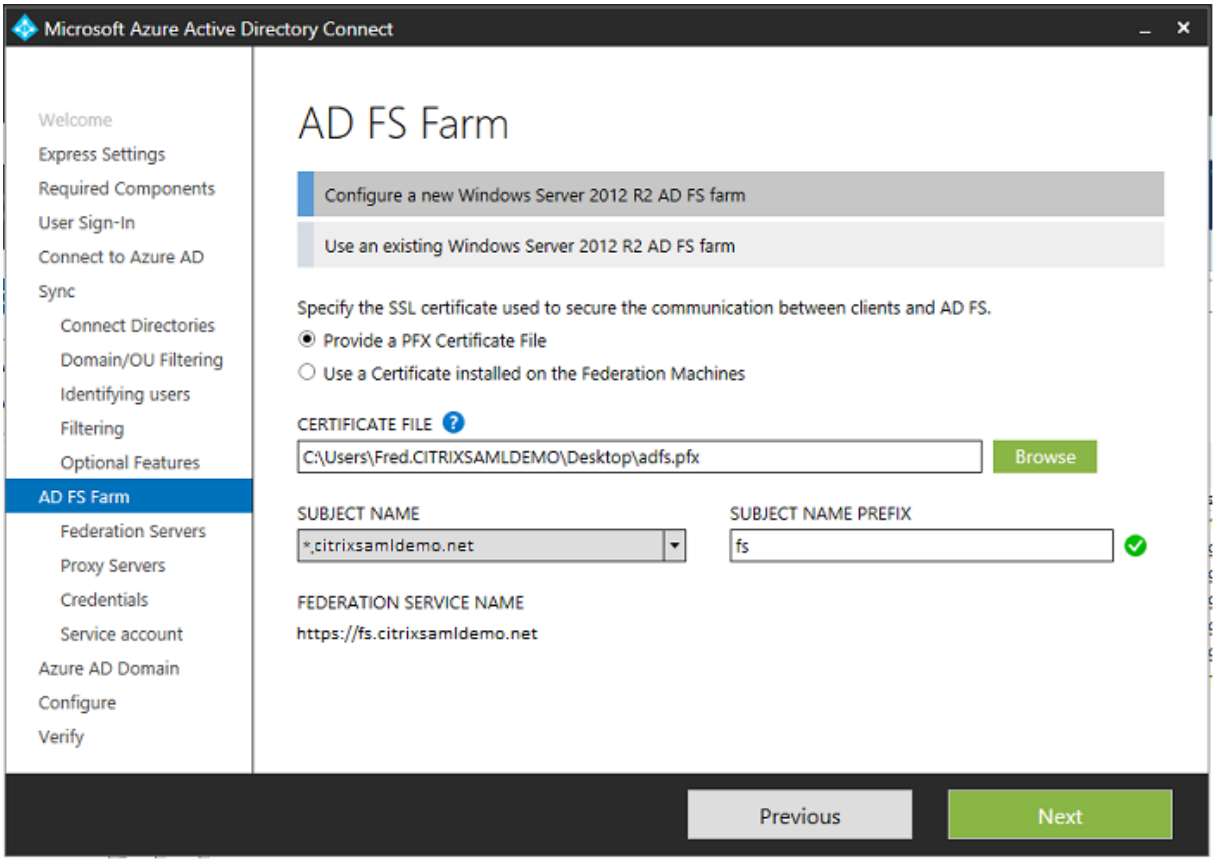

If desired, you can synchronize the Azure AD passwords with Active Directory. This is usually not required for ADFS-based authentication.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



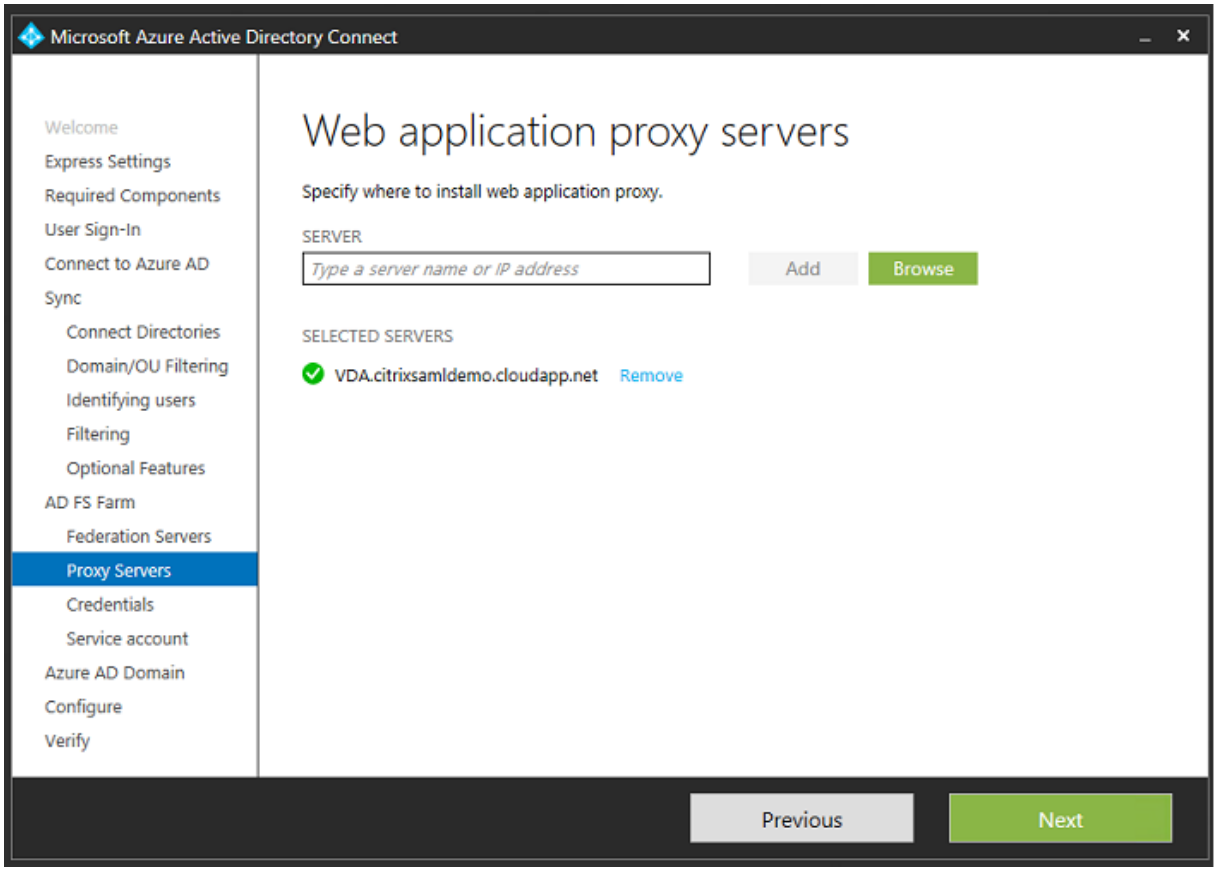

Select the certificate PFX file to use in AD FS, specifying fs.citrixsamldemo.net as the DNS name.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




When prompted to select a proxy server, enter the address of the wap.citrixsamldemo.net server. You may need to run the **Enable-PSRemoting** –**Force** cmdlet as an administrator on the Web Application Proxy server, so that Azure AD Connect can configure it.

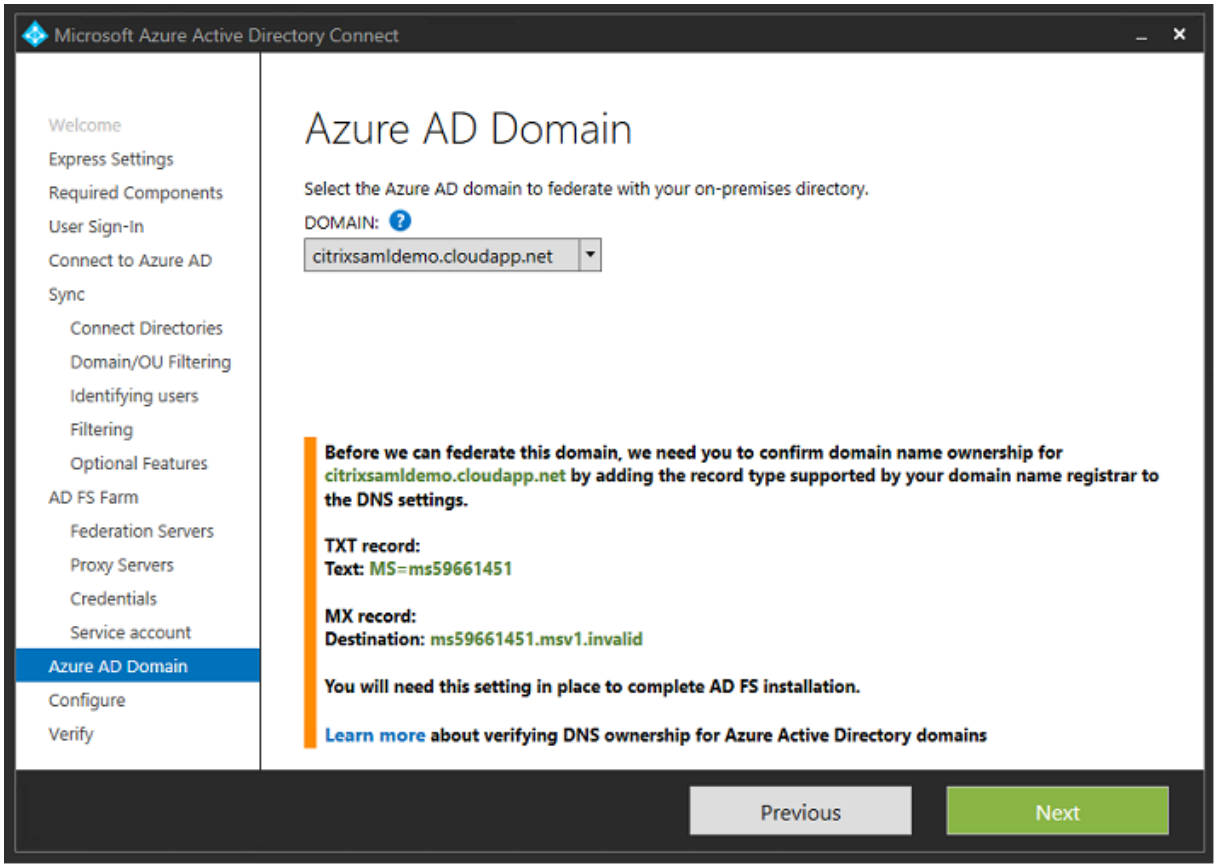
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



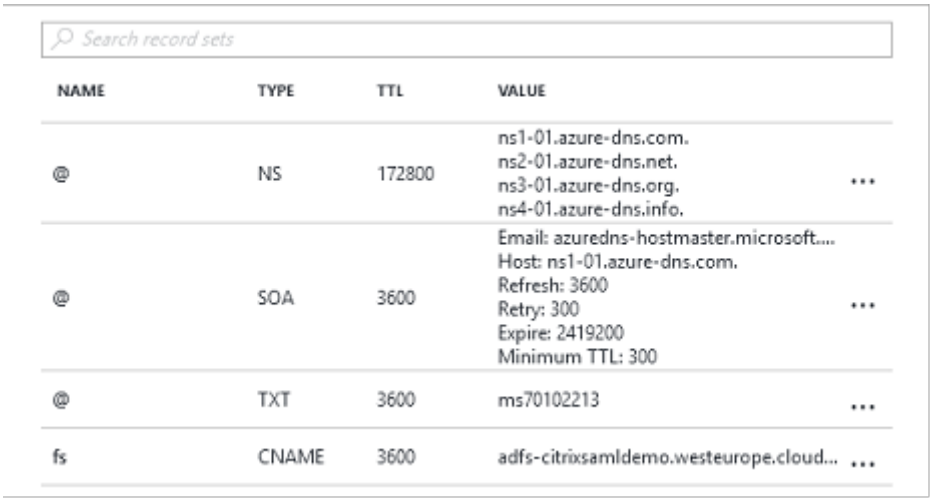

**Note:** If this step fails due to Remote PowerShell trust problems, try joining the Web Application Proxy server to the domain.

For the remaining steps of the wizard, use the standard administrator passwords, and create a service account for ADFS. Azure AD Connect will then prompt to validate the ownership of the DNS zone.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

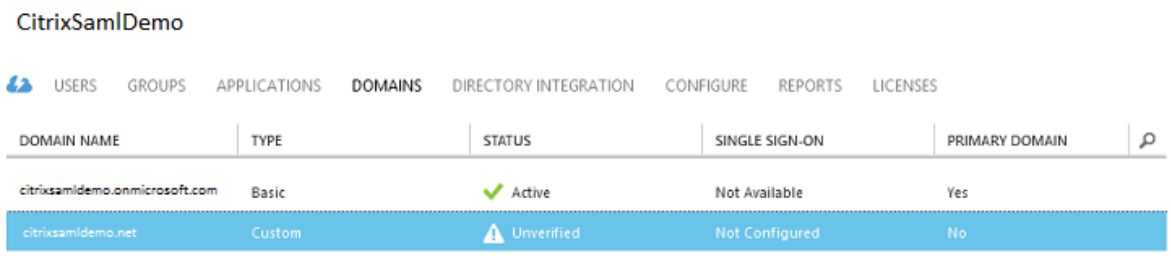



Add the TXT and MX records to the DNS address records in Azure.



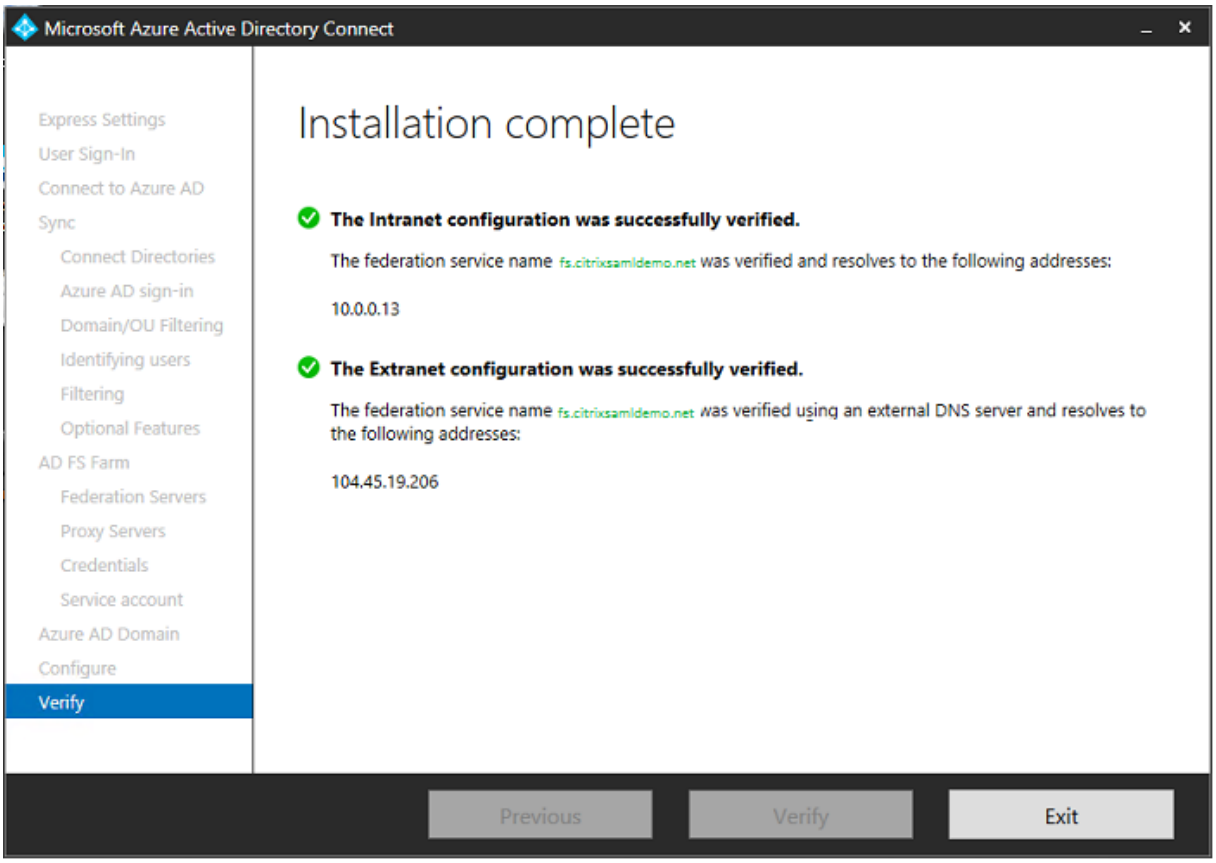

Click **Verify** in the Azure Management Console.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Note:** If this step fails, you can verify the domain before running Azure AD Connect.

When complete, the external address fs.citrixsamldemo.net is contacted over port 443.

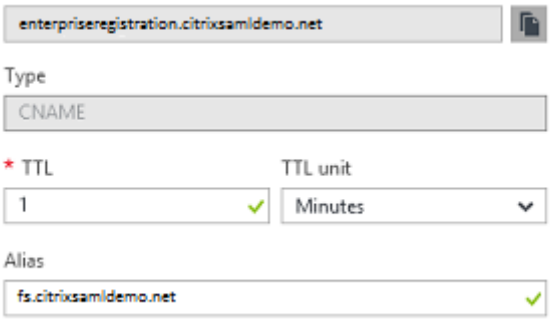



### Enable Azure AD Join

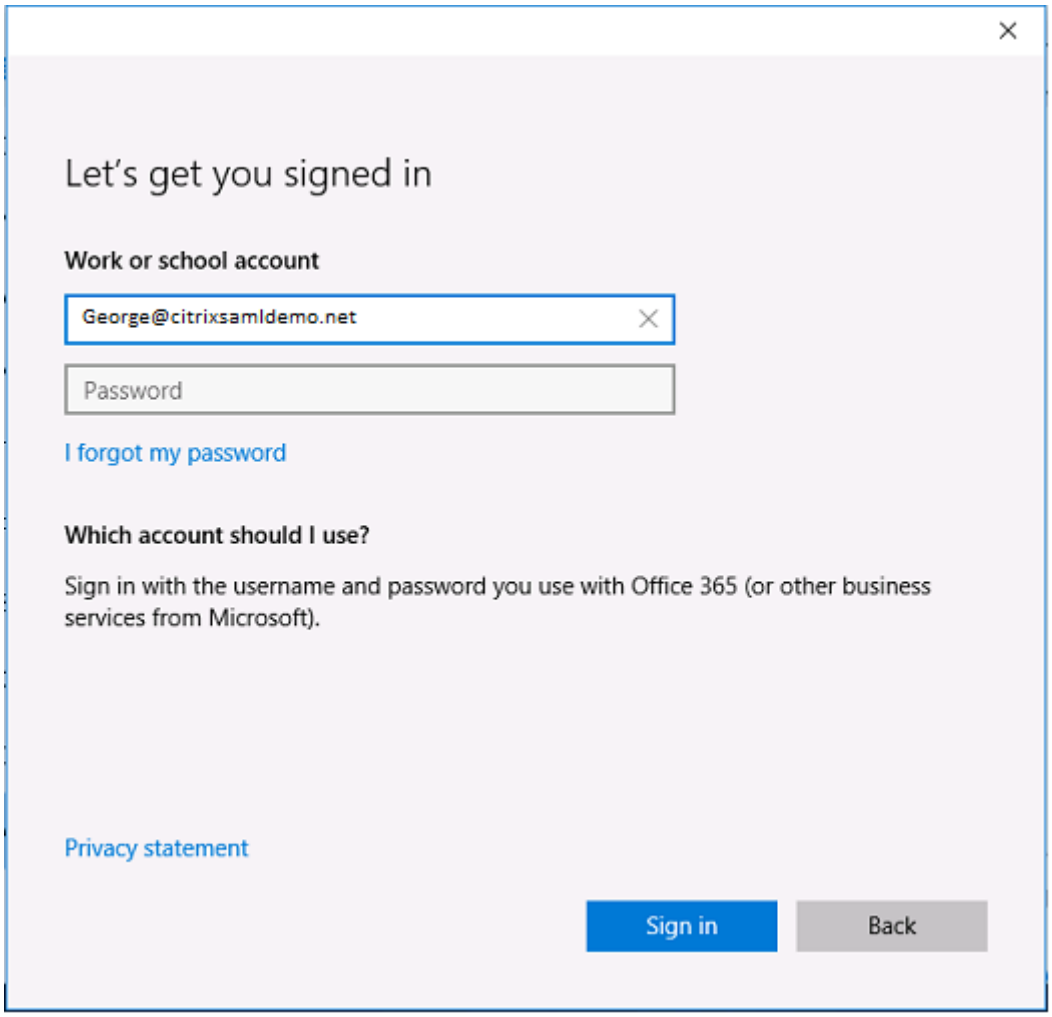
When a user enters an email address so that Windows 10 can perform Azure AD join, the DNS suffix is used to construct a CNAME DNS record that should point to ADFS: enterpriseregistration.<upnsuffix>.

In the example, this is fs.citrixsamldemo.net.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

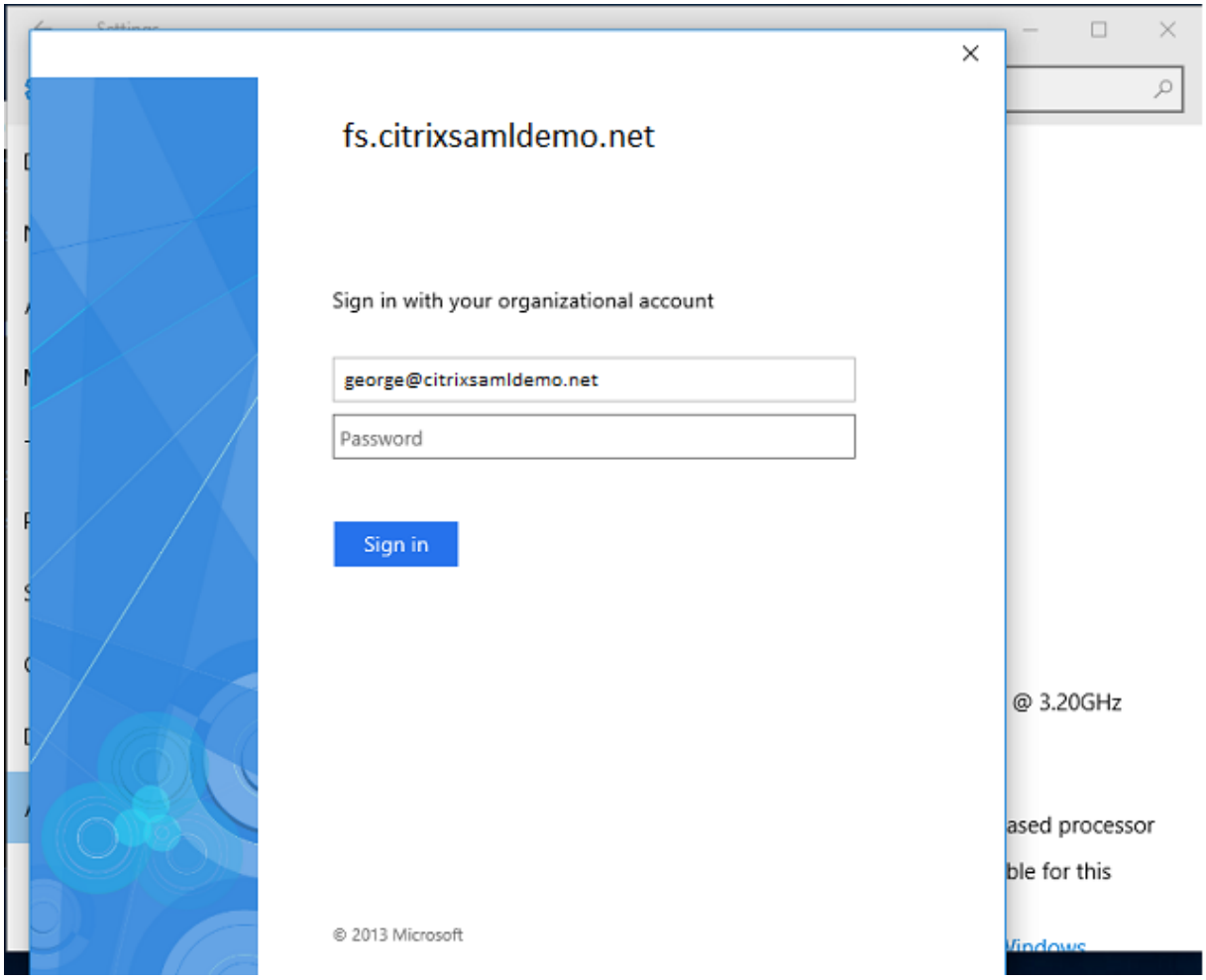


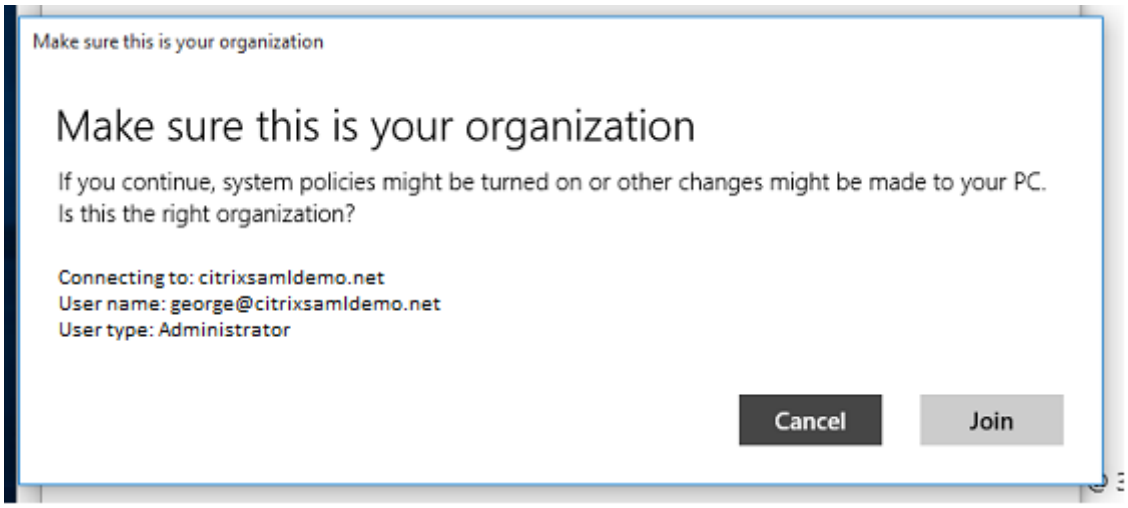

If you are not using a public CA, ensure that the ADFS root certificate is installed on the Windows 10 computer so that Windows trusts the ADFS server. Perform an Azure AD domain join using the standard user account generated earlier.



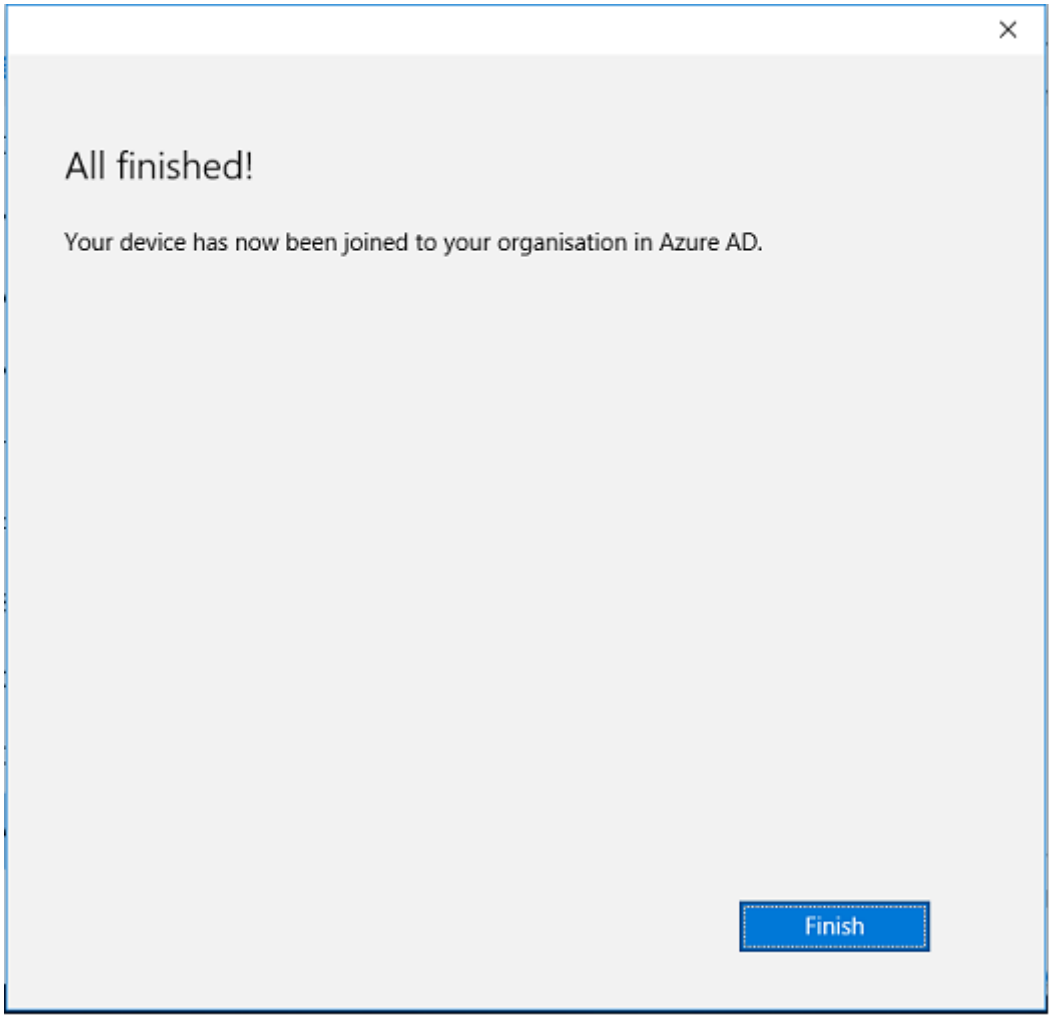

Note that the UPN must match the UPN recognized by the ADFS domain controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



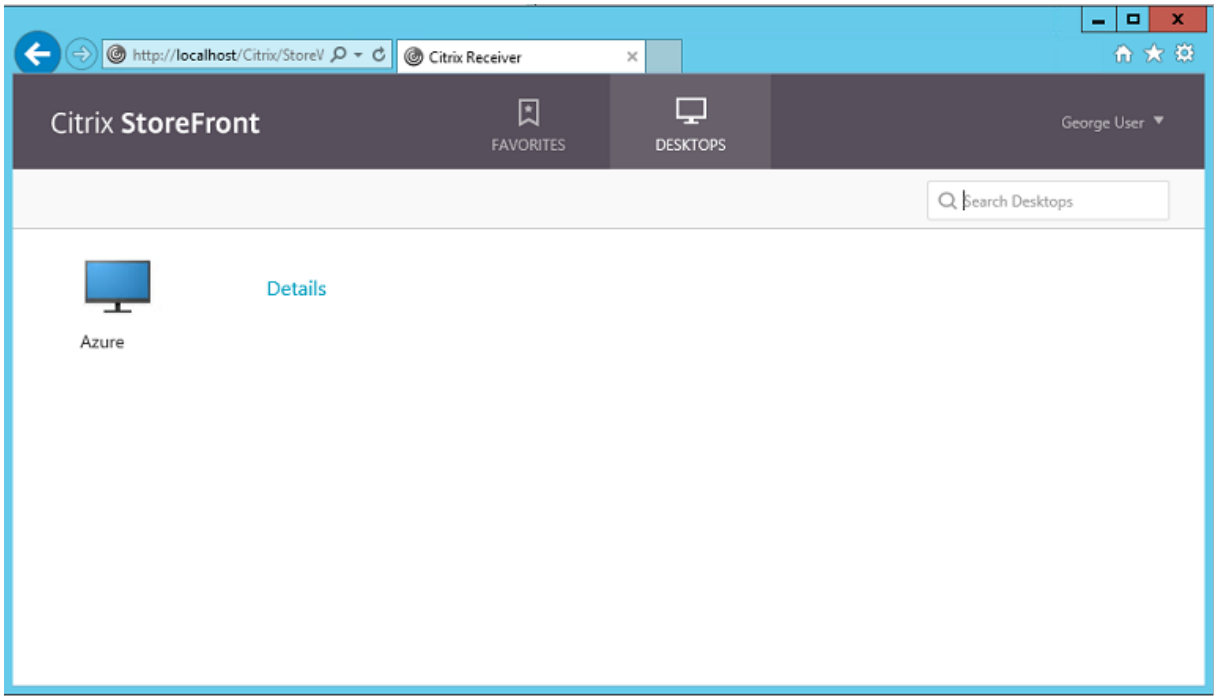

Verify that the Azure AD join was successful by restarting the machine and logging on, using the user's email address. When logged on, launch Microsoft Edge and connect to https://myapps.microsoft.com. The web site should use single sign-on automatically.

### Install XenApp or XenDesktop

You can install the Delivery Controller and VDA virtual machines in Azure directly from the XenApp or XenDesktop ISO in the usual way.

In this example, StoreFront is installed on the same server as the Delivery Controller. The VDA is installed as a standalone Windows 2012 R2 RDS worker, without integrating with Machine Creation Services (although that can optionally be configured). Check that the user George@citrixsamldemo.net can authenticate with a password, before continuing.

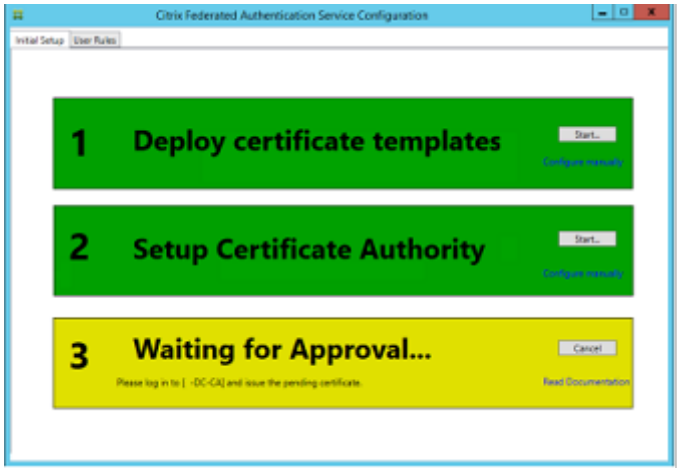
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



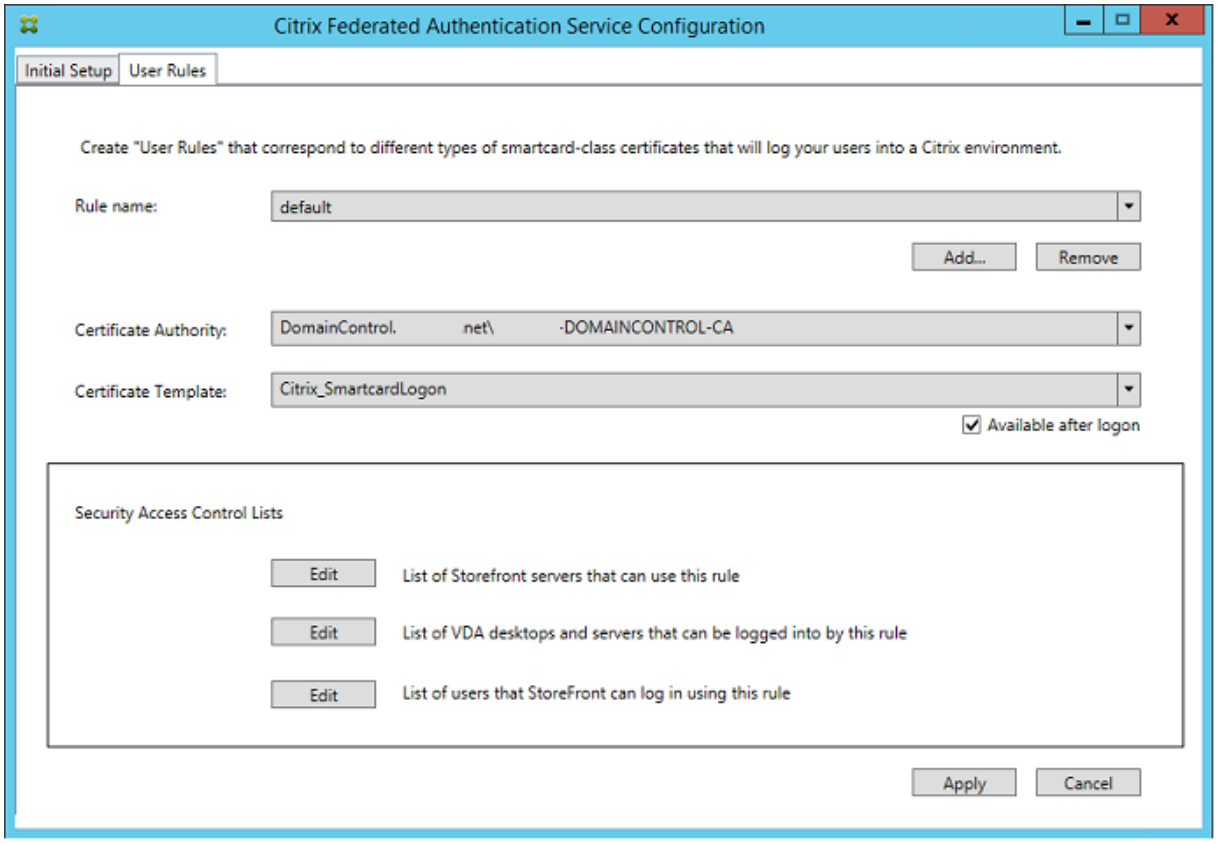

Run the **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet on the Controller to allow StoreFront to authenticate without the users' credentials.

### Install the Federated Authentication Service

Install the Federated Authentication Service (FAS) component on the ADFS server and configure a rule for the Controller to act as a trusted StoreFront.

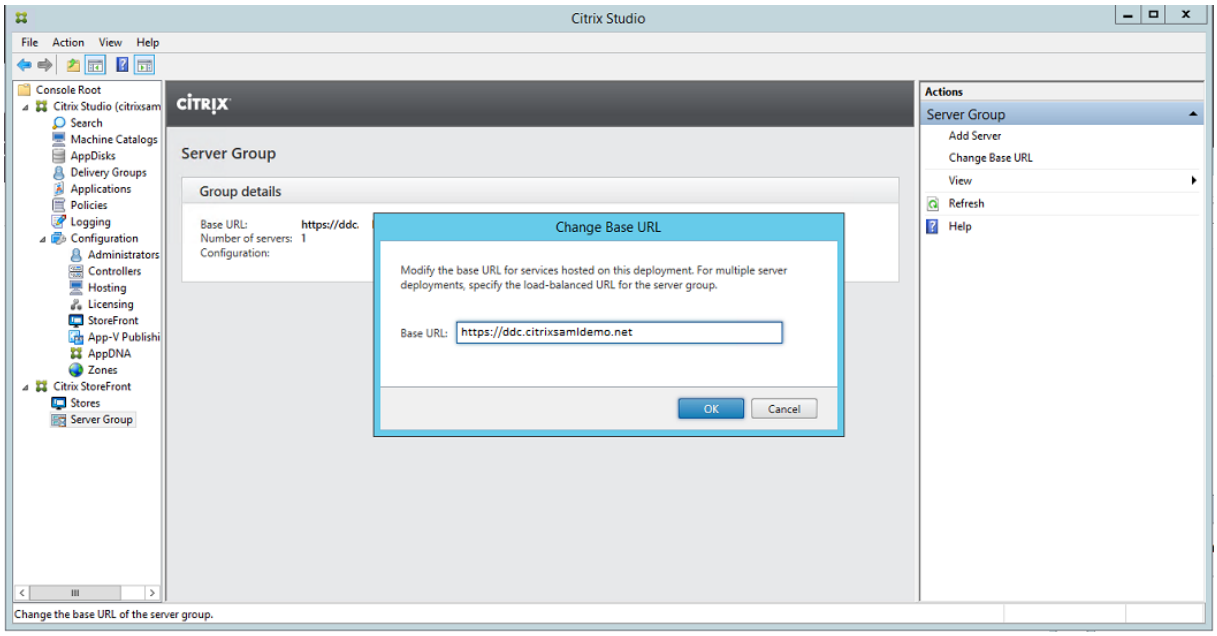



© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



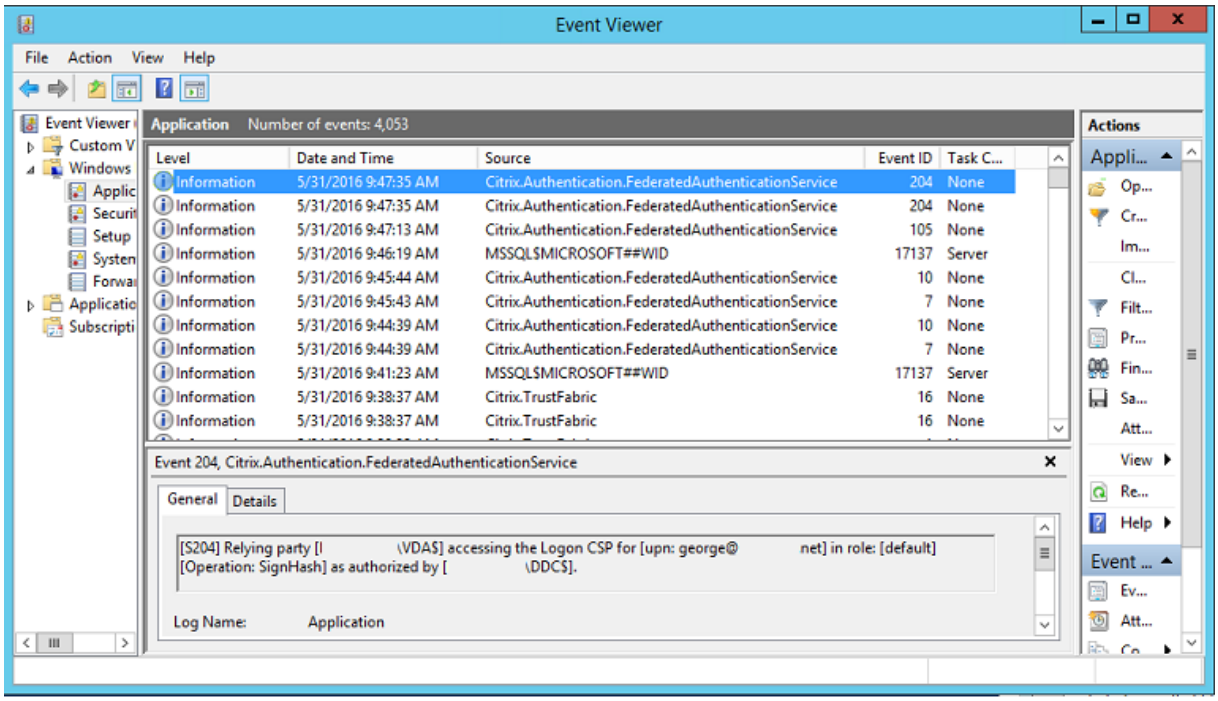

### Configure StoreFront

Request a computer certificate for the Delivery Controller, and configure IIS and StoreFront to use HTTPS by setting an IIS binding for port 443, and changing the StoreFront base address to https:.



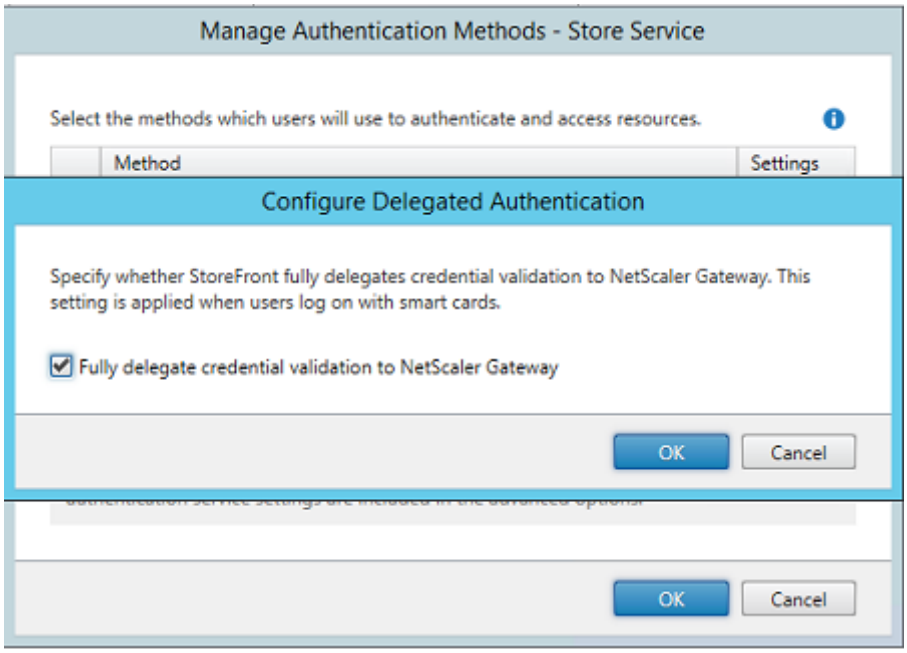

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Configure StoreFront to use the FAS server (use the PowerShell script in the Federated Authentication Service article), and test internally within Azure, ensuring that the logon uses the FAS by checking the event viewer on the FAS server.



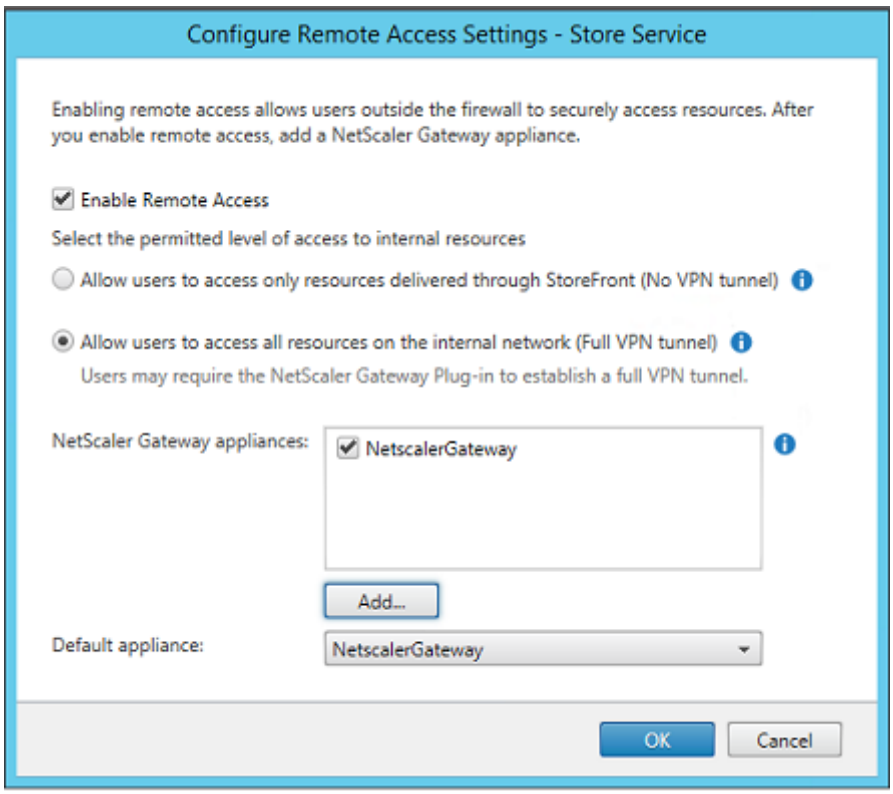

### Configure StoreFront to use NetScaler

Using the **Manage Authentication Methods** GUI in the StoreFront management console, configure StoreFront to use NetScaler to perform authentication.



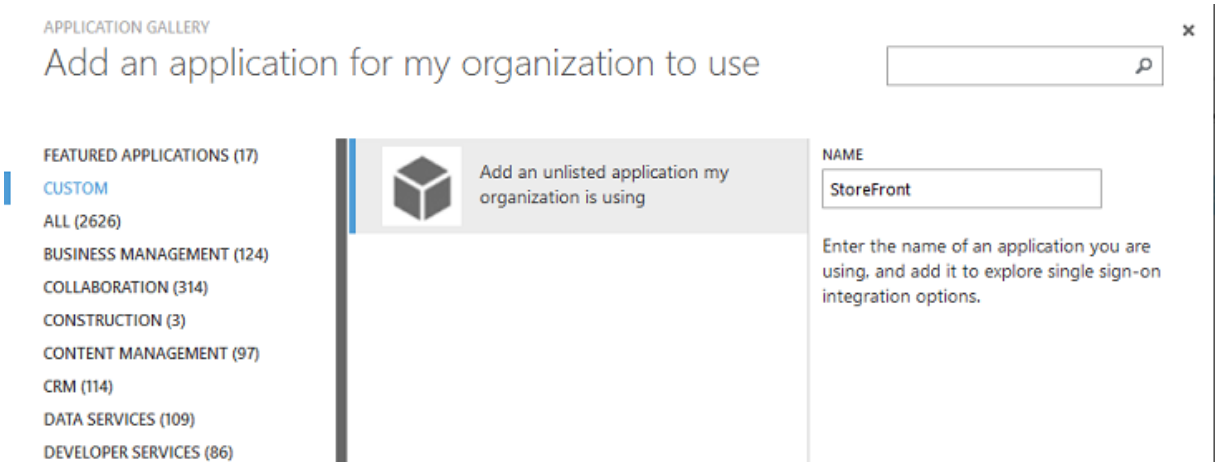

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To integrate NetScaler authentication options, configure a Secure Ticket Authority (STA) and configure the NetScaler Gateway address.




### Configure a new Azure AD application for Single Sign-on to StoreFront

This section uses the Azure AD SAML 2.0 Single Sign-on features, which currently require an Azure Active Directory Premium subscription. In the Azure AD management tool, select **New Application**, choosing **Add an application from the Gallery**.




Select **CUSTOM > Add an unlisted application my organization is using** to create a new custom

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

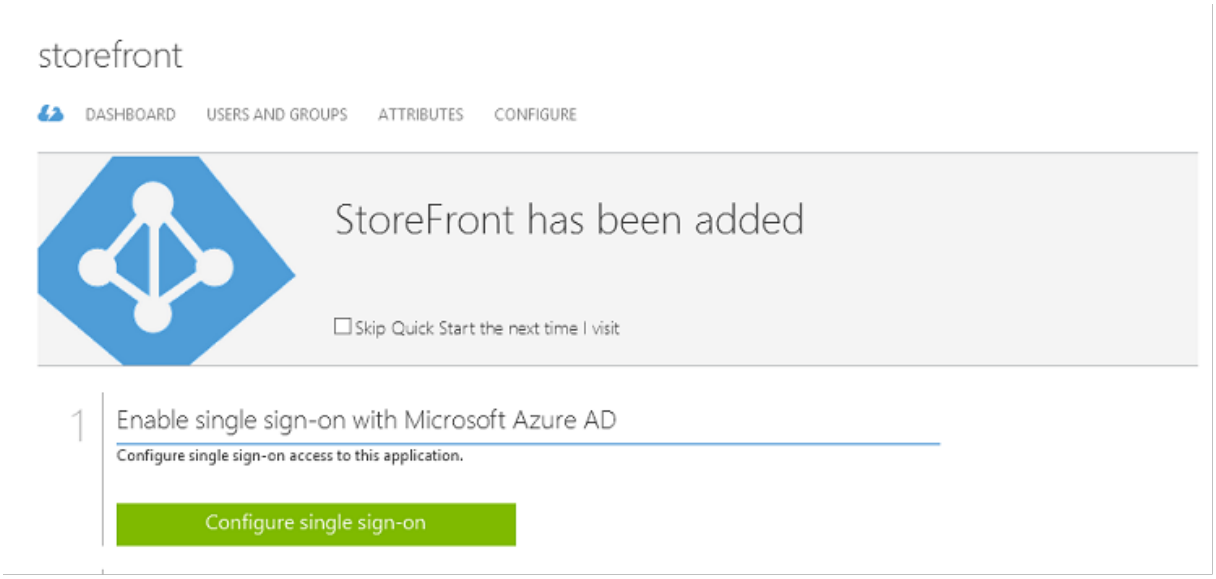
application for your users.

### Configure an icon

Create an image 215 by 215 pixels in size and upload it on the CONFIGURE page to use as an icon for the application.

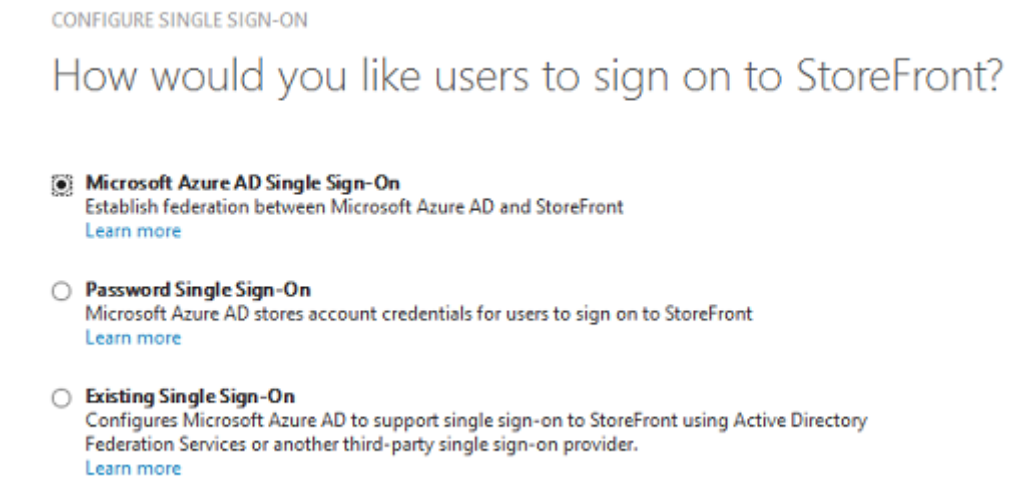
### Configure SAML authentication

Return to the Application dashboard overview page and select **Configure Single sign-on**.

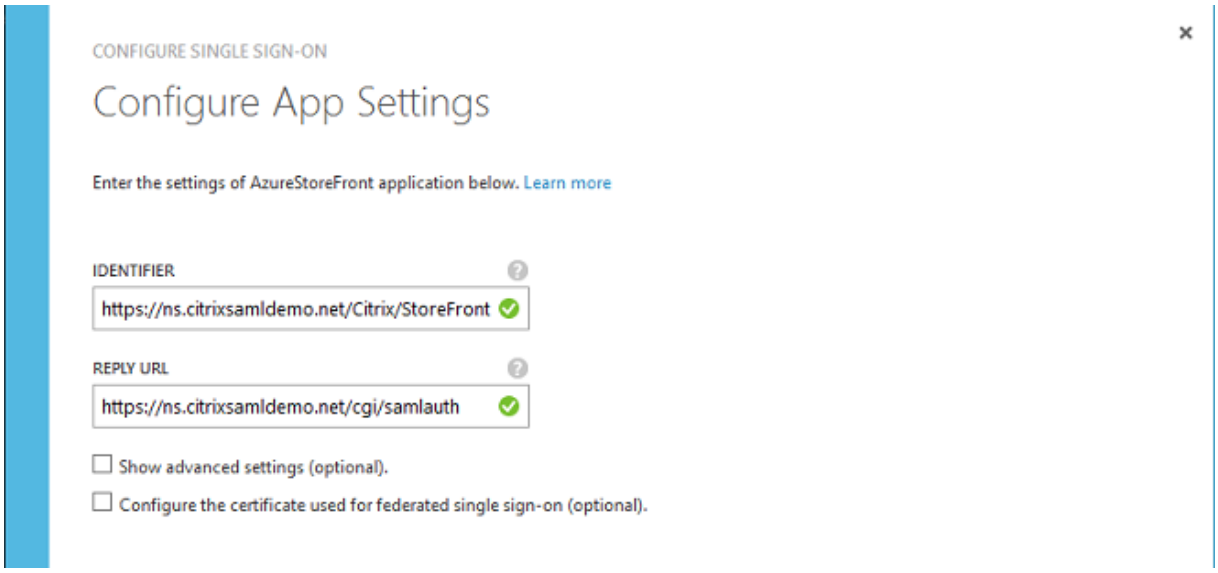



This deployment will use SAML 2.0 authentication, which corresponds to **Microsoft Azure AD Single Sign-On**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

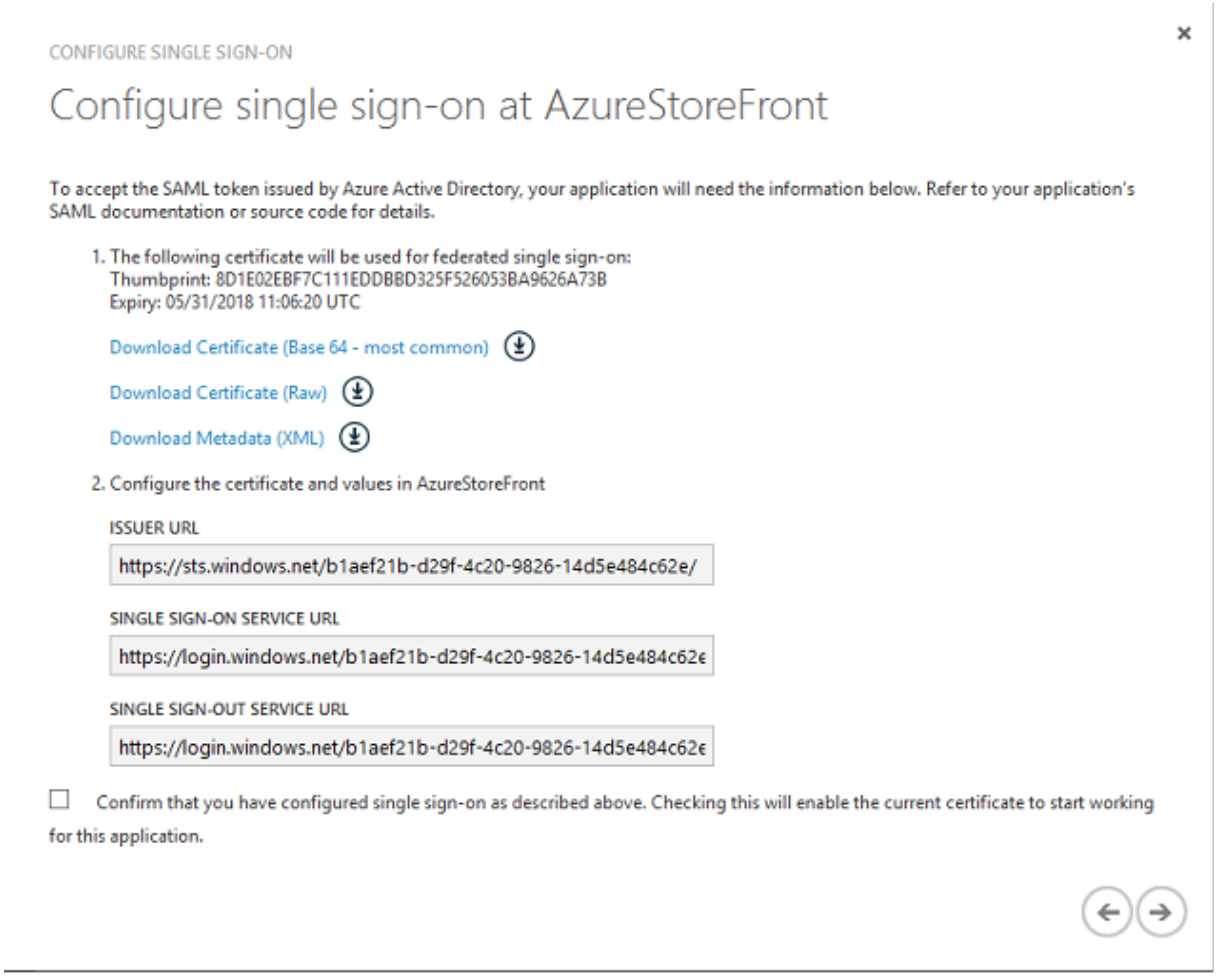



The **Identifier** can be an arbitrary string (it must match the configuration provided to NetScaler); in this example, the **Reply URL** is /cgi/samlauth on the NetScaler server.




The next page contains information that is used to configure NetScaler as a relying party to Azure AD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

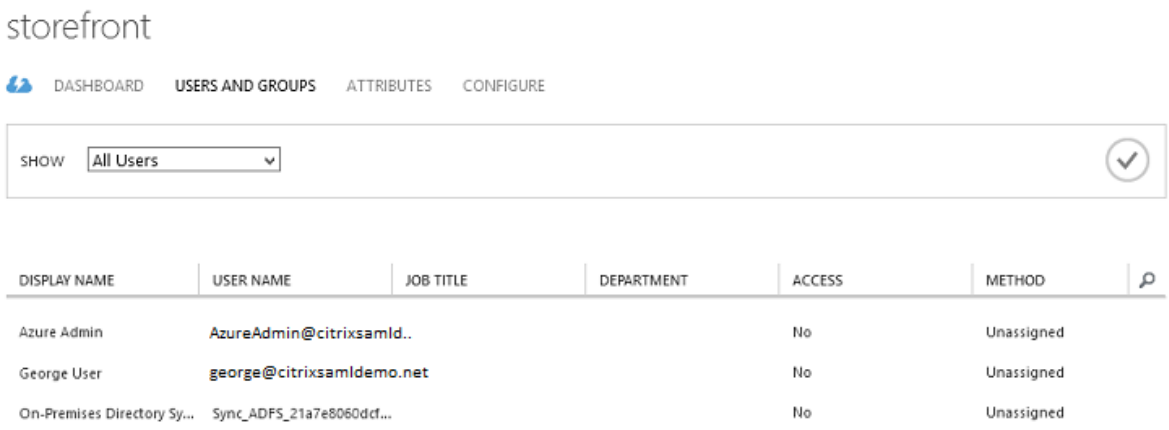



Download the base 64 trusted signing certificate and copy the sign-on and sign-out URLs. You will paste these in NetScaler configuration screens later.

### Assign the application to users

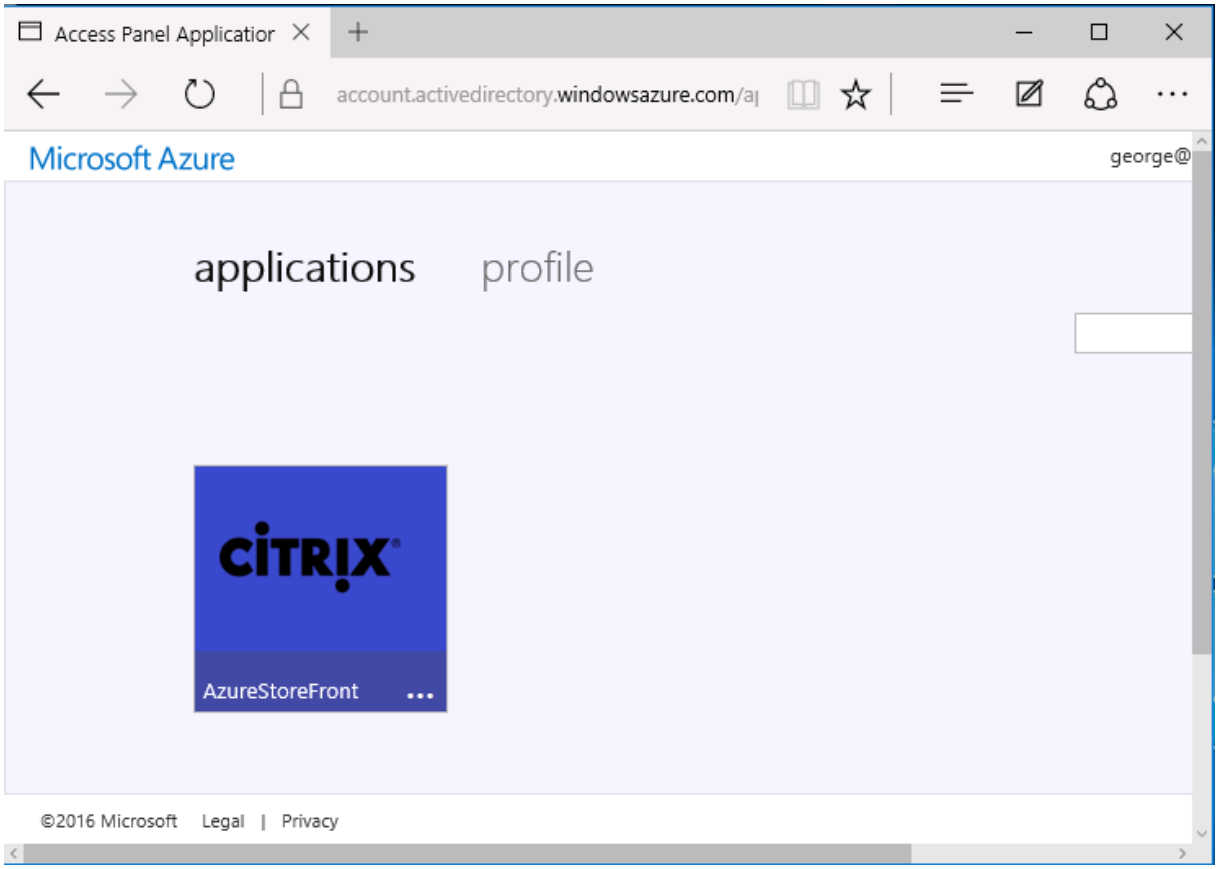
The final step is to enable the application so that it appears on users"myapps.microsoft.com"control page. This is done on the USERS AND GROUPS page. Assign access for the domain users accounts synchronized by Azure AD Connect. Other accounts can also be used, but they must be explicitly mapped because they do not conform to the <user>@<domain> pattern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**MyApps page**

When the application has been configured, it appears on the users'lists of Azure applications when they visit https://myapps.microsoft.com.

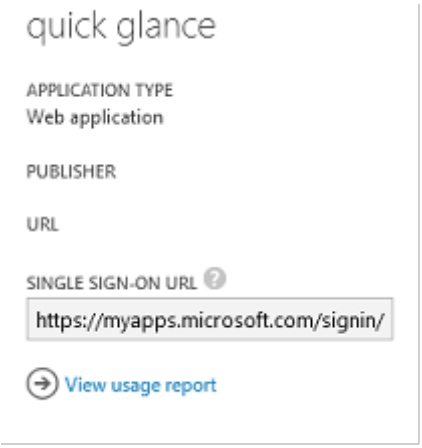



When it is Azure AD joined, Windows 10 supports single sign-on to Azure applications for the user who logs on. Clicking the icon takes the browser to the SAML cgi/samlauth web page that was configured earlier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Single sign-on URL

Return to the application in the Azure AD dashboard. There is now a single sign-on URL available for the application. This URL is used to provide web browser links or to create Start menu shortcuts that take users directly into StoreFront.




Paste this URL into a web browser to ensure that you are redirected by Azure AD to the NetScaler cgi/samlauth web page configured earlier. This works only for users who have been assigned, and will provide single sign-on only for Windows 10 Azure AD-joined logon sessions. (Other users will be prompted for Azure AD credentials.)

### Install and configure NetScaler Gateway

To remotely access the deployment, this example uses a separate VM running NetScaler. This can be purchased from the Azure Store. This example uses the "Bring your own License"version of NetScaler 11.0.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

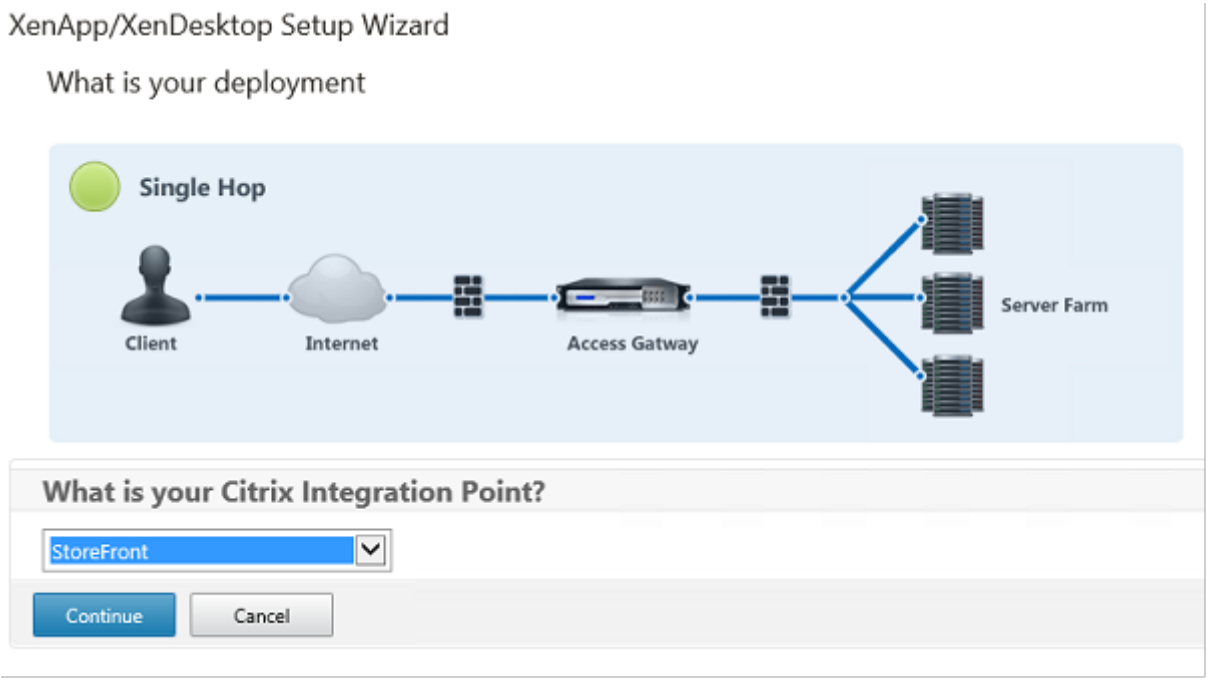
Log on to the NetScaler VM, pointing a web browser to the internal IP address, using the credentials specified when the user authenticated. Note that you must change the password of the nsroot user in an Azure AD VM.

Add licenses, selecting **reboot** after each license file is added, and point the DNS resolver to the Microsoft domain controller.

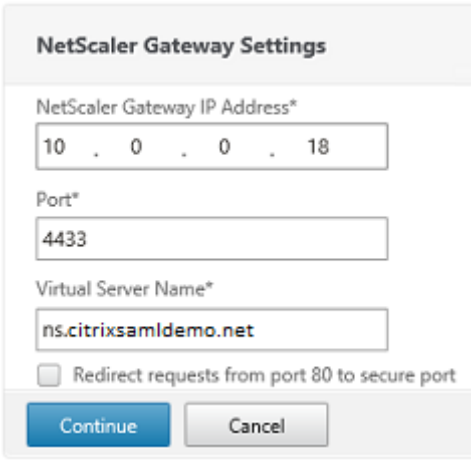
#### Run the XenApp and XenDesktop setup wizard

This example starts by configuring a simple StoreFront integration without SAML. After that deployment is working, it adds a SAML logon policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

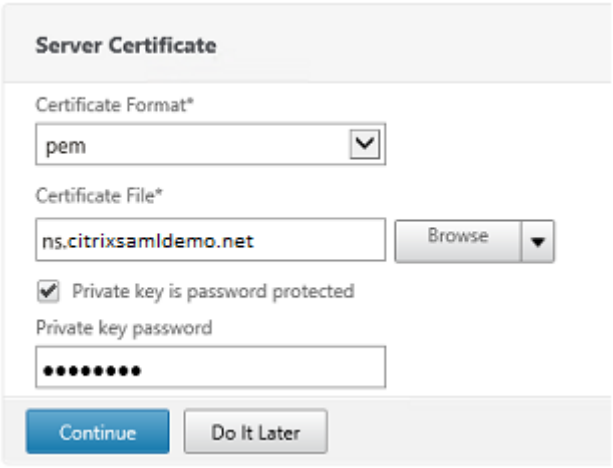



Select the standard NetScaler StoreFront settings. For use in Microsoft Azure, this example configures port 4433, rather than port 443. Alternatively, you can port-forward or remap the NetScaler administrative web site.



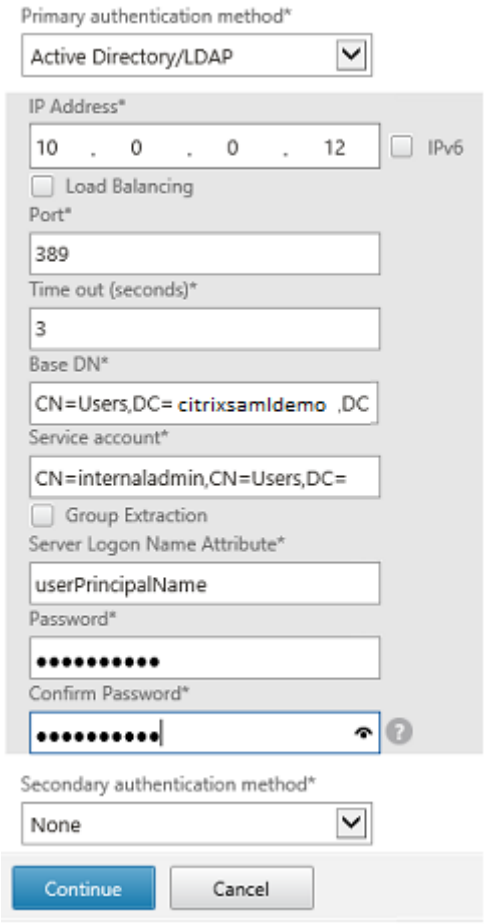

For simplicity, the example uploads an existing server certificate and private key stored in a file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Configure the domain controller for AD account management

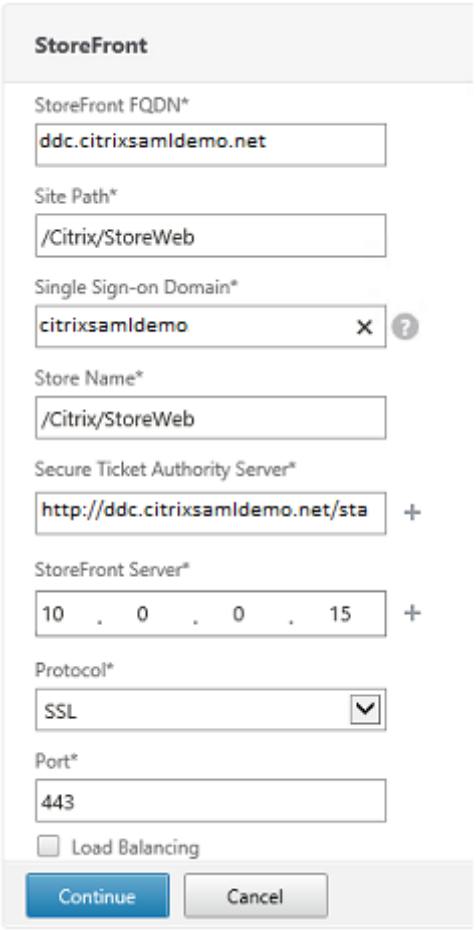
The domain controller will be used for account resolution, so add its IP address into the primary authentication method. Note the formats expected in each field in the dialog box.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

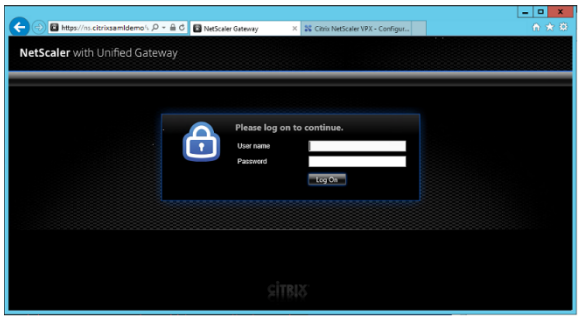
### Configure the StoreFront address

In this example, StoreFront has been configured using HTTPS, so select the SSL protocol options.




### Verify the NetScaler deployment

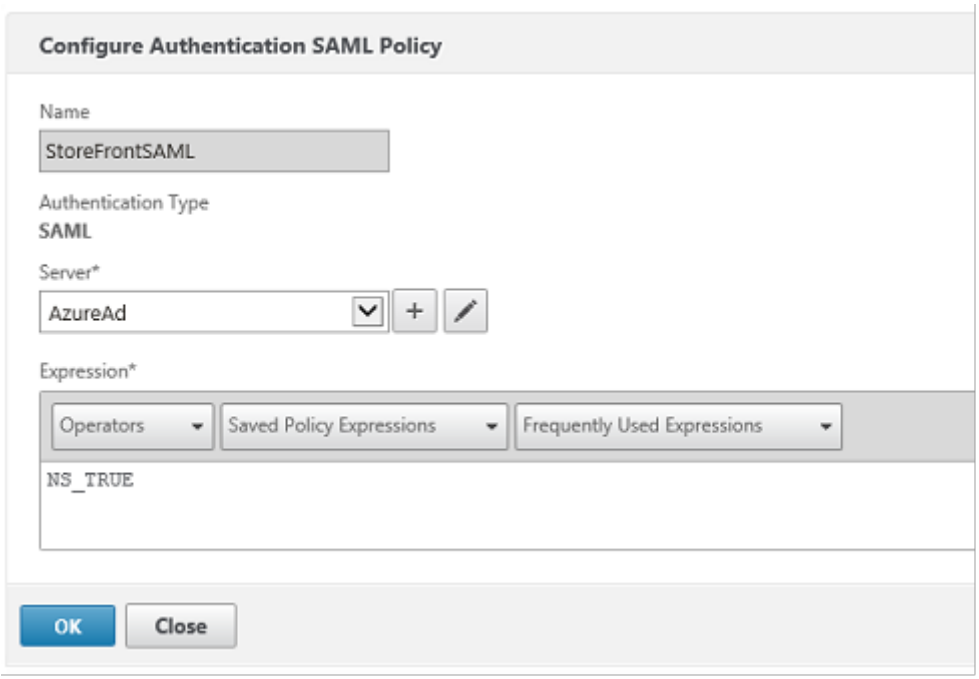
Connect to NetScaler and check that authentication and launch are successful with the username and password.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

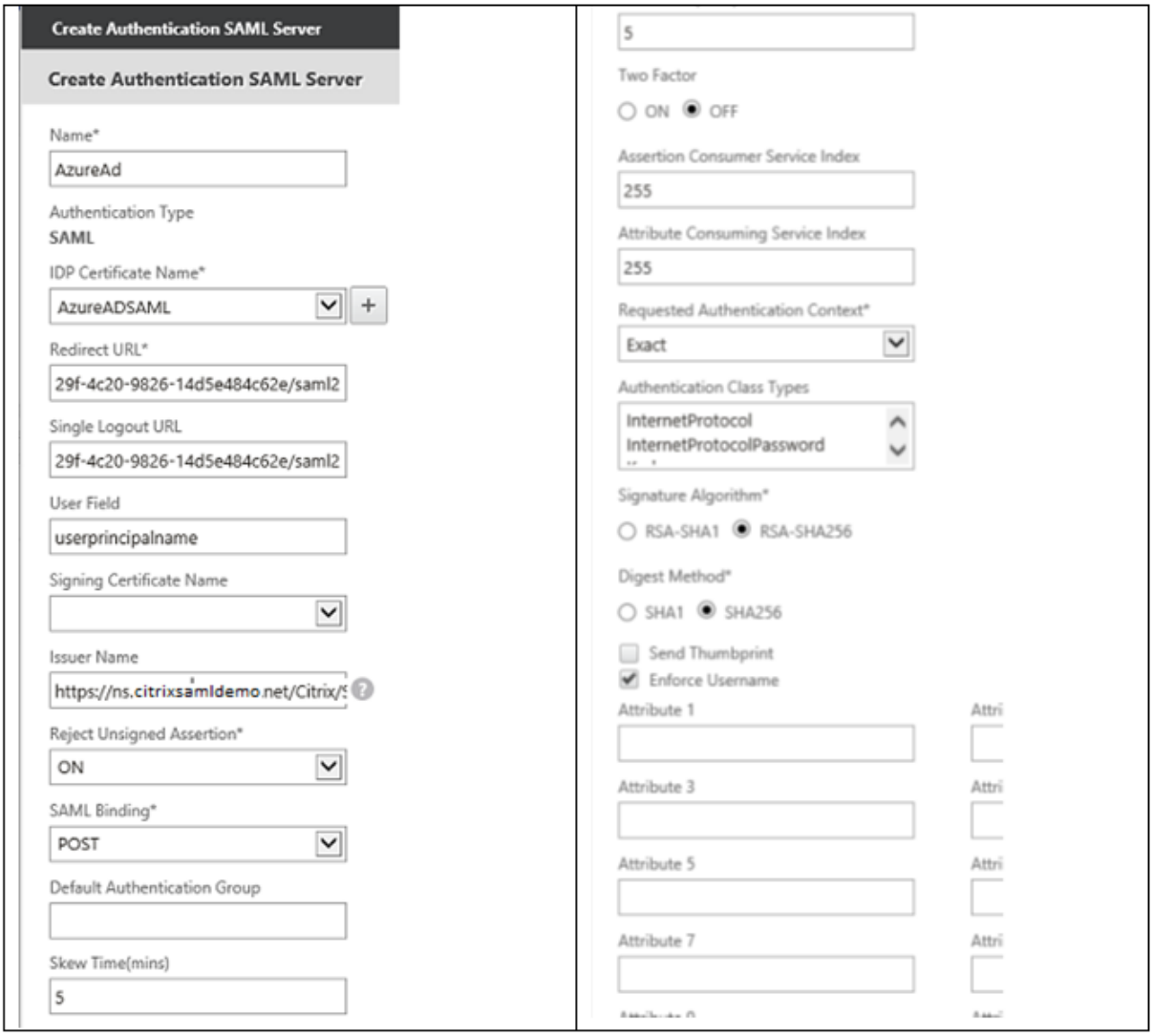
### Enable NetScaler SAML authentication support

Using SAML with StoreFront is similar to using SAMl with other web sites. Add a new SAML policy, with an expression of **NS_TRUE**.




Configure the new SAML IdP server, using information obtained from Azure AD earlier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

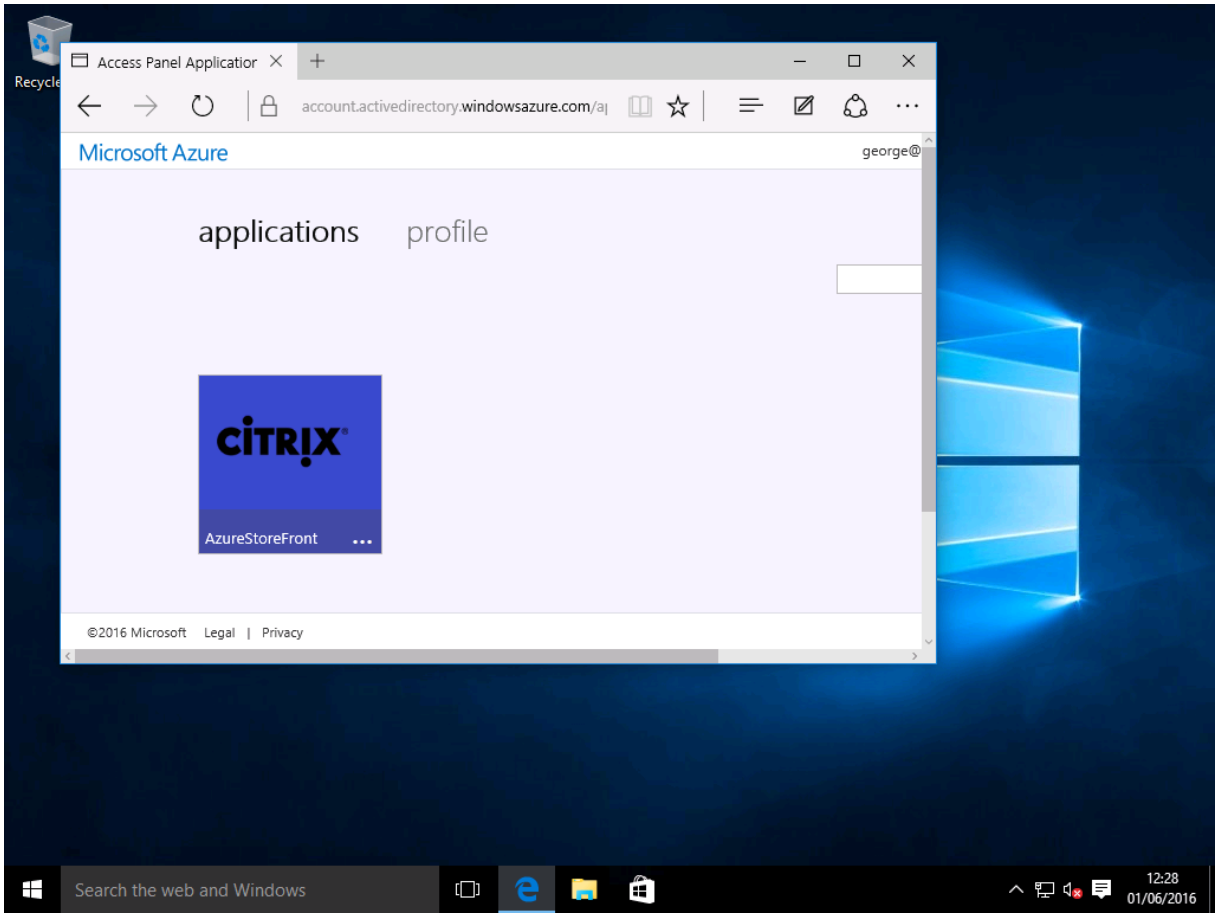



## Verify the end-to-end system

Log on to an Azure AD Joined Windows 10 desktop, using an account registered in Azure AD. Launch Microsoft Edge and connect to: https://myapps.microsoft.com.

The web browser should display the Azure AD applications for the user.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Verify that clicking the icon redirects you to an authenticated StoreFront server.

Similarly, verify that direct connections using the Single Sign-on URL and a direct connection to the NetScaler site redirect you to Microsoft Azure and back.

Finally, verify that non-Azure AD joined machines also function with the same URLs (although there will be a single explicit sign-on to Azure AD for the first connection).

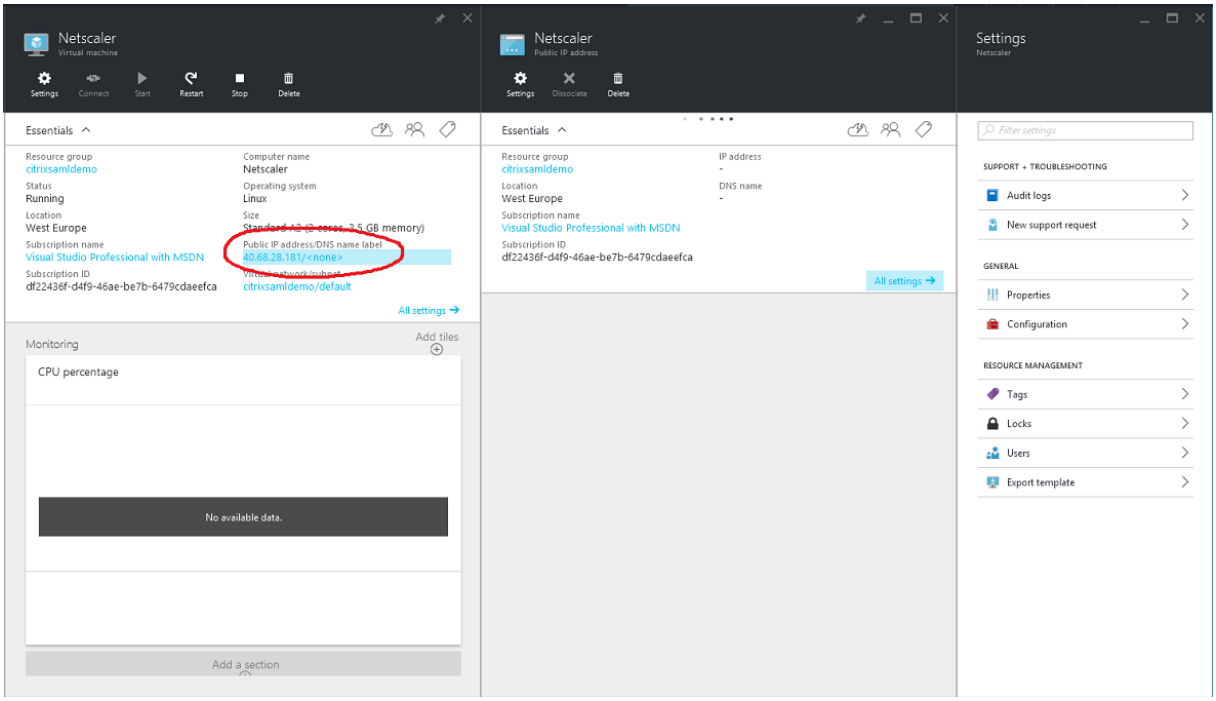
## Appendix

Several standard options should be configured when setting up a VM in Azure.

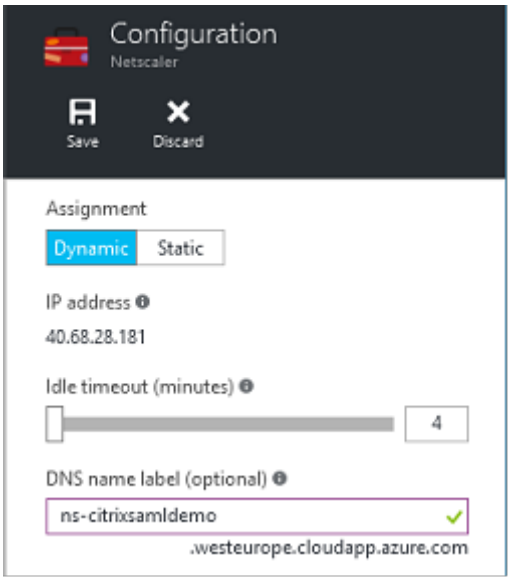
### Provide a public IP address and DNS address

Azure gives all VMs an IP address on the internal subnet (10.*.*.* in this example). By default a public IP address is also supplied, which can be referenced by a dynamically updated DNS label.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Select **Configuration** of the **Public IP address/DNS name label**. Choose a public DNS address for the VM. This can be used for CNAME references in other DNS zone files, ensuring that all DNS records remain correctly pointing to the VM, even if the IP address is reallocated.



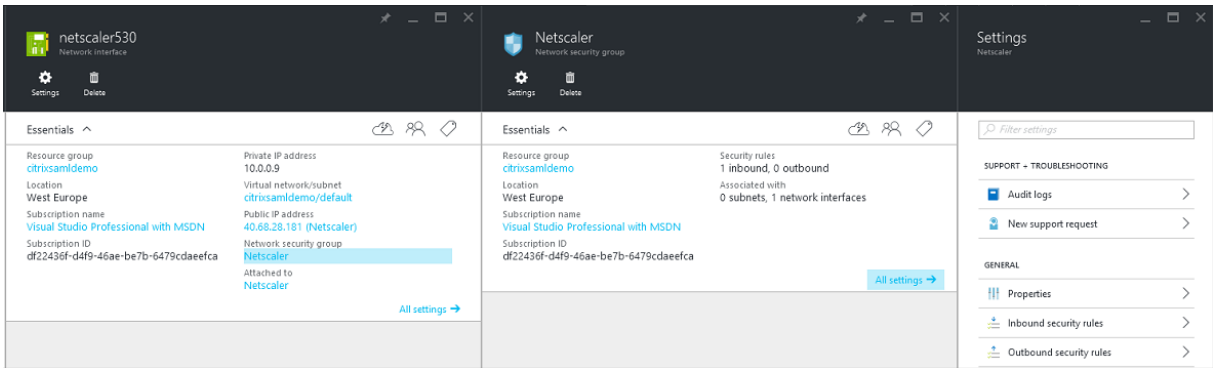

### Set up firewall rules (security group)

Each VM in a cloud has a set of firewall rules applied automatically, known as the security group. The security group controls traffic forwarded from the public to the private IP address. By default, Azure allows RDP to be forwarded to all VMs. The NetScaler and ADFS servers must also need to forward TLS

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

traffic (443).

Open **Network Interfaces** for a VM, and then click the **Network Security Group** label. Configure the **Inbound security rules** to allow appropriate network traffic.




### Related information

- The Federated Authentication Service article is the primary reference for FAS installation and configuration.
- The common FAS deployments are summarized in the Federated Authentication Service architectures overview article.
- "How-to"articles are introduced in the Federated Authentication Service configuration and management article.

## Federated Authentication System how-to: configuration and management

June 16, 2021

The following "how-to"articles provide advanced configuration and management guidance for the Federated Authentication System (FAS):

- Private key protection
- Certificate authority configuration
- Security and network management
- Troubleshoot Windows logon issues
- PowerShell SDK cmdlet help files

Related information:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The primary reference for FAS installation and initial setup is the Federated Authentication Service article.
- The Federated Authentication Service architectures overview article provides summaries of the major FAS architectures, plus links to other articles about the more complex architectures.

## Federated Authentication Service certificate authority configuration

November 3, 2021

This article describes the advanced configuration of the Citrix Federated Authentication Service (FAS) to integrate with certificate authority (CA) servers that are not supported by the FAS administration console. The instructions use PowerShell APIs provided by FAS. You should have a basic knowledge of PowerShell before executing any instructions in this article.

### Set up multiple CA servers for use in FAS

This section describes how to set up a single FAS server to use multiple CA servers to issue certificates. This allows load balancing and failover of the CA servers.

#### Step 1: Find out how many CA servers FAS is able to locate

Use the Get-FASMsCertificateAuthority cmdlet to determine which CA servers FAS can connect to. The following example shows that FAS can connect to three CA servers.

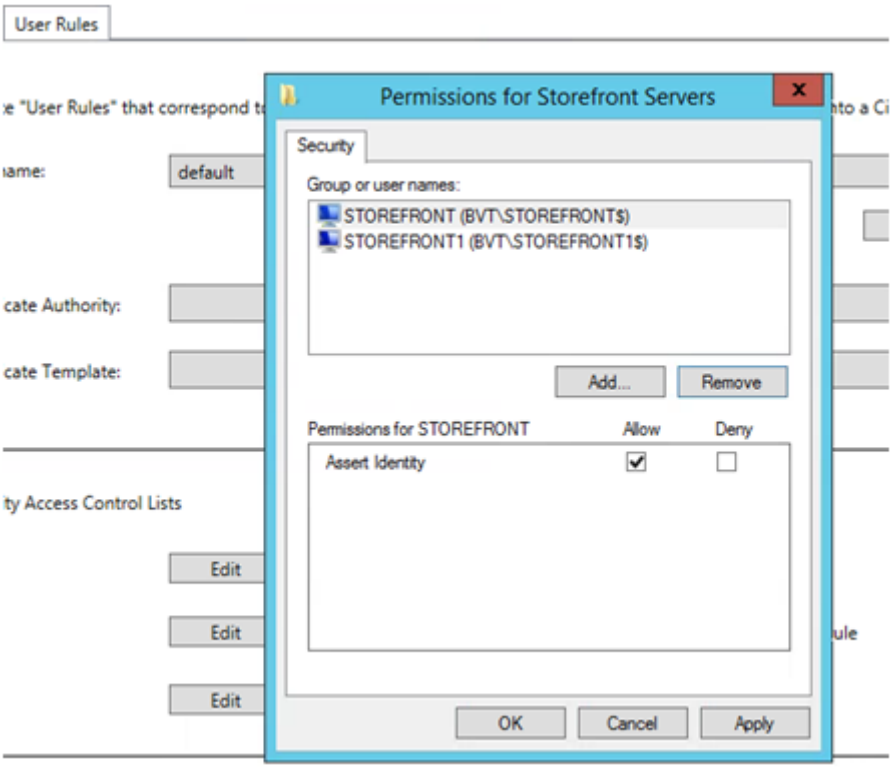
```
PS > Add-PSSnapin Citrix*
PS > Get-FasMsCertificateAuthority

Address                        IsDefault   PublishedTemplates
-------                        ---------   ------------------

DC1.bvt.local\bvt-DC1-CA       False       {
 Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local    False       {
 Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local    False       {
 Citrix_SmartcardLogon, Citrix_Regis...
```

#### Step 2: Modify the existing certificate definition

Citrix recommends that you create a role using the FAS administration console, rather than using PowerShell to create the role. This avoids the complication of having to add the SDL manually later. In

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

the following example, a role named ‘default’is created, with the access rule configured:



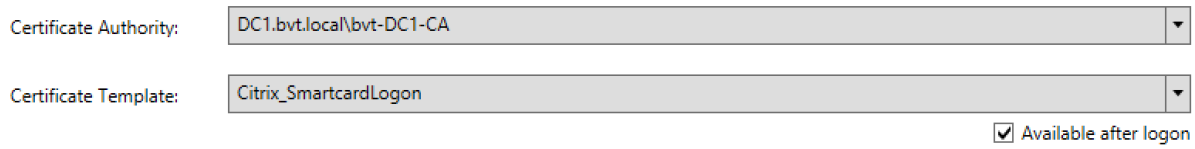

To add multiple CAs to the certificate authority field you must configure the certificate definition using PowerShell. (Adding multiple CAs is not supported from the FAS administration console in this release.)

First, you need the certificate definition name. The name cannot be determined from the administration console; use the Get-FASCertificateDefinition cmdlet.

```
PS > Get-FasCertificateDefinition

Name                          : default_Definition
CertificateAuthorities        : {
 DC1.bvt.local\bvt-DC1-CA }

MsTemplate                    : Citrix_SmartcardLogon
AuthorizationCertificate      : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids                    : {
  }

InSession                     : True
```

The UI equivalent is:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



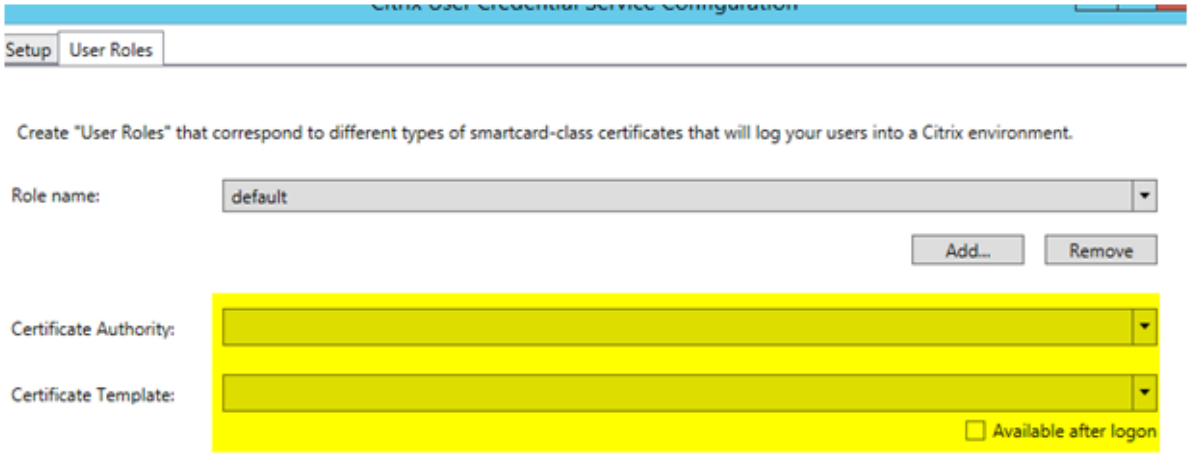

After you have the certificate definition name, modify the certificate definition to have a list of CertificateAuthorities, rather than just one:

```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

The Get-FASCertificateDefinition cmdlet now returns:

```
PS > Get-FasCertificateDefinition
Name                          : default_Definition
CertificateAuthorities        : {
 DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\
    ca2.bvt.local }

MsTemplate                    : Citrix_SmartcardLogon
AuthorizationCertificate      : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids                    : {
  }

InSession                     : True
```

After you configure multiple CA servers, the FAS administration console cannot be used to configure FAS. The 'Certificate Authority'and 'Certificate Template'fields are empty, as shown here:




> **Note:**
>
> If do you use the console to modify the access rule, your multiple CA configuration is overwritten. Just repeat step 2 to reconfigure with all the certificate authorities.

If you want to reconfigure the access rule ACLs from powershell and are unsure what values to supply,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

we suggest the following:

- Create a second rule (e.g. named “testing”), with a single CA.
- Configure the ACLs as required on the “testing”rule.
- Use PowerShell to inspect the ACL (Get-FasRule –name “testing”).
- Use PowerShell to apply the ACL to the original rule (Set-FasRule).
- Delete the “testing”rule as it is no longer needed.

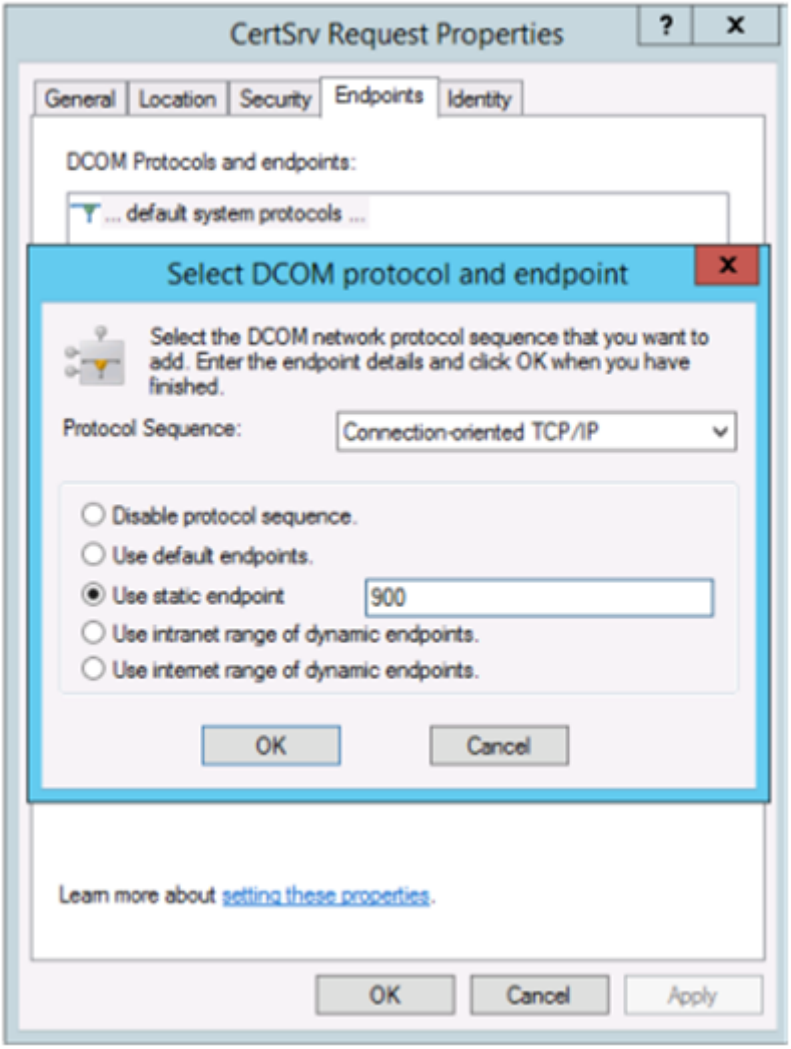
#### Expected behavior changes

After you configure the FAS server with multiple CA servers, user certificate generation is distributed among all the configured CA servers. Also, if one of the configured CA servers fails, the FAS server will switch to another available CA server.

### Configure the Microsoft CA for TCP access

By default the Microsoft CA uses DCOM for access. This can result in complexities when implementing firewall security, so Microsoft has a provision to switch to a static TCP port. On the Microsoft CA, use **Start>Run>dcomcnfg.exe** to open the DCOM configuration panel, expand *Computers>My computer>DCOM Config* to show the **CertSrv Request** node, then edit the properties of the CertSrv Request DCOM application:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Change the "Endpoints"to select a static endpoint and specify a TCP port number (900 in the graphic above).

Restart the Microsoft CA and submit a certificate request. If you run "netstat –a –n –b"you should see that certsvr is now listening on port 900:

```
 TCP    0.0.0.0:636            dc:0                   LISTENING
[lsass.exe]
 TCP    0.0.0.0:900            dc:0                   LISTENING
[certsrv.exe]
 TCP    0.0.0.0:3268           dc:0                   LISTENING
[lsass.exe]
 TCP    0.0.0.0:3269           dc:0                   LISTENING
```

There is no need to configure the FAS server (or any other machines using the CA), because DCOM has a negotiation stage using the RPC port. When a client needs to use DCOM, it connects to the DCOM RPC Service on the certificate server and requests access to a particular DCOM server. This triggers port 900 to be opened, and the DCOM server instructs the FAS server how to connect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Pre-generate user certificates

The logon time for users will significantly improve when user certificates are pre-generated within the FAS server. The following sections describe how it can be done, either for single or multiple FAS servers.

#### Get a list of Active Directory users

You can improve certificate generation by querying the AD and storing the list of users into a file (for example, a .csv file), as shown in the following example.

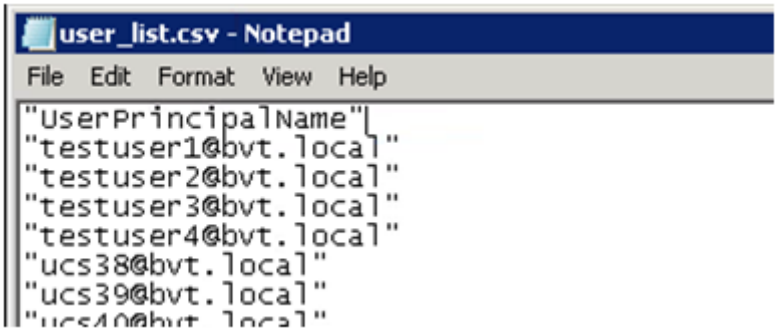
```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for
   Users, leave it blank to search all
$filename = "user_list.csv" # Filename to save

if ($searchbase -ne ""){

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -SearchBase $searchbase -Properties UserPrincipalName | Select
     UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -
     delimiter "," $filename
 }
  else {

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv
      -NoTypeInformation -Encoding utf8 -delimiter "," $filename
 }

<!--NeedCopy-->
```

Get-ADUser is a standard cmdlet to query for a list of users. The example above contains a filter argument to list only users with a UserPrincipalName and an account status of 'enabled.'

The SearchBase argument narrows which part of the AD to search for users. You can omit this if you want to include all users in AD. **Note:** This query might return a large number of users.

The CSV looks something like this:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**FAS server**

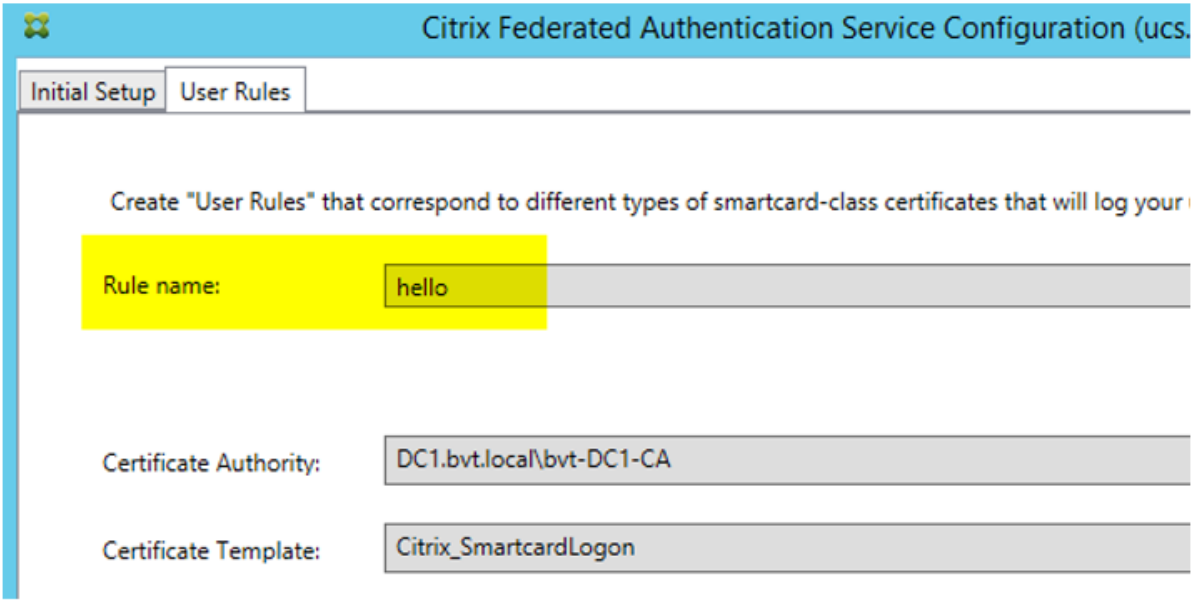
The following PowerShell script takes the previously-generated user list and creates a list of user certificates.

```
Add-PSSnapin Citrix.A*
$csv = "user_list.csv"
$rule = "default" # rule/role in your admin console
$users = Import-Csv -encoding utf8 $csv
foreach ( $user in $users )
{

    $server = Get-FasServerForUser -UserPrincipalNames $user.
       UserPrincipalName
    if( $server.Server -ne $NULL) {

        New-FasUserCertificate -Address $server.Server -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

    if( $server.Failover -ne $NULL) {

        New-FasUserCertificate -Address $server.Failover -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

 }

<!--NeedCopy-->
```

If you have more than one FAS server, a particular user's certificate will be generated twice: one in the main server, and the other in the failover server.

The script above is catered for a rule named 'default'. If you have a different rule name (for example, 'hello'), just change the $rule variable in the script.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Renew registration authority certificates

If more than one FAS server is in use, you can renew a FAS authorization certificate without affecting logged-on users. Note: Although you can also use the GUI to deauthorize and reauthorize FAS, that has the effect of resetting FAS configuration options.

Complete the following sequence:

1. Create a new authorization certificate: `New-FasAuthorizationCertificate`
2. Note the GUID of the new authorization certificate, as returned by: `Get-FasAuthorizationCertifica`
3. Place the FAS server into maintenance mode: `Set-FasServer –Address <FAS server> -MaintenanceMode $true`
4. Swap the new authorization certificate: `Set-FasCertificateDefinition –AuthorizationCert <GUID>`
5. Take the FAS server out of maintenance mode: `Set-FasServer –Address <FAS server> -MaintenanceMode $false`
6. Delete the old authorization certificate: `Remove-FasAuthorizationCertificate`

### Related information

- The Federated Authentication Service article is the primary reference for FAS installation and configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The common FAS deployments are summarized in the Federated Authentication Service architectures overview article.
- Other "how-to"articles are introduced in the Federated Authentication Service configuration and management article.

## Federated Authentication Service private key protection

June 24, 2021

### Introduction

Certificates are stored in the registry on the FAS server. The associated private keys are stored by means of the Network Service account of the FAS server and marked as non-exportable by default.

There are two types of private keys:

- The private key associated with the registration authority (RA) certificate, from the Citrix_RegistrationAuthority certificate template.
- The private keys associated with the user certificates, from the Citrix_SmartcardLogon certificate template.

There are actually two RA certificates: Citrix_RegistrationAuthority_ManualAuthorization (valid for 24 hours by default) and Citrix_RegistrationAuthority (valid for two years by default).

During step 3 of the Initial Setup in the FAS administration console, when the administrator clicks "Authorize"the FAS server generates a keypair and sends a Certificate Signing Request (CSR) to the CA for the Citrix_RegistrationAuthority_ManualAuthorization certificate. This is a temporary certificate, valid for 24 hours by default. The CA does not automatically issue this certificate; its issuance must be manually authorised on the CA by an administrator. Once the certificate is issued to the FAS server, FAS uses the Citrix_RegistrationAuthority_ManualAuthorization certificate to automatically obtain the Citrix_RegistrationAuthority certificate (valid for two years by default). The FAS server deletes the certificate and key for Citrix_RegistrationAuthority_ManualAuthorization as soon as it obtains the Citrix_RegistrationAuthority certificate.

The private key associated with the RA certificate is particularly sensitive, because the RA certificate policy allows whoever possesses the private key to issue certificate requests for the set of users configured in the template. As a consequence, whoever controls this key can connect to the environment as any of the users in the set.

You can configure the FAS server to protect private keys in a way that fits your organization's security requirements, using one of the following:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Microsoft Enhanced RSA and AES Cryptographic Provider or Microsoft Software Key Storage Provider for both the RA certificate and the user certificates' private keys.
- Microsoft Platform Key Storage Provider with a Trusted Platform Module (TPM) chip for the RA certificate's private key, and Microsoft Enhanced RSA and AES Cryptographic Provider or Microsoft Software Key Storage Provider for the user certificates' private keys.
- A Hardware Security Module (HSM) vendor's Cryptographic Service or Key Storage Provider with the HSM device for both the RA certificate and the user certificates' private keys.

### Private key configuration settings

Configure FAS to use one of the three options. Use a text editor to edit the Citrix.Authentication.FederatedAuthentic file. The default location of the file is in the Program Files\Citrix\Federated Authentication Service folder on the FAS server.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

The FAS reads the config file only when the service starts. If any values are changed, the FAS must be restarted before it reflects the new settings.

Set the relevant values in the Citrix.Authentication.FederatedAuthenticationService.exe.config file as follows:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (switch between CAPI and CNG APIs)

| Value | Comment |
|---|---|
| true | Use CAPI APIs |
| false (default) | Use CNG APIs |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (name of the provider to use)

| Value | Comment |
| --- | --- |
| Microsoft Enhanced RSA and AES Cryptographic Provider | Default CAPI provider |
| Microsoft Software Key Storage Provider | Default CNG Provider |
| Microsoft Platform Key Storage Provider | Default TPM provider. Note that TPM is not recommended for user keys. Use TPM for the RA key only. If you plan to run your FAS server in a virtualized environment, check with your TPM and hypervisor vendor whether virtualization is supported. |
| HSM_Vendor CSP/Key Storage Provider | Supplied by HSM vendor. The value differs between vendors. If you plan to run your FAS server in a virtualized environment, check with your HSM vendor whether virtualization is supported. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (Required only in case of CAPI API)

| Value | Comment |
| --- | --- |
| 24 | Default. Refers to Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Should always be 24 unless you are using an HSM with CAPI and the HSM vendor specifies otherwise. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (When FAS needs to perform a private key operation, it uses the value specified here) Controls the ‘‘exportable’’flag of private keys. Allows the use of TPM key storage, if supported by the hardware.

| Value | Comment |
| --- | --- |
| NoProtection | Private key can be exported. |
| GenerateNonExportableKey | Default. Private key cannot be exported. |

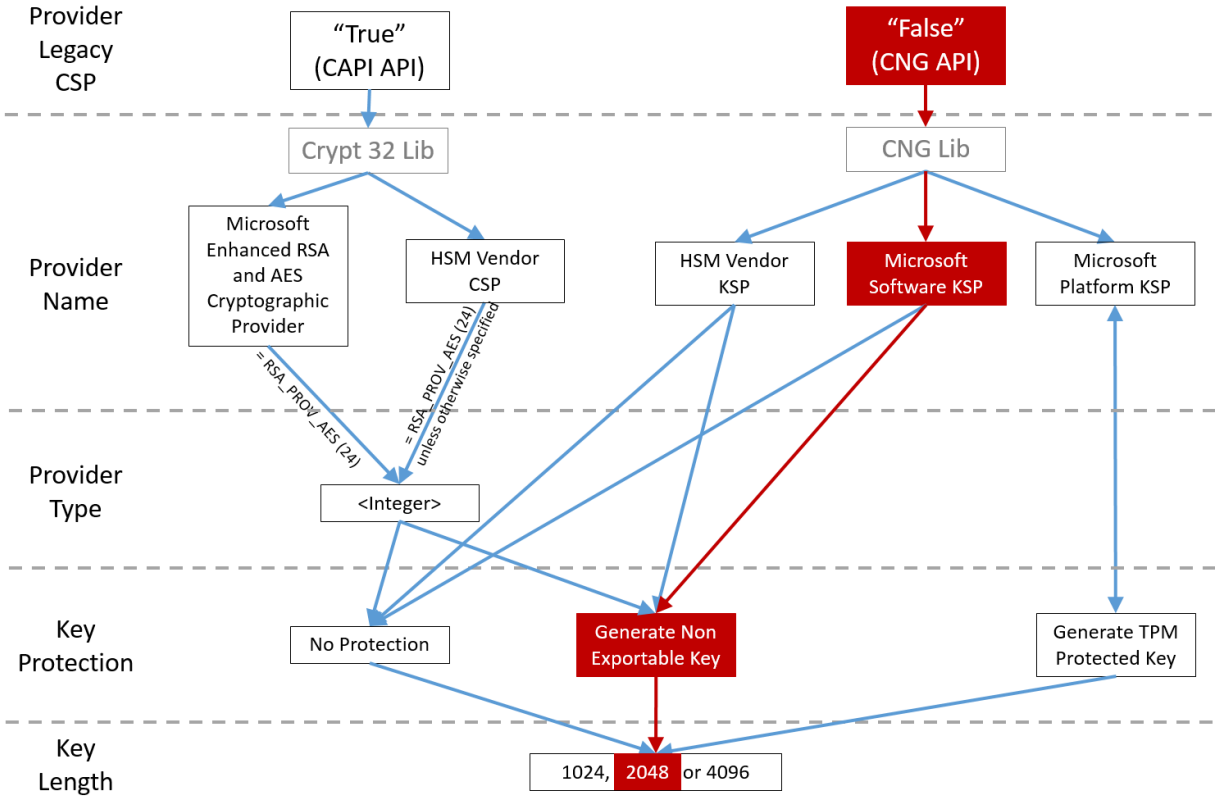
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Value | Comment |
| --- | --- |
| GenerateTPMProtectedKey | Private key will be managed using the TPM. Private key is stored via the ProviderName you specified in ProviderName (for example, Microsoft Platform Key Storage Provider) |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Specify size of private key in bits)

| Value | Comment |
| --- | --- |
| 2048 | Default. 1024 or 4096 can also be used. |

The config file settings are represented graphically as follows (installation defaults are shown in red):




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Configuration scenario examples

#### Example 1

This example covers the RA certificate private key and user certificates' private keys stored using the Microsoft Software Key Storage Provider

This is the default post-install configuration. No additional private key configuration is required.

#### Example 2

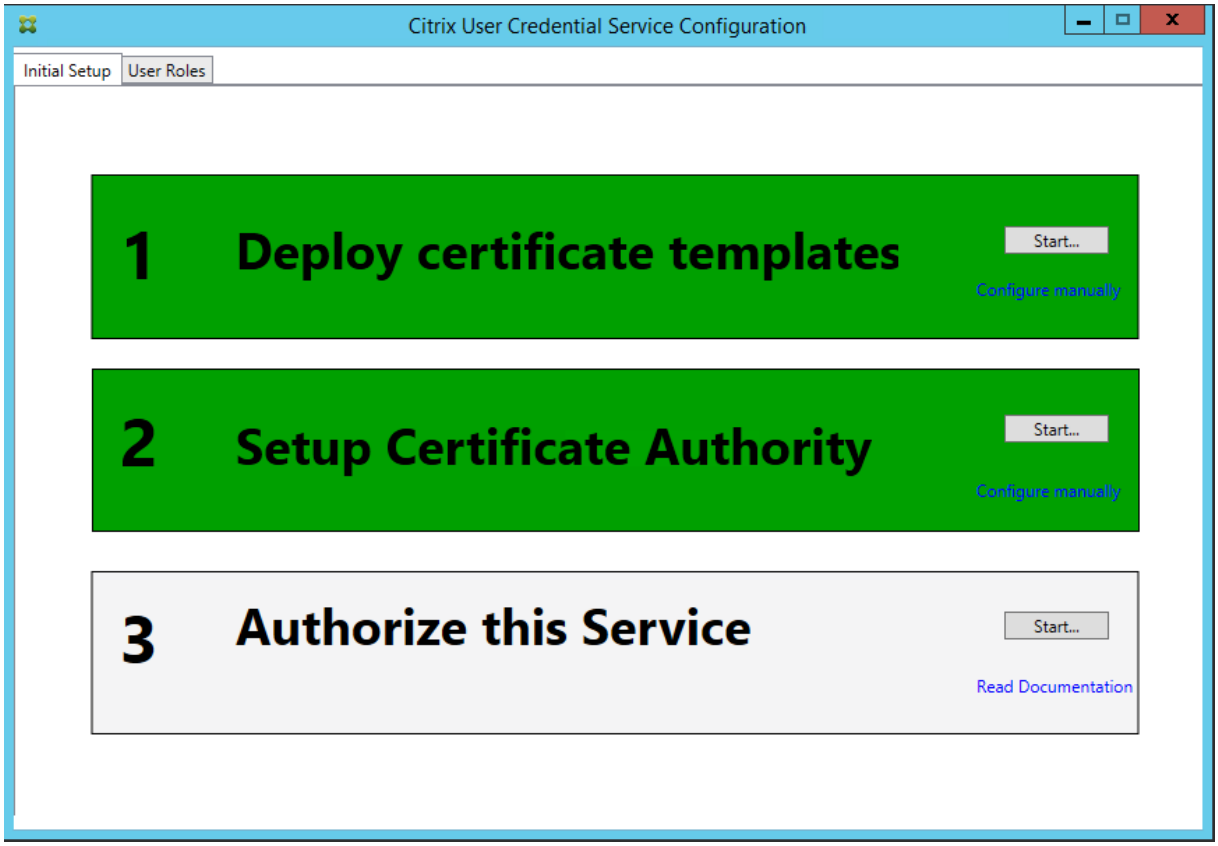
This example shows the RA certificate private key stored in the FAS server motherboard's hardware TPM via the Microsoft Platform Key Storage Provider, and user certificates' private keys stored using the Microsoft Software Key Storage Provider.

This scenario assumes that the TPM on your FAS server motherboard has been enabled in the BIOS according to the TPM manufacturer's documentation and then initialized in Windows; see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)?redirectedfrom=MSDN.

**Using PowerShell (recommended)** The RA certificate can be requested offline using PowerShell. This is recommended for organizations that do not want their CA to issue a RA certificate through an online CSR. An offline RA CSR cannot be made using the FAS administration console.

**Step 1:** During the initial setup of the FAS configuration using the administration console, complete only the first two steps: "Deploy certificate templates"and "Setup Certificate Authority."

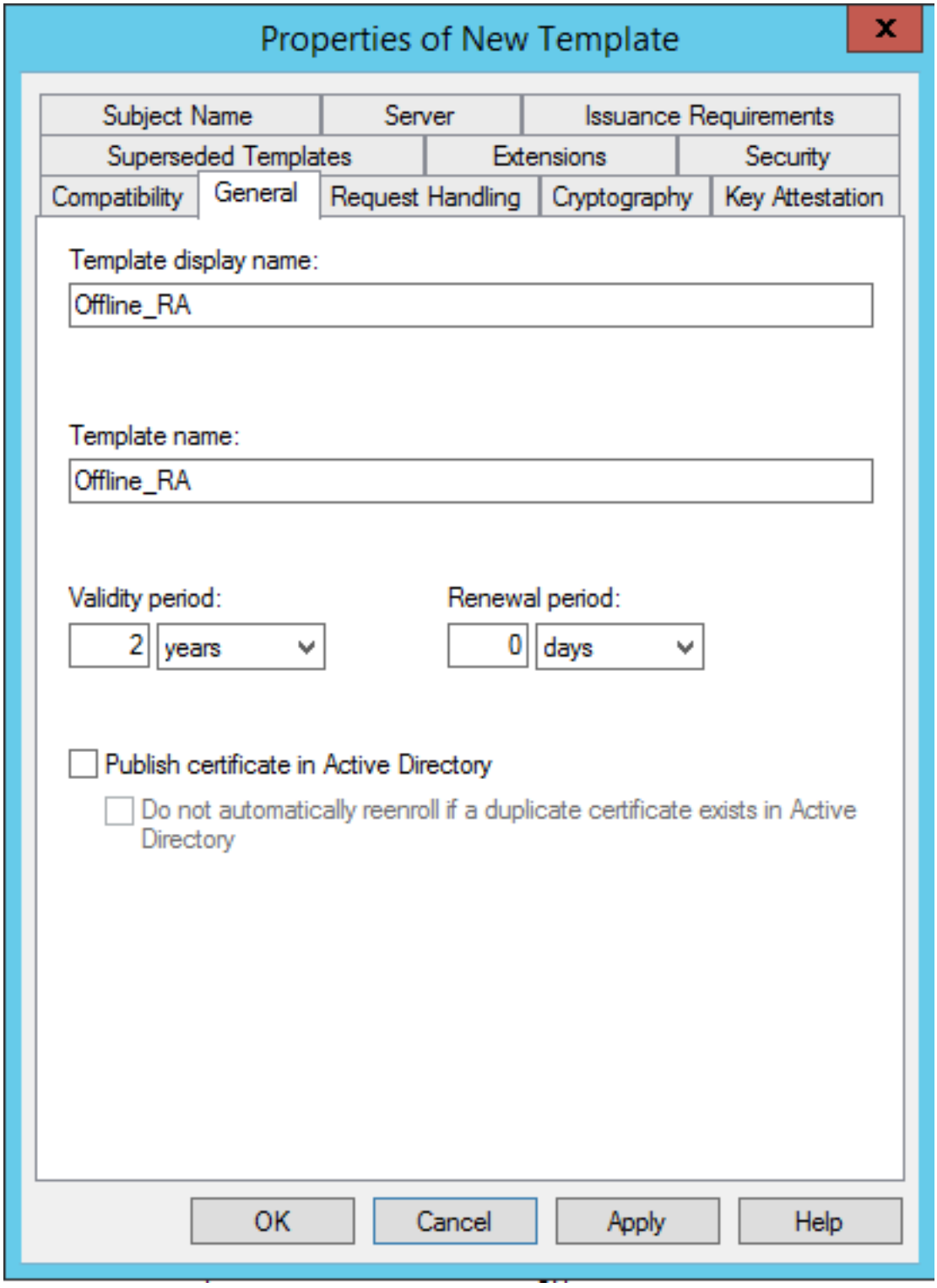
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Step 2:** On your CA server, add the Certificate Templates MMC snap-in. Right-click the **Citrix_RegistrationAuthority_ManualAuthorizatio**n template and select **Duplicate Template**.

Select the **General** tab. Change the name and validity period. In this example, the name is Offline_RA and the validity period is 2 years:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Step 3:** On your CA server, add the CA MMC snap-in. Right-click **Certificate Templates**. Select **New**, then click **Certificate Template to Issue**. Choose the template you just created.

**Step 4:** Load the following PowerShell cmdlets on the FAS server:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

**Step 5:** Generate the RSA keypair inside the FAS server's TPM and create the CSR by entering the following PowerShell cmdlet on the FAS server. **Note:** Some TPMs restrict key length. The default is key length is 2048 bits. Be sure to specify a key length supported by your hardware.

New-FasAuthorizationCertificateRequest -UseTPM $true -address <FQDN of FAS Server>

For example:

New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net

The following is displayed:

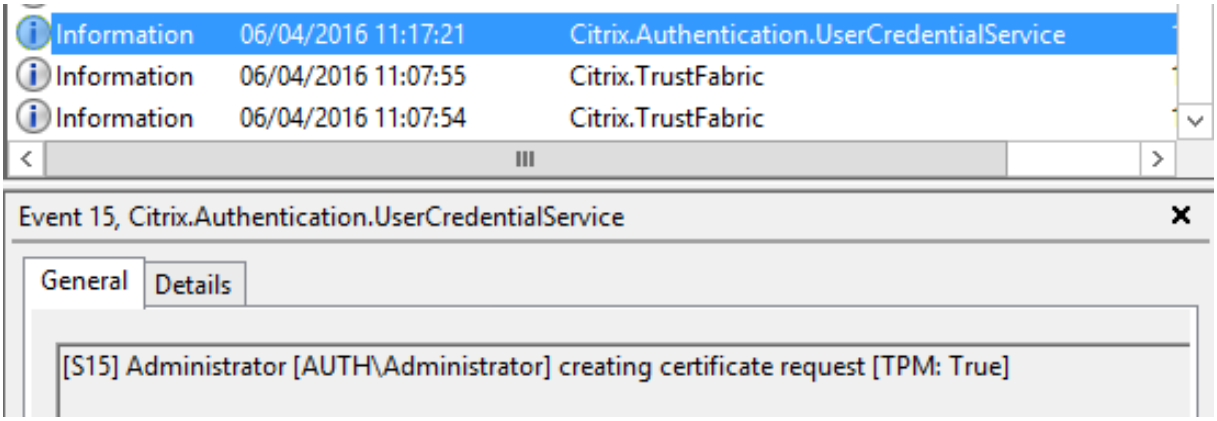
```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAf1bInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaM9MHOEFbepoSYOCAfunXW
                      snwIbXD91c/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPRgcq9XBwRjzpGj0g0VRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAUOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUZoAf6eLg1Uht2RUfb6d7Ns6+Mc+F5bFegLHs8c
                      Y1ITHOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4132xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

**Notes:**

- The Id GUID (in this example, "5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39") is required in a subsequent step.
- Think of this PowerShell cmdlet as a one-time "override"that is used to generate the private key for the RA certificate.
- When running this cmdlet, the values that are read from the config file when the FAS service started are checked to determine the key length to use (the default is 2048).
- Because -UseTPM is set to $true in this manual PowerShell-initiated RA certificate private key operation, the system ignores values from the file that do not match the settings required to use a TPM.
- Running this cmdlet does not change any settings in the config file.
- During subsequent automatic FAS-initiated user certificate private key operations, the values that were read from the file when the FAS service started will be used.
- It is also possible to set the KeyProtection value in the config file to GenerateTPMProtectedKey when the FAS server is issuing user certificates to generate user certificate private keys protected by the TPM.

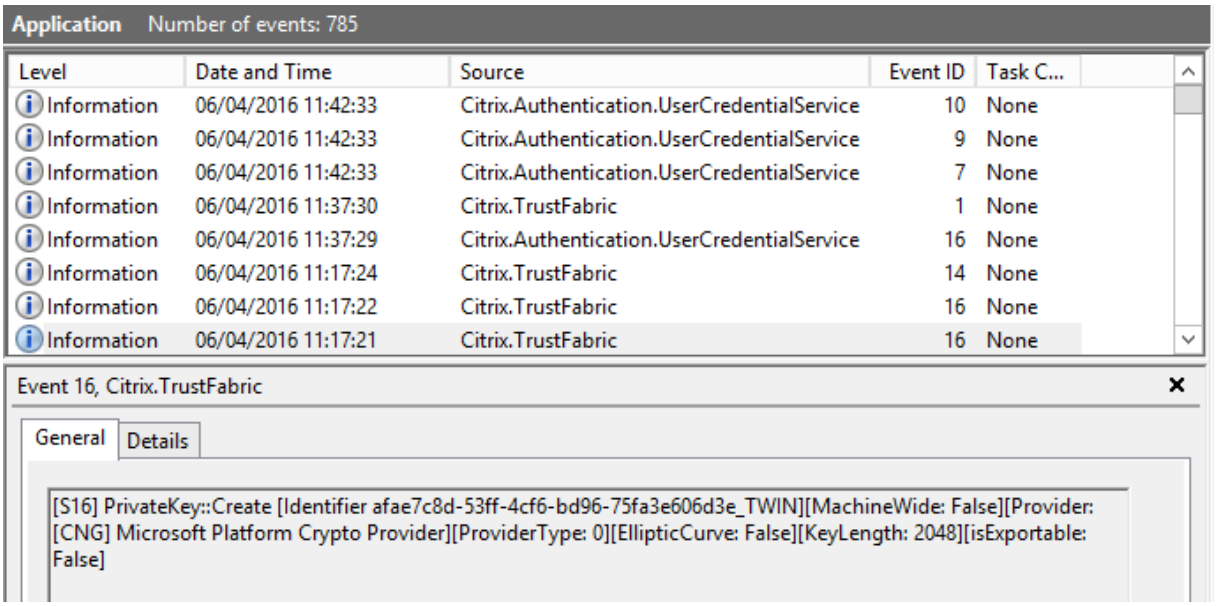
To verify that the TPM was used to generate the keypair, look in the application log in the Windows Event viewer on the FAS server, at the time that the keypair is generated.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Note "[TPM: True]"

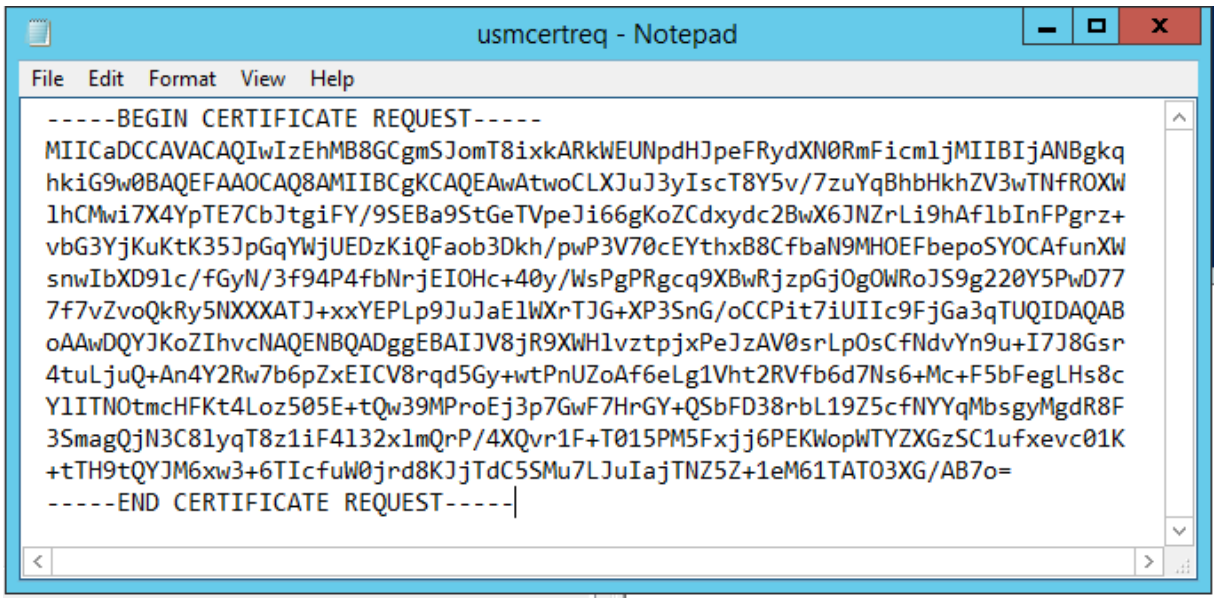
Followed by:




Note "Provider: [CNG] Microsoft Platform Crypto Provider"

**Step 6:** Copy the certificate request section into a text editor and save it to disk as a text file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Step 7:** Submit the CSR to your CA by typing the following into PowerShell on the FAS server:

certreq -submit -attrib "certificatetemplate:<certificate template from step 2>"<certificate request file from step 6>

For example:

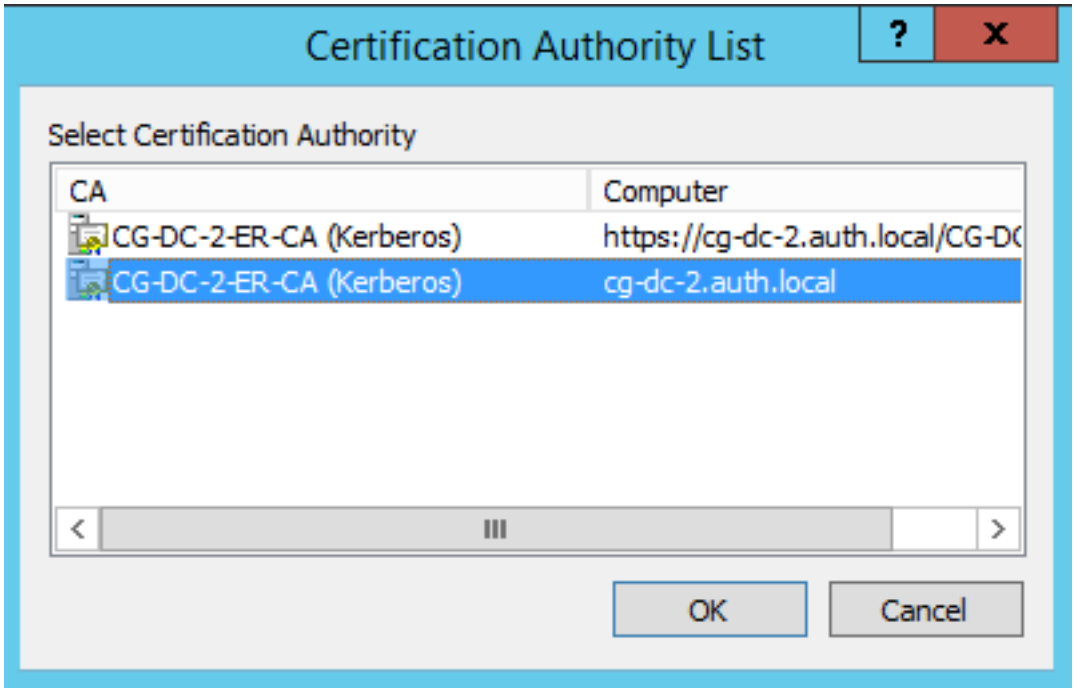
certreq -submit -attrib "certificatetemplate:Offline_RA"C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

The following is displayed:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E2950217702}
  ldap:
```

At this point a Certification Authority List window might appear. The CA in this example has both http (top) and DCOM (bottom) enrolment enabled. Select the DCOM option, if available:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



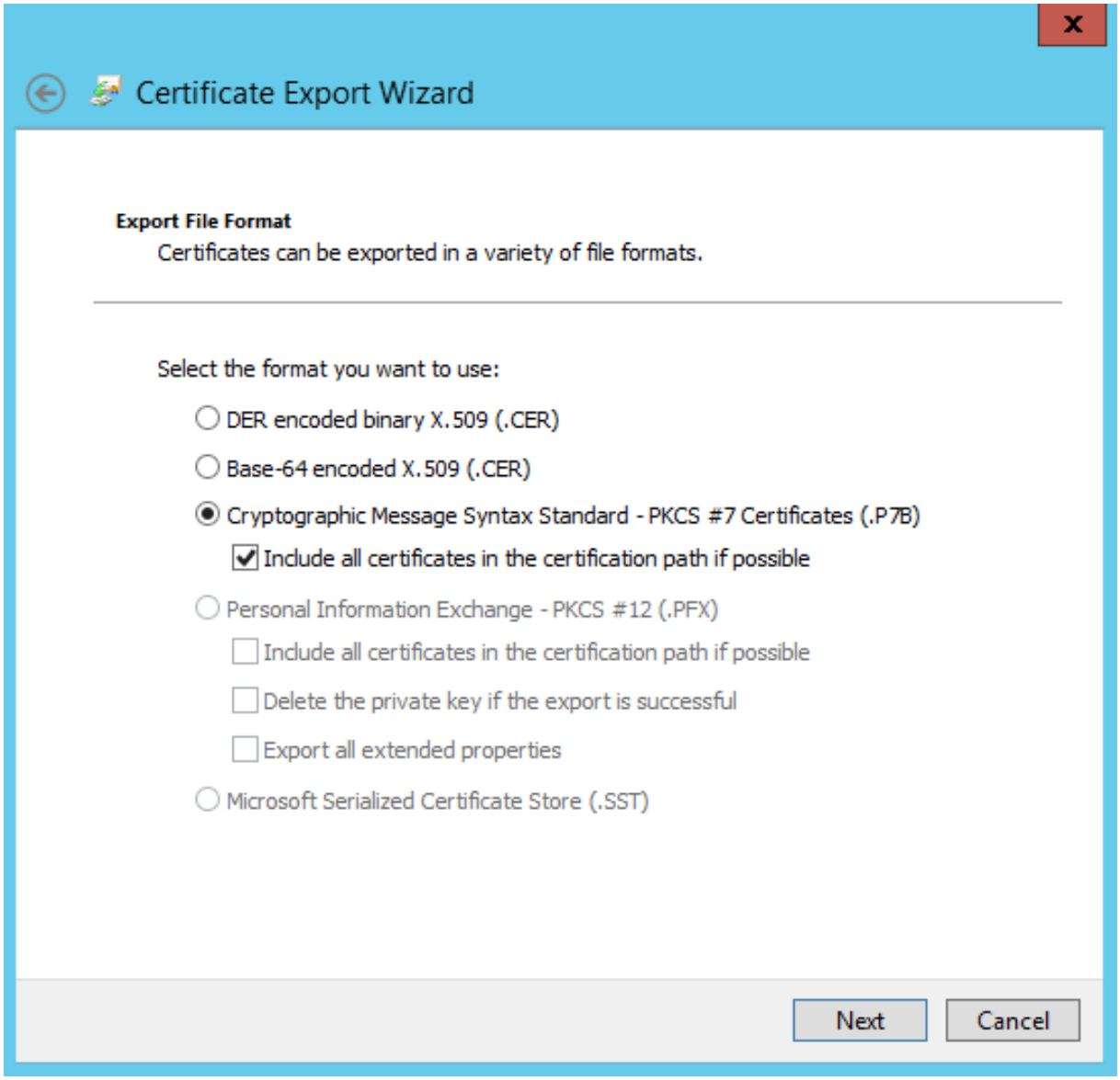

After the CA has been specified, PowerShell displays the RequestID:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

**Step 8:** On the CA server, in the CA MMC snap-in, click **Pending Requests**. Note the Request ID. Then right-click the request and choose **Issue**.

**Step 9:** Select the **Issued Certificates** node. Find the certificate that was just issued (the Request ID should match). Double-click to open the certificate. Select the **Details** tab. Click **Copy to File**. The Certificate Export Wizard launches. Click **Next.** Choose the following options for the file format:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The format must be "**Cryptographic Message Syntax Standard –PKCS #7 Certificates (.P7B)**"and "**Include all certificates in the certification path if possible**"must be checked.

**Step 10:** Copy the exported certificate file onto the FAS server.

**Step 11:** Import the RA certificate into the FAS server registry by entering the following PowerShell cmdlet on the FAS server:

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

For example:

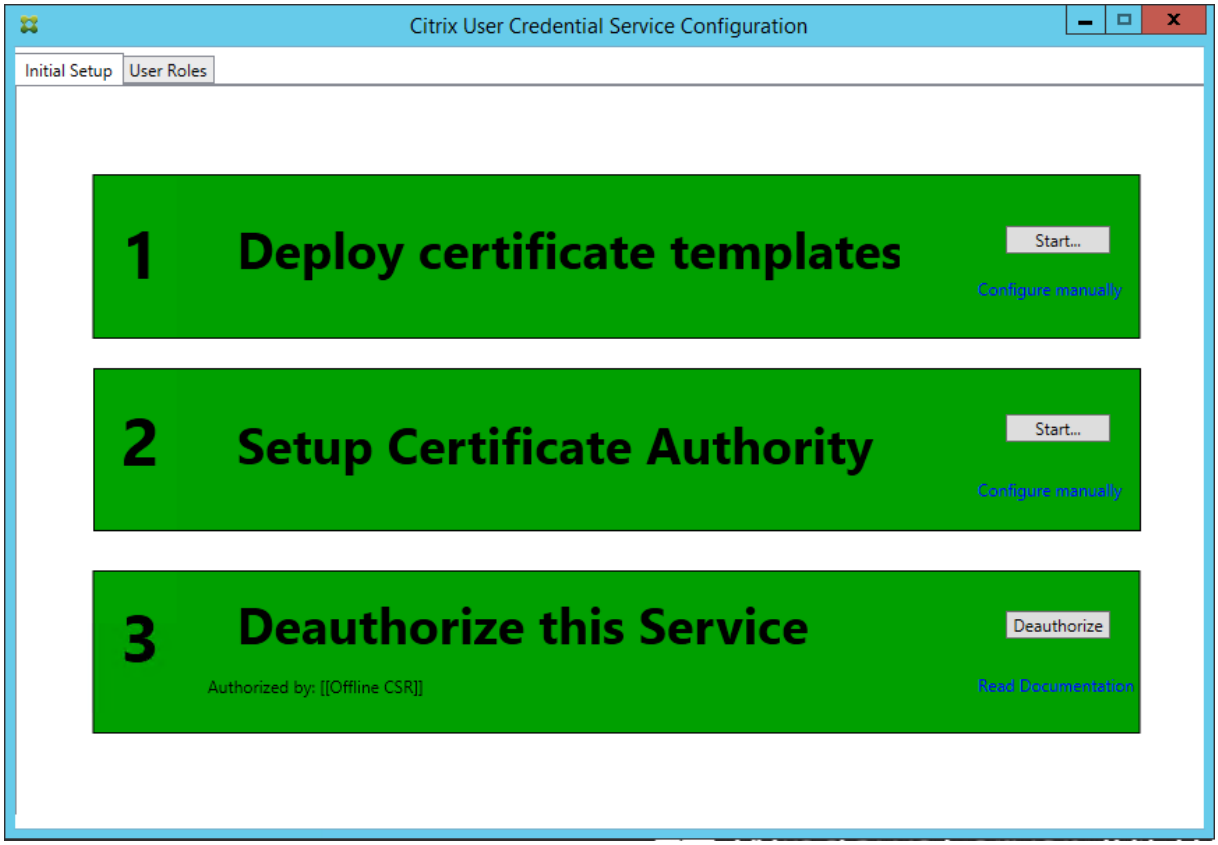
```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The following is displayed:

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102Dfc
CertificateRequest :
Status              : Ok
```

**Step 12:** Close the FAS administration console and then restart it.




Note that the step "Authorize this Service"has turned green, and now displays "Deauthorize this Service."The entry below indicates "Authorized by: Offline CSR"

**Step 13:** Select the User **Roles** tab in the FAS administration console and edit the settings described in the main FAS article.

**Note**: Deauthorizing the FAS through the administration console will delete the User Rule.

### Using the FAS management console

The FAS management console cannot do offline CSR, so using it is not recommended unless your organization allows online CSR for RA certificates.

When performing the FAS initial setup steps, after deploying certificate templates and setting up the CA, but before authorizing the service (step 3 in the configuration sequence):

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 1:** Edit the config file by changing the following line as follows:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

The file should now appear as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Some TPMs restrict key length. The default key length is 2048 bits. Be sure to specify a key length supported by your hardware.

**Step 2:** Authorize the service.

**Step 3:** Manually issue the pending certificate request from the CA server. After the RA certificate is obtained, step 3 in the setup sequence in the management console will be green. At this point, the RA certificate's private key will have generated in the TPM. The certificate will be valid for 2 years by default.

**Step 4:** Edit the config file back to the following:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

**Note**: Although FAS can generate user certificates with TPM protected keys, the TPM hardware may be too slow for large deployments.

**Step 5:** Restart the Citrix Federated Authentication Service. This forces the service to re-read the config file and reflect the changed values. The subsequent automatic private key operations will affect user certificate keys; those operations will not store the private keys in the TPM, but use the Microsoft Software Key Storage Provider.

**Step 6:** Select the User Roles tab in the FAS administration console and edit the settings as described in the main FAS article.

**Note:** Deauthorizing the FAS through the administration console will delete the User Rule.

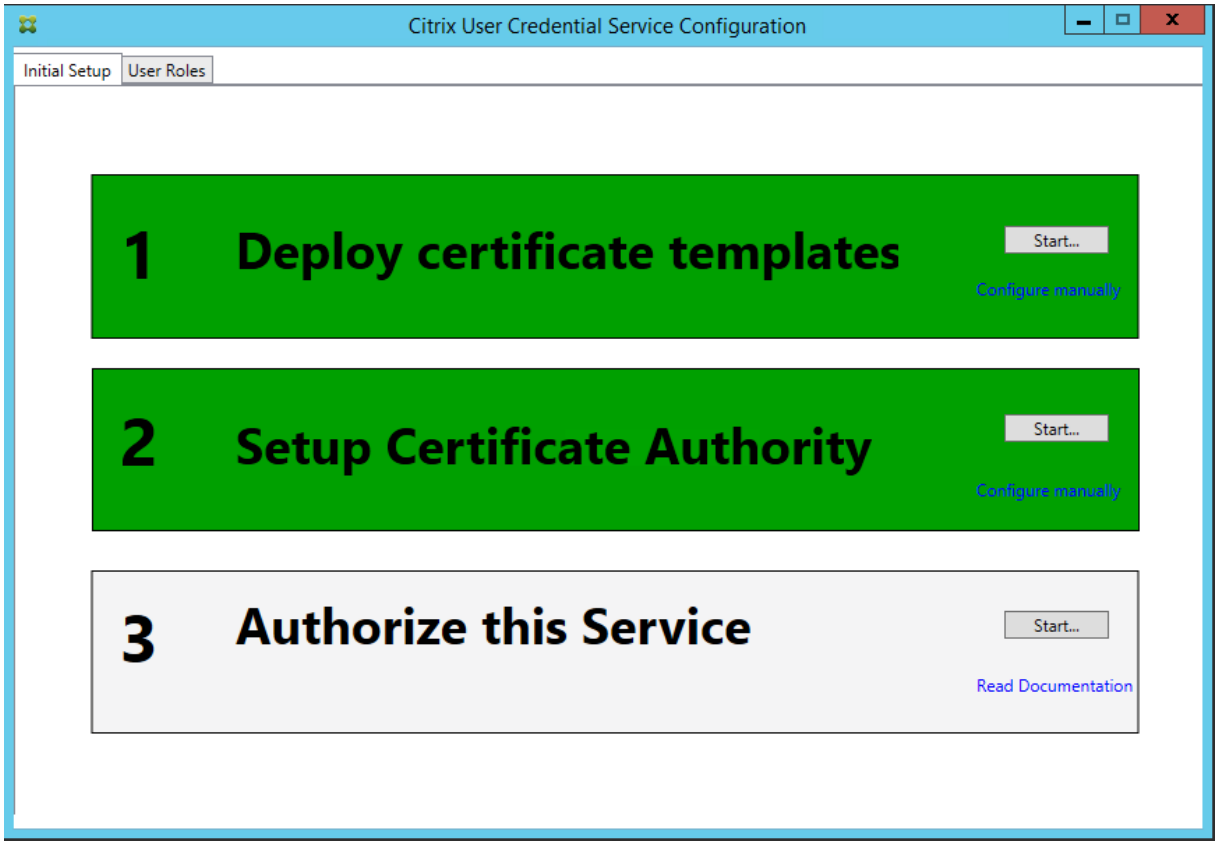
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Example 3**

This example covers an RA certificate private key and user certificates'private keys stored in an HSM. This example assumes a configured HSM. Your HSM will have a provider name, for example "HSM_Vendor's Key Storage Provider."

If you plan to run your FAS server in a virtualized environment, check with your HSM vendor about hypervisor support.

**Step 1.** During the initial setup of the FAS configuration using the administration console, complete only the first two steps: "Deploy certificate templates"and "Setup Certificate Authority."




**Step 2:** Consult your HSM vendor's documentation to determine what your HSM's ProviderName value should be. If your HSM uses CAPI, the provider might be referred to in the documentation as a Cryptographic Service Provider (CSP). If your HSM uses CNG, the provider might be referred to as a Key Storage Provider (KSP).

**Step 3:** Edit the config file as follows:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

The file should now appear as follows:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

This scenario assumes that your HSM uses CNG, so the ProviderLegacyCsp value is set to false. If your HSM uses CAPI, ProviderLegacyCsp value should be set to true. Consult your HSM vendor's documentation to determine whether your HSM uses CAPI or CNG. Also consult your HSM vendor's documentation on supported key lengths for asymmetric RSA key generation. In this example, the key length is set to the default of 2048 bits. Ensure that the key length you specify is supported by your hardware.

**Step 4:** Restart the Citrix Federated Authentication Service to read the values from the config file.

**Step 5:** Generate the RSA keypair inside the HSM and create the CSR by clicking **Authorize** in the Initial Setup tab of the FAS administration console.

**Step 6:** To verify that the keypair was generated in the HSM, check the application entries in the Windows Event log:

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

**Note:** [Provider: [CNG] HSM_Vendor's Key Storage Provider]

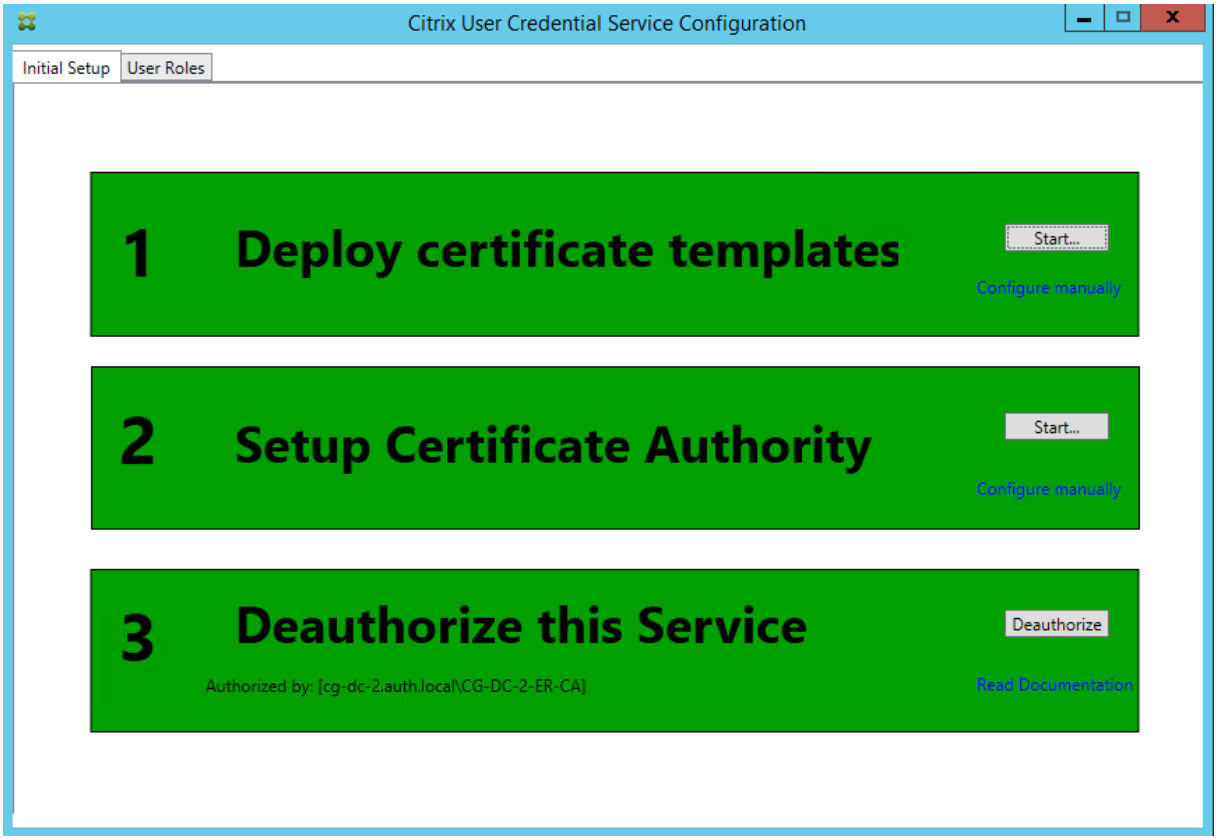
**Step 7:** On the CA server, in the CA MMC, select the **Pending Requests** node:

| Request ID | Binary Request | Request Status Code | Request Disposition Message | Request Submission Date | Requester Name | Request Country/Region |
|---|---|---|---|---|---|---|
| 107 | -----BEGIN NE... | The operation compl... | Taken Under Submission | 07/04/2016 14:04 | AUTH\UCSHSM$ | |

Right-click the request and select **Issue**.

Note that the step "Authorize this Service"has turned green, and now displays "Deauthorize this Service."The entry below indicates "Authorized by: [<CA Name>]"

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Step 8:** Select the **User Roles** tab in the FAS administration console and edit the settings as described in the main FAS article.

**Note:** Deauthorizing the FAS through the administration console will delete the User Rule.

### FAS certificate storage

FAS does not use the Microsoft certificate store on the FAS server to store its certificates. It uses the registry.

**Note:** When using an HSM to store private keys, HSM containers are identified with a GUID. The GUID for the private key in the HSM matches the GUID for the equivalent certificate in the registry.

To determine the GUID for the RA certificate, enter the following PowerShell cmdlets on the FAS server:

Add-pssnapin Citrix.a*

Get-FasAuthorizationCertificate –address <FAS server FQDN>

For example:

Get-FasAuthorizationCertificate –address cg-fas-2.auth.net

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                     MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
                     hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                     Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORholV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                     3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                     oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                     bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                     PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                     Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                     H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                     -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

To obtain a list of user certificates, enter:

Get-FasUserCertificate –address <FAS server FQDN>

For example:

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

### Related information

- The Federated Authentication Service article is the primary reference for FAS installation and configuration.
- The common FAS deployments are summarized in the Federated Authentication Services architectures overview article.
- Other "how-to"articles are introduced in the Federated Authentication Service configuration and management article.

## Federated Authentication Service security and network configuration

June 16, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

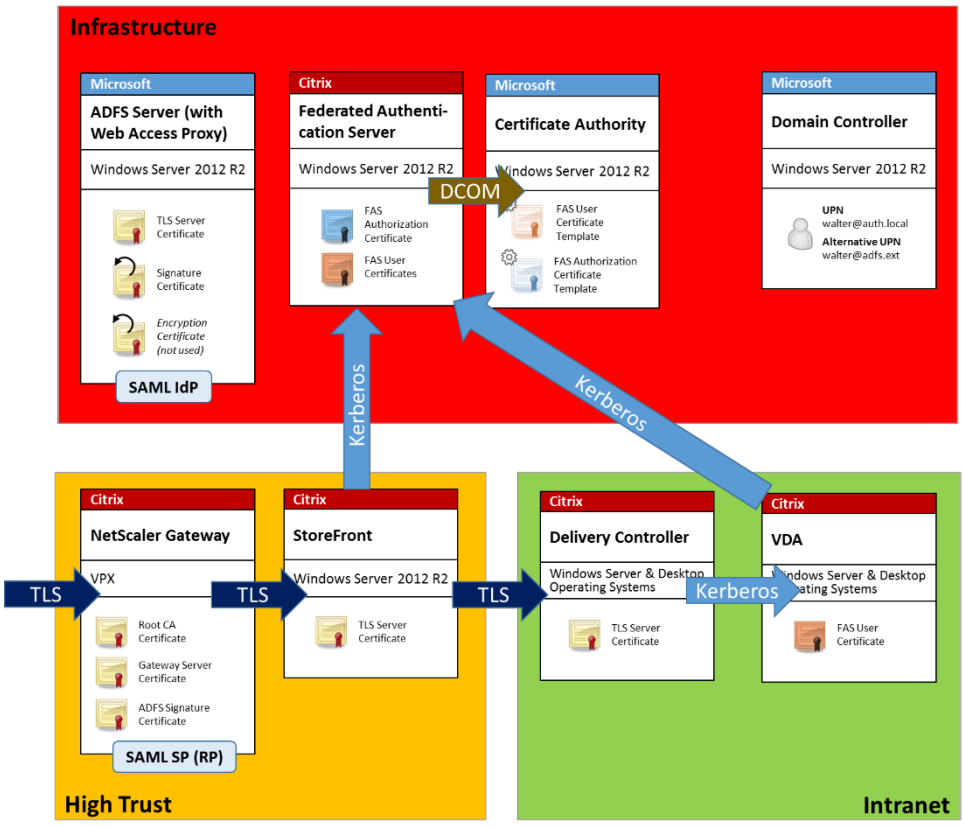
The Citrix Federated Authentication Service (FAS) is tightly integrated with Microsoft Active Directory and the Microsoft certification authority (CA). It is essential to ensure that the system is managed and secured appropriately, developing a security policy as you would for a domain controller or other critical infrastructure.

This document provides an overview of security issues to consider when deploying the FAS. It also provides an overview of features available that may assist in securing your infrastructure.

## Network architecture

The following diagram shows the main components and security boundaries used in an FAS deployment.

The FAS server should be treated as part of the security-critical infrastructure, along with the CA and domain controller. In a federated environment, Citrix NetScaler and Citrix StoreFront are components that are trusted to perform user authentication; other XenApp and XenDesktop components are unaffected by introducing the FAS.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Firewall and network security

Communication between NetScaler, StoreFront and the Delivery Controller components should be protected by TLS over port 443. The StoreFront server performs only outgoing connections, and the NetScaler Gateway should accept only connections over the Internet using HTTPS port 443.

The StoreFront server contacts the FAS server over port 80 using mutually authenticated Kerberos. Authentication uses the Kerberos HOST/fqdn identity of the FAS server, and the Kerberos machine account identity of the StoreFront server. This generates a single use "credential handle"needed by the Citrix Virtual Delivery Agent (VDA) to log on the user.

When an HDX session is connected to the VDA, the VDA also contacts the FAS server over port 80. Authentication uses the Kerberos HOST/fqdn identity of the FAS server, and the Kerberos machine identity of the VDA. Additionally, the VDA must supply the "credential handle"to access the certificate and private key.

The Microsoft CA accepts communication using Kerberos authenticated DCOM, which can be configured to use a fixed TCP port. The CA additionally requires that the FAS server supply a CMC packet signed by a trusted enrollment agent certificate.

| Server | Firewall Ports |
|---|---|
| Federated Authentication Service | [in] Kerberos over HTTP from StoreFront and VDAs, [out] DCOM to Microsoft CA |
| Netscaler | [in] HTTPS from client machines, [in/out] HTTPS to/from StoreFront server, [out] HDX to VDA |
| StoreFront | [in] HTTPS from NetScaler, [out] HTTPS to Delivery Controller, [out] Kerberos HTTP to FAS |
| Delivery Controller | [in] HTTPS from StoreFront server, [in/out] Kerberos over HTTP from VDAs |
| VDA | [in/out] Kerberos over HTTP from Delivery Controller, [in] HDX from NetScaler Gateway, [out] Kerberos HTTP to FAS |
| Microsoft CA | [in] DCOM & signed from FAS |

### Administration responsibilities

Administration of the environment can be divided into the following groups:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Responsibility |
| --- | --- |
| Enterprise Administrator | Install and secure certificate templates in the forest |
| Domain Administrator | Configure Group Policy settings |
| CA Administrator | Configure the certificate authority |
| FAS Administrator | Install and configure the FAS server |
| StoreFront/Netscaler Admin | Configure user authentication |
| XenDesktop Administrator | Configure VDAs and Controllers |

Each administrator controls different aspects of the overall security model, allowing a defense-in-depth approach to securing the system.

### Group Policy settings

Trusted FAS machines are identified by a lookup table of "index number -> FQDN"configured through Group Policy. When contacting an FAS server, clients verify the FAS server's HOST\<fqdn> Kerberos identity. All servers that access the FAS server must have identical FQDN configurations for the same index; otherwise, StoreFront and VDAs may contact different FAS servers.

To avoid misconfiguration, Citrix recommends that a single policy be applied to all machines in the environment. Take care when modifying the list of FAS servers, especially when removing or reordering entries.

Control of this GPO should be limited to FAS administrators (and/or domain administrators) who install and decommission FAS servers. Take care to avoid reusing a machine FQDN name shortly after decommissioning an FAS server.

### Certificate templates

If you do not want to use the Citrix_SmartcardLogon certificate template supplied with the FAS, you can modify a copy of it. The following modifications are supported.

#### Rename a certificate template

If you want to rename the Citrix_SmartcardLogon to match your organizational template naming standard, you must:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Create a copy of the certificate template and rename it to match your organizational template naming standard.
- Use FAS PowerShell commands to administer FAS, rather than the administrative user interface. (The administrative user interface is only intended for use with the Citrix default template names.)
  - Either use the Microsoft MMC Certificate Templates snap-in or the Publish-FasMsTemplate command to publish your template, and
  - Use the New-FasCertificateDefinition command to configure FAS with the name of your template.

#### Modify General properties

You can modify the Validity period in the certificate template.

Do not modify the Renewal period. FAS ignores this setting in the certificate template. FAS automatically renews the certificate halfway through its validity period.

#### Modify Request Handling properties

Do not modify these properties. FAS ignores these settings in the certificate template. FAS always deselects **Allow private key to be exported** and deselects **Renew with same key**.

#### Modify Cryptography properties

Do not modify these properties. FAS ignores these settings in the certificate template.

Refer to Federated Authentication Service private key protection for equivalent settings that FAS provides.

#### Modify Key Attestation properties

Do not modify these properties. FAS does not support key attestation.

#### Modify Superseded Templates properties

Do not modify these properties. FAS does not support superseding templates.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Modify Extensions properties

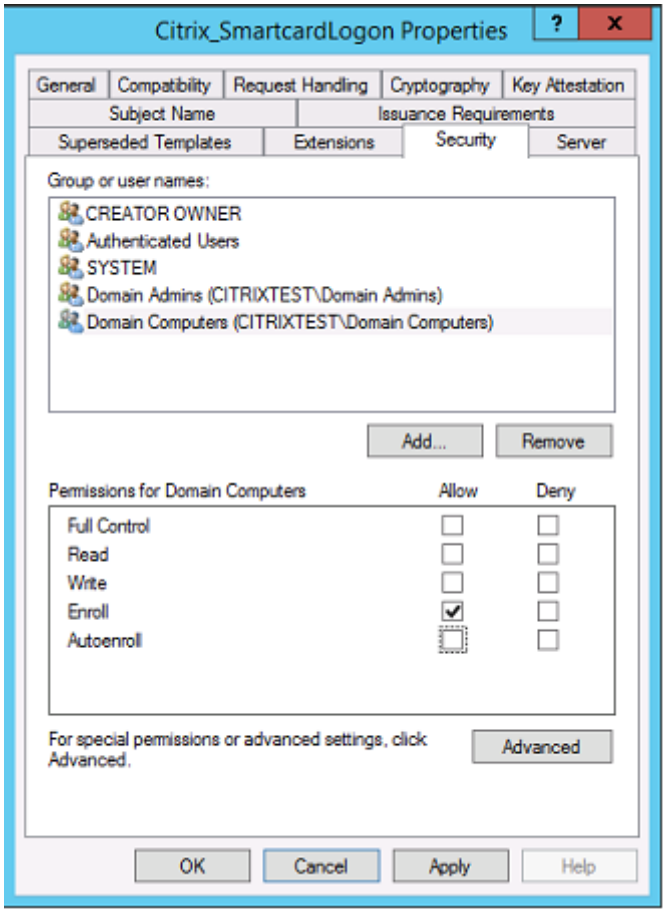
You can modify these settings to match your organizational policy.

**Note:** Inappropriate Extension settings may cause security issues, or result in unusable certificates.

### Modify Security properties

Citrix recommends that you modify these settings to Allow the **Read** and **Enroll** permissions for only the machine accounts of the FAS servers. No other permissions are required by the FAS service. However, as with other certificate templates, you may want to:

- allow administrators to Read or Write the template
- allow authenticated users to Read the template




### Modify Subject Name properties

You can modify these settings to match your organizational policy, if needed.

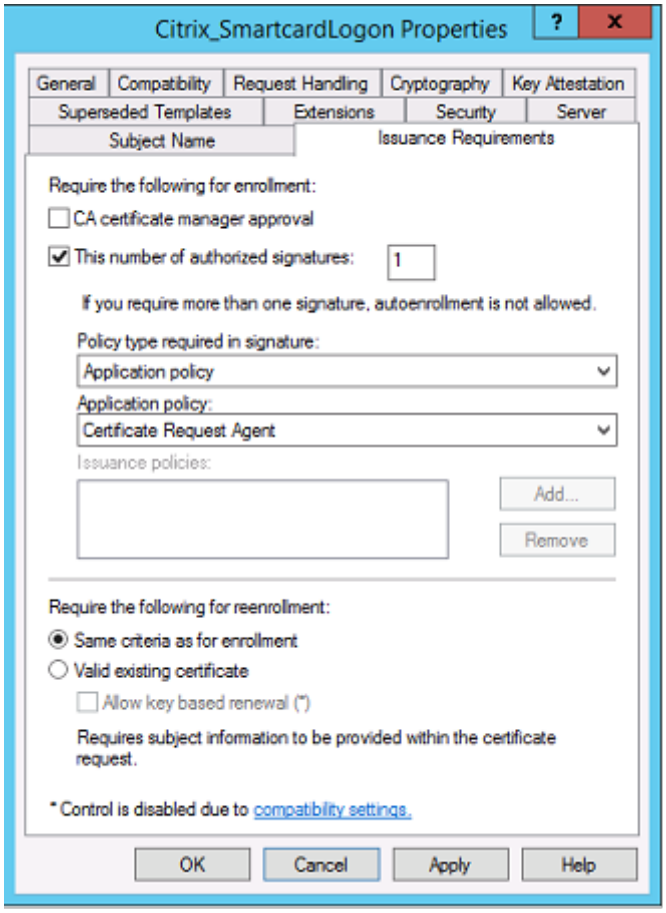
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Modify Server properties

Although Citrix does not recommend it, you can modify these settings to match your organizational policy, if needed.

### Modify Issuance requirements properties

Do not modify these settings. These settings should be as shown:




### Modify Compatibility properties

You can modify these settings. The setting must be at least **Windows Server 2003 CAs** (schema version 2). However, FAS supports only Windows Server 2008 and later CAs. Also, as explained above, FAS ignores the additional settings available by selecting **Windows Server 2008 CAs** (schema version 3) or **Windows Server 2012 CAs** (schema version 4).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Certificate authority administration

The CA administrator is responsible for the configuration of the CA server and the issuing certificate private key that it uses.

### Publishing templates

For a certificate authority to issue certificates based on a template supplied by the enterprise administrator, the CA administrator must choose to publish that template.

A simple security practice is to publish only the RA certificate templates when the FAS servers are being installed, or to insist on a completely offline issuance process. In either case, the CA administrator should maintain complete control over authorizing RA certificate requests, and have a policy for authorizing FAS servers.

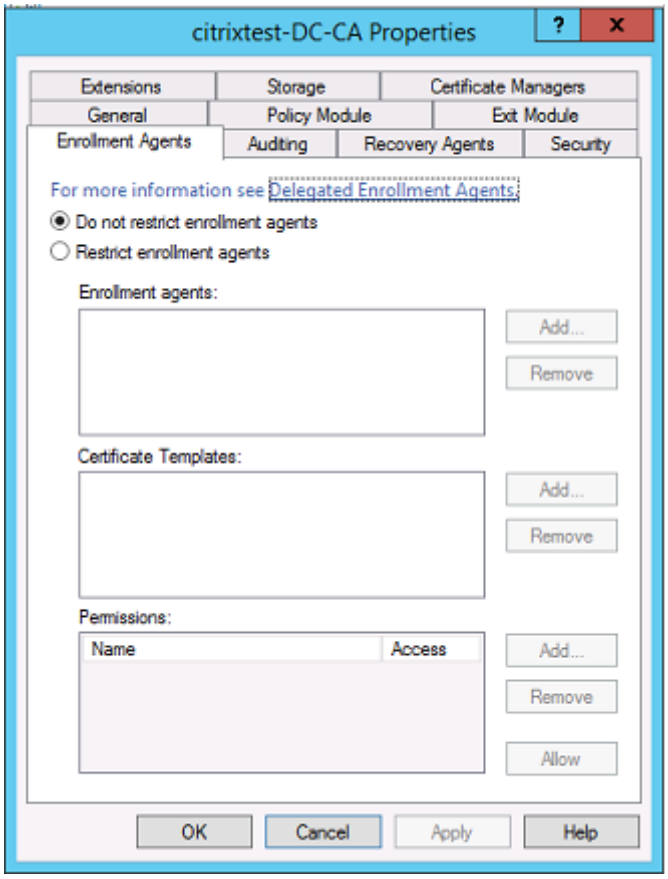
### Firewall settings

Generally, the CA administrator will also have control of the network firewall settings of the CA, allowing control over incoming connections. The CA administrator can configure DCOM TCP and firewall rules so that only FAS servers can request certificates.

### Restricted enrollment

By default any holder of an RA certificate can issue certificates to any user, using any certificate template that allows access. This should be restricted to a group of non-privileged users using the ‘‘Restrict enrollment agents’’CA property.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




#### Policy modules and auditing

For advanced deployments, custom security modules can be used to track and veto certificate issuance.

### FAS administration

The FAS has several security features.

#### Restrict StoreFront, users, and VDAs through an ACL

At the center of the FAS security model is the control for which Kerberos accounts can access functionality:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Access Vector | Description |
| --- | --- |
| StoreFront [IdP] | These Kerberos accounts are trusted to declare that a user has been correctly authenticated. If one of these accounts is compromised, then certificates can be created and used for users allowed by the configuration of the FAS. |
| VDAs [Relying party] | These are the machines that are allowed to access the certificates and private keys. A credential handle retrieved by the IdP is also needed, so a compromised VDA account in this group has limited scope to attack the system. |
| Users | This controls which users can be asserted by the IdP. Note that there is overlap with the "Restricted Enrollment Agent"configuration options at the CA. In general, it is advisable to include only non-privileged accounts in this list. This prevents a compromised StoreFront account from escalating privileges to a higher administrative level. In particular, domain administrator accounts should not be allowed by this ACL. |

### Configure rules

Rules are useful if multiple independent XenApp or XenDesktop deployments use the same FAS server infrastructure. Each rule has a separate set of configuration options; in particular, the ACLs can be configured independently.

### Configure the CA and templates

Different certificate templates and CAs can be configured for different access rights. Advanced configurations may choose to use less or more powerful certificates, depending on the environment. For example, users identified as "external"may have a certificate with fewer privileges than "internal" users.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### In-session and authentication certificates

The FAS administrator can control whether the certificate used to authenticate is available for use in the user's session. For example, this could be used to have only "signing"certificates available in-session, with the more powerful "logon"certificate being used only at logon.

#### Private key protection and key length

The FAS administrator can configure FAS to store private keys in a Hardware Security Module (HSM) or Trusted Platform Module (TPM). Citrix recommends that at least the RA certificate private key is protected by storing it in a TPM; this option is provided as part of the "offline"certificate request process.

Similarly, user certificate private keys can be stored in a TPM or HSM. All keys should be generated as "non-exportable"and be at least 2048 bits in length.

#### Event logs

The FAS server provides detailed configuration and runtime event logs, which can be used for auditing and intrusion detection.

#### Administrative access and administration tools

The FAS includes remote administration features (mutually authenticated Kerberos) and tools. Members of the "Local Administrators Group"have full control over FAS configuration. This list should be carefully maintained.

### XenApp, XenDesktop, and VDA administrators

In general, the use of the FAS doesn't change the security model of the Delivery Controller and VDA administrators, as the FAS "credential handle"simply replaces the "Active Directory password."Controller and VDA administration groups should contain only trusted users. Auditing and event logs should be maintained.

### General Windows server security

All servers should be fully patched and have standard firewall and anti-virus software available. Security-critical infrastructure servers should be kept in a physically secure location, with care taken over disk encryption and virtual machine maintenance options.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Auditing and event logs should be stored securely on a remote machine.

RDP access should be limited to authorized administrators. Where possible, user accounts should require smart card logon, especially for CA and domain administrator accounts.

### Related information

- The Federated Authentication Service article is the primary reference for FAS installation and configuration.
- FAS architectures are introduced in the Federated Authentication Service architectures overview article.
- Other "how-to"articles are introduced in the Federated Authentication Service configuration and management article.

## Federated Authentication Service troubleshoot Windows logon issues

June 16, 2021

This article describes the logs and error messages Windows provides when a user logs on using certificates and/or smart cards. These logs provide information you can use to troubleshoot authentication failures.

### Certificates and public key infrastructure

Windows Active Directory maintains several certificate stores that manage certificates for users logging on.

- **NTAuth certificate store**: To authenticate to Windows, the CA immediately issuing user certificates (that is, no chaining is supported) must be placed in the NTAuth store. To see these certificates, from the certutil program, enter: certutil –viewstore –enterprise NTAuth.
- **Root and intermediate certificate stores:** Usually, certificate logon systems can provide only a single certificate, so if a chain is in use, the intermediate certificate store on all machines must include these certificates. The root certificate must be in the Trusted Root Store, and the penultimate certificate must be in the NTAuth store.
- **Logon certificate extensions and Group Policy:** Windows can be configured to enforce verification of EKUs and other certificate policies. See the Microsoft documentation: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)?redirectedfrom=MSDN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Registry policy | Description |
| --- | --- |
| AllowCertificatesWithNoEKU | When disabled, certificates must include the smart card logon Extended Key Usage (EKU). |
| AllowSignatureOnlyKeys | By default, Windows filters out certificates private keys that do not allow RSA decryption. This option overrides that filter. |
| AllowTimeInvalidCertificates | By default, Windows filters out expired certificates. This option overrides that filter. |
| EnumerateECCCerts | Enables elliptic curve authentication. |
| X509HintsNeeded | If a certificate does not contain a unique User Principal Name (UPN), or it could be ambiguous, this option allows users to manually specify their Windows logon account. |
| UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors | Disables revocation checking (usually set on the domain controller). |

- **Domain controller certificates**: To authenticate Kerberos connections, all servers must have appropriate "Domain Controller"certificates. These can be requested using the "Local Computer Certificate Personal Store"MMC snap-in menu.

## UPN name and certificate mapping

It is recommended that user certificates include a unique User Principal Name (UPN) in the Subject Alternate Name extension.

### UPN names in Active Directory

By default, every user in Active Directory has an implicit UPN based on the pattern <samUsername>@<domainNetBios> and <samUsername>@<domainFQDN>. The available domains and FQDNs are included in the RootDSE entry for the forest. Note that a single domain can have multiple FQDN addresses registered in the RootDSE.

Additionally, every user in Active Directory has an explicit UPN and altUserPrincipalNames. These are LDAP entries that specify the UPN for the user.

When searching for users by UPN, Windows looks first in the current domain (based on the identity of the process looking up the UPN) for explicit UPNs, then alterative UPNs. If there are no matches, it looks up the implicit UPN, which may resolve to different domains in the forest.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Certificate Mapping Service

If a certificate does not include an explicit UPN, Active Directory has the option to store an exact public certificate for each use in an "x509certificate"attribute. To resolve such a certificate to a user, a computer can query for this attribute directly (by default, in a single domain).

An option is provided for the user to specify a user account that speeds up this search, and also allows this feature to be used in a cross-domain environment.

If there are multiple domains in the forest, and the user does not explicitly specify a domain, the Active Directory rootDSE specifies the location of the Certificate Mapping Service. This is usually located on a global catalog machine, and has a cached view of all x509certificate attributes in the forest. This computer can be used to efficiently find a user account in any domain, based on only the certificate.

### Control logon domain controller selection

When an environment contains multiple domain controllers, it is useful to see and restrict which domain controller is used for authentication, so that logs can be enabled and retrieved.

#### Control domain controller selection

To force Windows to use a particular Windows domain controller for logon, you can explicitly set the list of domain controllers that a Windows machine uses by configuring the lmhosts file: \Windows\System32\drivers\etc\lmhosts.

There is usually a sample file named "lmhosts.sam"in that location. Simply include a line:

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

Where "1.2.3.4"is the IP address of the domain controller named "dcnetbiosname"in the "mydomain" domain.

After a restart, the Windows machine uses that information to log on to mydomain. Note that this configuration must be reverted when debugging is complete.

#### Identify the domain controller in use

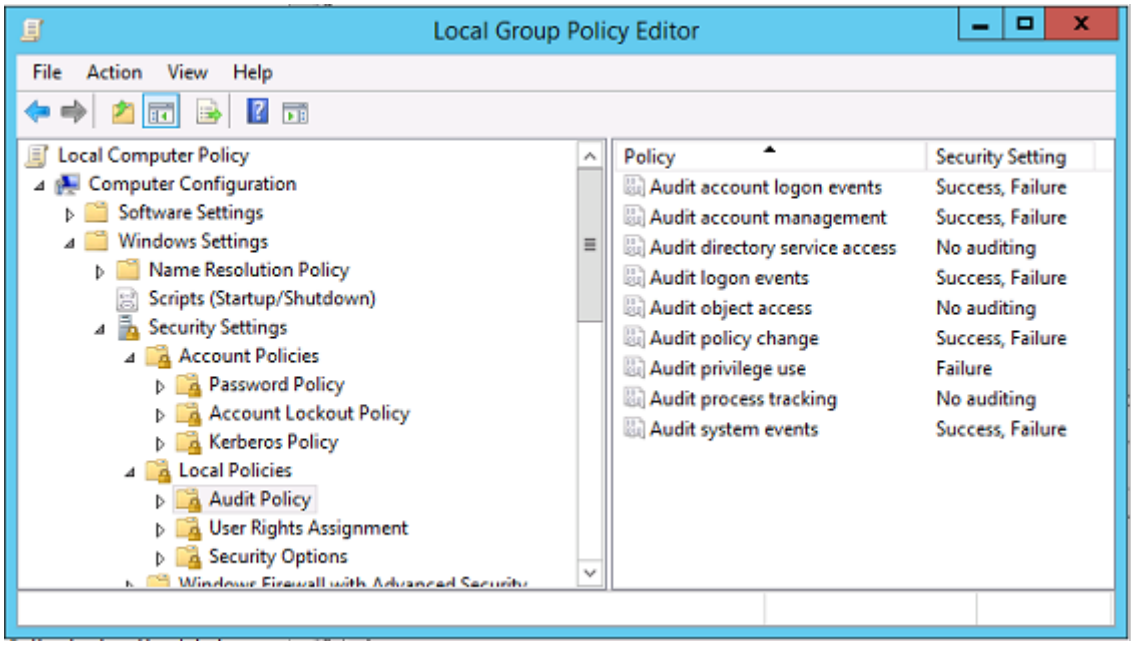
At logon, Windows sets an MSDOS environment variable with the domain controller that logged the user on. To see this, start the command prompt with the command: **echo %LOGONSERVER%**.

Logs relating to authentication are stored on the computer returned by this command.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Enable account audit events

By default, Windows domain controllers do not enable full account audit logs. This can be controlled through audit policies in the security settings in the Group Policy editor. After they are enabled, the domain controller produces extra event log information in the security log file.




### Certificate validation logs

#### Check certificate validity

If a smartcard certificate is exported as a DER certificate (no private key required), you can validate it with the command: certutil –verify user.cer

#### Enable CAPI logging

On the domain controller and users machine, open the event viewer and enable logging for Microsoft-/Windows/CAPI2/Operational Logs.

You can control CAPI logging with the registry keys at: CurrentControlSet\Services\crypt32.

| Value | Description |
|---|---|
| DiagLevel (DWORD) | Verbosity level (0 to 5) |
| DiagMatchAnyMask (QUADWORD) | Event filter (use 0xffffff for all) |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Value | Description |
| --- | --- |
| DiagProcessName (MULTI_SZ) | Filter by process name (for example, LSASS.exe) |

**CAPI logs**

| Message | Description |
| --- | --- |
| Build Chain | LSA called CertGetCertificateChain (includes result) |
| Verify Revocation | LSA called CertVerifyRevocation (includes result) |
| X509 Objects | In verbose mode, certificates and Certificate Revocation Lists (CRLs) are dumped to AppData\LocalLow\Microsoft\X509Objects |
| Verify Chain Policy | LSA called CertVerifyChainPolicy (includes parameters) |

**Error messages**

| Error code | Description |
| --- | --- |
| Certificate not trusted | The smart card certificate could not be built using certificates in the computer's intermediate and trusted root certificate stores. |
| Certificate revocation check error | The CRL for the smart card could not be downloaded from the address specified by the certificate CRL distribution point. If revocation checking is mandated, this prevents logon from succeeding. See the Certificates and public key infrastructure section. |
| Certificate Usage errors | The certificate is not suitable for logon. For example, it might be a server certificate or a signing certificate. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Kerberos logs

To enable Kerberos logging, on the domain controller and the end user machine, create the following registry values:

| Hive | Value name | Value [DWORD] |
|---|---|---|
| CurrentControlSet\Control\Lsa\Kerberos\Parameters | LogLevel | 0x1 |
| CurrentControlSet\Control\Lsa\Kerberos\Parameters | KerbDebugLevel | 0xffffffff |
| CurrentControlSet\Services\Kdc | KdcDebugLevel | 0x1 |
| CurrentControlSet\Services\Kdc | KdcExtraLogLevel | 0x1f |

Kerberos logging is output to the System event log.

- Messages such as "untrusted certificate"should be easy to diagnose.
- Two error codes are informational, and can be safely ignored:
  - KDC_ERR_PREAUTH_REQUIRED (used for backward compatibility with older domain controllers)
  - Unknown error 0x4b

### Event log messages

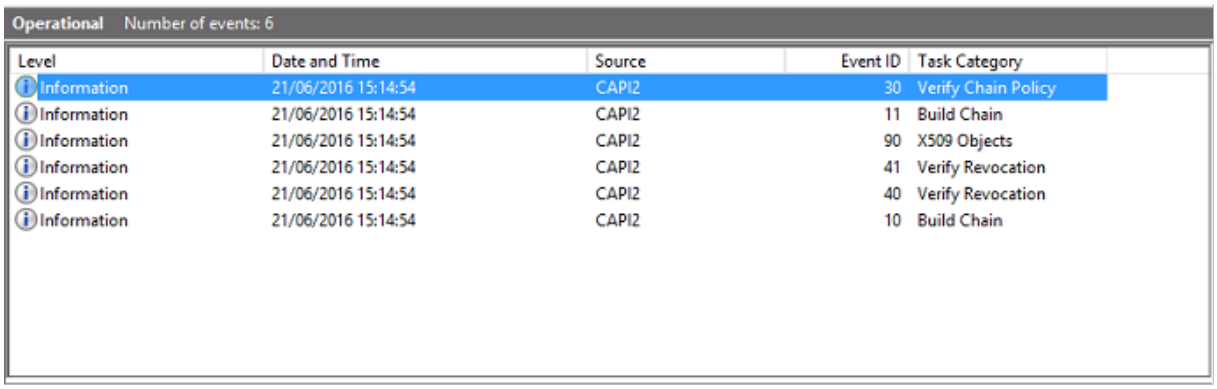
This section describes the expected log entries on the domain controller and workstation when the user logs on with a certificate.

- Domain controller CAPI2 log
- Domain controller security logs
- VDA security log
- VDA CAPI log
- VDA system log

### Domain controller CAPI2 log

During a logon, the domain controller validates the caller's certificate, producing a sequence of log entries in the following form.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



Operational Number of events: 6

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Information | 21/06/2016 15:14:54 | CAPI2 | 30 | Verify Chain Policy |
| Information | 21/06/2016 15:14:54 | CAPI2 | 11 | Build Chain |
| Information | 21/06/2016 15:14:54 | CAPI2 | 90 | X509 Objects |
| Information | 21/06/2016 15:14:54 | CAPI2 | 41 | Verify Revocation |
| Information | 21/06/2016 15:14:54 | CAPI2 | 40 | Verify Revocation |
| Information | 21/06/2016 15:14:54 | CAPI2 | 10 | Build Chain |

The final event log message shows lsass.exe on the domain controller constructing a chain based on the certificate provided by the VDA, and verifying it for validity (including revocation). The result is returned as "ERROR_SUCCESS".

- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [ **type**] CERT_CHAIN_POLICY_NT_AUTH
    - [ **constant**] 6
  - **Certificate**
    - [ **fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [ **subjectName**] fred
  - **CertificateChain**
    - [ **chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [ **value**] 0
  - **Status**
    - [ **chainIndex**] -1
    - [ **elementIndex**] -1
  - **EventAuxInfo**
    - [ **ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [ **TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [ **SeqNumber**] 1
  - **Result**
    - [ **value**] 0

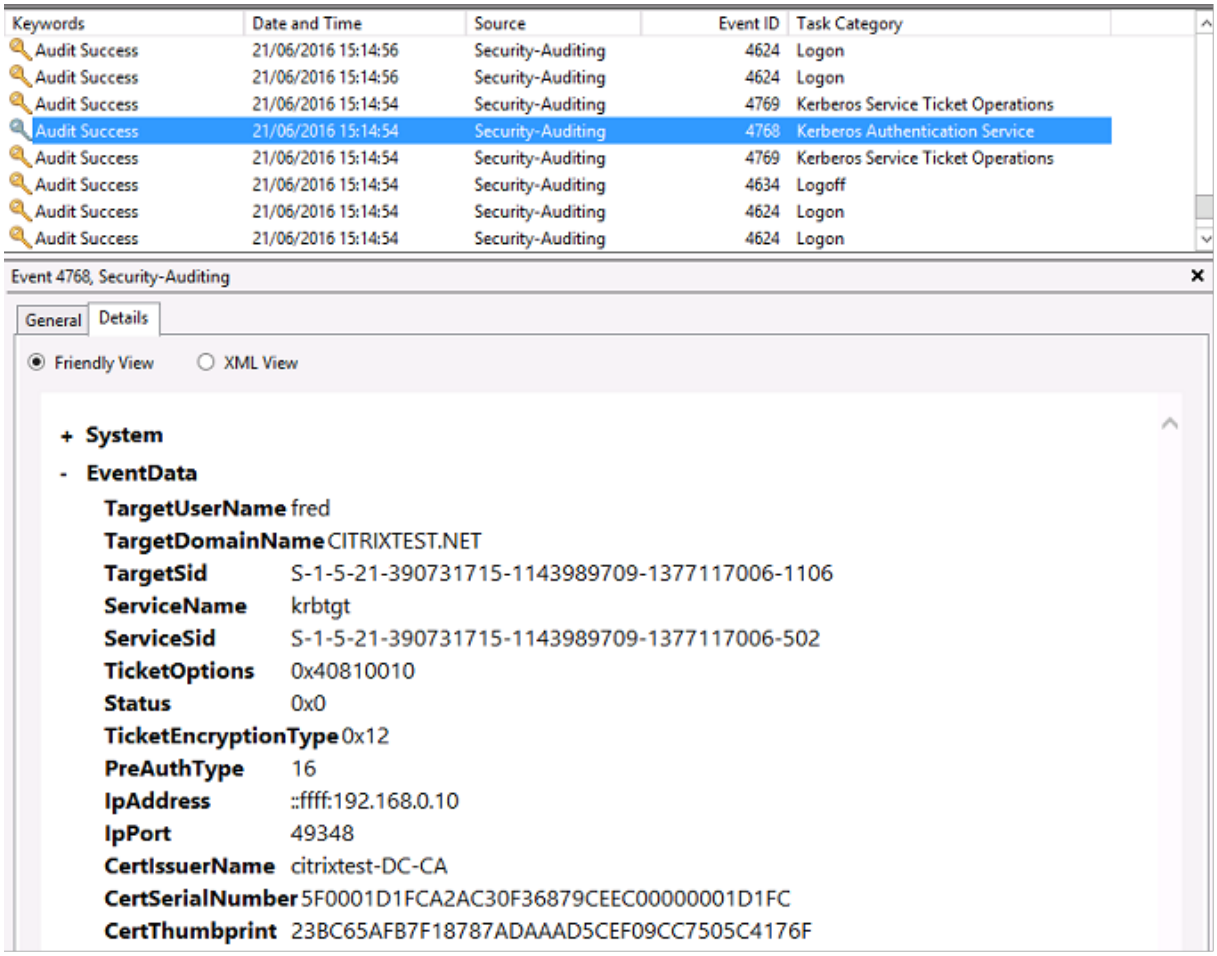
### Domain controller security log

The domain controller shows a sequence of logon events, the key event being 4768, where the certificate is used to issue the Kerberos Ticket Granting Ticket (krbtgt).

The messages before this show the machine account of the server authenticating to the domain con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

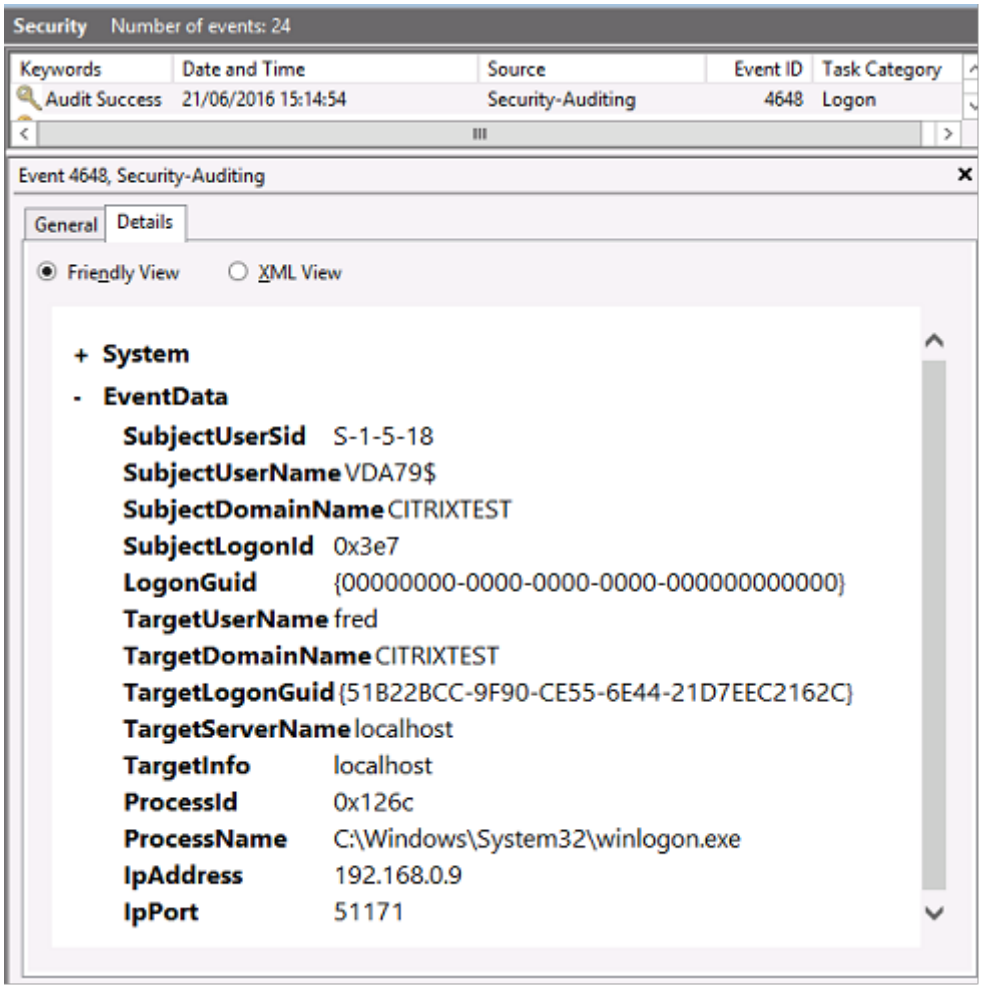
troller. The messages following this show the user account belonging to the new krbtgt being used to authenticate to the domain controller.




### VDA security log

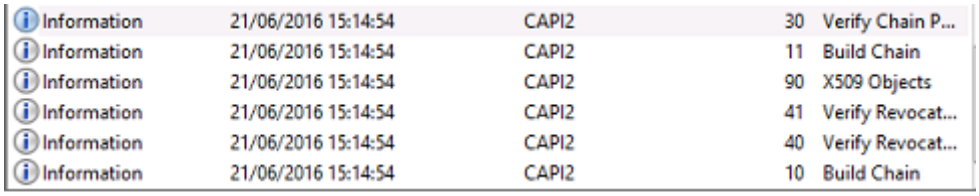
The VDA security audit log corresponding to the logon event is the entry with event ID 4648, originating from winlogon.exe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

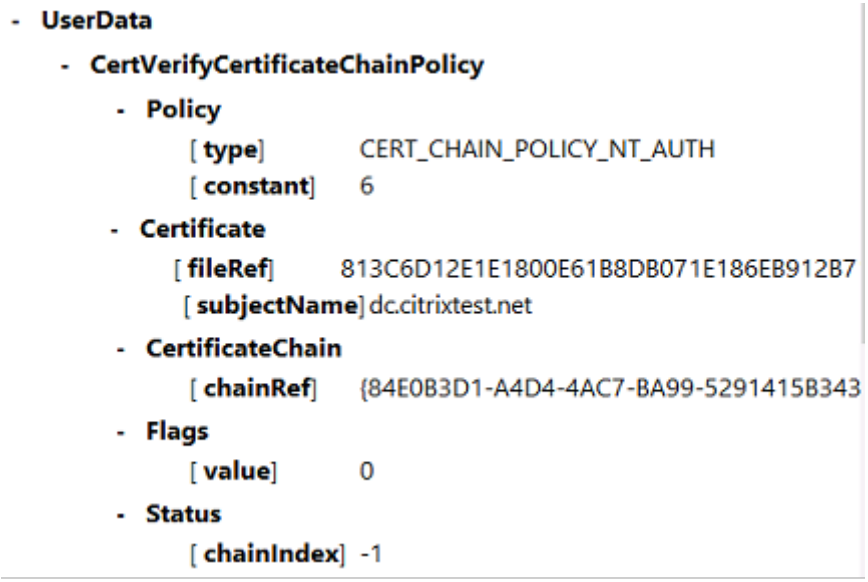



### VDA CAPI log

This example VDA CAPI log shows a single chain build and verification sequence from lsass.exe, validating the domain controller certificate (dc.citrixtest.net).

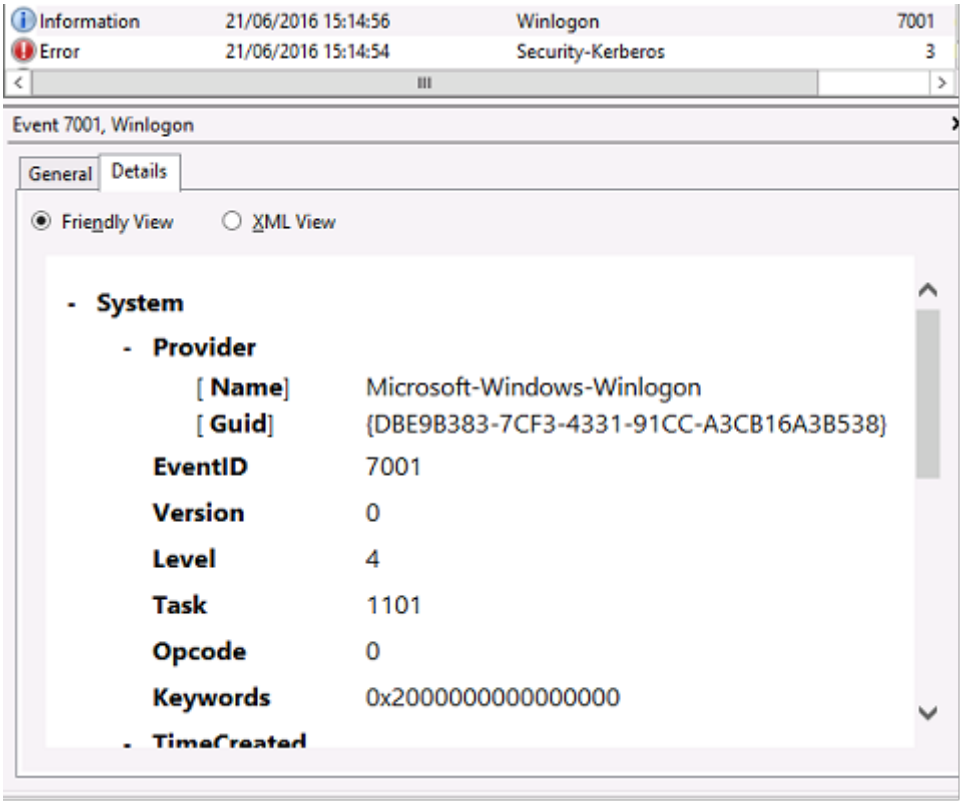



© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### VDA system log

When Kerberos logging is enabled, the system log shows the error KDC_ERR_PREAUTH_REQUIRED (which can be ignored), and an entry from Winlogon showing that the Kerberos logon was successful.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### End user error messages

This section lists common error messages displayed to a user on the Windows logon page.

| Error message displayed | Description and reference |
| --- | --- |
| Invalid Username or Password | The computer believes that you have a valid certificate and private key, but the Kerberos domain controller has rejected the connection. See the *Kerberos logs* section of this article. |
| The system could not log you on. Your credentials could not be verified. | The domain controller cannot be contacted, or the domain controller does not have appropriate certificates installed. |
| The request is not supported | Re-enroll the "Domain Controller"and "Domain Controller Authentication"certificates on the domain controller, as described in CTX206156. This is usually worth trying, even when the existing certificates appear to be valid. |
| The system could not log you on. The smartcard certificate used for authentication was not trusted. | The intermediate and root certificates are not installed on the local computer. See CTX206156 for instructions on installing smart card certificates on non-domain joined computers. Also, see the *Certificates and public key infrastructure* section in this article. |
| You cannot logon because smart card logon is not supported for your account. | A workgroup user account has not been fully configured for smart card logon. |
| The requested key does not exist | A certificate references a private key that is not accessible. This can happen when a PIV card is not completely configured and is missing the CHUID or CCC file. |
| An error occurred when trying to use the smart card | The smart card middleware was not installed correctly. See CTX206156 for smart card installation instructions. |
| Insert a smart card | The smart card or reader was not detected. If the smart card is inserted, this message indicates a hardware or middleware issue. See CTX206156 for smart card installation instructions. |
| The PIN is incorrect | The smart card rejected a PIN entered by the user. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Error message displayed | Description and reference |
| --- | --- |
| No valid smart card certificate could be found. | The extensions on the certificate might not be set correctly, or the RSA key is too short (<2048 bits). See CTX206901 for information about generating valid smart card certificates. |
| The smart card is blocked | A smart card has been locked (for example, the user entered an incorrect pin multiple times). An administrator may have access to the pin unlock (puk) code for the card, and can reset the user pin using a tool provided by the smart card vendor. If the puk code is not available, or locked out, the card must be reset to factory settings. |
| Bad Request | A smart card private key does not support the cryptography required by the domain controller. For example, the domain controller might have requested a "private key decryption,"but the smart card supports only signing. This usually indicates that the extensions on the certificate are not set correctly, or the RSA key is too short (<2048 bits). See CTX206901 for information about generating valid smart card certificates. |

### Related information

- Configuring a domain for smart card logon: https://support.citrix.com/article/CTX206156
- Smartcard logon policies: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)?redirectedfrom=MSDN
- Enabling CAPI logging: https://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Enabling Kerberos logging: https://support.microsoft.com/en-us/kb/262177
- Guidelines for enabling smart card logon with third-party certification authorities: https://support.microsoft.com/en-us/kb/281245

## Federated Authentication Service PowerShell cmdlets

June 16, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

You can use the Federated Authentication Service administration console for simple deployments; however, the PowerShell interface offers more advanced options. If you plan to use options that are not available in the console, Citrix recommends using only PowerShell for configuration.

The following command adds the FAS PowerShell cmdlets:

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

In a PowerShell window, you can use Get-Help <*cmdlet name*> to display cmdlet help.

The zip file linked below contains help files for all FAS PowerShell SDK cmdlets. To use it, click the link, which will download the zip file. Then extract its content to a local folder. The index.html file lists all cmdlets, with links to individual cmdlet help files.

Federated Authentication Service PowerShell cmdlet help files

## Graphics

April 4, 2019

Citrix HDX graphics include an extensive set of graphics acceleration and encoding technologies that optimizes the delivery of rich graphics applications from XenApp and XenDesktop. 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 (for example, OpenGL Software Accelerator). 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 XenApp and XenDesktop.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The HDX 3D Pro capabilities in XenApp and XenDesktop 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 desktop OS

By using HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Desktop 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 server OS

HDX 3D Pro allows graphics-heavy applications running in Windows Server 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

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, delivering a fluid and interactive user experience to users of virtual apps and desktops.

### OpenGL Software Accelerator

The OpenGL Software Accelerator is a software rasterizer for OpenGL applications such as ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, computer-aided design, and computer-aided manufacturing. Sometimes, the OpenGL Software Accelerator can eliminate the need to use graphics cards to deliver a good user experience with OpenGL applications.

## Related information

- Thinwire
- HDX 3D Pro
- GPU acceleration for Windows Desktop OS

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- GPU acceleration for Windows Server OS
- Framehawk
- OpenGL Software Accelerator

## Framehawk

October 29, 2018

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, delivering a fluid and interactive user experience to users of virtual apps and desktops. Framehawk might be a suitable choice for users on long-haul (high latency) broadband network connections where a small amount of packet loss can degrade the user experience. We suggest using adaptive transport for this use case - for more information, see Adaptive transport.

You can use Citrix policy templates to implement Framehawk for a set of users and access scenarios in a way that is appropriate for your organization. Framehawk targets single-screen mobile use cases such as laptops and tablets. Use Framehawk where the business value of real time interactive performance justifies the extra cost in server resources and the requirement for a broadband connection.

### How Framehawk maintains a smooth user experience

Think of Framehawk as a software implementation of the human eye, looking at what's in the frame buffer and discerning the different types of content on the screen. What's important to the user? When areas of the screen are changing rapidly, like video or moving graphics, it doesn't matter to the human eye if some pixels are lost because they are quickly overwritten with new data.

But when it comes to static areas of the screen, such as the icons in the notification area or a toolbar, or text after scrolling to where the user wants to start reading, the human eye is fussy. A user expects those areas to be pixel perfect. Unlike protocols aiming to be technically accurate from a **ones and zeros** perspective, Framehawk aims to be relevant to the human being who is using the technology.

Framehawk includes a next-generation Quality of Service signal amplifier plus a time-based heat map for a finer-grained and more efficient identification of workloads. It uses autonomic, self-healing transforms in addition to data compression, and avoids retransmission of data to maintain click response, linearity, and a consistent cadence. On a lossy network connection, Framehawk can hide loss with interpolation, and the user still perceives good image quality while enjoying a more fluid experience. In addition, Framehawk algorithms intelligently distinguish between different types of packet loss. For example, random loss (send more data to compensate) versus congestion loss (don't send more data because the channel is already clogged).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The Framehawk Intent Engine in Citrix Receiver distinguishes between scrolling up or down, zooming, moving to the left or right, reading, typing, and other common actions. The engine also manages the communication back to the Virtual Delivery Agent (VDA) using a shared dictionary. If the user is trying to read, the visual quality of the text must be excellent. If the user is scrolling, it must be quick and smooth. And it has to be interruptible, so that the user is always in control of the interaction with the application or desktop.

By measuring cadence on the network connection (**gearing**, analogous to tension on a bicycle chain), the Framehawk logic reacts more quickly, providing a superior experience over high latency connections. This unique and patented gearing system provides constant up-to-date feedback on network conditions, allowing Framehawk to react immediately to changes in bandwidth, latency, and loss.

### Design considerations using Thinwire and Framehawk

While Thinwire has led the industry in bandwidth efficiency and is suited to a broad range of access scenarios and network conditions, it uses TCP for reliable data communications. Therefore, it must retransmit packets on a lossy or overburdened network, leading to lag in the user experience. Thinwire over an enlightened data transport (EDT) layer is available, addressing the limitations of TCP on high latency network connections.

Framehawk uses a data transport layer built on top of (User Datagram Protocol (UDP). UDP is a small part of how Framehawk overcomes lossiness, as you can see when comparing the performance of Framehawk with other UDP-based protocols. UDP provides an important foundation to the human-centric techniques that set Framehawk apart.

How much bandwidth does Framehawk require?

The meaning of broadband wireless depends on several factors, including how many users are sharing the connection, the quality of the connection, and apps being used. For optimal performance, Citrix suggests a base of 4 Mbps or 5 Mbps plus about 150 Kbps per concurrent user.

Our bandwidth recommendation for Thinwire is generally a base of 1.5 Mbps plus 150 Kbps per user. For details, see the XenApp and XenDesktop bandwidth blog). At 3% packet loss, you will find that Thinwire over TCP needs much more bandwidth than Framehawk to maintain a positive user experience.

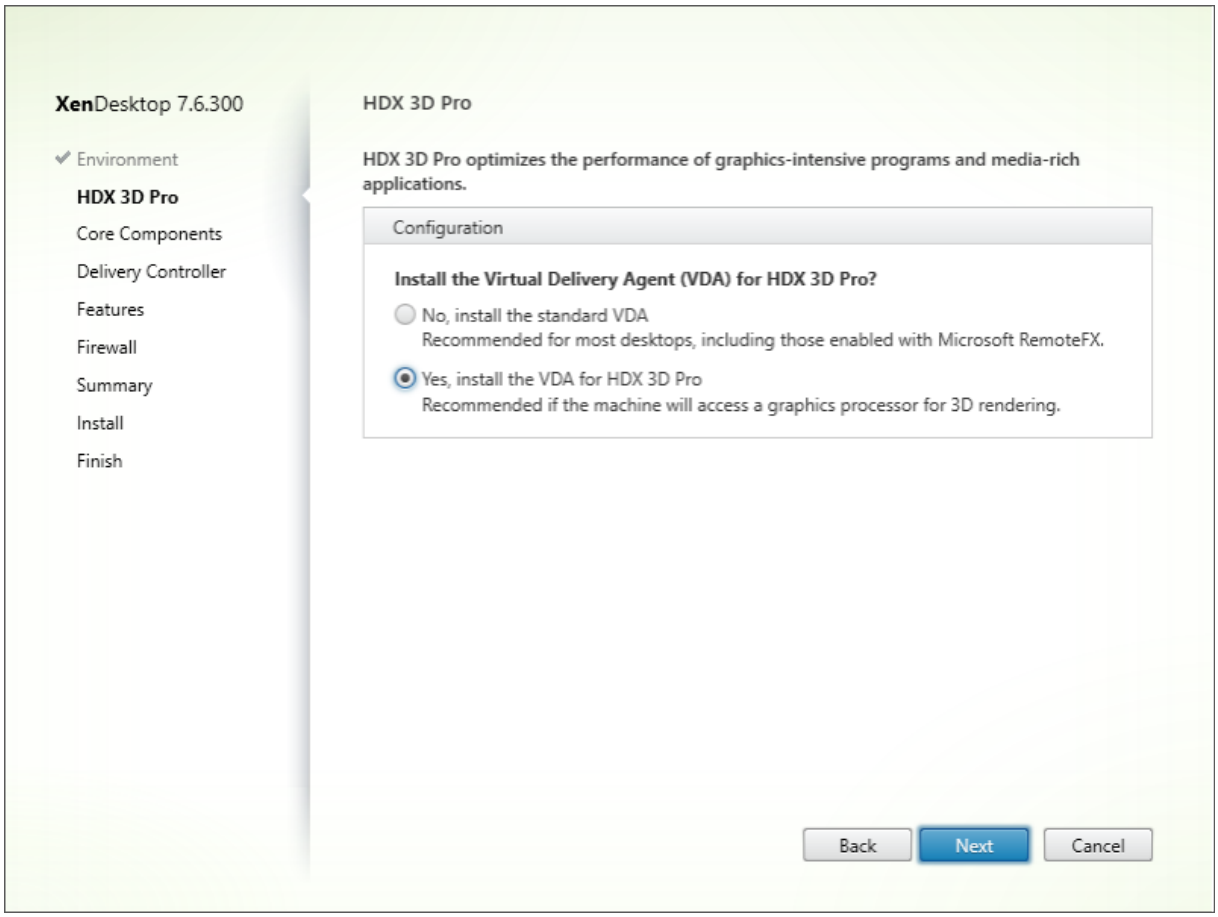
Thinwire remains the primary display remoting channel in the ICA protocol. Framehawk is disabled by default. Citrix recommends enabling it selectively to address the broadband wireless access scenarios in your organization. Remember that Framehawk requires considerably more server resources (CPU and memory) than Thinwire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Framehawk and HDX 3D Pro

Framehawk supports all the HDX 3D Pro use cases, both for XenApp (Server OS) and XenDesktop (Desktop OS) apps. It was validated in customer environments with 400-500 ms latency and 1-2% packet loss. Thus, providing good interactivity using typical 3D modeling apps such as AutoCAD, Siemens NX, and others. This support extends the ability to view and manipulate large CAD models while on the move, or working from an offshore location or poor network conditions. (Organizations that have a requirement to deliver 3D applications over long haul network connections are encouraged to use adaptive transport. For more information, see Adaptive transport.)

Enabling this functionality doesn't require any additional configuration tasks. When installing the VDA, select the 3DPro option at the beginning of the installation:




By using this selection, HDX uses the GPU vendor video driver rather than the Citrix video driver. It defaults to full-screen H.264 encoding over Thinwire rather than the usual default of Adaptive Display and Selective H.264 encoding.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Requirements and considerations

Framehawk requires minimum VDA 7.6.300 and Group Policy Management 7.6.300.

The endpoint must have a minimum Citrix Receiver for Windows 4.3.100 or Citrix Receiver for iOS 6.0.1.

By default, Framehawk uses a bidirectional User Datagram Protocol (UDP) port range (3224-3324) to exchange Framehawk display channel data with Citrix Receiver. The range can be customized in a policy setting called **Framehawk display channel port range**. Each concurrent connection between the client and the virtual desktop requires a unique port. For multi-user OS environments, such as XenApp servers, define sufficient ports to support the maximum number of concurrent user sessions. For a single-user OS, such as VDI desktops, it is sufficient to define a single UDP port. Framehawk attempts to use the first defined port, working up to the final port specified in the range. This applies both when passing through NetScaler Gateway, and internal connections directly to the StoreFront server.

For remote access, a NetScaler Gateway must be deployed. By default, NetScaler uses UDP port 443 for encrypted communication between the client Citrix Receivers and the Gateway. This port must be open on any external firewalls to allow secure communication in both directions. The feature is known as Datagram Transport Security (DTLS).

> **Note:**
>
> Framehawk/DTLS connections are not supported on FIPS appliances.

Encrypted Framehawk connections are supported, starting with NetScaler Gateway version 11.0.62 and NetScaler Unified Gateway version 11.0.64.34 or later.

NetScaler High Availability (HA) is supported from XenApp and XenDesktop 7.12.

Consider the following best practices before implementing Framehawk:

- Contact your Security administrator to confirm UDP ports defined for Framehawk are open on the firewall. The installation process does not automatically configure the firewall.
- Often, NetScaler Gateway might be installed in the DMZ, flanked by firewalls on both the external and the internal side. Ensure UDP port 443 is open on the external firewall. Ensure UDP ports 3224-3324 are open on the internal firewall if the environment is using the default port ranges.

### Configuration

> **Caution:**
>
> Citrix recommends that you enable Framehawk only for users who are likely to experience high

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> packet loss. We also recommend that you do not enable Framehawk as a universal policy for all objects in the Site.

Framehawk is disabled by default. When enabled, the server attempts to use Framehawk for user graphics and input. If the prerequisites are not met for any reason, the connection is established using the default mode (Thinwire).

The following policy settings affect Framehawk:

- Framehawk display channel: Enables or disables the feature.
- Framehawk display channel port range: Specifies the range of UDP port numbers (lowest port number to highest) that the VDA uses to exchange Framehawk display channel data with the user device. The VDA attempts to use each port, starting at the lowest port number and incrementing for each subsequent attempt. The port handles inbound and outbound traffic.

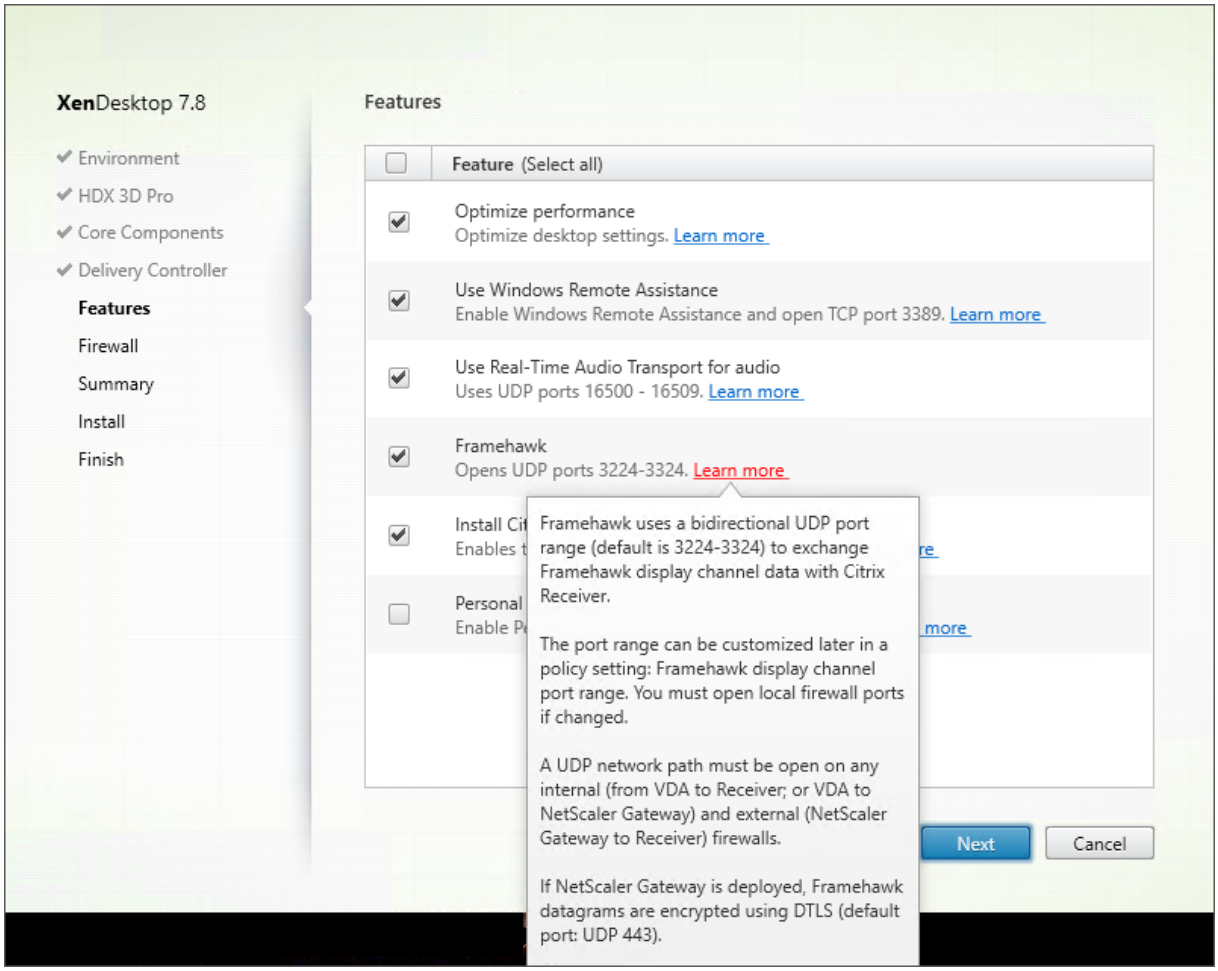
### Opening ports for the Framehawk display channel

From XenApp and XenDesktop 7.8, an option is available to reconfigure the Firewall during the **Features** step of the VDA installer. This check box opens UDP ports 3224-3324 on the Windows Firewall, if selected. Manual Firewall configuration is required in some circumstances:

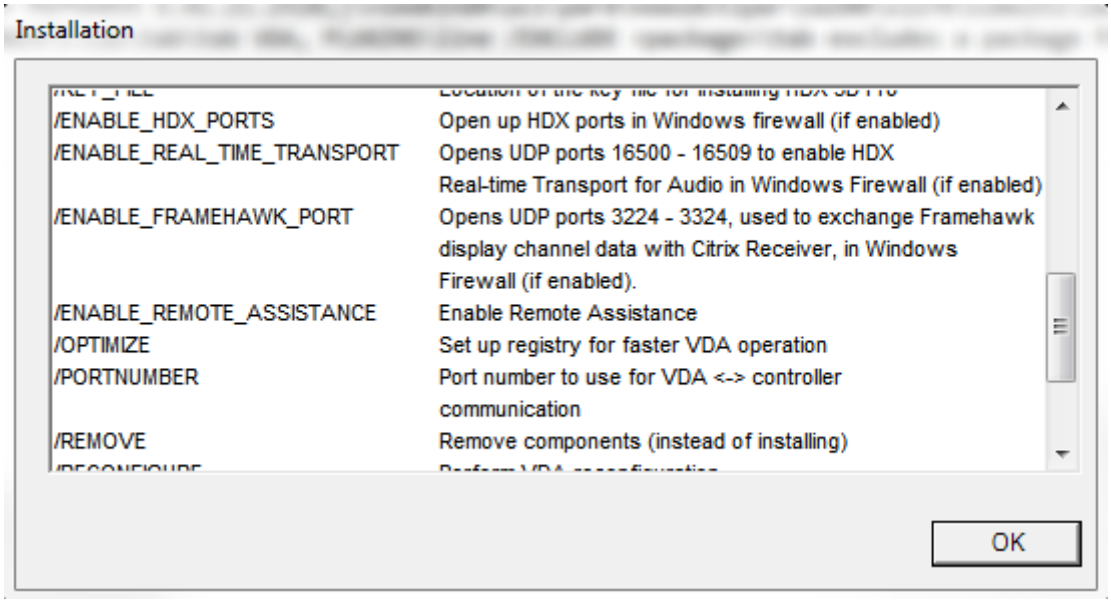
- For any network Firewalls.
  or
- The default port range is customized.

To open these UDP ports, select the **Framehawk** check box:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



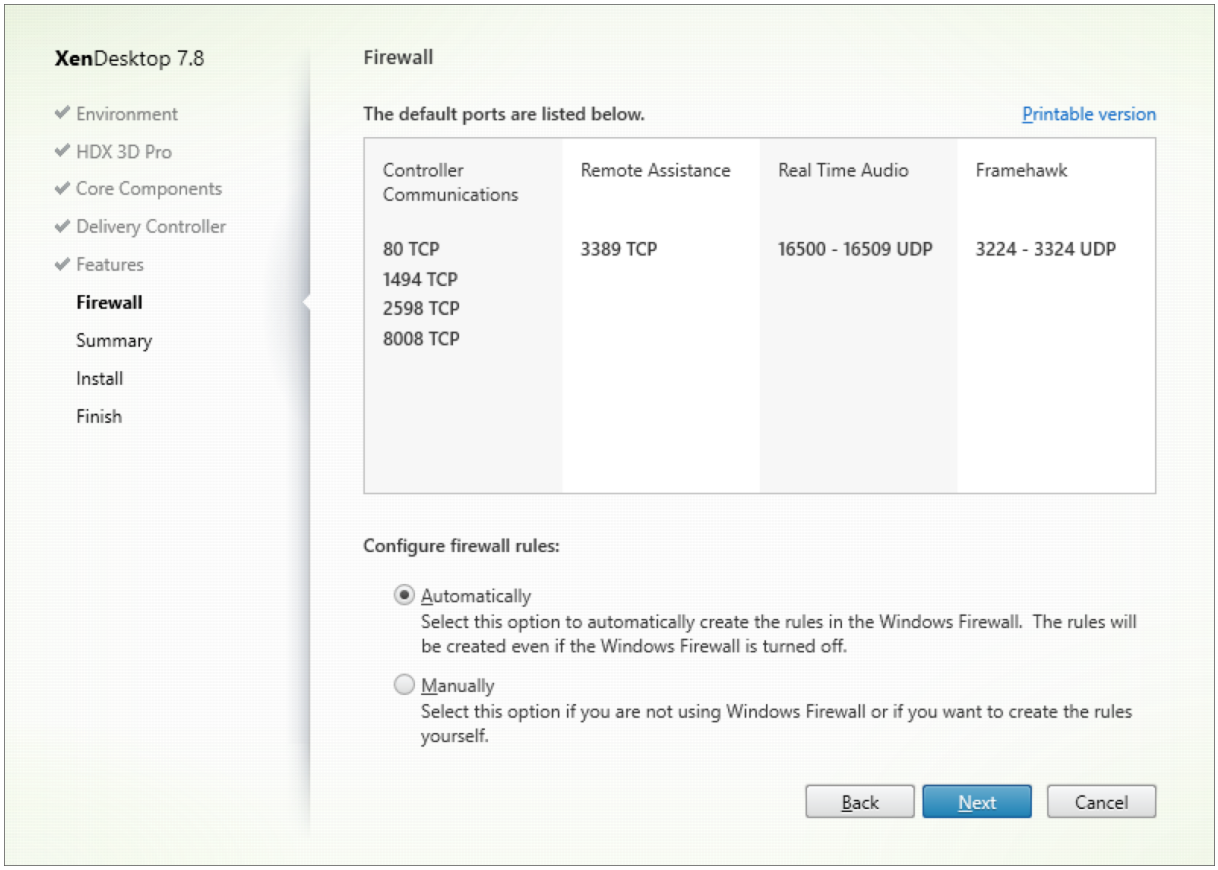

You can also use the command line to open UDP ports for Framehawk using **/ENABLE_FRAMEHAWK_PORT**:




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

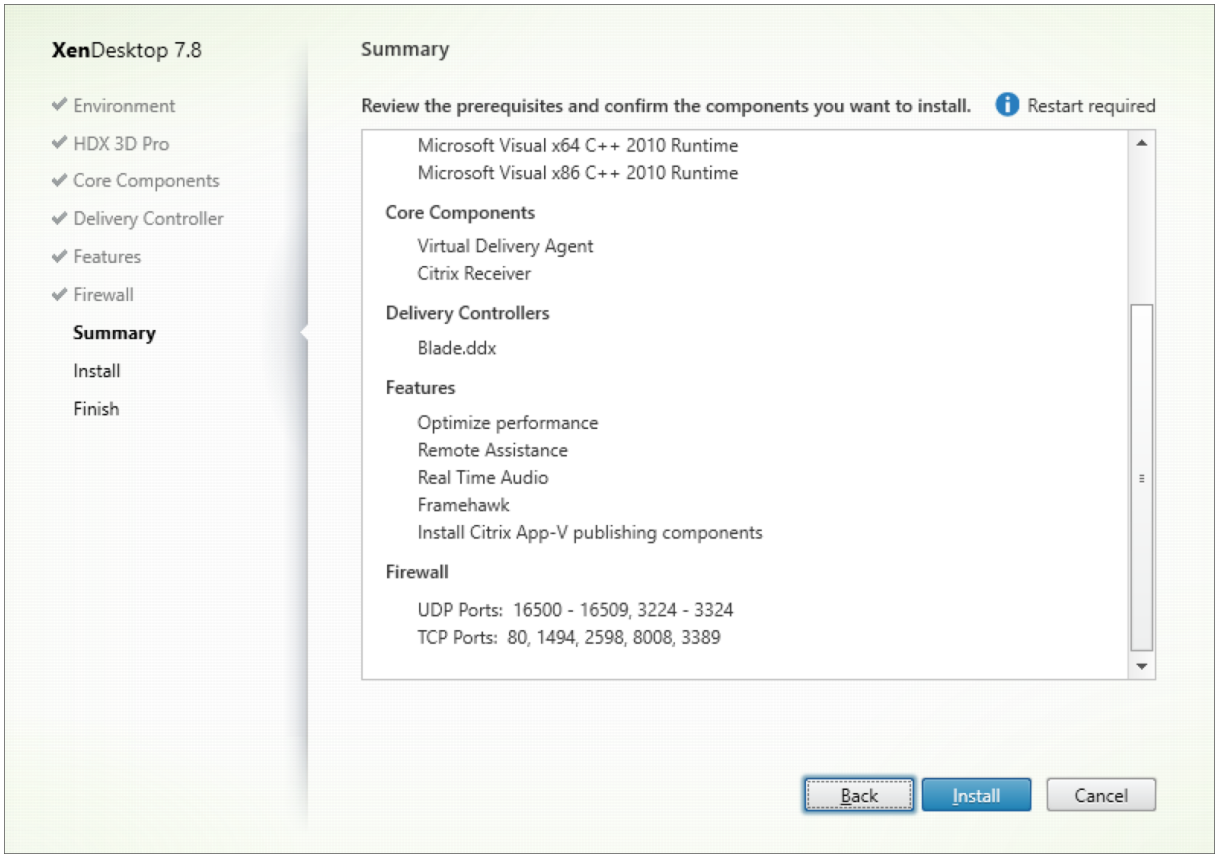
### Verifying Framehawk UDP port assignments

During installation, you can verify the UDP ports assigned to Framehawk in the **Firewall** screen:




The **Summary** screen indicates if the Framehawk feature is enabled:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### NetScaler Gateway support for Framehawk

Encrypted Framehawk traffic is supported on NetScaler Gateway 11.0.62.10 or later, and NetScaler Unified Gateway 11.0.64.34 or later.

- NetScaler Gateway refers to the deployment architecture where the Gateway VPN vServer is directly accessible from the end user device. That is, the VPN vServer has a public IP address assigned and the user connects to this IP address directly.
- NetScaler with Unified Gateway refers to the deployment where the Gateway VPN vServer is bound as a target to the Content Switching vServer (CS). In this deployment, CS vServer has the public internet protocol address and the Gateway VPN vServer has a dummy internet protocol address.

To enable Framehawk support on NetScaler Gateway, the DTLS parameter on the Gateway VPN vServer level must be enabled. After the parameter is enabled and the components on XenApp or XenDesktop are updated correctly, Framehawk audio, video, and interactive traffic is encrypted between the Gateway VPN vServer and the user device.

NetScaler Gateway, Unified Gateway, and NetScaler Gateway + global server load balancing are supported with Framehawk.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The following scenarios are not supported with Framehawk:

- HDX Insight
- NetScaler Gateway in IPv6 mode
- NetScaler Gateway Double Hop
- NetScaler Gateway with Cluster setup

| Scenario | Framehawk Support |
|---|---|
| NetScaler Gateway | Yes |
| NetScaler + global server load balancing | Yes |
| NetScaler with Unified Gateway | Yes. **Note:** Unified Gateway version 11.0.64.34 and later is supported. |
| HDX Insight | No |
| NetScaler Gateway in IPv6 mode | No |
| NetScaler Gateway Double Hop | No |
| Multiple Secure Ticket Authority on NetScaler Gateway | Yes |
| NetScaler Gateway and High Availability | Yes |
| NetScaler Gateway and Cluster setup | No |

### Configuring NetScaler for Framehawk support

To enable Framehawk support on NetScaler Gateway, enable the DTLS parameter on the Gateway VPN *vServer *level. After the parameter is enabled and the components on XenApp or XenDesktop are updated correctly, Framehawk audio, video, and interactive traffic is encrypted between the Gateway VPN vServer and the user device.

This configuration is required if you are enabling UDP encryption on NetScaler Gateway for remote access.

When configuring NetScaler for Framehawk support:

- Ensure UDP port 443 is open on any external firewalls
- Ensure CGP port (default 2598) is open on any external firewalls
- Enable DTLS in the settings for the VPN virtual server
- Unbind and rebind the SSL cert-key pair. This step is not required if you are using NetScaler version 11.0.64.34 or later.

To configure NetScaler Gateway for Framehawk support:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Deploy and configure NetScaler Gateway to communicate with StoreFront and authenticate users for XenApp and XenDesktop.
2. In the NetScaler Configuration tab, expand NetScaler Gateway, and select **Virtual Servers**.
3. Click **Edit** to display Basic Settings for the VPN Virtual Server; verify the state of the DTLS setting.
4. Click **More** to display more configuration options:
5. Select **DTLS** to provide communications security for datagram protocols such as Framehawk. Click **OK**. The Basic Settings area for the VPN Virtual Server shows that the DTLS flag is set to **True**.
6. Reopen the Server Certificate Binding screen, and click **+** to bind the certificate key pair.
7. Choose the certificate key pair from earlier, click **Select**.
8. Save the changes to the server certificate binding.
9. After saving, the certificate key pair appears. Click **Bind**.
10. Ignore the **No usable ciphers configured on the SSL vserver/service** warning message, if it appears.

#### Steps for older NetScaler Gateway versions

If you are using a version of NetScaler Gateway older than 11.0.64.34:

1. Reopen the Server Certificate Binding screen, and click + to bind the certificate key pair.
2. Choose the certificate key pair from earlier, click **Select**.
3. Save the changes to the server certificate binding.
4. After saving, the certificate key pair appears. Click **Bind**.
5. Ignore the **No usable ciphers configured on the SSL vserver/service** warning message, if it appears.

To configure Unified Gateway for Framehawk support:

1. Ensure that Unified Gateway is installed and properly configured. For additional information, see Unified Gateway information on the Citrix Product Documentation site.
2. Enable the DTLS parameter on the VPN *vServer, *which is bound to CS *vServer* as Target *vServer*.

### Limitations

If there are stale DNS entries for the NetScaler Gateway virtual server on the client device, adaptive transport and Framehawk might fall back to TCP transport instead of UDP transport. If fallback to TCP transport occurs, flush the DNS cache on the client and reconnect to establish the session using UDP transport.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Support for other VPN products

NetScaler Gateway is the only SSL VPN product to support the UDP encryption required by Framehawk. If another SSL VPN or an incorrect version of NetScaler Gateway is used, the Framehawk policy might fail to apply. Traditional IPsec VPN products support Framehawk without any modifications.

### Configure Citrix Receiver for iOS to support Framehawk

To configure older versions of Citrix Receiver for iOS to support Framehawk, you must manually edit default.ica.

1. On the StoreFront server, access the App_Data directory of your store in c:\inetpub\wwwroot\.
2. Open the default.ica file and add the following line in the WFClient section: Framehawk=On
3. Save the changes.

This procedure allows Framehawk sessions to be established from a compatible Citrix Receiver on iOS devices. This step is not required if you are using Citrix Receiver for Windows.

> **Note:**
>
> When using Citrix Receiver for iOS version 7.0 and later, you do not have to add the parameter **Framehawk=On** explicitly in the default.ica file.

### Monitoring Framehawk

You can monitor the use and performance of Framehawk from Citrix Director. The HDX Virtual Channel Details view contains useful information for troubleshooting and monitoring Framehawk in any session. To view Framehawk related metrics, select **Graphics-Framehawk**.

If the Framehawk connection is established, you see **Provider = VD3D** and **Connected = True** in the details page. It is normal for the virtual channel state to be idle, because it monitors the signaling channel, which is used only during the initial handshake. This page also provides other useful statistics about the connection.

If you encounter issues, see the Framehawk troubleshooting blog.

## HDX 3D Pro

October 29, 2018

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The HDX 3D Pro capabilities of XenApp and XenDesktop 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 more information about choosing the standard or HDX 3D Pro VDA, see "Step 5. Choose whether to enable HDX 3D Pro mode" in the Install VDAs article.

All supported Citrix Receivers 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 Receiver for Windows and Citrix Receiver for Linux. For more information on supported versions of Citrix Receiver, see Lifecycle Milestones for Citrix Receiver.

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 Desktop OS machines and Windows Server OS machines. For more information, see GPU acceleration for Windows Desktop OS and GPU acceleration for Windows Server OS.

HDX 3D Pro is compatible with GPU passthrough and GPU virtualization technologies offered by the following hypervisors, in addition to bare metal:

- Citrix XenServer
  - GPU passthrough with NVIDIA GRID and Intel GVT-d
  - GPU virtualization with NVIDIA GRID and Intel GVT-g
- Microsoft Hyper V
  - GPU passthrough (Discrete Device Assignment) with NVIDIA GRID and AMD

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- VMware vSphere
  - GPU passthrough (vDGA) with NVIDIA GRID, Intel, and AMD IOMMU
  - GPU virtualization with NVIDIA GRID and AMD MxGPU

For the supported XenServer versions, see Citrix XenServer 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 Server OS

October 29, 2018

HDX 3D Pro allows graphics-heavy applications running in Windows Server 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, the server's CPU is not slowed by graphics rendering. Additionally, 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, a GPU accessed by XenApp can be shared by multiple users 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.

You can install multiple GPUs on a hypervisor and assign VMs to each of these GPUs on a one-to-one basis: either install a graphics card with more than one GPU, or install multiple graphics cards with one or more GPUs each. Mixing heterogeneous graphics cards on a server is not recommended.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Virtual machines require direct passthrough access to a GPU, which is available with Citrix XenServer, VMware vSphere vDGA and Intel GVT-d. When HDX 3D Pro is used with GPU Passthrough, each GPU in the server supports one multi-user virtual machine.

GPU Sharing does not depend on any specific graphics card.

- When running on a hypervisor, select a hardware platform and graphics cards that are compatible with your hypervisor's GPU Passthrough implementation. The list of hardware that has passed certification testing with XenServer GPU Passthrough is available at GPU Passthrough Devices.
- 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 extremely overloaded, this could cause instability or a crash of the graphics card driver. 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 https://www.techpowerup.com/gpuz/.

### DirectX, Direct3D, and WPF rendering

DirectX, Direct3D, and WPF rendering is 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 Server OS sessions:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- [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 Desktop OS

October 29, 2018

With HDX 3D Pro you can deliver graphically intensive applications as part of hosted desktops or applications on Desktop 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 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.

Using GPU virtualization, multiple virtual machines can directly access the graphics processing power of a single physical GPU. The true hardware GPU sharing provides desktops suitable for users with complex and demanding design requirements. GPU virtualization for NVIDIA GRID cards (see NVIDIA GRID) uses the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems. GPU virtualization is also supported for 5th and 6th Generation Intel CPUs with Intel Iris Pro graphics

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

with Intel GVT-g. For more information on these families of Intel processors, see 5th Generation Intel Core Processors and 6th Generation Intel Core i5 Processors. GPU virtualization is also supported for AMD FirePro S-Series server cards, see AMD Professional Graphics virtualization solution.

HDX 3D Pro offers the following features:

- Adaptive H.264-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 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 significantly more network and processing resources.

  When using lossless compression:

  - The lossless indicator, a system tray icon, notifies the user if the screen displayed is a lossy frame or a lossless frame. This 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 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 HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKLM_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 more information on virtual key codes, see Virtual-Key Codes on MSDN.
  - For example:
    * For F10, set K=0x79
    * For Ctrl + F10, set C=1, K=0x79

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

* 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 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.

- Multiple and high resolution monitor support. For desktop 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, 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 GRID architecture. HDX 3D Pro supports NVIDIA GRID cards (see NVIDIA GRID) for GPU passthrough and GPU sharing. NVIDIA GRID 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 GRID 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 https://www.citrix.com/intel and https://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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

XenServer and Hyper-V are supported with GPU passthrough. For more information, see AMD Virtualization Solution.

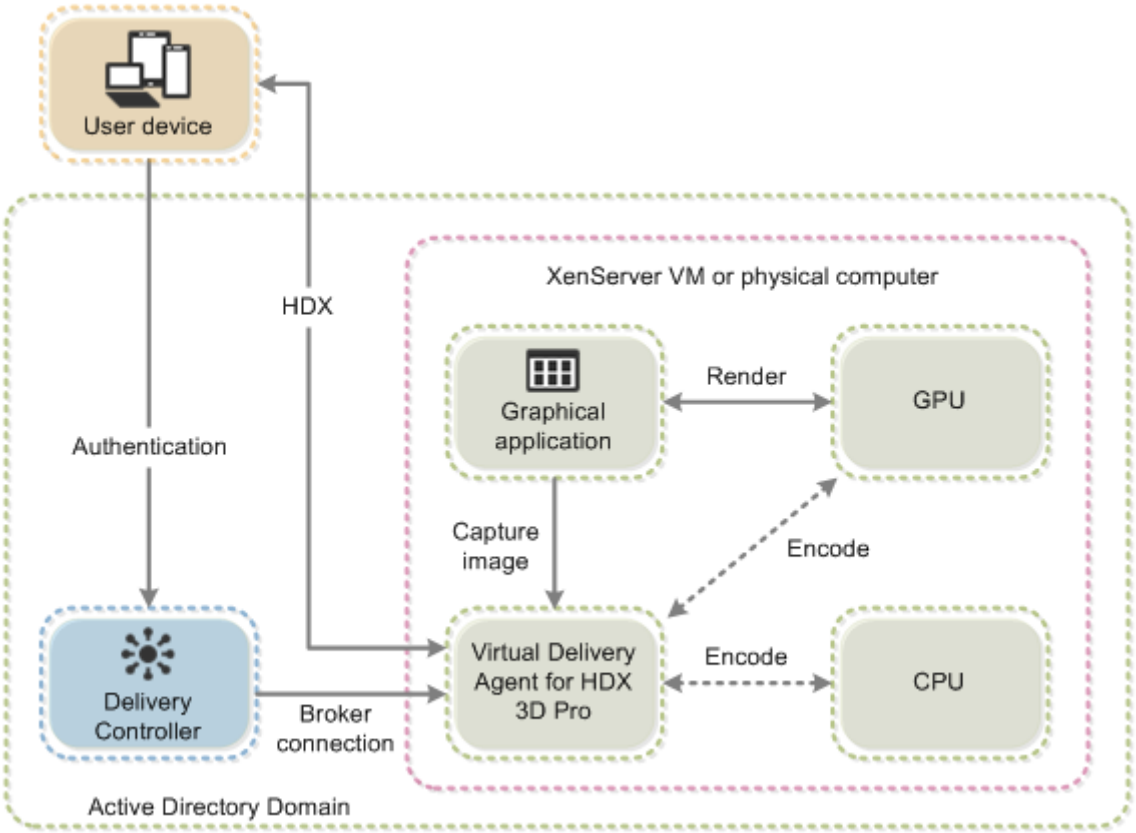
- Access to a high-performance video encoder for NVIDIA GPUs and Intel Iris Pro graphics processors. This feature is controlled by a policy setting (enabled by default) and allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA will fall back 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 Receiver and accesses the virtual application or desktop, the Controller authenticates the user and 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 through a direct HDX connection between Citrix Receiver and the VDA for HDX 3D Pro.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Install the VDA for HDX 3D Pro

When you use the installer's graphical interface to install a VDA for Windows Desktop OS, select Yes on the HDX 3D Pro page. When using the command line interface, include the /enable_hdx_3d_pro option with the XenDesktop VdaSetup.exe command.

To upgrade HDX 3D Pro, uninstall both the separate HDX 3D for Professional Graphics component and the VDA before installing the VDA in HDX 3D Pro mode. Similarly, to switch from the standard VDA mode for Windows Desktop OS to the 3D Pro mode, uninstall the standard VDA and then install the VDA in HDX 3D Pro mode.

| Standard Mode | HDX 3D Pro mode |
| --- | --- |
| Generally best for virtual desktops without graphics hardware acceleration, and for Remote PC Access. | Generally best for data center desktops with graphics hardware acceleration, unless more than four monitors are required. |
| Any GPU can be used for Remote PC Access, with some app compatibility limitations: On Windows 7, 8, and 8.1, GPU acceleration for DirectX feature levels up to 9.3. Some DirectX 10, 11, 12 applications may not run if they do not tolerate fallback to DirectX 9. On Windows 10, GPU acceleration is provided for windowed DirectX 10, 11, and 12 apps. DX 9 apps are rendered by WARP. DX apps cannot be used in full-screen mode. OpenGL application acceleration in remote sessions if supported by the GPU vendor (currently only NVIDIA). | Supports GPU acceleration with any GPU, however console blanking, non-standard screen resolutions and true multi-monitor support require NVIDIA GRID, Intel Iris Pro, or AMD RapidFire graphics. Leverages graphics vendor's driver for broadest application compatibility: All 3D APIs (DirectX or OpenGL) that the GPU supports. Full-screen 3D app support with Intel Iris Pro (Win10 only) and NVIDIA GRID and AMD RapidFire. Support for custom driver extensions and APIs. For example, CUDA or OpenCL. |
| Arbitrary monitor resolutions (limit determined by Windows OS and performance) and up to eight monitors. | Supports up to four monitors. |
| H.264 hardware encoding available with Intel Iris Pro graphics processors. | H.264 hardware encoding available with Intel Iris Pro graphics processors and NVIDIA cards. |

### Install and upgrade NVIDIA drivers

The NVIDIA GRID API provides direct access to the frame buffer of the GPU, providing the fastest possible frame rate for a smooth and interactive user experience. If you install NVIDIA drivers before you install a VDA with HDX 3D Pro, NVIDIA GRID is enabled by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To enable NVIDIA GRID on a VM, disable Microsoft Basic Display Adapter from the Device Manager. Run the following command and then restart the VDA: **NVFBCEnable.exe -enable -noreset**

If you install NVIDIA drivers after you install a VDA with HDX 3D Pro, NVIDIA GRID is disabled. Enable NVIDIA GRID by using the NVFBCEnable tool provided by NVIDIA.

To disable NVIDIA GRID, run the following command and then restart the VDA: **NVFBCEnable.exe -disable -noreset**

### Install Intel graphics drivers

You can install the Intel graphics drivers before installing the VDA. The following step is only required if you install Intel drivers after you install a VDA with HDX 3D Pro or if the Intel driver has been updated.

In order to enable the Intel drivers required for multi-monitor support, run the following command using the GfxDisplayTool.exe, then restart the VDA: **GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exe is included with the VDA installer. The GfxDisplayTool.exe is in C:\Program Files\Citrix\ICAServices.

> **Note:**
>
> Uninstalling NVIDIA or Intel drivers within ICA sessions is not supported.

### 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 for the duration of 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 Receiver - Desktop Viewer Preferences.

When multiple users share a connection with limited bandwidth (for example, at a branch office), Citrix recommends that you use the Overall session bandwidth limit policy setting to limit the bandwidth available to each user. This ensures that the available bandwidth does not fluctuate widely as users log on and off. Because HDX 3D Pro automatically adjusts to make use of all the available bandwidth, large variations in the available bandwidth over the course of user sessions can negatively impact performance.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 at all times.

For users of a 3D mouse, Citrix recommends that you increase the priority of the Generic USB Redirection virtual channel to 0. For information about changing the virtual channel priority, see CTX128190.

## OpenGL Software Accelerator

July 23, 2018

The OpenGL Software Accelerator is a software rasterizer for OpenGL applications such as ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, and CAD/CAM applications. Sometimes, the OpenGL Software Accelerator can eliminate the need to use graphics cards to deliver a good user experience when using OpenGL applications.

> **Important**
>
> We provide the OpenGL Software Accelerator *as is* and must be tested using all applications because it might not support some applications. If the Windows OpenGL rasterizer does not provide adequate performance, it is a solution to try . If the OpenGL Software Accelerator supports your applications, you can use it as a way to avoid the cost of GPU hardware.

The OpenGL Software Accelerator is provided in the support folder on the installation media, and is supported on all valid VDA platforms.

When to try the OpenGL Software Accelerator:

- On servers without graphics processing hardware, and the performance of OpenGL applications running in virtual machines on XenServer or other hypervisors is an issue. For some applications, the OpenGL Accelerator outperforms the Microsoft OpenGL software rasterizer that is included in Windows because the OpenGL Accelerator uses SSE4.1 and AVX. OpenGL Accelerator also supports applications using OpenGL versions up to 2.1.
- For applications running on a workstation, first try the default version of OpenGL support provided by the workstation graphics adapter. If the graphics card is the latest version, usually it delivers the best performance. If the graphics card is an earlier version or does not deliver satisfactory performance, try the OpenGL Software Accelerator.
- 3D OpenGL applications that are not adequately delivered using CPU-based software rasterization might benefit from OpenGL GPU hardware acceleration. This feature can be used on bare metal or virtual machines.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Thinwire

November 1, 2018

## Introduction

Thinwire is the Citrix default display remoting technology used in XenApp and XenDesktop.

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 XenApp and XenDesktop.

## Thinwire or Framehawk

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.

Framehawk should be used for mobile workers on broadband wireless connections where packet loss can be intermittently high.

## HDX 3D Pro

In its default configuration, Thinwire can deliver 3D or highly interactive graphics, however enabling HDX 3D Pro mode during the installation of the VDA for Desktop OS is a good option for such scenarios. The 3D Pro mode configures Thinwire with full-screen H.264 encoding for graphics transmission. This provides a more fluid experience for 3D professional graphics. For more information, see HDX 3D Pro and GPU acceleration for Windows Desktop 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

- The policy setting which drives the behavior of Thinwire, **Use video codec for compression**, is available on VDA versions in XenApp and XenDesktop 7.6 FP3 and later. The **Use video codec when preferred** option is the default setting on VDA versions XenApp and XenDesktop 7.9 and later.
- All Citrix Receivers support Thinwire. Some Citrix Receivers 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 Receiver.
- 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.

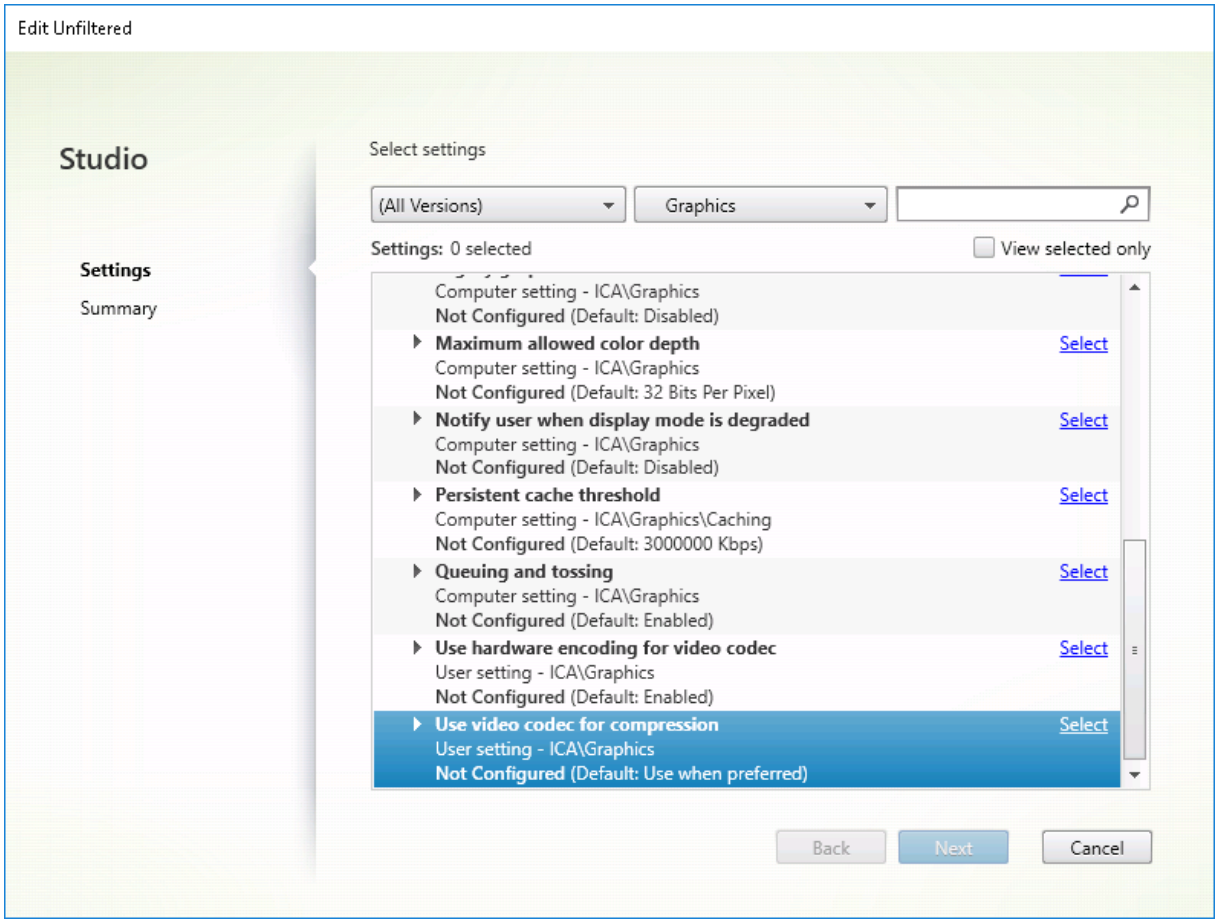
### Configuration

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 only in the part of the screen where the image is moving.
  - **For the entire screen**. Delivers Thinwire with full-screen H.264 to optimize for improved user experience and bandwidth, especially in cases with heavy use of 3D graphics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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

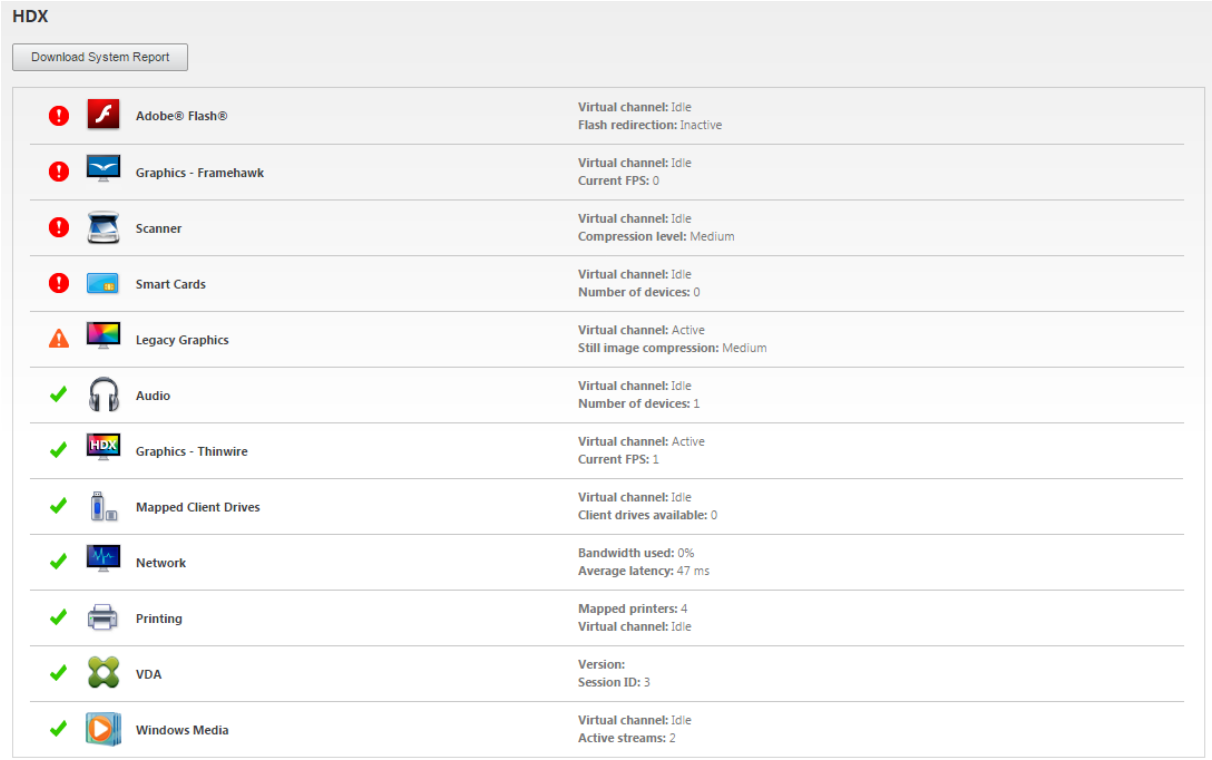
You can monitor the use and performance of Thinwire from Citrix Director. The HDX virtual channel details view contains useful information for troubleshooting and monitoring Thinwire in any session. To view Thinwire-related metrics:

1. In Director, search for a user, machine or endpoint, open an active session and click **Details**. Or,

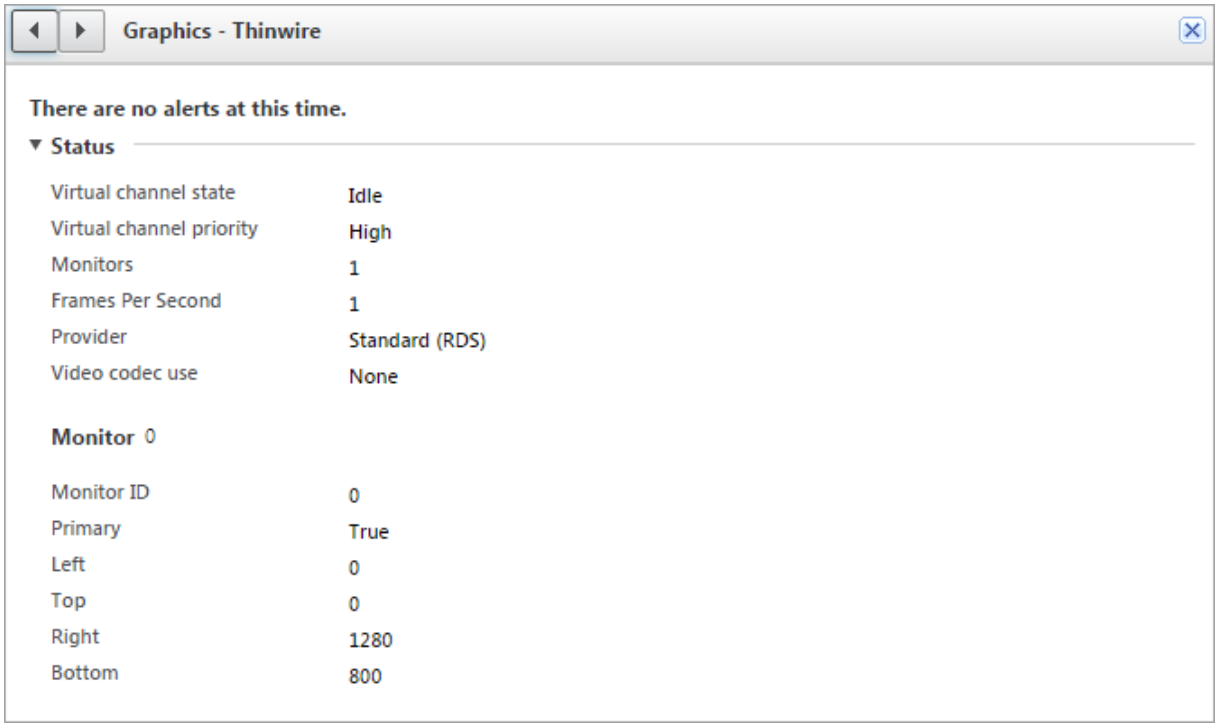
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

you can select **Filters** > **Sessions** > **All Sessions**, open an active session and click **Details**.

2. Scroll down to the **HDX** panel.




1. Select **Graphics - Thinwire**.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Multimedia

July 3, 2018

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 cost-per-user.

With server-rendered multimedia delivery, audio and video content is decoded and rendered on the XenApp or XenDesktop server by the application. The content is then compressed and delivered over the ICA protocol to the Citrix Receiver 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 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 and NVIDIA NVENC technologies provided hardware-accelerated H.264 encoding.

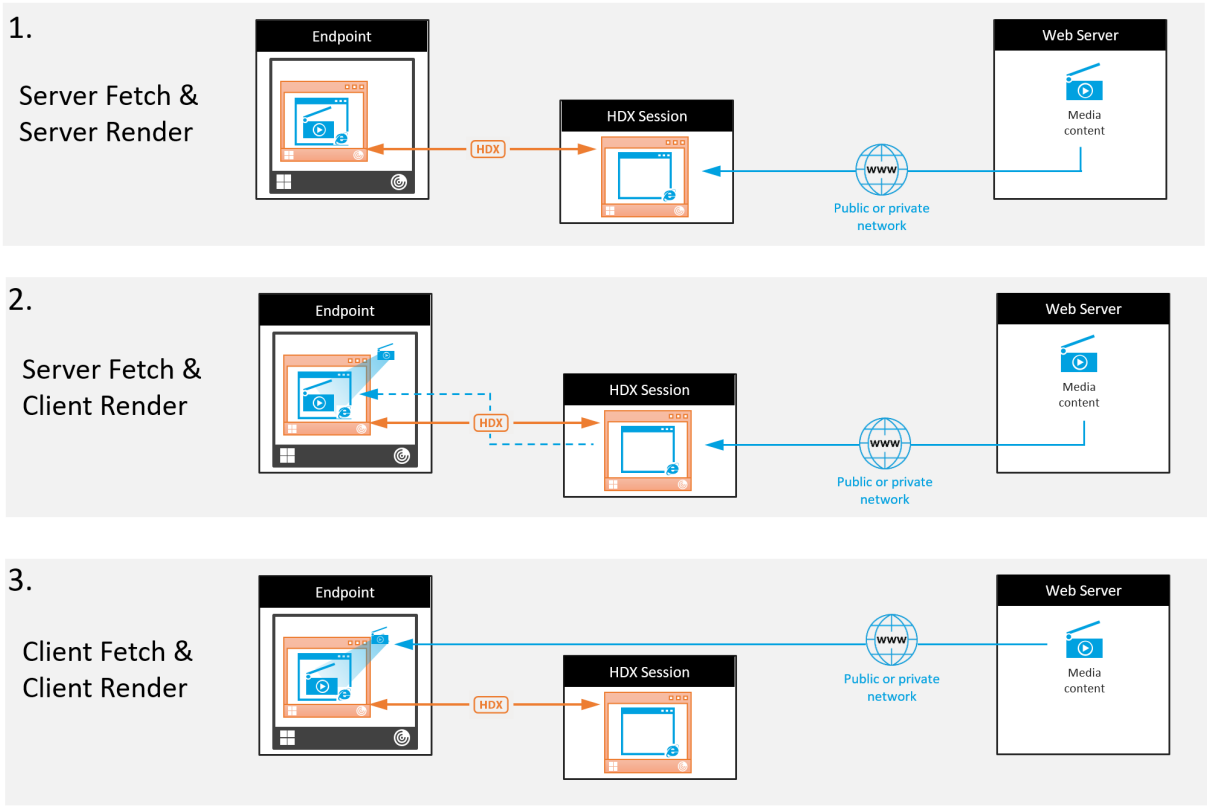
Because most servers do not offer hardware acceleration for video compression, server scalability is negatively impacted if all video processing is done on the server CPU. To maintain high server scalability, many multimedia formats can be redirected to the user device for local rendering. Windows Media redirection offloads the server for a wide variety of media formats typically associated with the Windows Media Player.

Flash redirection redirects Adobe Flash video content to a Flash player running locally on the user device.
HTML5 video has become popular, and Citrix introduced a redirection technology for this type of content.
Also, you can apply the general contact redirection technologies Host-to-client redirection and Local App Access to 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. This advantage of this approach is that the decoding and presentation is offloaded to the client devices, saving CPU cycles on the server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 URL of the media content before it is 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 only control commands are sent from the server. However, the media content is not always accessible to the clients.

### Framework and platform

Desktop operating systems (Windows, Mac OS X, and Linux) provide multimedia frameworks that enable the faster and easier 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

| Media redirection | Support |
|---|---|
| HDX Flash redirection | No |
| Windows Media redirection | Yes |
| HTML5 Video redirection | Yes |
| Audio redirection | N0 |

### Related information

- Audio features

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Flash redirection
- HTML5 multimedia redirection
- Windows Media redirection
- General content redirection

## Audio features

October 28, 2021

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**
>
> Although it is best to deliver audio using User Datagram Protocol (UDP) rather than TCP, UDP audio encryption using DTLS is available only between NetScaler Gateway and Citrix Receiver. Therefore, sometimes it might be preferable to use TCP transport. TCP supports end-to-end TLS encryption from the VDA to Citrix Receiver.

### 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, and 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), because it may introduce latency into the audio path that is not suitable for real-time communications. The optimized for speech policy setting is recommended for real-time audio, regardless of the selected transport protocol.

When 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device; see "Audio setting policies for user devices"later in this article.

### Client audio redirection

To allow users to receive audio from an application on a server through speakers or other sound devices (such as headphones) on the user device, leave the Client audio redirection setting at its default (Allowed).

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; see "Audio setting policies for user devices"later in this article.

### 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, users are alerted when servers that are not trusted by their user devices try to access microphones, and can choose to accept or reject access prior to using the microphone. Users can disable this alert on Citrix Receiver.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device; see "Audio setting policies for user devices"later in this article.

### 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 even if they are not plugged in until after the user session has been established.

This setting applies only to Windows Server 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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; see "Audio setting policies for user devices"later in this article.

### 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 time of installation), opening up a UDP port on the server for connections that use Audio over UDP Real-time Transport. Citrix recommends configuring UDP/RTP for audio, to ensure the best possible user experience in the event of network congestion or packet loss. For real time audio such as softphone applications, UDP audio is now preferred more than EDT. UDP allows for packet loss without retransmission, ensuring that no latency is added on connections with high packet loss.

> **Important:**
>
> Audio data transmitted with UDP is not encrypted when NetScaler Gateway is not in the path. If NetScaler Gateway is configured to access XenApp and XenDesktop resources then audio traffic between the endpoint device and NetScaler Gateway is secured using the DTLS protocol.

The Audio UDP port range specifies the range of port numbers that the Virtual Delivery Agent (VDA) uses to exchange audio packet data with the user device.

By default, the range is 16500–16509.

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; see "Audio setting policies for user devices"later in this article.

### 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 Receiver > User Experience.
3. For **Client audio settings**, select **Not Configured**, **Enabled**, or **Disabled**.
    - **Not Configured**. By default Audio Redirection is enabled with high quality audio or previously configured custom audio settings.
    - **Enabled**. Audio redirection is enabled with selected options.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Disabled**. Audio redirection is disabled.

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 NetScaler Gateway, select **Allow Real-Time Transport Through gateway**. NetScaler Gateway must be configured with DTLS. For more information, see UDP Audio Through a NetScaler Gateway.

As an Administrator, if you do not have control on endpoint devices to make these changes, for example in the case of BYOD or home computers, then use the default.ica attributes from StoreFront to enable UDP Audio.

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 entries below under the [Application] section.

```
; This is to enable Real-Time Transport
EnableRtpAudio=true
; This is to Allow Real-Time Transport Through gateway
EnableUDPThroughGateway=true
; This is to set audio quality to Medium
AudioBandwidthLimit=1
; UDP Port range
RtpAudioLowestPort=16500
RtpAudioHighestPort=16509
 <!--NeedCopy-->
```

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 echo. The effectiveness of echo cancellation is sensitive to the distance between the speakers and the microphone. Devices can not be 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> 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.

XenApp and XenDesktop support several alternatives for delivering softphones.

- **Control mode**. The hosted softphone simply controls a physical telephone set. In this mode, no audio traffic goes through the XenApp or XenDesktop server.
- **HDX RealTime optimized softphone support**. The media engine runs on user device, and Voice over Internet Protocol (VoIP) traffic flows peer-to-peer. For examples, see:
  - HDX RealTime Optimization Pack, which optimizes the delivery of Microsoft Skype for Business and Lync.
  - Cisco Virtualization Experience Media Engine (VXME) for Jabber.
  - Avaya VDI Communicator for one-X Communicator and one-X Agent. (The one-X Agent can be used only as a remote control app for desktop phones.)
- **Local App Access**. A XenApp and XenDesktop feature that allows an application such as a softphone to run locally on the end user Windows device yet appear seamlessly integrated with their virtual/published desktop. This offloads all audio processing to the user device. For more information, see Local App Access and URL redirection.
- **HDX RealTime generic softphone support.** VoIP-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 Receiver.

Generic softphone support is a feature of HDX RealTime. This approach to softphone delivery is especially useful when:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 needed for optimized delivery of the softphone has not been installed on the user device or is not 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 XenApp and XenDesktop:

- How the softphone application is delivered to the virtual/published desktop.
- How the audio is delivered to and from the end user headset, microphone, and speakers, or USB telephone set.

XenApp and XenDesktop include numerous technologies to support generic softphone delivery:

- Optimized-for-Speech codec for fast encode of real-time audio and bandwidth efficiency.
- Low latency audio stack.
- Server-side jitter buffer to smooth out the audio when 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 Receiver versions for Windows, Linux, Chrome, and Mac also are VoIP capable. Citrix Receiver for Windows offers these features:

- Client-side jitter buffer - Ensures smooth audio even when 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 (QoS)-based routing over the network.
- ICA supports four TCP and two UDP streams. One of the UDP streams supports real-time audio over RTP.

For a summary of Citrix Receiver capabilities, see Citrix Receiver Feature Matrix.

***System configuration recommendations***

**Client Hardware and Software:** For optimal audio quality, we recommend the latest version of Citrix Receiver and a good quality headset with acoustic echo cancellation (AEC). Citrix Receiver versions for Windows, Linux, and Mac support VoIP. Also, Dell Wyse offers VoIP 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

virtual CPUs reduces the thread switching latency. Therefore, we recommend that you configure two vCPUs in a XenDesktop 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 Local Area Network (LAN) and Wide Area Network (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 Citrix SD-WAN between the data center and the remote office to maintain a high Quality-of-Service. Citrix SD-WAN supports Multi-Stream ICA, including UDP. Also, in the case of a single TCP stream, it is possible to distinguish the priorities of various ICA virtual channels to ensure that high priority real-time audio data gets preferential treatment.

With Direct Workload Connection, audio-over-UDP can be encrypted using Citrix SD-WAN after authentication through the Gateway.

Use Director or the HDX Monitor to validate your HDX configuration.

Remote user connections: NetScaler Gateway 11 supports DTLS to deliver UDP/RTP traffic natively (without encapsulation in TCP).
You must open firewalls bidirectionally for UDP traffic over Port 443.

Codec selection and bandwidth consumption:
Between the user device and the Virtual Delivery Agent (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 better voice quality but has a bandwidth requirement of 80–100 kilobits per second per call (depending on Network Layer2 overheads).
- G729 provides good voice quality and has a low bandwidth requirement of 30–40 kilobits per second per call (depending on Network Layer 2 overheads).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### *Delivering softphone applications to the virtual desktop*

There are two methods by which you can deliver a softphone to the XenDesktop virtual desktop:

- The application can be installed in the virtual desktop image.
- The application can be streamed to the virtual desktop using Microsoft App-V. This approach has manageability advantages because the virtual desktop image is kept uncluttered. After being streamed to the virtual desktop, the application runs in that environment as if it had been 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**. Useful to support audio devices having buttons and/or a display, human interface device (HID), if the user device is on a LAN or LAN-like connection back to the XenApp or XenDesktop 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, compresses it, and 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-IP (VoIP). 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 stereophonic 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 because 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, but Citrix Audio Virtual Channel is preferred because it is optimized for audio traffic. The primary exception is when using an audio device with buttons such as 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

phone set or headset that control features by sending a signal back to the softphone. This isn't an issue with buttons that work locally on the device.

## Browser content redirection

April 29, 2021

Redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC. Only the viewport (the user's visible area of a webpage) is redirected to the endpoint.
Browser content redirection doesn't redirect the user interface (the address bar, toolbar, and so forth) of the browser on the VDA.

### System Requirements

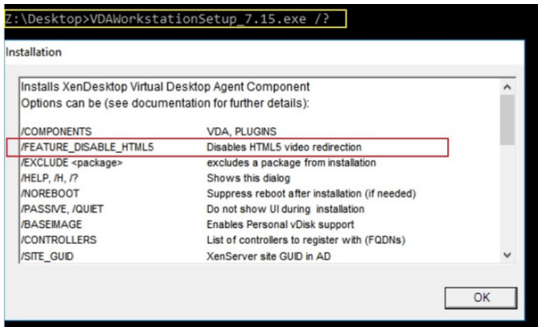
These requirements are specifically for the BCR.msi with XenApp and XenDesktop 7.15 LTSR CU5. Disregard any browser content redirection system requirements listed in any other versions of XenApp, XenDesktop, and Citrix Virtual Apps and Desktops.

- Version 7.15 LTSR CU5 or later on both the Delivery Controller and the VDA.
- Citrix Workspace app for Windows 1809 or later.
- Citrix Receiver for Linux 13.9.1 or later.
- BCR.msi - available from the Citrix downloads page.
- Chrome (with the browser content redirection extension installed from the Chrome Web Store) or Internet Explorer 11 (with the Browser Helper Object (BHO) Citrix HDXJsInjector enabled)

### Installation

1. Install or upgrade the VDA with Version 7.15 LTSR CU5 by using the command line /FEATURE_DISABLE_HTML5 option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




This option removes the HTML5 video redirection feature, which must be done before running the BCR.msi. BCR.msi adds the feature back during installation, and also adds the browser content redirection services. When this step is complete, open the services.msc console and verify that the **Citrix HDX HTML5 Video Redirection Service** is not listed.

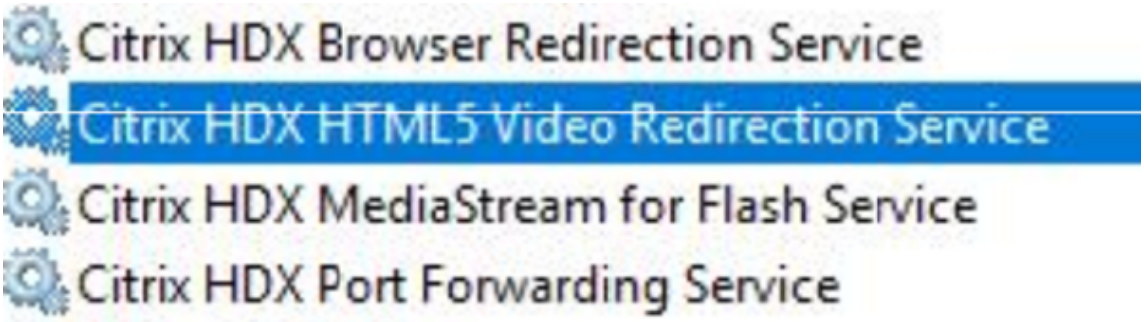
2. Start the browser content redirection installation with the BCR.msi. Depending on your system, the BCR.msi installs its files under:

   C:\Program Files\Citrix\ICAService

   or

   C:\Program Files (x86)\Citrix\ICAService

   Because the installation is fast, the dialog box might close quickly. If that occurs, rerun services.msc and verify that these services were added.

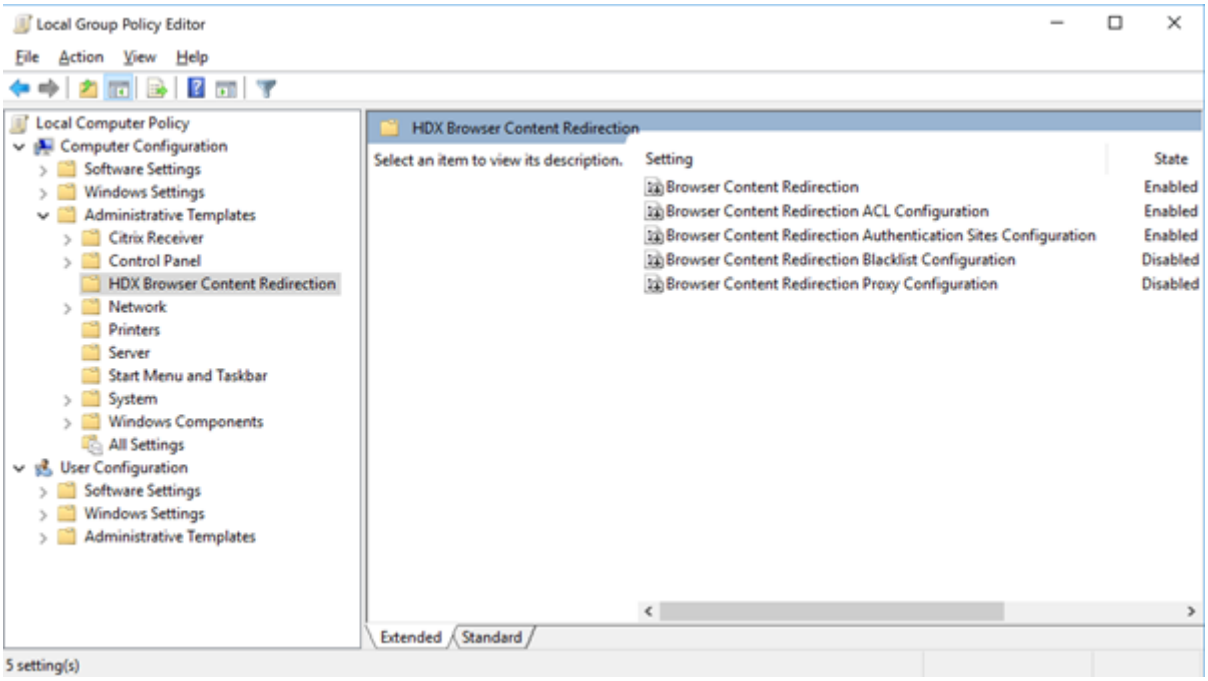



## Policies

You can control policies using the HKEY_LOCAL_MACHINE registries on the VDA or the **HDX Browser Content Redirection** Citrix administration template for the Group Policy Management Console.

You can download the template from the citrix.com download page under Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Components. Citrix Studio does not contain these policies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




For more policy information, see Browser content redirection policy settings. For troubleshooting information, see the Knowledge Center article, CTX230052.

## Flash redirection

November 1, 2018

> **Important**
>
> On July 25, 2017, Adobe announced End of Life (EOL) for Flash. Adobe plans to stop updating and distributing the Flash Player at the end of 2020.
>
> Microsoft announced that they are phasing out Flash support in Internet Explorer before the Adobe date. They are removing Flash from Windows by the end of 2020. When that happens, users can no longer enable or run Flash in Internet Explorer.
>
> Citrix aligns with Microsoft policy and continues to maintain and support HDX Flash Redirection until the end of 2020. We haven't decided in which versions of XenApp and XenDesktop to exclude the Flash Redirection code, but we recommend that you switch to HTML5 Video Redirection whenever possible. HTML5 Video Redirection is ideal to control the multimedia content. For example, corporate communications videos, training videos, or when a third party hosts the content.
>
> For more information about HTML5 Video Redirection, see HTML5 multimedia redirection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Flash Redirection offloads the processing of most Adobe Flash content (including animations, videos, and applications) to users'LAN- and WAN-connected Windows and 32-bit Linux x86 devices, which reduces server and network load. This results in greater scalability while ensuring a high definition user experience. Configuring Flash Redirection requires both server-side and client-side settings.

> **Caution:**
>
> Flash Redirection involves significant interaction between the user device and server components. Use this feature only in environments where security separation between the user device and server is not required. Additionally, configure user devices to use this feature only with trusted servers. Because Flash Redirection requires the Adobe Flash Player to be installed on the user device, enable this feature only if the Flash Player itself is secured.

Flash Redirection is supported on both clients and servers. If the client supports second generation Flash Redirection, Flash content renders on the client. Flash Redirection features include support for user connections over WAN, intelligent fallback, and a URL compatibility list; see below for details.

Flash Redirection uses Windows event logging on the server to log Flash events. The event log indicates whether Flash Redirection is being used and provides details about issues. The following are common to all events logged by Flash Redirection:

- Flash Redirection reports events to the Application log.
- On Windows 10, Windows 8 and Windows 7 systems, a Flash Redirection-specific log appears in the Applications and Services Logs node.
- The Source value is Flash.
- The Category value is None.

For the latest updates to HDX Flash compatibility, see CTX136588.

### Configure Flash Redirection on the server

To configure Flash Redirection on the server, use the following Citrix policy settings. For details, see Flash Redirection policy settings.

- By default, Flash Redirection is enabled. To override this default behavior for individual web pages and Flash instances, use the Flash URL compatibility list setting.
- Flash intelligent fallback - detects instances of small Flash "movies"(such as those frequently used to play advertisements) and renders them on the server instead of redirecting them for rendering on the user device. This optimization does not cause any interruption or failure in the loading of the web page or the Flash application. By default, Flash intelligent fallback is enabled. To redirect all instances of Flash content for rendering on the user device, disable this policy setting. Note that some Flash content may not be successfully redirected.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Flash server-side content fetching URL list allows you to specify websites whose Flash content should be downloaded to the server and then transferred to the user device for rendering. (By default, Flash Redirection downloads Flash content directly to the user device with client-side fetching.) This setting works with (and requires) the Enable server-side content fetching setting on the user device and is intended primarily for use with Intranet sites and internal Flash applications; see below for details. It also works with most Internet sites and can be used when the user device does not have direct access to the Internet (for example, when the XenApp or XenDesktop server provides that connection).
  Note: Server-side content fetching does not support Flash applications using Real Time Messaging Protocols (RTMP); instead, server-side rendering is used, which supports HTTP and HTTPS.
- Flash URL compatibility list - specifies where Flash content from listed websites is rendered: on the user device, on the server, or blocked.
- Flash background color list - enables you to match the colors of web pages and Flash instances, which improves the appearance of the web page when using Flash Redirection.

### Configure Flash Redirection on the user device

Install Citrix Receiver and Adobe Flash Player on the user device. No further configuration is required on the user device.

You can change the default settings using Active Directory Group Policy Objects. Import and add the HDX MediaStream Flash Redirection - Client administrative template (HdxFlashClient.adm), which is available in the following folders:

- For 32-bit computers: %Program Files%\Citrix\ICA Client\Configuration\language
- For 64-bit computers: %Program Files (x86)%\Citrix\ICA Client\Configuration\language

The policy settings appear under Administrative Templates > Classic Administrative Templates (ADM) > HDX MediaStream Flash Redirection - Client. See the Microsoft Active Directory documentation for details about GPOs and templates.

**Change when Flash Redirection is used:**

Together with server-side settings, the Enable HDX MediaStream Flash Redirection on the user device policy setting controls whether Adobe Flash content is redirected to the user device for local rendering. By default, Flash Redirection is enabled and uses intelligent network detection to determine when to play Flash content on the user device.

If no configuration is set and Desktop Lock is used, Flash Redirection is enabled on the user device by default.

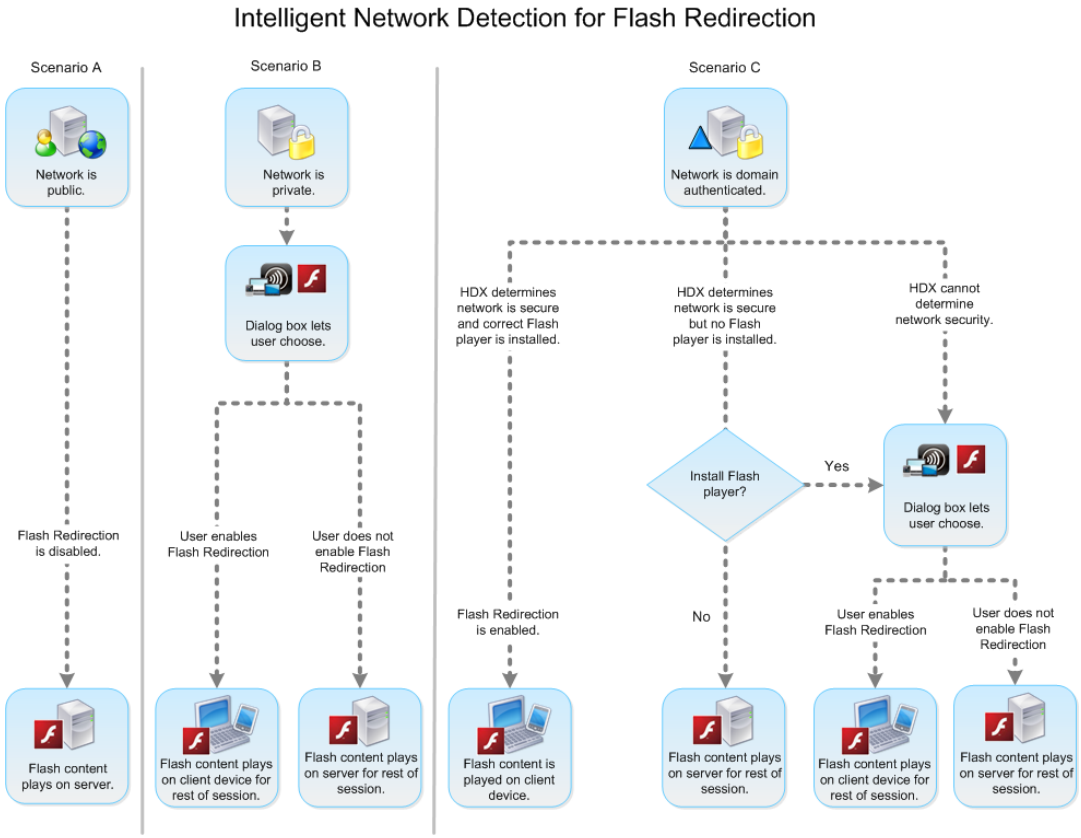
To change when Flash Redirection is used or to disable Flash Redirection on the user device:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. From the Setting list, select Enable HDX MediaStream Flash Redirection on the user device and click policy setting.
2. Select Not Configured, Enabled (the default), or Disabled.
3. If you select Enabled, choose an option from the Use HDX MediaStream Flash Redirection list:

    - To use the latest Flash Redirection functionality when the required configuration is present, and revert to server-side rendering when it is not, select Only with Second Generation.
    - To always use Flash Redirection, select Always. Flash content plays on the user device.
    - To never use Flash Redirection, select Never. Flash content plays on the server.
    - To use intelligent network detection to assess the security level of the client-side network to determine when using Flash Redirection is appropriate, select Ask (the default). If the security of the network cannot be determined, the user is asked whether to use Flash Redirection. If the network security level cannot be determined, the user is prompted to choose whether to use Flash Redirection.

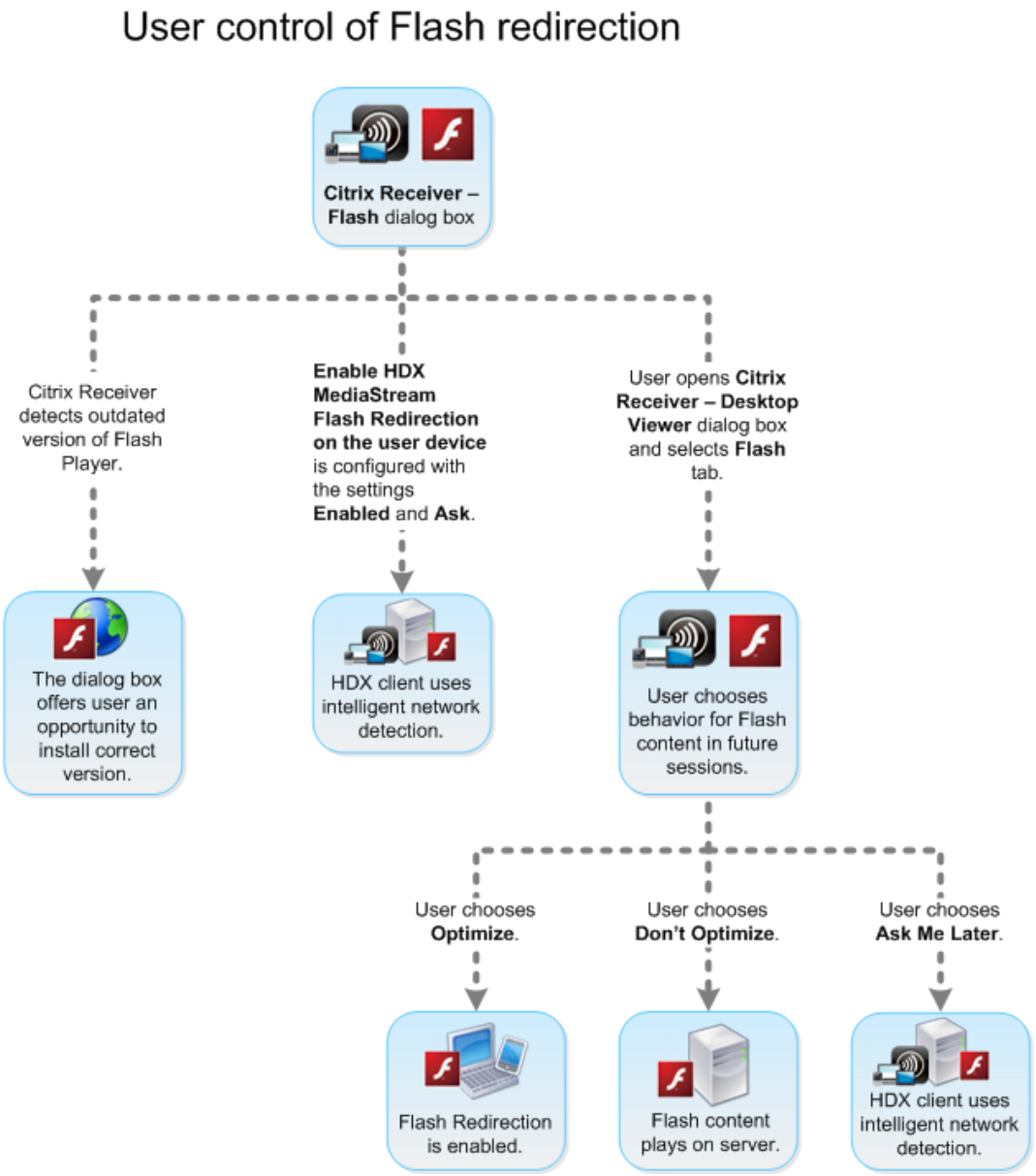
      The following illustration indicates how Flash Redirection is handled for various network types.




Users can override intelligent network detection from the Citrix Receiver - Desktop Viewer Preferences dialog box by selecting Optimize or Don't Optimize in the Flash tab. The choices available vary depending on how Flash Redirection is configured on the user

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

device, as shown in the following illustration.




**Synchronize client-side HTTP cookies with the server-side:**

Synchronization of the client-side HTTP cookies with the server-side is disabled by default. Enable synchronization to download HTTP cookies from the server; those HTTP cookies are then used for client-side content fetching and are available as needed by sites containing Flash content.

> **Note:**
>
> Client-side cookies are not replaced during the synchronization; they remain available even if the synchronization policy is later disabled.

1. From the Setting list, select Enable synchronization of the client-side HTTP cookies with the

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

server-side and click policy setting.
2. Select Not Configured, Enabled, or Disabled (the default).

**Enable server-side content fetching:**

By default, Flash Redirection downloads Adobe Flash content directly to the user device, where it is played. Enabling server-side content fetching causes the Flash content to download to the server and then be sent to the user device. Unless there is an overriding policy (such as a site blocked with the Flash URL compatibility list policy setting), the Flash content plays on the user device.

Server-side content fetching is frequently used when the user device connects to internal sites through NetScaler Gateway and when the user device does not have direct access to the Internet.

> **Note:**
>
> Server-side content fetching does not support Flash applications using Real Time Messaging Protocols (RTMP). Instead, server-side rendering is used for such sites.

Flash Redirection supports three enabling options for server-side content fetching. Two of these options include the ability to cache server-side content on the user device, which improves performance because content that is reused is already available on the user device for rendering. The contents of this cache are stored separately from other HTTP content cached on the user device.

Fallback to server-side content fetching begins automatically when any of the enabling options is selected and client-side fetching of .swf files fails.

Enabling server-side content fetching requires settings on both the client device and the server.

1. From the Setting list, select Enable server-side content fetching and click policy setting.
2. Select Not Configured, Enabled, or Disabled (the default). If you enable this setting, choose an option from the Server-side content fetching state list:

| Option | Description |
|---|---|
| Disabled | Disables server-side content fetching, overriding the Flash server-side content fetching URL list setting on the server. Server-side content fetching fallback is also disabled. |
| Enabled | Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available, but Flash content is not cached. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Option | Description |
| --- | --- |
| Enabled (persistent caching) | Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available. Content obtained through server-side fetching is cached on the user device and stored from session to session. |
| Enabled (temporary caching) | Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available. Content obtained through server-side fetching is cached on the user device and deleted at the end of the session. |

3. On the server, enable the Flash server-side content fetching URL list policy setting and populate it with target URLs.

**Redirect user devices to other servers for client-side content fetching:**

To redirect an attempt to obtain Flash content, use the URL rewriting rules for client-side content fetching setting, which is a second generation Flash Redirection feature. When configuring this feature, you provide two URL patterns; when the user device attempts to fetch content from a website matching the first pattern (the URL match pattern), it is redirected to the website specified by the second pattern (the rewritten URL format).

You can use this setting to compensate for content delivery networks (CDN). Some websites delivering Flash content use CDN redirection to enable the user to obtain the content from the nearest of a group of servers containing the same content. When using Flash Redirection client-side content fetching, the Flash content is requested from the user device, while the rest of the web page on which the Flash content resides is requested by the server. If CDN is in use, the server request is redirected to the nearest server, and the user device request follows to the same location. This may not be the location closest to the user device; depending on distance, there could be a noticeable delay between the loading of the web page and the playing of the Flash content.

1. From the Setting list, select URL rewriting rules for client-side content fetching and click policy setting.
2. Select Not Configured, Enabled, or Disabled. Not Configured is the default; Disabled causes any URL rewriting rules specified in the next step to be ignored.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. If you enable the setting, click Show. Using Perl regular expression syntax, type the URL match pattern in the Value name box and the rewritten URL format in the Value box.

### Minimum version checking for Flash redirection

> **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.

You can add registry settings to specify the minimum version required for Flash redirection for client devices accessing VDAs using Citrix Receiver for Windows or Citrix Receiver for Linux. This security feature ensures that an outdated Flash version is not used.

**ServerFlashPlayerVersionMinimum** is a string value that specifies the minimum version of the Flash Player required on the ICA Server (VDA).

**ClientFlashPlayerVersionMinimum** is a string value that specifies the minimum version of the Flash Player required on the ICA Client (Citrix Receiver).

These version strings can be specified as "10"or "10.2"or "10.2.140". Only the major, minor and build numbers will be compared. The revision number will be ignored. For example, for a version string specified as "10"with only the major number specified, the minor and build numbers will be assumed to be zero.

**FlashPlayerVersionComparisonMask** is a DWORD value that when set to zero will disable comparing the version of the Flash Player on the ICA Client against the Flash Player on the ICA Server. The comparison mask has other values, but these should not be used because the meaning of any non-zero mask may change. It is recommended to only set the comparison mask to zero for the desired clients. It is not recommended to set the comparison mask under the client agnostic settings. If a comparison mask is not specified, Flash redirection will require that the ICA Client has a Flash Player with greater or equal version to the Flash Player on the ICA Server. It will do so by comparing only the major version number of the Flash Player.

For redirection to occur, the client and server minimum checks must be successful in addition to the check using the comparison mask.

The subkey ClientID0x51 specifies Citrix Receiver for Linux. The subkey ClientID0x1 specifies Citrix Receiver for Windows. This subkey is named by appending the hexadecimal Client Product ID (without any leading zeros) to the string "ClientID".

**32-bit VDA example registry configuration:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] Client agnostic settings

“ClientFlashPlayerVersionMinimum”=”13.0”Minimum version required for the ICA client “Server-FlashPlayerVersionMinimum”=”13.0”Minimum version required for the ICA server [HKEY_LOCAL_MACHINE\SOFTW Windows ICA Client settings

“ClientFlashPlayerVersionMinimum”=”16.0.0”This specifies the minimum version of the Flash Player required for the Windows client [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\Pse Linux ICA Client settings

“FlashPlayerVersionComparisonMask”=dword:00000000 This disables the version comparison-check for the linux client (checking to see that the client has a more recent Flash Player than the server) “ClientFlashPlayerVersionMinimum”=”11.2.0”This specifies the minimum version of the Flash Player for the Linux client.

**64-bit VDA example registry configuration:**

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

“ClientFlashPlayerVersionMinimum”=”13.0”“ServerFlashPlayerVersionMinimum”=”13.0”[HKEY_LOCAL_MACHINE

“ClientFlashPlayerVersionMinimum”=”16.0.0”[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMed

“FlashPlayerVersionComparisonMask”=dword:00000000 “ClientFlashPlayerVersionMinimum”=” 11.2.0”

## HTML5 multimedia redirection

October 29, 2018

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 hard drive as it's received and is played from the hard 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. Use the developer tools in your browser to inspect the video element in the webpage and find the source (an mp4 container format) in the HTML5 video tag:

```
<video src="https://www.citrix.com/content/dam/citrix61/en_us/images/offsite/html5-redirect.mp4"controls=""style="width:800px;"></video>
```

### Comparison between 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:

- Server side render
- Server fetch client render
- Client side fetching and rendering

Control these by using policies. For more information, see Multimedia policy settings.

Minimum versions of Citrix Receiver:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Citrix Receiver for Windows 4.5
- Citrix Receiver for Linux 13.5

Minimum VDA browser version and 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
  - Windows Server 2008 R2
- **Firefox 47** Manually add the certificates to the Firefox certificate store or configure Firefox to search for certificates from a Windows trusted certificate store. For more information, see https://wiki.mozilla.org/CA:AddRootToFirefox
  - Windows 10 x86 (1607 RS1) and x64 (1607 RS1)
  - Windows 7 x86 and x64
  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 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
  - Windows Server 2008 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 =

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

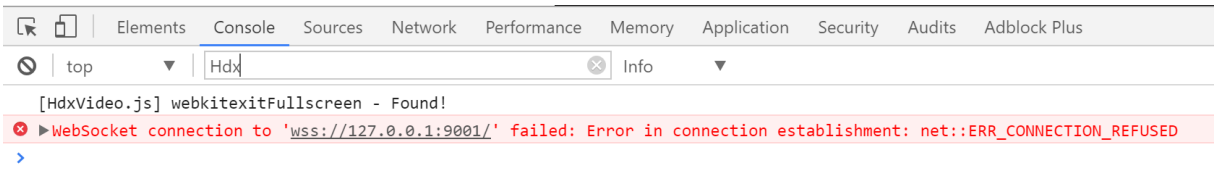
In this release, this feature is available for controlled webpages only. It requires the addition of the HdxVideo.js JavaScript (included in the XenDesktop and XenApp Installation media) to the webpages where the HTML5 multimedia content is available. For example, videos on an internal training site.

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 there are no errors related to HdxVideo.js by inspecting the console in the developers tool windows of your browser. For example:




## Windows Media redirection

July 3, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenDesktop Collector to perform a Citrix Diagnosis Facility (CDF) trace from HostMMTransport.dll to determine the method used.

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.

## General Content Redirection

April 2, 2019

Content redirection allows you to control whether users access information with applications published on servers or with 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 are better. This type of redirection is supported only on Server OS VDAs (not Desktop OS VDAs).

### Local App Access and URL redirection

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Local App Access seamlessly integrates locally installed Windows applications in to a hosted desktop environment without changing from one computer to another.

### USB and client drive consideration

HDX technology provides **generic USB redirection** for specialty devices that don't have optimized support or where it is unsuitable.

### Related information

- Client folder redirection
- Host to client redirection
- Local App Access and URL redirection
- USB and client drive considerations
- Multimedia

## Client folder redirection

July 19, 2018

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 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 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 Desktop OS machines only.

Client folder redirection for an external USB drive will not be 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 Receiver supplied with this release.

> **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 Reg-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> istry 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 the latest version of Citrix Receiver is installed.
    b) From the Citrix Receiver installation directory, start CtxCFRUI.exe.
    c) Select 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

January 18, 2019

Content redirection allows you to control whether users access information by using applications published on servers or applications running locally on user devices.

**Host to client redirection** is one type of content redirection. It is supported only on Server OS VDAs (not Desktop OS VDAs).

- When host to client redirection is enabled, URLs are intercepted at the server VDA and sent to the user device. The web browser or multimedia player on the user device opens these URLs.
- If you enable host to client redirection and the user device fails to connect to a URL, the URL is redirected back to the server VDA.
- When host to client redirection is disabled, users open the URLs with web browsers or multimedia players on the server VDA.
- When host to client redirection is enabled, users cannot disable it.

Host to client redirection was previously known as **server to client redirection**.

### When to use host to client redirection

You might consider using host to client redirection in specific but uncommon cases, for performance, compatibility, or compliance. Normally, other forms of content redirection are better.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Performance:**

You can use host to client redirection for performance, so that whenever an application is installed on the user device, it is used in preference to an application on the VDA.

Keep in mind that host to client redirection improves performance only under specific conditions, because the VDA already optimizes Adobe Flash and other types of multimedia content. First, consider using the other approaches (policy settings) noted in the tables in this article, rather than host to client redirection. Those settings offer more flexibility and usually give a better user experience, particularly for less-powerful user devices.

**Compatibility:**

You can use host to client redirection for compatibility in the following use cases:

- You use content types other than HTML or multimedia (for example, a custom URL type).
- You use a legacy media format (such as Real Media) that is not supported by the VDA multimedia player using multimedia redirection.
- The application for the content type is used by only a few users who already have the application installed on their user device.
- The VDA cannot access certain websites (for example, websites internal to another organization).

**Compliance:**

You can use host to client redirection for compliance in the following use cases:

- The application or content licensing agreement does not permit publishing via the VDA.
- Organizational policy does not permit a document being uploaded to the VDA.

Some situations are more likely in complex environments, and also if the user device and the VDA belong to different organizations.

## User device considerations

Environments can have many different types of user devices.

| User device | Situation or environment | Content redirection approach |
|---|---|---|
| Tablet | - | Any approach (see next table) |
| Laptop PC | - | Any approach (see next table) |
| Desktop PC | Users use a wide range of apps installed on the user device | Any approach (see next table) |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| User device | Situation or environment | Content redirection approach |
|---|---|---|
| Desktop PC | Users use only a few known apps that are installed on the user device | Local App Access |
| Desktop PC | Users use no apps installed on the user device | Multimedia redirection and/or Flash redirection |
| Desktop appliance | Vendor supports multimedia redirection and/or Flash redirection | Multimedia redirection and/or Flash redirection |
| Thin client | Vendor supports multimedia redirection, Flash redirection, and host to client redirection | Any approach (see next table) |
| Zero client | Vendor supports multimedia redirection and/or Flash redirection | Multimedia redirection and/or Flash redirection |

Use the following examples to help guide your content redirection approach.

| URLs link | Situation or environment | Content redirection approach |
|---|---|---|
| Webpage or document | The VDA cannot access the URL | Host to client redirection |
| Webpage | The webpage contains Adobe Flash | Flash redirection |
| Multimedia file or stream | The VDA has a compatible multimedia player | Multimedia redirection |
| Multimedia file or stream | The VDA does not have a compatible multimedia player | Host to client redirection |
| Document | The VDA does not have an application for that document type | Host to client redirection |
| Document | Do not download the document to the user device | No redirection |
| Document | Do not upload the document to the VDA | Host to client redirection |
| Custom URL type | The VDA does not have an application for that custom URL type | Host to client redirection |

Citrix Receiver for Windows, Citrix Receiver for Mac, Citrix Receiver for Linux, Citrix Receiver for HTML5,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

and Citrix Receiver for Chrome support Host to client redirection.

To use host to client redirection, the user device must have a web browser, multimedia player, or other application that is suitable for the content. If the user device is a desktop appliance, thin client, or zero client, confirm that it has suitable applications and is sufficiently powerful.

User devices enabled for Local App Access use a different mechanism for content redirection, and do not require host to client content redirection.

You can use Citrix policies to prevent host to client content redirection for unsuitable devices.

### How users experience host to client redirection

Host to client redirection is used when URLs are:

- Embedded as hyperlinks in an application (for example, in an email message or document).
- Selected through VDA application menus or dialogs, if the application uses the Windows ShellExecuteEx API.
- Typed in the Windows Run dialog.

Host to client redirection is not used for URLs in a web browser (either in a webpage or typed in the address bar of the web browser).

> **Note**
>
> If users change their default web browser on the VDA (for example, using Set Default Programs), that change can interfere with host to client redirection for applications.

When host to client content redirection is enabled, the app that opens the URL depends on the configuration of the user device for the URL type and the content type. For example:

- An HTTP URL that has an HTML content type opens in the default web browser.
- An HTTP URL that has a PDF content type might open in the default web browser, or it might open in another application.

Host to client content redirection doesn't control this user device configuration. If you do not control the configuration of the user device, consider using Flash redirection and multimedia redirection, rather than host to client content redirection.

The following URL types are opened locally through user devices when host to client redirection is enabled:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player and QuickTime)
- RTSPU (Real Player and QuickTime)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- PNM (Legacy Real Player)
- MMS (Microsoft Media Format)

You can change the list of URL types for host to client redirection, to remove and add URL types, including custom URL types.

### Enable host to client redirection

Enabling host to client redirection starts by enabling a Citrix policy setting.

The Host to client redirection policy setting is located in the File Redirection policy settings section. By default, this setting is disabled.

In addition, you might need to set registry keys and Group Policy for the server VDAs, depending on the VDA OS.

- If the server VDA is Windows Server 2008 R2 SP1, you do not need to set registry keys or Group Policy.
- If the server VDA is Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016, you must set registry keys and Group Policy.

> **Warning**
>
> 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.

### Registry changes

1. Copy the text between **Reg file start** and **Reg file end** below, and paste it in Notepad.
2. Save the Notepad file using **Save As** as type **All Files** and the name **ServerFTA.reg**.
3. Distribute the **ServerFTA.reg** file to the servers using Active Directory Group Policy.

---

```
--  Reg file start --

Windows Registry Editor Version 5.00


[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]

@="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"


[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0"

"ApplicationName"="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]

"http"="ServerFTAHTML"

"https"="ServerFTAHTML"



[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]

"Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"

-- Reg file end -- ---
```

### Group Policy changes

Create an XML file. Copy the text between **xml file start** and **xml file end** the example, paste it in the XML file, and then save the file as **ServerFTAdefaultPolicy.xml**.

---

```
-- xml file start --

<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>

-- xml file end -- ---
```

From the current Group Policy management console, navigate to: **Computer configuration** > **Administrative Templates** > **Windows Components** > **File Explorer** > **Set a default associations configuration file,** and provide the ServerFTAdefaultPolicy.xml file you created.

### Change the list of URL types for host to client redirection

To change the list of URL types for host to client redirection, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

To delete URL types from the list, set DisableServerFTA and NoRedirectClasses:

Name: DisableServerFTA

Type: REG_DWORD

Data: 1

Name: NoRedirectClasses
Type: REG_MULTI_SZ
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 add URL types to the list, set ExtraURLProtocols:

Name: ExtraURLProtocols

Type: REG_MULTI_SZ

Data: Specify any combination of URL types. Each URL type must include the :// suffix; separate multiple values by using semicolons. For example:

customtype1://;customtype2://

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Enable host to client redirection for a specific set of websites

To enable host to client redirection for a specific set of websites, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

Name: ValidSites

Type: REG_MULTI_SZ

Data: Specify any combination of fully qualified domain names (FQDNs). Type multiple FQDNs on separate lines. An FQDN can include a wildcard in the leftmost position only. This matches a single level of domain, which is consistent with the rules in RFC 6125. For example:

```
www.example.com
```

```
*.example.com
```

## 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

- Desktop OS or Server OS VDAs
- Citrix Workspace app for Windows
- Internet Explorer 11

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Local App Access and URL redirection

October 21, 2020

## Introduction

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without changing from one computer 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 double-hop latency when applications are hosted separately from the virtual desktop, 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, such as DVD burners and TV tuners.

In XenApp and XenDesktop, hosted desktop sessions use URL redirection to launch 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 XenApp or XenDesktop server to the user's computer

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Rendered in the environment in which they are launched (not redirected)

To specify the redirection path of content from specific Web sites, 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 —Web sites 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 but instead sees uk.msn.com.
- Multimedia content —Web sites 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. Although there is Flash redirection feature, this complements by redirecting sites with other media types such as Silverlight. This is in a very secure environment. That is, the URLs that are approved by the administrator 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 launches local applications when a file is encountered in the session. If the local app is launched, 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

Local App Access is supported on the valid operating systems for VDAs for Windows Server OS and VDAs for Windows Desktop OS, and requires Citrix Receiver 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

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 Local App Access is used with a virtual desktop that runs in windowed mode or does not cover all monitors.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - For multiple monitors, when one monitor is maximized it becomes the default desktop for all applications launched in that session, even if subsequent applications typically launch on another monitor.
  - The feature supports one VDA; there is no integration with multiple concurrent VDAs.

- Some applications can behave unexpectedly, affecting users:
  - Users might be confused with drive letters, 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 launched 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. This includes applications that open to 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, such as grouping 32-bit local applications with 64-bit VDA applications.
  - Applications cannot be launched using COM. For example, if you click an embedded Office document from within an Office application, the process launch 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, those 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 new 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 launch consistently when using these shortcuts.

### 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 usually 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 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Install the Citrix Workspace app on the local client machine. You can enable both features during the Citrix Workspace app installation or you can enable Local App Access template using the Group Policy editor.
- Set the **Allow local app access** policy setting to **Enabled**. You can also configure URL allow list and block list policy settings for URL redirection. For more information, see Local App Access policy settings.

#### Enable Local App Access and URL redirection

To enable Local App Access for all local applications, follow these steps:

1. 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 allow 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 block 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 these steps:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Enable URL redirection when you install the Citrix Workspace app for all users on a machine. Doing so also registers the browser add-ons required for URL redirection.
2. From the command prompt, run the appropriate command to install the Citrix Workspace app using one of the following options:
   - For CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - For CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

#### Enable the Local App Access template using the Group Policy editor

> **Note:**
>
> - Before you enable the Local App Access template using the Group Policy editor, add the receiver.admx/adml template files to the local GPO. For more information, see Configuring the Group Policy Object administrative template.
> - Citrix Workspace app for Windows template files are available in the local GPO in **Administrative Templates > Citrix Components > Citrix Workspace** folder only when you add the CitrixBase.admx/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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 is 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 the 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 the 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 block list.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## USB and client drive considerations

August 20, 2020

HDX technology provides **optimized support** for most popular USB devices. This includes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Monitors
- Mice
- Keyboards
- VoIP 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 example:

- The USB device has additional advanced features that are not part of optimized support, such as a mouse or webcam with additional buttons.
- Users need functions which are not part of optimized support, such as burning a CD.
- 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 may not have a driver available for Citrix Receiver for Android.
- The version of Citrix Receiver does not provide 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.

> **Note**
>
> - 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 to avoid inconsistent and unexpected behavior.
> - The Citrix policy setting Client USB device optimization rules is a specific setting for generic USB redirection, for a particular of USB device. It is not optimized support as described

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

here.

- Client USB plug and play device redirection is a related feature that provides optimized support for devices such as cameras and media players that use the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP). Client USB plug and play redirection is not part of generic USB redirection. For the list of supported VDA versions, see Default policy settings.

### Performance considerations for USB devices

With generic USB redirection, for some types of USB devices, network latency and bandwidth can affect user experience and USB device operation. For example, timing-sensitive devices may not operate correctly over high-latency low-bandwidth links. Use optimized support instead where possible.

Some USB devices require high bandwith to be usable, for example a 3D mouse (used with 3D apps that also typically require high bandwidth). You can avoid performance problems using Citrix polices. 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 may be sensitive.

USB devices are often used to distribute malware. Configuration of Citrix Receiver, XenApp and XenDesktop can reduce, but not eliminate, risk from these USB devices. This 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: only use USB devices that have been obtained from a trustworthy source; not to 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Receivers support generic USB redirection:

- Citrix Receiver for Windows, see Configuring USB support
- Citrix Receiver for Mac, see Configuring Citrix Receiver for Mac
- Citrix Receiver for Linux, see Optimize
- Citrix Receiver for Chrome OS, see What's new

For Citrix Receiver versions, see the Citrix Receiver feature matrix.

If you are using earlier versions of Citrix Receiver, refer to Citrix Receiver documentation to confirm that generic USB redirection is supported. Refer to Citrix Receiver documentation for any restrictions on USB device types that are supported.

Generic USB redirection is supported for desktop sessions from VDA for Desktop OS version 7.6 through current.

Generic USB redirection is supported for desktop sessions from VDA for Server 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 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 CTX123569. Some USB devices do not operate correctly with generic USB redirection.

### Configure generic USB redirection

You can control which types of USB devices use generic USB redirection. This is separately configurable:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Receiver, using Citrix Receiver-dependent mechanisms. For example, Citrix Receiver for Windows is configured with registry settings that can be controlled by an Administrative Template. By default, USB redirection is allowed for certain classes of USB devices and denied for others; for more information, see Configuring USB support in the Citrix Receiver for Windows documentation for details.

This separate configuration provides flexibility. For example:

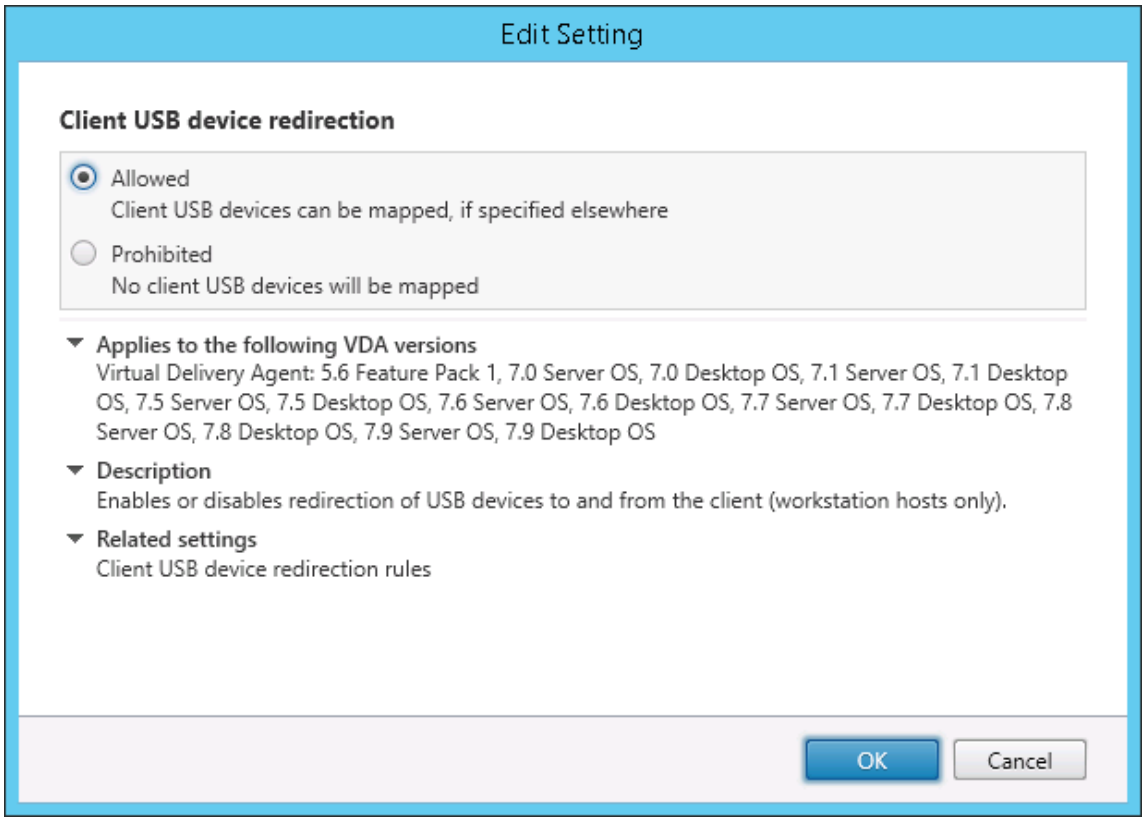
- If two different organizations or departments are responsible for Citrix Receiver and VDA they can enforce control separately. This would apply when a user in one organization accesses an application in another organization.
- If USB devices should be allowed only for certain users or for users only connecting over LAN (rather than with NetScaler Gateway), this can be controlled with Citrix policy settings.

### Enable generic USB redirection

To enable generic USB Redirection, configure both Citrix policy settings and Citrix Receiver.

In Citrix policy settings:

1. Add the Client USB device redirection to a policy and set its value to **Allowed**.

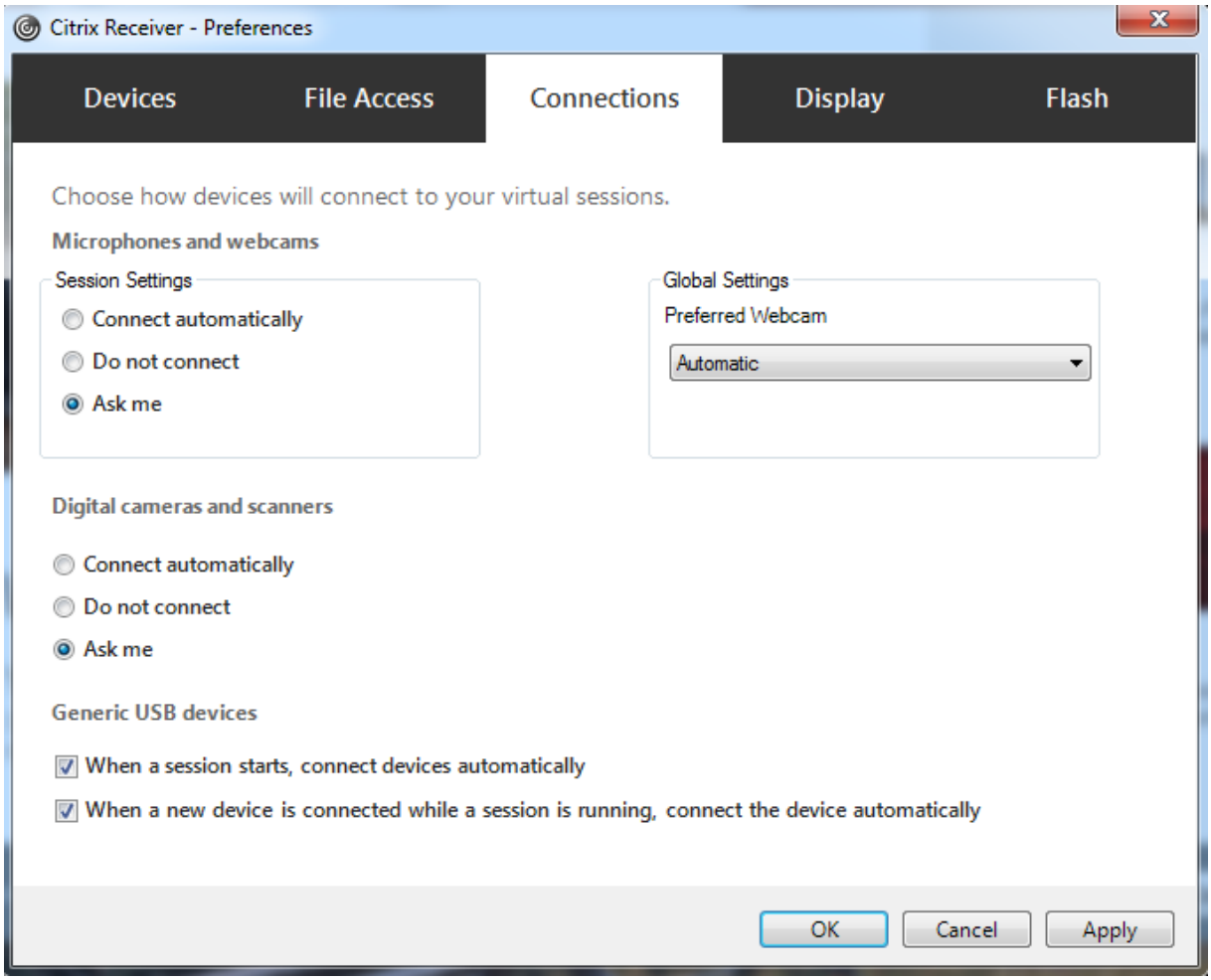



© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receiver:

3. Enable USB support when you install Citrix Receiver on user devices. You can do this using an Administrative template or in Citrix Receiver for Windows > Preferences > Connections.




If you specified USB policy rules for the VDA in the previous step, specify those same policy rules for Citrix Receiver.

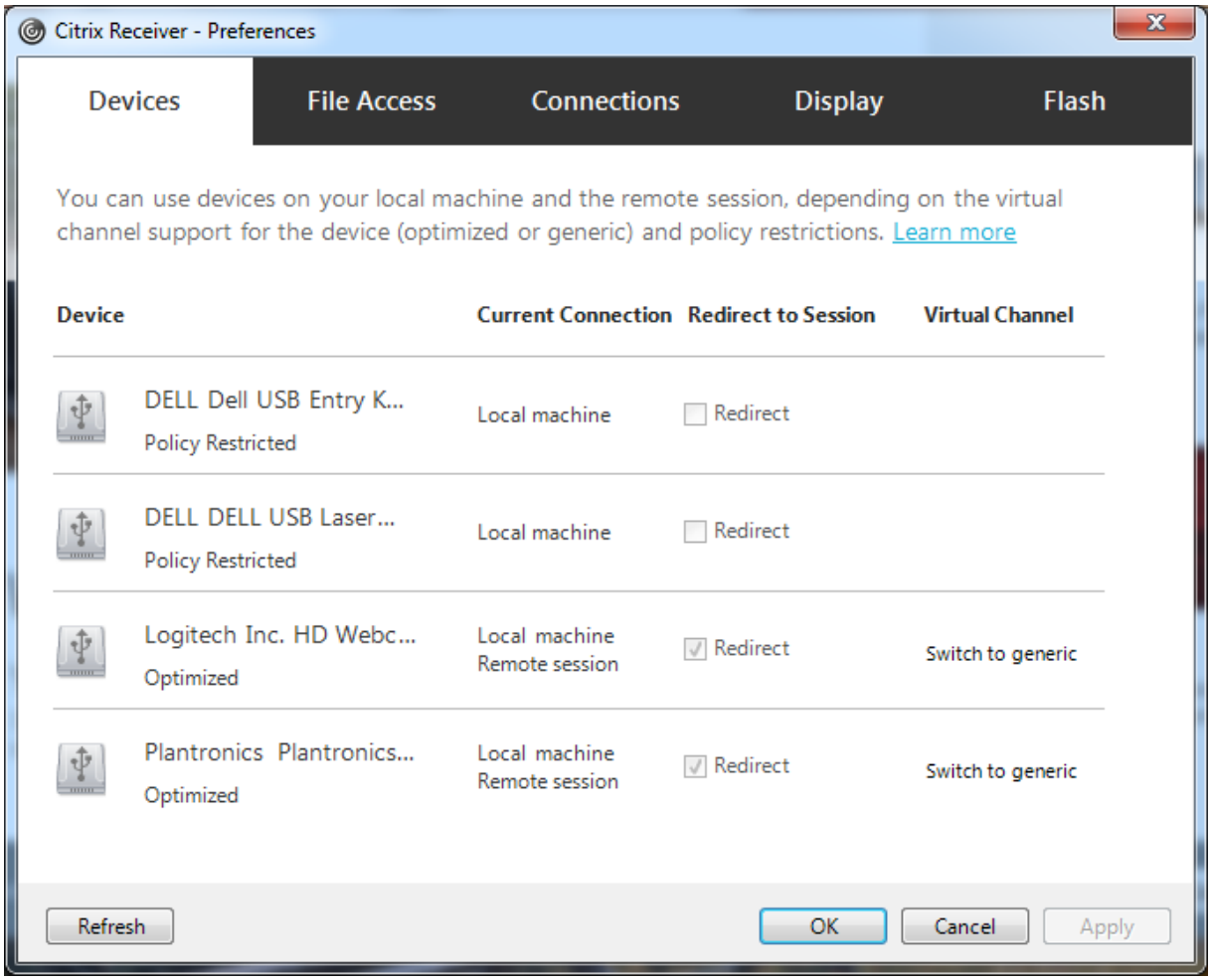
For thin clients, consult the manufacturer for details of USB support and any required configuration.

### 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 automatically connect USB devices. USB devices are also automatically redirected when operating in Desktop Appliance mode and the connection bar is not present.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Users can explicitly redirect devices that are not automatically redirected by selecting the devices from the USB device list. Users can get more help on how to do this in the Citrix Receiver 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 Receiver, 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 CTX123015.

> **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Receiver and the VDA.

For generic USB redirection, you will 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 may use the vendor-defined or HID device class.

For more precise control, you will also need to know the Vendor ID, Product ID, and Release ID. You can get this information from the device vendor.

> **Important**
>
> Malicious USB devices may 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 Receiver, to override the default USB policy rules.

For the VDA:

- Edit the administrator override rules for the Server 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 Receiver 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 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.

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 as explained below. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Web site at https://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 new policy rules, note the following:

- Rules are case-insensitive.
- Rules may 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
<!--NeedCopy-->
```

- The following example shows an administrator-defined USB policy rule for a defined class, subclass, and protocol:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
  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
<!--NeedCopy-->
```

### Use and remove USB devices

Users can connect a USB device before or after starting a virtual session.

When using Citrix Receiver for Windows, the following apply:

- Devices connected after a session starts 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 is part of XenApp and XenDesktop 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 with mapped drive letters. To configure client drive mapping, use the **Client removable drives** setting 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, controlled by Citrix polices. 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 | No |
| Safe to remove device during a session | No | Yes, provided users follow operating system recommendations for safe removal |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 will be 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 (see https://support.citrix.com/article/CTX123015) and a mass storage device is inserted either before or after a session starts, it will be redirected using generic USB redirection.

> **Note**
>
> USB redirection is supported over lower bandwidth connections, for example 50 Kbps, however copying large files will not 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 modifying files and folders on mapped client-devices, enable the **Read-only client drive access** policy setting. When adding this setting to a policy, make sure the **Client drive redirection** setting is set to **Allowed** and is also added to the policy.

## Print

October 29, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Server 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:

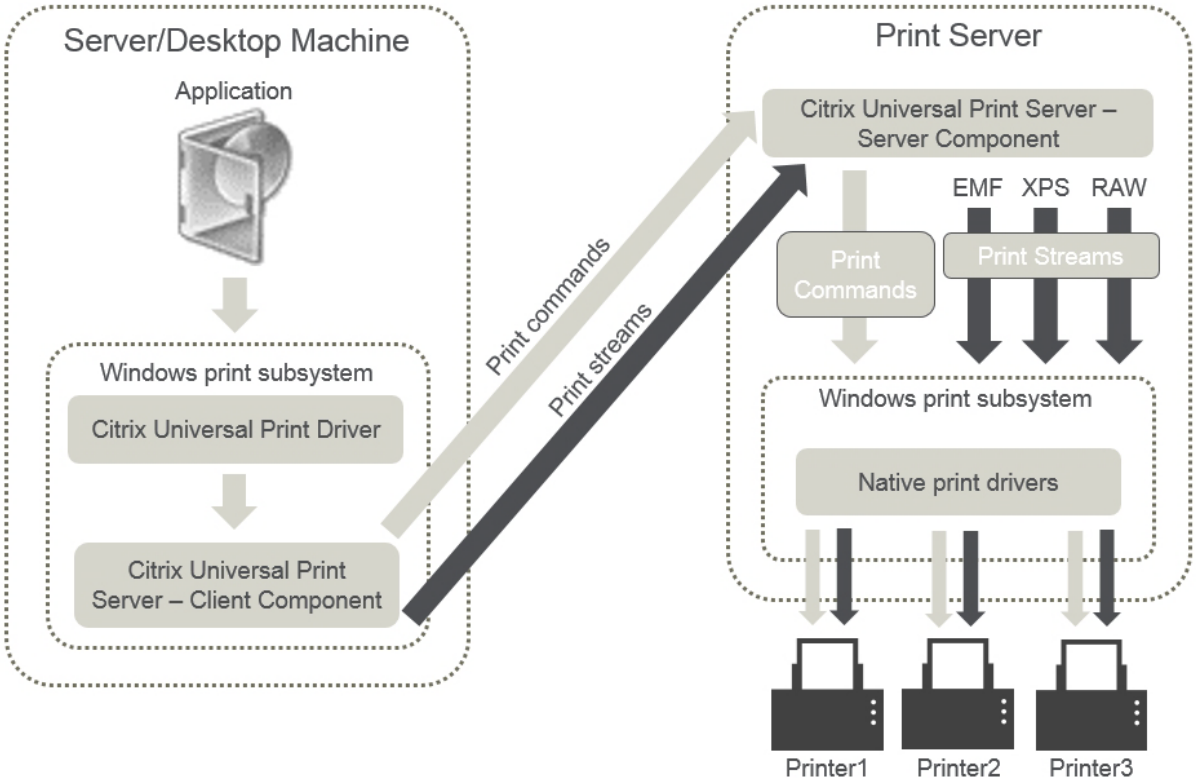
A client component, **UPClient** - Enable the UPClient on each Server OS machine that provisions session network printers and uses the Universal print driver.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Server OS machines using the Printer driver mapping and compatibility policy setting.

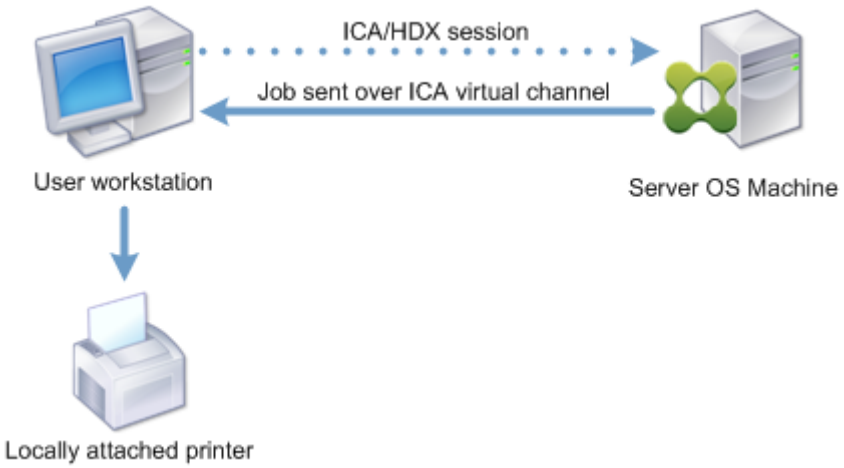
## Print job routing

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 Server 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

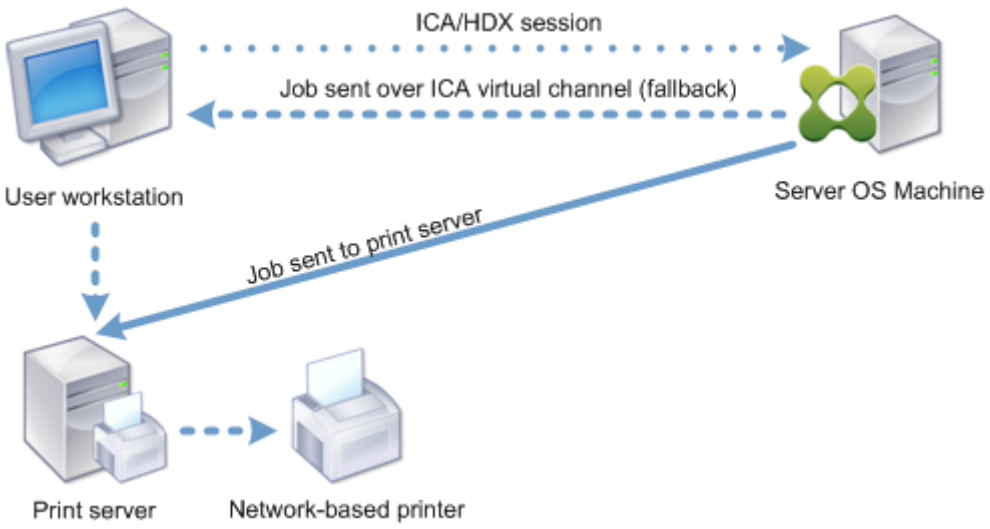
By default, all print jobs destined for network printers route from the Server OS machine, across the network, and directly to the print server. However, print jobs are automatically routed over the ICA connection in the following situations:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- If the virtual desktop or application cannot contact the print server.
- If the native printer driver is not available on the Server 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 XenApp or XenDesktop 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 |

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 Receiver installation. It fetches the incoming print stream for the XenApp or XenDesktop session. It then forwards the print stream to the

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

local printing subsystem where the print job is rendered using the device specific printer drivers. In addition to Citrix UPD, the Citrix PDF Universal Printer driver can be installed separately with Citrix Receiver for HTML5 and Citrix Receiver for Chrome.

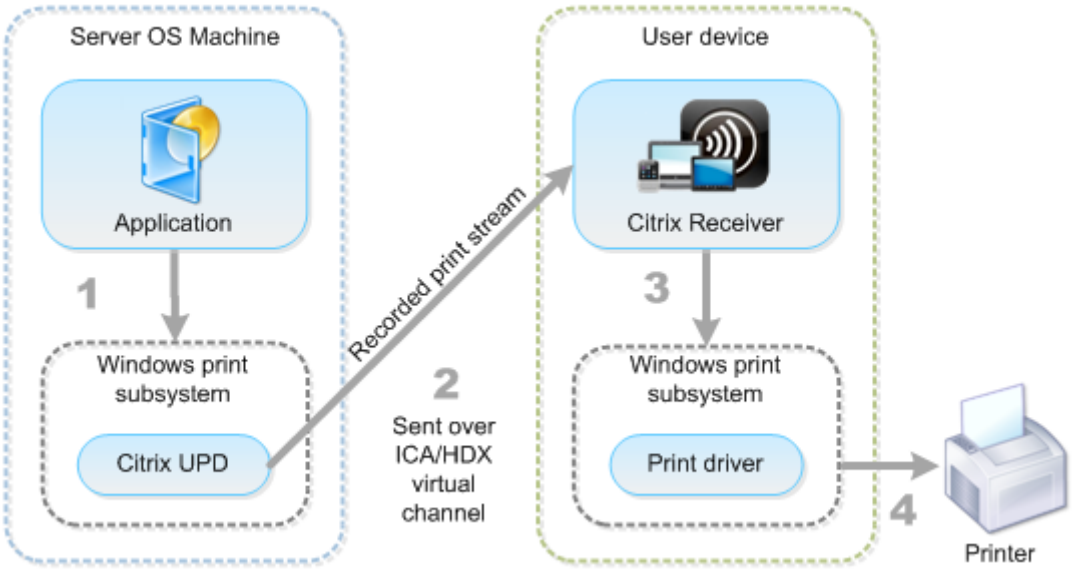
The Citrix UPD supports the following print formats:

- 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.

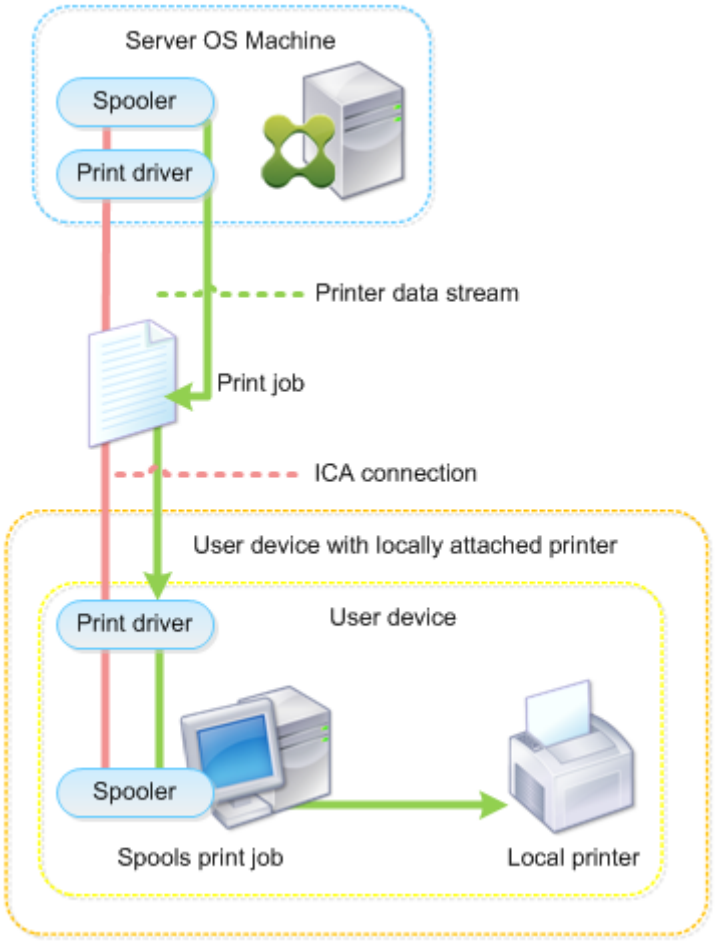



© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Server 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 Server 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 Server OS machines.
- Whether to create driver compatibility lists.

### Related content

- Printing configuration example

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Best practices, security considerations, and default operations
- Print policies and preferences
- Provision printers
- Maintain the printing environment

## Printing configuration example

October 29, 2018

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.

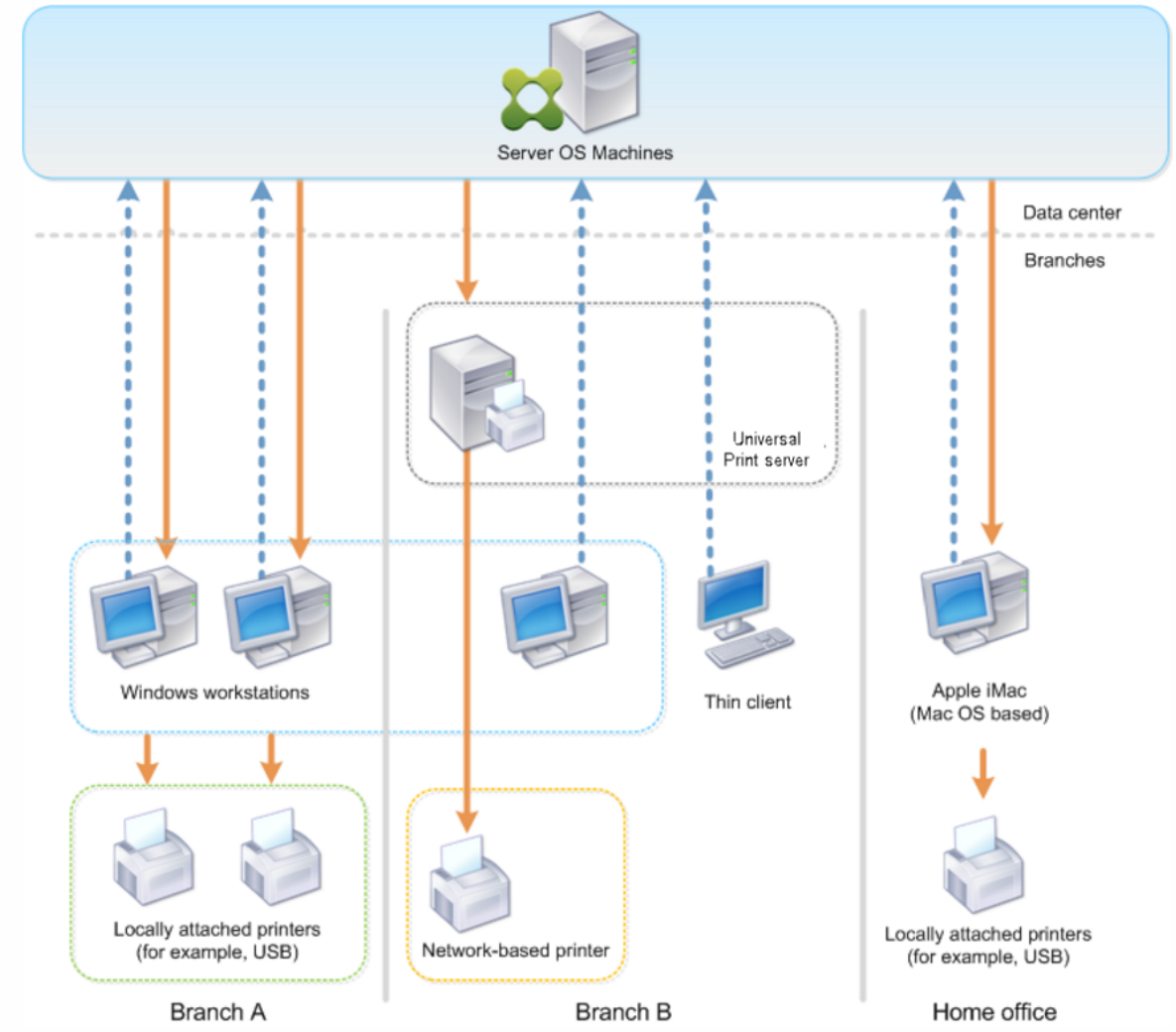
When designing your printing configuration, try to give users the same experience in a session as they have when printing from local user devices.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Server 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. Server 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

October 29, 2018

### 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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Server 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.

- The system uses the Windows version of the printer driver if it is available on the Server 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

October 29, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receiver 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 Server 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 Server OS machine.
- **On the Server 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Server 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 Server 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

November 1, 2018

### 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 Server OS machine that allows local or network printing from any device, including thin clients and tablets.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp and XenDesktop Virtual Delivery Agent (VDA) standalone package for Windows Desktop OS or Windows Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **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**.

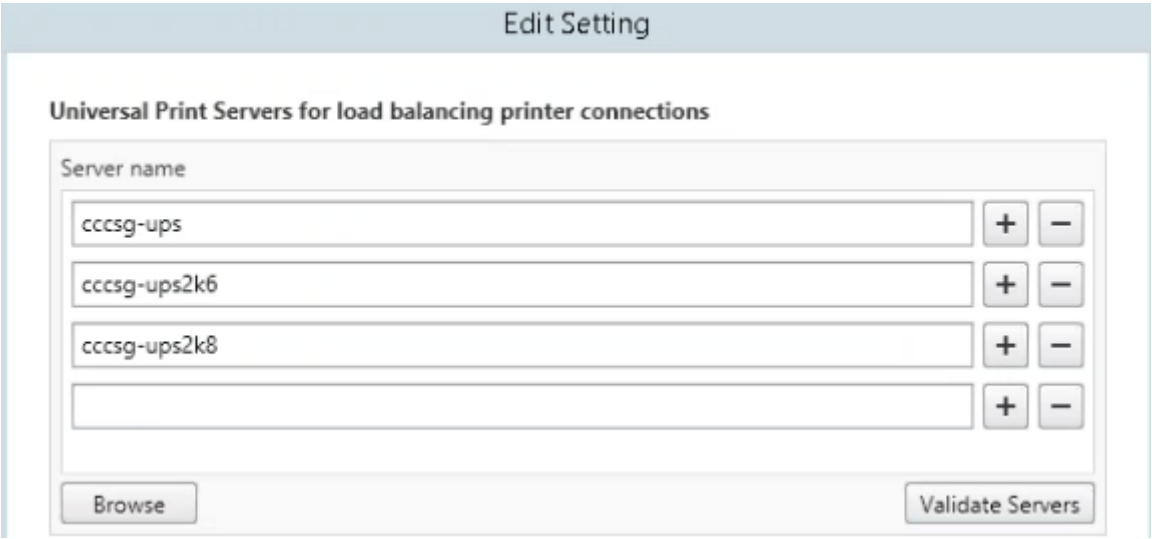
To change the default port of HTTP 8080 for Universal Print Server communication to XenApp and XenDesktop VDAs, the following registry must also be created and the port number value modified on the Universal Print Server computer(s):

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




- **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. |

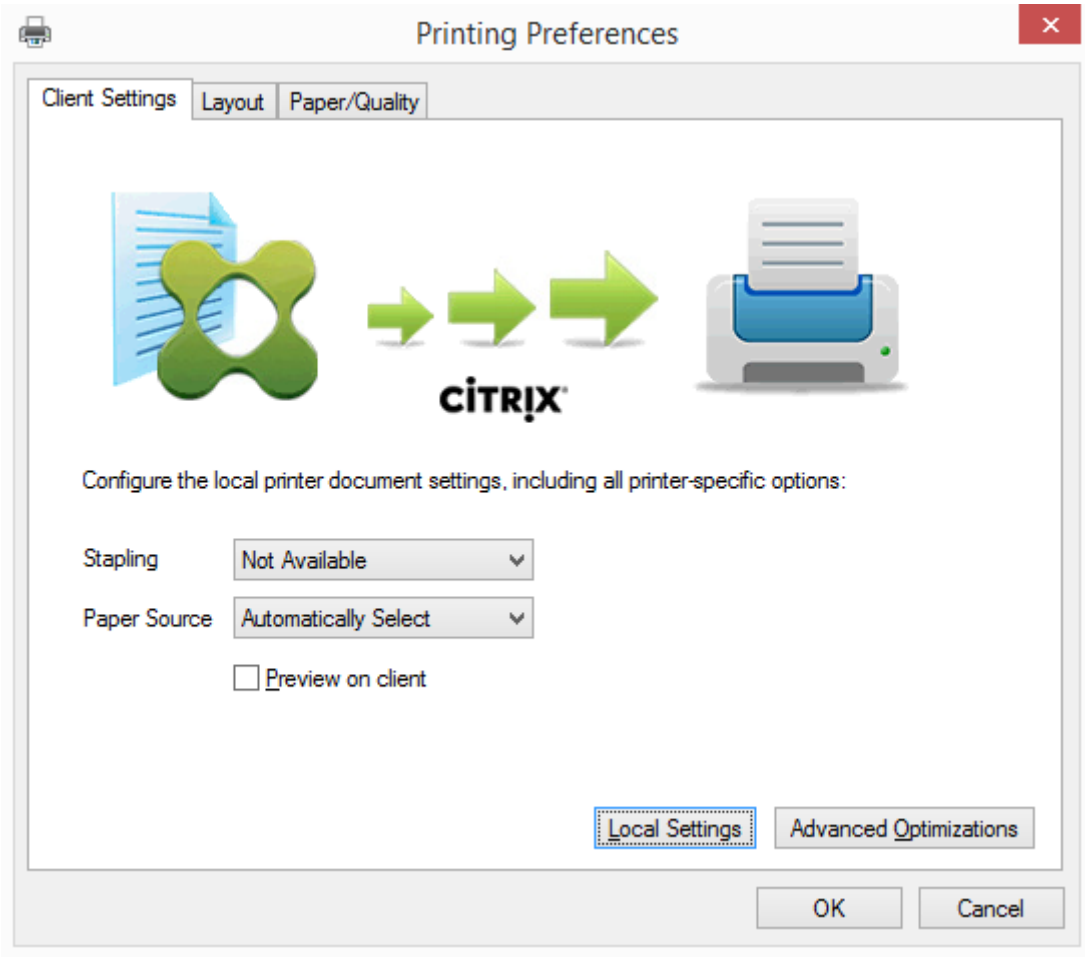
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Policy setting | Interaction |
| --- | --- |

**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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receivers 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 Receivers, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

October 29, 2018

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 Server 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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - 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 Server 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 Server 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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| | | Printing Pathway |
|---|---|---|
| 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 |
| Local network server printers (Printers from a network print server that are added to a Server 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.

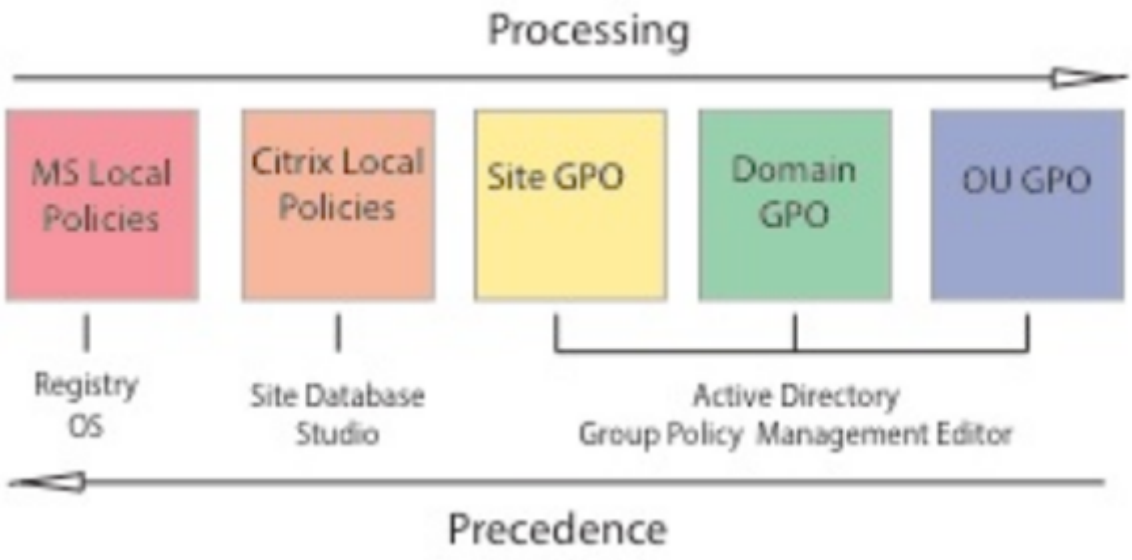
## Policies

October 29, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 could 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. Active Directory applies all policies (end user, endpoint, organizational unit, and domain).
4. The end user logs on to Receiver 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

November 1, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

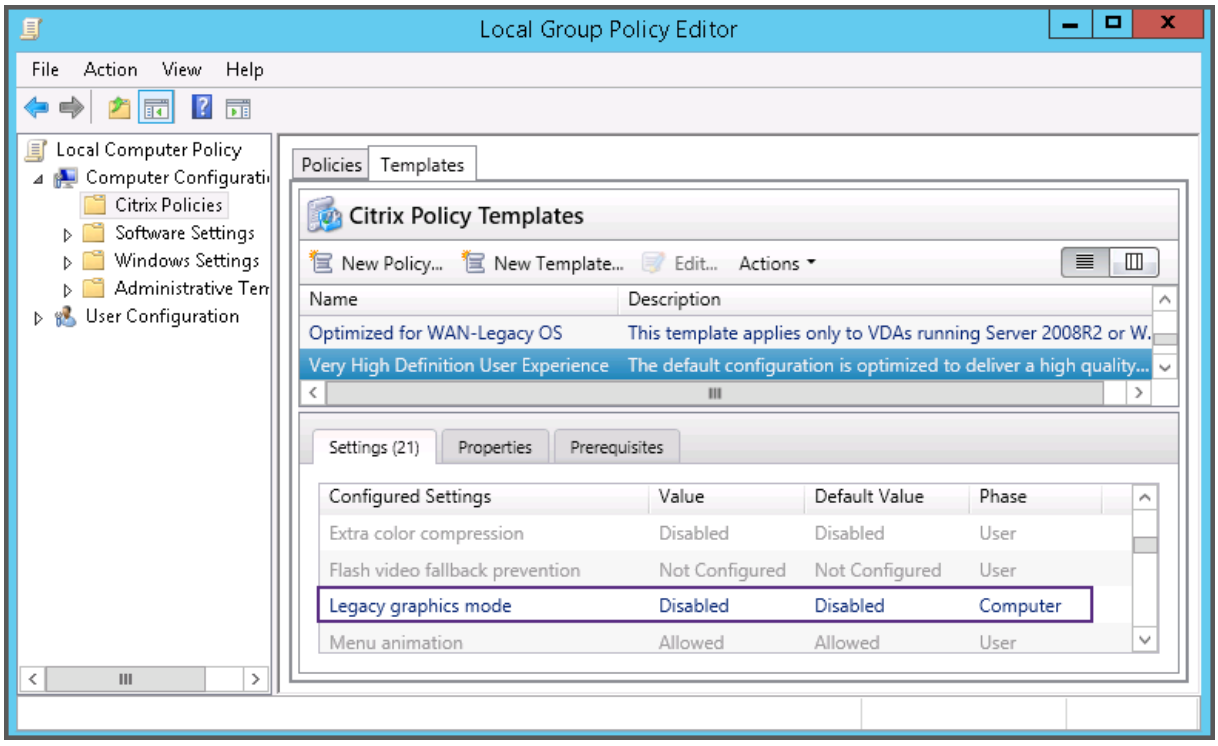
You can refine your search by selecting a specific product version or by selecting a category. For an unfiltered search, select All Settings.

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.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Policy templates

February 21, 2019

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 will be 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 or exported. For additional templates and updates to the built-in templates, see CTX202000.

For considerations when using templates to create policies, see CTX202330.

## Built-in Citrix templates

The following policy templates are available:

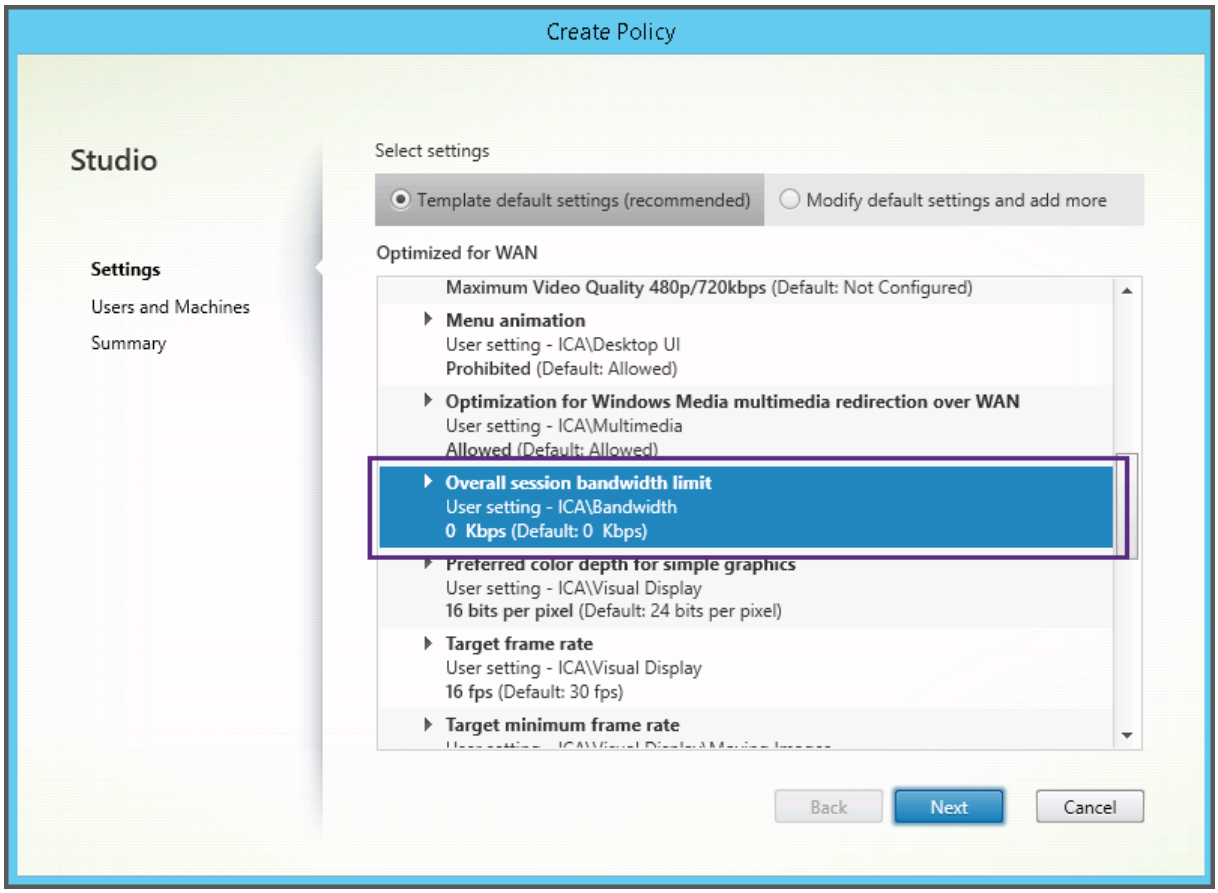
- **Very High Definition User Experience**. This template enforces default settings which maximize the user experience. Use this template in scenarios where multiple policies are processed in order of precedence.
- **High Server Scalability**. Apply this template to economize on server resources. This 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 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 XenDesktop. (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 with 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp and XenDesktop. This template includes settings which will disable access to printing, clipboard, peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices. Applying this template may use more bandwidth and reduce user density per server.

While we recommend using the built-in Citrix templates with their default settings, you will find 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 will understand this setting is likely to apply to the scenario.




If you are working with a deployment (policy management and VDAs) prior to XenApp and XenDesktop 7.6 FP3, and require High Server Scalability and Optimized for WAN templates, please use the Legacy OS versions of these templates when these apply.

> **Note**
>
> Built-in templates are created and updated by Citrix. You cannot modify or delete these templates.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Create and manage templates using Studio

To create a new 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 new 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 should not be included. Enter a name for the template.

After you click **Finish**, the new template appears on the **Templates** tab.

To create a new 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 new 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 should not be included. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Policies node and then select
Citrix Policies. Choose the appropriate action below.

| Task | Instruction |
| --- | --- |
| Create a new template from an existing policy | On the Policies tab, select the policy and then select Actions > Save as Template. |
| Create a new policy from an existing template | On the Templates tab, select the template and then click New Policy. |
| Create a new 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. |
| 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 XenApp and XenDesktop Site's database. This means that the policy template files are controlled by Windows administrative permissions 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 new templates. However, because templates are local files, no changes are actually 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Create policies

November 1, 2018

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 re-evaluates policies at 90-minute intervals and applied either when the virtual desktop restarts or when a user logs on.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. |
| Citrix CloudBridge | Whether or not a user session is launched through Citrix CloudBridge. **Note:** You can add only one Citrix CloudBridge assignment to a policy. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Assignment Name | Applies a policy based on |
| --- | --- |
| Client IP Address | IP address of the user device used to connect to the session. IPv4 examples: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6 examples: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Client Name | Name of the user device. Exact match: ClientABCName. Using wildcard: Client*Name |
| Delivery Group | Delivery Group membership. |
| Delivery Group type | Type of desktop or application: private desktop, shared desktop, private application, or shared application. |
| Organizational Unit (OU) | Organizational unit. |
| Tag | Tags. **Note:** To ensure that policies are applied correctly when using tags, install the hotfix at CTX142439. |
| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. |
| 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

July 6, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Desktop OS VDA connects to Server OS VDA, Citrix policies act on the Desktop 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 Desktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

October 29, 2018

The following tables list policy settings, their default, and the Virtual Delivery Agent (VDA) versions to which they apply.

### ICA

| Name | Default setting | VDA |
|---|---|---|
| Client clipboard redirection | Allowed | All VDA versions |
| Desktop launches | Prohibited | VDA for Server OS 7 through current |
| EDT | Off | VDA 7.13. See Adaptive Transport. |
| ICA listener connection timeout | 120000 milliseconds | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| ICA listener port number | 1494 | All VDA versions |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
|---|---|---|
| Launching of non-published programs during client connection | Prohibited | VDA for Server OS 7 through current |
| Client clipboard write allowed formats | No formats are specified | VDA 7.6 through current |
| 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 |

### 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 Server 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 |
|---|---|---|
| Auto client reconnect | Allowed | All VDA versions |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| Auto client reconnect authentication | Do not require authentication | All VDA versions |
| Auto client reconnect logging | Do not log auto-reconnect events | All VDA versions |

### 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 Server OS 7 through current, VDA for Desktop OS 7 through current |
| Client USB device redirection bandwidth limit percent | 0 | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop 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 Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| HDX MediaStream Multimedia Acceleration bandwidth limit percent | 0 | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop 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 |
| Printer redirection bandwidth limit percent | 0 | All VDA versions |
| TWAIN device redirection bandwidth limit | 0 Kbps | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| TWAIN device redirection bandwidth limit percent | 0 | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 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 Server OS 7 through current, VDA for Desktop OS 7 through current |

### ICA/Desktop UI

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 Desktop OS 7 through current |
| Desktop Composition Redirection graphics quality | Medium | VDA 5.6, VDA for Desktop OS 7 through current |
| 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 Server 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 Server OS 7 through current |
| Preserve client drive letters | Disabled | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| Read-only client drive access | Disabled | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Special folder redirection | Allowed | Web Interface deployments only; VDA for Server 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 Desktop 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 Server OS 7 through current, VDA for Desktop OS 7 through current |
| Image caching | Enabled | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
|---|---|---|
| Legacy graphics mode | Disabled | VDA for Server OS 7 through current, VDA for Desktop 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 Server OS 7 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 bps | VDA for Server 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 Server OS 7 through current, VDA for Desktop OS 7 through current |
| URL redirection black list | No sites are specified | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| URL redirection white list | No sites are specified | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

### ICA/Mobile Experience

| Name | Default setting | VDA |
| --- | --- | --- |
| Automatic keyboard display | Prohibited | VDA 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Launch touch-optimized desktop | Allowed | VDA 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop 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 Server OS 7 through current, VDA for Desktop OS 7 through current |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### ICA/Multimedia

| Name | Default setting | VDA |
|---|---|---|
| HTML5 video redirection | Prohibited | VDA 7.12 through current |
| Limit video quality | Not configured | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Multimedia conferencing | Allowed | All VDA versions |
| Optimization for Windows Media multimedia redirection over WAN | Allowed | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Use GPU for optimizing Windows Media multimedia redirection over WAN | Prohibited | VDA for Server OS 7 through current, VDA for Desktop 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 Server OS 7 through current, VDA for Desktop 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 |
| Windows Media Redirection buffer size use | Disabled | VDA 5, 5.5, 5.6 FP1 |

### ICA/Multi-Stream Connections

| Name | Default setting | VDA |
|---|---|---|
| Audio over UDP | Allowed | VDA for Server OS 7 through current |
| Audio UDP port range | 16500, 16509 | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| Multi-Port policy | Primary port (2598) has High Priority | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Multi-Stream computer setting | Disabled | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Multi-Stream user setting | Disabled | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

### 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
|---|---|---|
| Printer assignments | User's current printer is used as the default printer for the session | All VDA versions |
| 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 | All VDA versions |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 versions |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 caching of embedded fonts = 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 |
| Universal printing print quality limit | No limit | All VDA versions |

### ICA/Security

| Name | Default setting | VDA |
| --- | --- | --- |
| SecureICA minimum encryption level | Basic | VDA for Server OS 7 through current |

### ICA/Server Limits

| Name | Default setting | VDA |
| --- | --- | --- |
| Server idle timer interval | 0 milliseconds | VDA for Server OS 7 through current |

### ICA/Session Limits

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| Disconnected session timer | Disabled | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| Disconnected session timer interval | 1440 minutes | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| Session connection timer | Disabled | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| Session connection timer interval | 1440 minutes | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| Session idle timer | Enabledf | VDA 5, 5.5, 5.6 FP1, VDA for Desktop OS 7 through current |
| Session idle timer interval | 1440 minutes | VDA 5, 5.5, 5.6 FP1, VDA for Desktop 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 Server OS 7 through current |
| Use local time of client | Use server time zone | All VDA versions |

### ICA/TWAIN Devices

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| Client TWAIN device redirection | Allowed | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| TWAIN compression level | Medium | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop 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 Server OS 7 through current, VDA for Desktop 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 |
| Visual quality | Medium | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

### ICA/Visual Display/Moving Images

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| Minimum image quality | Normal | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Moving image compression | Enabled | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Progressive compression level | None | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Progressive compression threshold value | 2147483647 Kbps | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Target minimum frame rate | 10 fps | VDA 5.5, 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

### ICA/Visual Display/Still Images

| Name | Default setting | VDA |
| --- | --- | --- |
| Extra color compression | Disabled | All VDA versions |
| 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| WebSockets connections | Prohibited | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| WebSockets port number | 8008 | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| WebSockets trusted origin server list | The wildcard, *, is used to trust all Receiver for Web URLs | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

### Load Management

| Name | Default setting | VDA |
| --- | --- | --- |
| Concurrent logon tolerance | 2 | VDA for Server OS 7 through current |
| CPU usage | Disabled | VDA for Server OS 7 through current |
| CPU usage excluded process priority | Below Normal or Low | VDA for Server OS 7 through current |
| Disk usage | Disabled | VDA for Server OS 7 through current |
| Maximum number of sessions | 250 | VDA for Server OS 7 through current |
| Memory usage | Disabled | VDA for Server OS 7 through current |
| Memory usage base load | Zero load: 768MB | VDA for Server OS 7 through current |

### Profile Management/Advanced settings

| Name | Default setting | VDA |
| --- | --- | --- |
| Disable automatic configuration | Disabled | All VDA versions |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
|---|---|---|
| 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 |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 |
| 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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
|---|---|---|
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| 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 |
| 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Name | Default setting | VDA |
| --- | --- | --- |
| StoreFront accounts list | No stores are specified | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |

### Virtual Delivery Agent

| Name | Default setting | VDA |
| --- | --- | --- |
| Controller registration IPv6 netmask | No netmask is specified | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Controller registration port | 80 | All VDA versions |
| Controller SIDs | No SIDs are specified | All VDA versions |
| Controllers | No controllers are specified | All VDA versions |
| Enable auto update of controllers | Enabled | VDA for Server OS 7 through current, VDA for Desktop OS 7 through current |
| Only use IPv6 controller registration | Disabled | VDA for Server OS 7 through current, VDA for Desktop 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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

October 29, 2018

Policies contain settings that are applied when the policy is enforced. Descriptions in this section also indicate if additional 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.

### 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| For this task | Use this policy setting |
| --- | --- |
| 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 |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| For this task | Use this policy setting |
| --- | --- |
| 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 |
| 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 and 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Graphics and multimedia

| 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 Flash content is rendered in sessions | Flash default behavior |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| For this task | Use this policy setting |
|---|---|
| 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 |
| 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<br>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

October 29, 2018

The ICA section contains policy settings related to ICA listener connections and mapping to the clipboard.

### Adaptive transport

This setting allows or prevents data transport over EDT as primary and fallback to TCP.

By default, adaptive transport is disabled (**Off**) and TCP is always used.

1. In Studio, enable the policy setting, HDX adaptive transport (it is disabled by default). 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Diagnostic mode**. EDT is forced on and fall back 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 using 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML format is disabled by default. To enable this feature:

- Ensure **Client clipboard redirection** is set to allowed.
- Ensure **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**.

**Note**: Enabling HTML format clipboard copy support (CF_HTML) copies any scripts (if they exist) 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.

Additional custom formats can be added. 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.

### Desktop launches

This setting allows or prevents non-administrative users in a VDA Direct Access Users group connecting to a session on that VDA using an ICA connection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

By default, non-administrative users cannot connect to these sessions.

This setting has no effect on 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 effect on non-administrative users 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

**Note:** This setting applies only to Virtual Delivery Agents 5.0, 5.5, and 5.6 Feature Pack 1.

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 Receiver or plug-in that connects to the server.

### Launching 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.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML format is disabled by default. To enable this feature:

- Ensure **Client clipboard redirection** is set to allowed.
- Ensure **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**.

**Note**: Enabling HTML format clipboard copy support (CF_HTML) copies any scripts (if they exist) 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.

More custom formats can be added. 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.

## Auto client reconnect policy settings

October 29, 2018

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, auto client reconnect uses only the policy settings from Citrix Studio. Updates to these policies in Studio synchronize auto client reconnect from server to

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

client. With older versions of Citrix Receiver for Windows, to configure auto client reconnect, use a Studio policy and modify 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 Receiver 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. Once a session is timed 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 Receiver tries to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

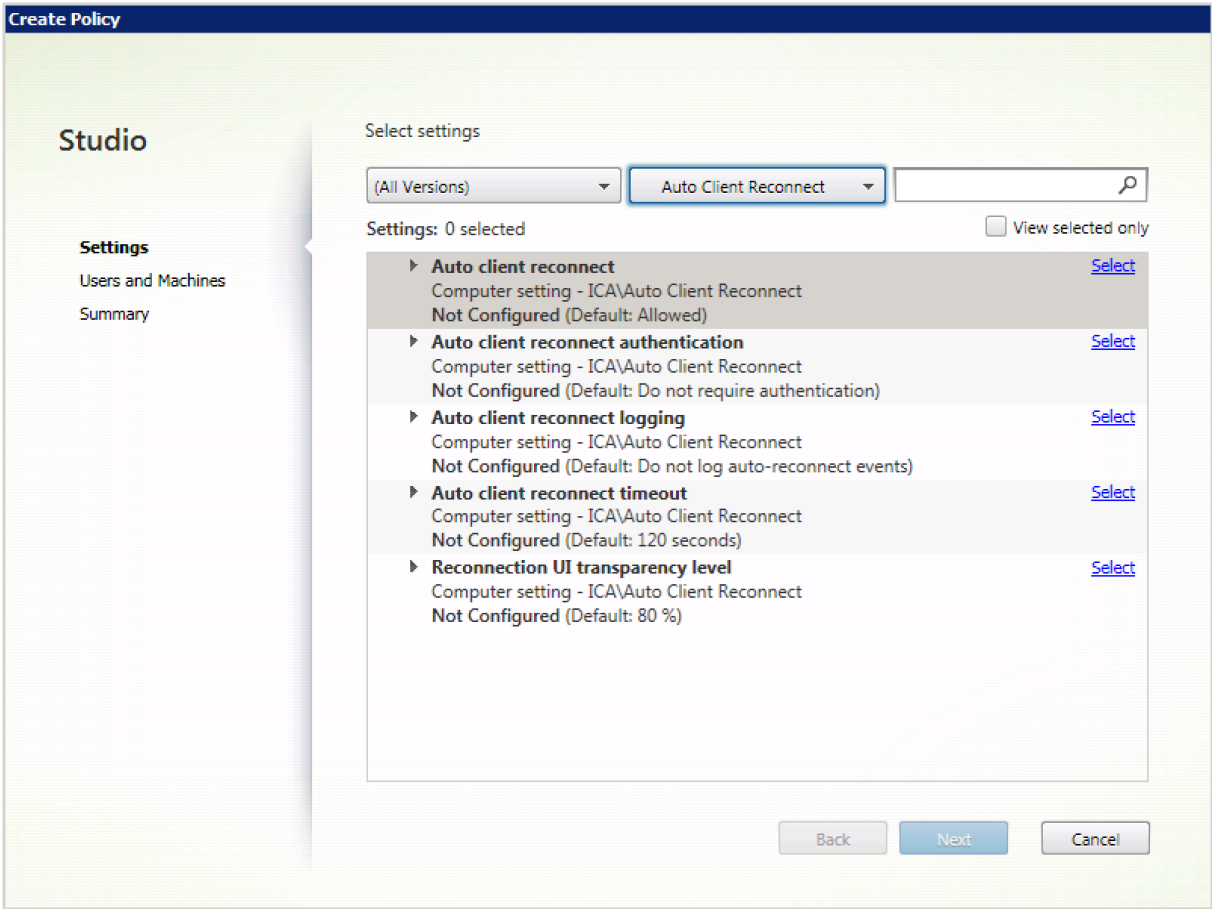
For user sessions, when automatic reconnect is allowed, Citrix Receiver tries to reconnect to the session for a specified period, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period is two minutes. To change this period, edit the policy.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### 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 Receiver. When this setting is configured, cookies are not used. Instead, a dialog box is displayed to users requesting credentials when Citrix Receiver 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. Click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. Click **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. Click **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. Click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Audio policy settings

July 6, 2018

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 Server 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 IP (VoIP) applications, to deliver media applications in challenging network connections with lines less than 512 Kbps, or significant congestion and packet loss. This codec offers very 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

and consuming low bandwidth. If VoIP quality is unsatisfactory, ensure that the Audio over UDP Real-time Transport policy setting is set to Allowed.

Currently, 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 the challenging network connections like very low (less than 512Kbps) 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 utilization and network congestion.

Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption is doubled.

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 may 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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receiver.

On Windows Server 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

April 4, 2019

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 may 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 (with the 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 (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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 (with 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 (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.

### 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 (with 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 (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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 (with 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 (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

### 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 (with 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 (with the lower value) is applied.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 (with 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 (with 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 (with 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 (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.

### 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 (with 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 (with 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 (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.

## Bidirectional content redirection policy settings

February 3, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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:

```
*.xyz.com;https://www.example.com
```

## Client sensors policy settings

July 6, 2018

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 Receiver 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:

- A location-enabled application should not 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - Provide a user option to clear location data that is cached by the application. (Citrix Receiver 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.
- A secure connection (for example, using TLS or a VPN) should be enforced when using location services. Citrix Receiver should connect to trusted servers.
- Consider obtaining legal advice regarding the use of location services.

## Desktop UI policy settings

July 6, 2018

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.

### 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 turn off 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.

By default, this is set to high.

Choose from High, Medium, Low, or Lossless quality.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Desktop wallpaper

This setting allows or prevents wallpaper showing in user sessions.

By default, user sessions can show wallpaper.

To turn off 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. This means that if the desktop is set to discard changes when the session ends, a user who has enabled menu animations in a session may 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

July 6, 2018

The End User Monitoring section contains policy settings for measuring session traffic.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

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 already 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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, 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

July 6, 2018

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, make sure 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Client drive redirection

This setting enables or disables file redirection to and from drives on the user device.

By default, file redirection is enabled.

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, make sure 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 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, make sure 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 floppy drives are automatically connected when users log on, configure the Auto connect client drives setting.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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, make sure 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 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, make sure 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 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, make sure 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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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, make sure 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 modifying files or folders on mapped client drives.

By default, files and folders on mapped client drives can be modified.

If set to Enabled, files and folders are accessible with read-only permissions.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed.

### Special folder redirection

This setting allows or prevents Citrix Receiver 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 Receiver 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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, make sure 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 are typically characterized by relatively high bandwidth and high latency. However, if there is a connection or disk fault, the client file or files being written may end in an undefined state. If this happens, 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.

Citrix recommends enabling asynchronous disk writes only for users who need remote connectivity with good file access speed and who can easily recover files or data lost in the event of connection or disk failure.

When adding this setting to a policy, make sure that the Client drive redirection setting is present and set to Allowed. If this setting is disabled, asynchronous writes will not occur.

## Flash Redirection policy settings

October 29, 2018

The Flash Redirection section contains policy settings for handling Flash content in user sessions.

### Flash acceleration

This setting enables or disables Flash content rendering on user devices instead of the server. By default, client-side Flash content rendering is enabled.

Note: This setting is used for legacy Flash redirection with the Citrix online plug-in 12.1.

When enabled, this setting reduces network and server load by rendering Flash content on the user device. Additionally, the Flash URL compatibility list setting forces Flash content from specific websites to be rendered on the server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

On the user device, the Enable HDX MediaStream for Flash on the user device setting must be enabled as well.

When this setting is disabled, Flash content from all websites, regardless of URL, is rendered on the server. To allow only certain websites to render Flash content on the user device, configure the Flash URL compatibility list setting.

### Flash background color list

This setting enables you to set key colors for given URLs.

By default, no key colors are specified.

Key colors appear behind client-rendered Flash and help provide visible region detection. The key color specified should be rare; otherwise, visible region detection might not work properly.

Valid entries consist of a URL (with optional wildcards at the beginning or end) followed by a 24-bit RGB color hexadecimal code. For example: `https://citrix.com 000003`.

Ensure that the URL specified is the URL for the Flash content, which might be different from the URL of the website.

> **Warning**
>
> Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

On VDA machines running Windows 8 or Windows 2012, this setting might fail to set key colors for the URL. If this occurs, edit the registry on the VDA machine.

For 32-bit machines, use this registry setting:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] “ForceHDXFlashEnabled”=dword:00000001

For 64-bit machines, use this registry setting:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] “ForceHDXFlashEnabled”=dword:00000001

### Flash backwards compatibility

This setting enables or disables the use of original, legacy Flash redirection features with older versions of Citrix Receiver (formerly the Citrix online plug-in).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

By default, this setting is enabled.

On the user device, the Enable HDX MediaStream for Flash on the user device setting must also be enabled.

Second generation Flash redirection features are enabled for use with Citrix Receiver 3.0. Legacy redirection features are supported for use with the Citrix online plug-in 12.1. To ensure second generation Flash redirection features are used, both the server and the user device must have second generation Flash redirection enabled. If legacy redirection is enabled on either the server or the user device, legacy redirection features are used.

### Flash default behavior

This setting establishes the default behavior for second generation Flash acceleration.

By default, Flash acceleration is enabled.

To configure this setting, choose one of the following options:

- Enable Flash acceleration. Flash Redirection is used.
- Block Flash Player. Flash Redirection and server-side rendering are not used. The user cannot view any Flash content.
- Disable Flash acceleration. Flash Redirection is not used. The user can view server-side rendered Flash content if a version of Adobe Flash Player for Windows Internet Explorer compatible with the content is installed on the server.

This setting can be overridden for individual Web pages and Flash instances based on the configuration of the Flash URL compatibility list setting. Additionally, the user device must have the Enable HDX MediaStream for Flash on the user device setting enabled.

### Flash event logging

This setting enables Flash events to be recorded in the Windows application event log.

By default, logging is allowed.

On computers running Windows 7 or Windows Vista, a Flash redirection-specific log appears in the Applications and Services Log node.

### Flash intelligent fallback

This setting enables or disables automatic attempts to employ server-side rendering for Flash Player instances where client-side rendering is either unnecessary or provides a poor user experience.

By default, this setting is enabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Flash latency threshold

This setting specifies a threshold between 0-30 milliseconds to determine where Adobe Flash content is rendered.

By default, the threshold is 30 milliseconds.

During startup, HDX MediaStream for Flash measures the current latency between the server and user device. If the latency is under the threshold, HDX MediaStream for Flash is used to render Flash content on the user device. If the latency is above the threshold, the network server renders the content if an Adobe Flash player is available there.

When enabling this setting, make sure the Flash backwards compatibility setting is also present and set to Enabled.

Note: Applies only when using HDX MediaStream Flash redirection in Legacy mode.

### Flash video fallback prevention

This setting specifies if and how "small"flash content is rendered and displayed to users.

By default, this setting is not configured.

To configure this setting, choose one of the following options:

- **Only small content.** Only intelligent fallback content will be rendered on the server; other Flash content will be replaced with an error *.swf.
- **Only small content with a supported client.** Only intelligent fallback content will be rendered on the server if the client is currently using Flash Redirection; other content will be replaced with an error *.swf.
- **No server side content.** All content on the server will be replaced with an error *swf.

To use this policy setting you should specify an error *.swf file. This error *.swf will replace any content that you do not want to be rendered on the VDA.

### Flash video fallback prevention error *.swf

This setting specifies the URL of the error message which is displayed to users to replace Flash instances when the server load management policies are in use. For example:

```
http://domainName.tld/sample/path/error.swf
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Flash server-side content fetching URL list

This setting specifies websites whose Flash content can be downloaded to the server and then transferred to the user device for rendering.

By default, no sites are specified.

This setting is used when the user device does not have direct access to the Internet; the server provides that connection. Additionally, the user device must have the Enable server-side content fetching setting enabled.

Second generation Flash redirection includes a fallback to server-side content fetching for Flash .swf files. If the user device is unable to fetch Flash content from a Web site, and the Web site is specified in the Flash server-side content fetching URL list, server-side content fetching occurs automatically.

When adding URLs to the list:

- Add the URL of the Flash application instead of the top-level HTML page that initiates the Flash Player.
- Use an asterisk (*) at the beginning or end of the URL as a wildcard.
- Use a trailing wildcard to allow all child URLs (`http://www.citrix.com/*`).
- The prefixes `http://` and `https://` are used when present, but are not required for valid list entries.

### Flash URL compatibility list

This setting specifies the rules which determine whether Flash content on certain websites is rendered on the user device, rendered on the server, or blocked from rendering.

By default, no rules are specified.

When adding URLs to the list:

- Prioritize the list with the most important URLs, actions, and rendering locations at the top.
- Use an asterisk (*) at the beginning or end of the URL as a wildcard.
- Use a trailing wildcard to refer to all child URLs (`https://www.citrix.com/*`).
- The prefixes `http://` and `https://` are used when present, but are not required for valid list entries.
- Add to this list websites whose Flash content does not render correctly on the user device and select either the Render on Server or Block options.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Graphics policy settings

May 18, 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.

## 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 greater 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 greater resolution, increase the limit. Calculate the maximum memory required using the equation:

Memory depth in bytes = (color-depth-in-bits-per-pixel) / 8) * (vertical-resolution-in-pixels) * (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) * (600) * (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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 are 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, and Peek window preview modes.

| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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; it does not control whether images are cached. Images are cached if the Legacy graphics mode setting is enabled.

### Legacy graphics mode

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 Knowledge Center article CTX202687 for more information on optimizing graphics modes and policies in XenApp and XenDesktop 7.6 FP3 and later.

### 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 Desktop OS VDAs using a WDDM driver as the primary display driver, such as Windows 8, this setting has no effect. For Windows Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

### 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 are replaced by another image.

By default, queuing and tossing is enabled.

This 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 (H.264) to compress graphics when video decoding is available on the endpoint. When **For the entire screen** is chosen the video codec will be applied as the default codec for all. When **For actively changing regions** is selected the video codec will be used for areas where there is constant change on the screen, other data will use still image compression and bitmap caching. When video decoding is not available on the endpoint, or when you specify **Do not use**, a combination of still image compression and bitmap caching is used. When **Use video codec when preferred** is selected, the system chooses, based on various factors. The results may vary between versions as the selection method is enhanced.

Select **Use video codec 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 a lot of server-rendered video or other graphically intense applications.

The default is **Use video codec when preferred**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Use hardware encoding for video

This setting allows the use of graphics hardware, if available, to compress screen elements with video (H.264) codec. If such hardware is not available, the VDA will fall 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 Receiver that supports H.264 decoding can be used with NVENC hardware encoding.

Lossy (4:2:0) and visually lossless (4:4:4) compression are supported. Visually lossless (graphics policy setting, Allow visually lossless compression) requires Receiver for Windows 4.5 or later.

#### NVIDIA

For NVIDIA GRID GPUs, hardware encoding is supported with VDAs for Desktop OS in HDX 3D Pro mode.

NVIDIA GPUs must support NVENC hardware encoding. For a list of supported GPUs, see NVIDIA video codec SDK.

NVIDIA GRID requires driver version 3.1 or later. NVIDIA Quadro requires driver version 362.56 or later. Citrix recommends drivers from the NVIDIA Release R361 branch.

Lossless text, a feature of the VDA when configured in standard mode (not HDX 3D Pro), is not compatible with NVENC hardware encoding. If it has been enabled in HDX 3D Pro mode, lossless text takes priority over NVENC hardware encoding.

Selective use of the H.264 hardware codec for actively changing regions is not supported.

#### Intel

For Intel Iris Pro graphics processors, hardware encoding is supported with VDAs for Desktop OS (in standard or HDX 3D Pro mode) and VDAs for Server 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 the Intel website: Remote Displays SDK.

Lossless text is supported.

Selective use of the H.264 hardware codec for actively changing regions is supported.

Supported with Windows 10 and Windows Server 2012 and higher.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

On VDAs in 3D Pro mode, 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.

## Caching policy settings

March 1, 2019

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

July 6, 2018

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

July 6, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Local App Access policy settings

July 6, 2018

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 launches a locally-installed application, that application appears to run within their virtual desktop, even though it is actually running locally.

By default, local app access is prohibited.

### URL redirection black list

This setting specifies websites that are redirected to and launched in the local Web browser. This 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 white list

This setting specifies websites that are rendered in the environment in which they are launched.

By default, no sites are specified.

## Mobile experience policy settings

October 29, 2018

The Mobile Experience section contains policy settings for handling the Citrix Mobility Pack.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Receiver 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 Receiver for iOS session setting to use the Windows combo box.

By default, the Remote the combo box feature is prohibited.

## Multimedia policy settings

October 21, 2021

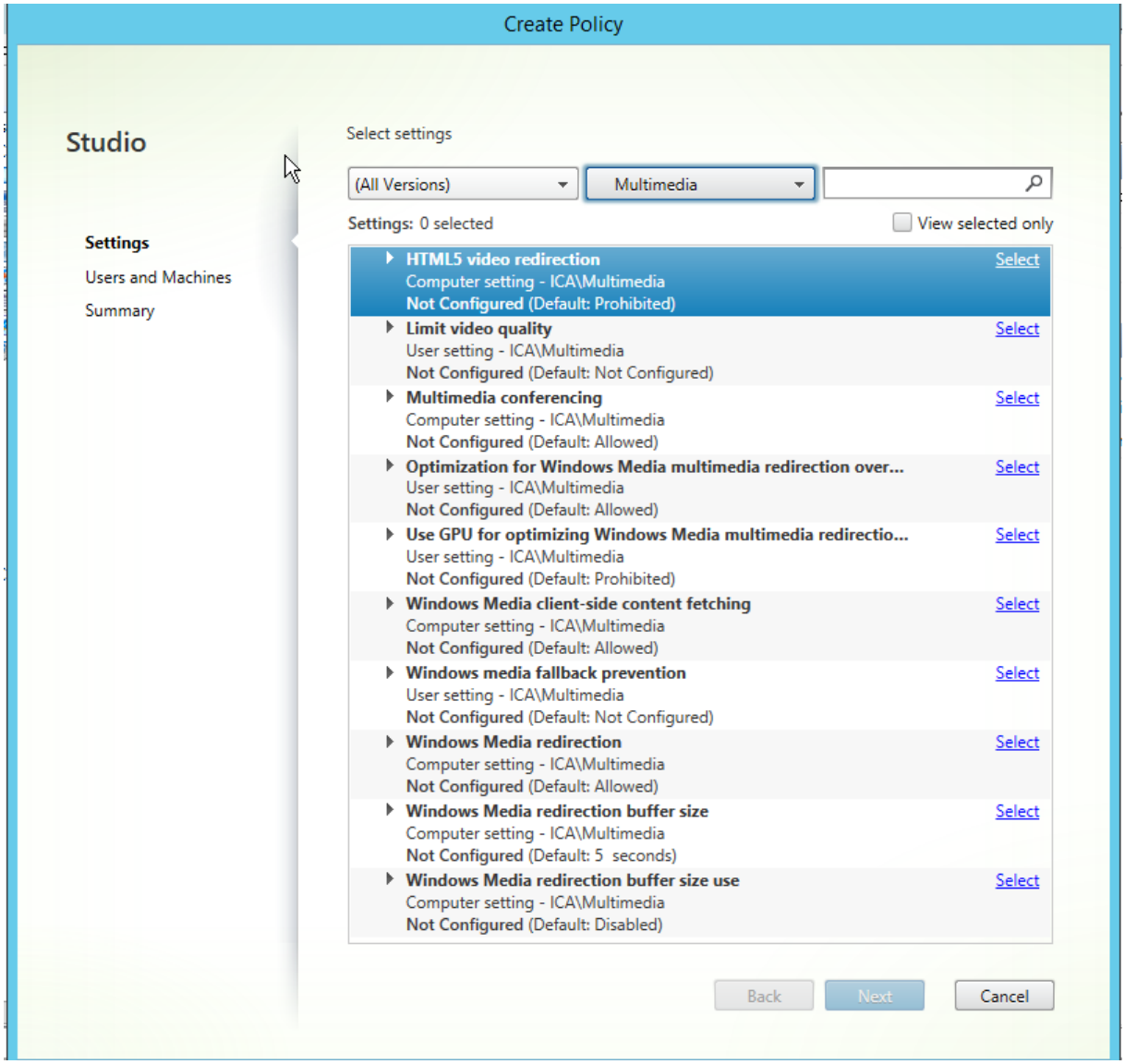
The Multimedia section contains policy settings for managing streaming HTML5 and Windows audio and video in user sessions.

### HTML5 video redirection

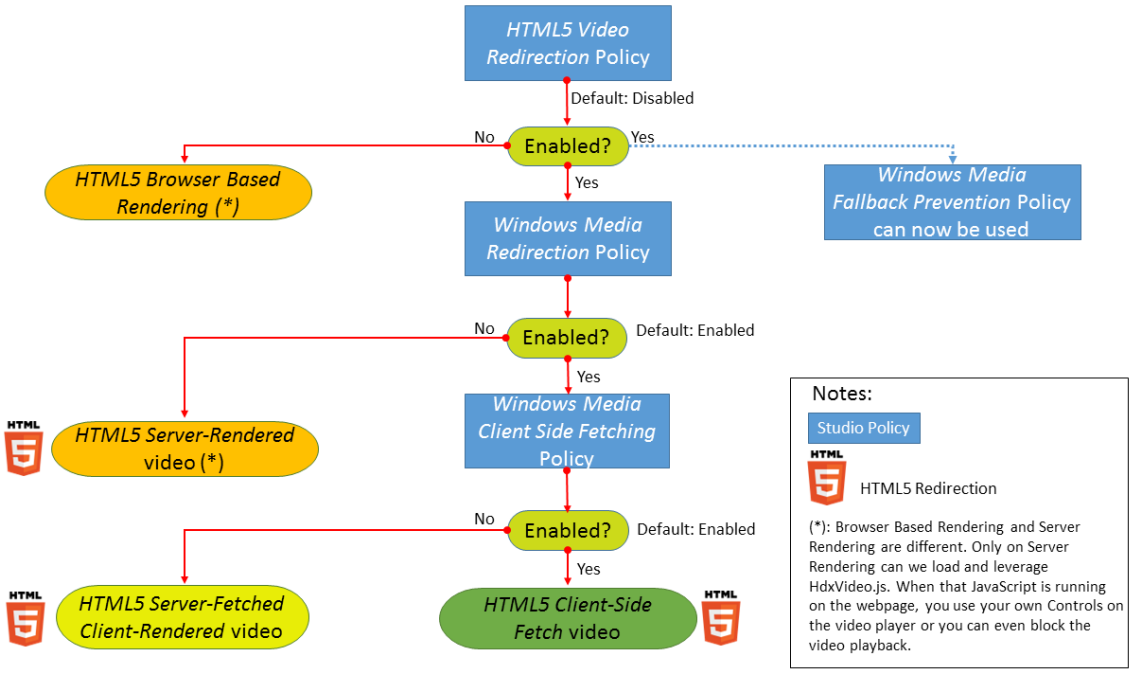
Controls and optimizes the way XenApp and XenDesktop servers deliver HTML5 multimedia web content to users.

By default, this setting is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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, XenApp and XenDesktop defaults to 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

(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/virtualization/hdx/html5-redirect.html.

#### TLS and HTML5 video redirection

You can use HTML5 video 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, 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 on the Local System, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### 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 networks, 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 both HTML5 and Windows Media. For it to work with HTML5, set the ***HTML 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.

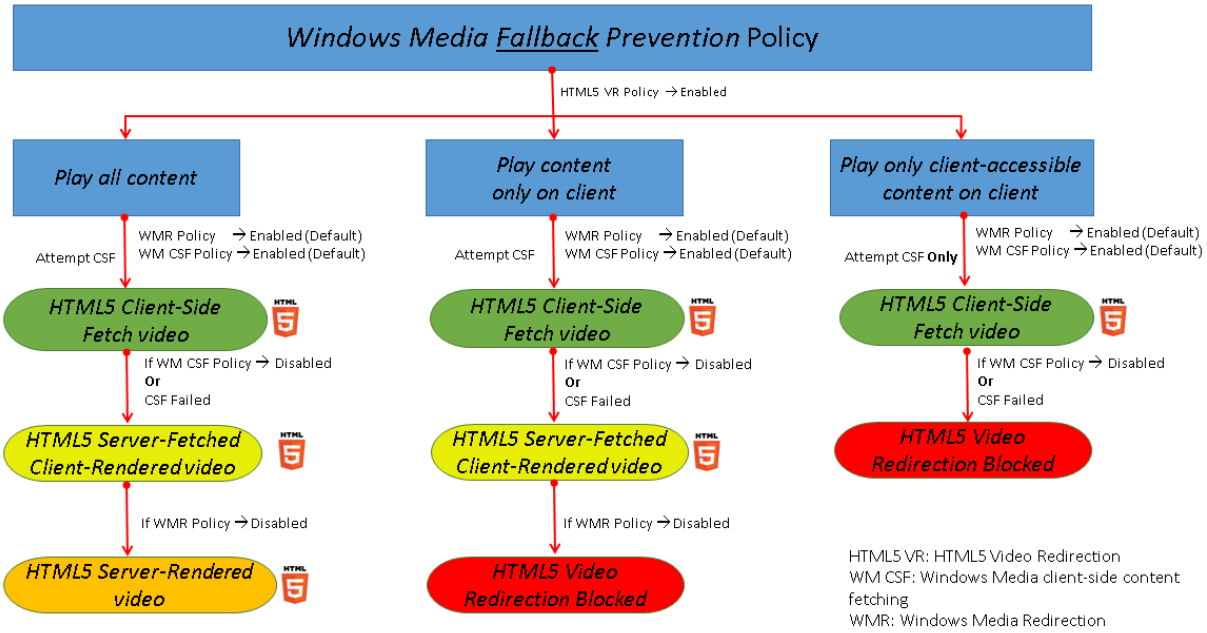
By default, this setting is not configured. When the setting is set to Not Confgured, the behavior is the same as **Play all content**.

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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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.

> **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.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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, the **Enable audio** policy is not configured on the client. To allow users to run multimedia applications in ICA sessions, turn on audio or give users permission to turn on audio in their client 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

February 7, 2020

The Multi-Stream Connections section contains policy settings for managing Quality of Service (QoS) 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 Realtime Transport.

### Audio UDP port range

This setting specifies the range of port numbers (in the form 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

incrementing by two for each subsequent attempt. Each port handles both inbound and outbound traffic.

By default, this 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 modify 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.

If you use Citrix 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 (QoS).

When configuring this setting, reboot the server to ensure changes take effect.

Important: Using this policy setting in conjunction with bandwidth limit policy settings such as Overall session bandwidth limit may produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Multi-Stream user setting

This setting enables or disables Multi-Stream on the user device.

By default, Multi-Stream is disabled for all users.

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 may produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

## Port redirection policy settings

October 29, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

July 23, 2018

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 will be 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 will be 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

By default, no printers are specified.

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.

### 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 6, 2018

The Client Printers section contains policy settings for client printers, including settings to autocreate client printers, retain printer properties, and connect to print servers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

Note: Hotfixes that address the issues with this policy setting are available as Knowledge Center articles CTX141565 and CTX141566.

This setting enables or disables autocreation 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 autocreated.

The following policy settings are related:

- Universal print driver usage
- Universal driver preference

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp 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.

## Drivers policy settings

July 6, 2018

The Drivers section contains policy settings related to printer drivers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Automatic installation of in-box printer drivers

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

July 6, 2018

The Universal Print Server section contains policy settings for handling the Universal Print Server.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp and XenDesktop 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 XenApp and XenDesktop. 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 and that all servers have an identical set of shared printers installed. This operation may take some time.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

November 1, 2018

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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

The Security section contains the policy setting for configuring session encryption and encryption of logon data.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 XenApp and XenDesktop.

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 with 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 with RC5 128-bit encryption and the client connection using Basic encryption.
- RC5 (40 bit) encrypts the client connection with RC5 40-bit encryption.
- RC5 (56 bit) encrypts the client connection with RC5 56-bit encryption.
- RC5 (128 bit) encrypts the client connection with 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Server limits policy settings

October 29, 2018

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).

> **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. This message is a Microsoft dialog box that is not controlled by Citrix policy settings. For more information, see CTX118618.

## Session limits policy settings

October 21, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 1440 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 1440 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 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 1440 minutes (24 hours).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Session reliability policy settings

February 16, 2022

The session reliability section includes policy settings for managing session reliability connections.

## Session reliability connections

This setting allows or prevents sessions to be kept open during a loss of network connectivity. Session reliability, along with auto client reconnection, allows users to automatically reconnect to their Citrix Receiver sessions after recovering from network disruptions. By default, session reliability is Allowed.

The settings in Citrix Studio are enforced on the client for the following:

- Citrix Workspace app 1808 and later
- Citrix Receiver for Windows 4.7 and later

Citrix Studio policy overrides Citrix Receiver Group Policy Object on the clients. 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. Also, set 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 they're using until network connectivity resumes.

With session reliability, the session is kept 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. User 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, trying to reconnect the user to the disconnected session.

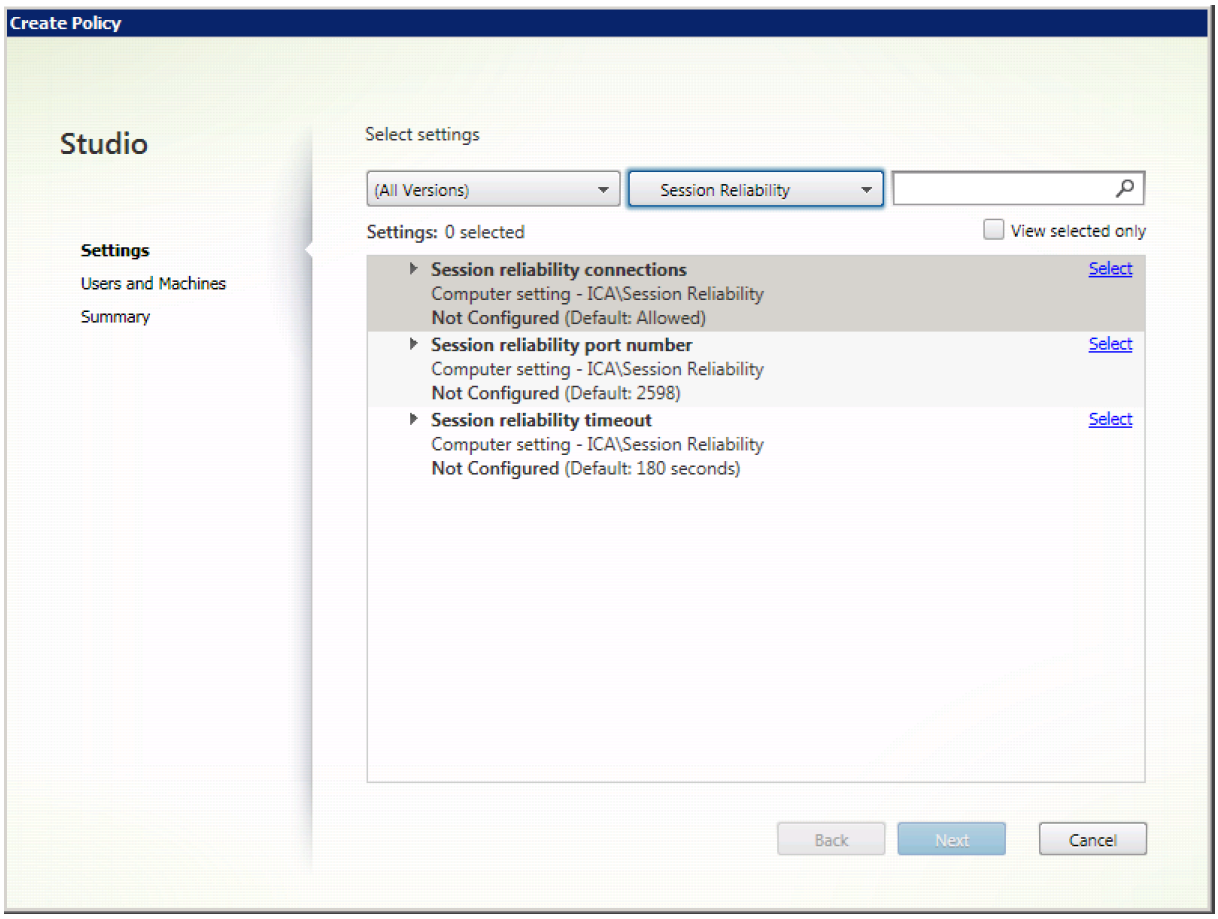
By default, session reliability is Allowed.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Note:**
>
> When Citrix ADC is in use, you must select **Enable session reliability** in the Citrix StoreFront > **Manage Citrix Gateways** / **Secure Ticket Authority** to proxy ICA connections.

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 modify session reliability port number:

1. Start Citrix Studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. This time is the time that 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**.

## Time zone control policy settings

July 23, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Use local time of client

This setting determines the time zone setting of the user session. This can be either the time zone of the user session or the time zone of the user device.

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 (User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection).

## TWAIN devices policy settings

July 1, 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

> **Note:**
>
> TWAIN redirection is not supported when using 64-bit applications.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# USB devices policy settings

December 6, 2019

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 device is allowed by the USB policy settings. 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 below for available modes.

### Good to know

- For the use of Wacom signature pads and tablets, Citrix recommends that you disable the screen saver. Steps on how to do this 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 XenApp and XenDesktop policies.
- Signature devices work across XenApp and XenDesktop and do not require a driver to be used as a signature device. Wacom has additional software that can be installed to customize the device further. See https://www.wacom.com/.
- Drawing tablets. Certain drawing input devices may present as an HID device on PCI/ACPI buses and are not supported. These devices should be attached on a USB host controller on the client to be redirected inside a XenDesktop session.

Policy rules take the format of tag=value expressions separated by whitespace. The following tags are supported:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. Click **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, as a four digit hexadecimal number. |
| PID | Product ID from the device descriptor, as a four digit hexadecimal number. |
| REL | Release 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. |

When creating new policy rules, remember:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Rules are case-insensitive.
- Rules may 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.
- Refer to the USB class codes available from the USB Implementers Forum, Inc. web site.

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:"with no 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.

## Visual display policy settings

March 1, 2019

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 will fall back to 24-bit (default) color depth if the 8-bit setting is applied on VDA version 7.11 and earlier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 is set to 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** - In cases where preserving image data is vital (for example, when displaying X-ray images where no loss of quality is acceptable), select Always lossless to ensure lossy data is never sent to the user device.

If the **Legacy graphics mode** setting is enabled, the **Visual quality** setting has no effect in the policy.

## Moving images policy settings

November 1, 2018

The Moving Images section contains settings that enable you to remove or alter compression for dynamic images.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

November 1, 2018

The Still Images section contains settings that enable you to remove or alter compression for static images.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Receiver 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

July 6, 2018

The WebSockets section contains policy settings for accessing virtual desktops and hosted applications with Citrix Receiver 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Receiver for Web, expressed as URLs. Only WebSockets connections originating from one of these addresses is accepted by the server.

By default, the wildcard * is used to trust all Citrix Receiver 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 should 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

August 17, 2018

The Load Management section contains policy settings for enabling and configuring load management between servers delivering Windows Server 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

April 14, 2020

The Profile Management section contains policy settings for enabling profile management and specifying which groups to include in and exclude from profile management processing.

Other information (such as the names of the equivalent .ini file settings and which version of profile management is required for a policy setting) is available in Profile Management Policies.

## Advanced policy settings

August 8, 2019

The Advanced settings section contains policy settings relating to the advanced configuration of Profile management.

### Disable automatic configuration

This setting enables profile management to examine your environment, for example, to check for the presence of Personal vDisks and configure Group Policy accordingly. Only Profile management policies in the Not Configured state are adjusted, so any customizations made previously 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 XenApp 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 above on different OSs:

| | Server OS | Desktop 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. |
| 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**.

By default, automatic configuration is allowed.

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 your environment changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Log off user if a problem is encountered

This setting enables Profile management to log a user off if a problem is encountered; for example, if the user store is unavailable. When enabled, an error message is displayed to the user before they are logged off. When disabled, users are given a temporary profile.

By default, this setting is disabled and users are given a temporary profile if a problem is encountered.

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.

### Number of retries when accessing locked files

This setting specifies the number of attempts Profile management makes to access locked files.

By default, this is set to five retries.

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.

### Process Internet cookie files on logoff

This setting enables Profile management to process index.dat on logoff to remove Internet cookies left in the file system after sustained browsing that can lead to profile bloat. Enabling this setting increases logoff times, so only enable it if you experience this issue.

By default, this setting is disabled and Profile management does not process index.dat on logoff.

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 processing of Index.dat takes place.

## Basic policy settings

July 6, 2018

The Basic settings section contains policy settings relating to the basic configuration of Profile management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Active write back

This setting enables modified files and folders (but not registry settings) to be synchronized to the user store during a session, before logoff.

By default, synchronization to the user store during a session 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 enabled.

### Enable Profile management

This setting enables Profile management to process logons and logoffs.

By default, this is setting is disabled to facilitate deployment.

Important: Citrix recommends enabling Profile management only after carrying out all other setup tasks and testing how Citrix user profiles perform in your environment.

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, Profile management does not process Windows user profiles in any way.

### Excluded groups

This setting specifies which computer local groups and domain groups (local, global, and universal) are excluded from Profile management processing.

When enabled, Profile management does not process members of the specified user groups.

By default, this setting is disabled and members of all user groups are processed.

Specify domain groups in the form <DOMAIN NAME>\<GROUP NAME>.

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, members of all user groups are processed.

### Offline profile support

This setting enables offline profile support, allowing profiles to synchronize with the user store at the earliest opportunity after a network disconnection.

By default, support for offline profiles is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

This setting is applicable to laptop or mobile users who roam. When a network disconnection occurs, profiles remain intact on the laptop or device even after restarting or hibernating. As mobile users work, their profiles are updated locally and are synchronized with the user store when the network connection is re-established.

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, support for offline profiles is disabled.

### Path to user store

This setting specifies the path to the directory (user store) in which user settings, such as registry settings and synchronized files, are saved.

By default, the Windows directory on the home drive is used.

If this setting is disabled, user settings are saved in the Windows subdirectory of the home directory.

The path can be:

- **A relative path**.This must be relative to the home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.
- **An absolute UNC path**. This typically specifies a server share or a DFS namespace.
- **Disabled or unconfigured**. In this case, a value of #homeDirectory#\Windows is assumed.

Use the following types of variables when configuring this policy setting:

- System environment variables enclosed in percent signs (for example, %ProfVer%). Note that system environment variables generally require additional setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile management variables. For more information, see the Profile management documentation.

You can also use the %username% and %userdomain% user environment variables and create custom attributes to fully define organizational variables such as location or users. 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$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! might expand to \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Important: Whichever attributes or variables you use, check that this setting expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in \\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profile, set the path to the user store as \\server\profiles$\JohnSmith.Finance\v2x64, not the \UPM_Profile subfolder.

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 Windows directory on the home drive is used.

### Process logons of local administrators

This setting specifies whether or not logons of members of the BUILTIN\Administrators group are processed. This allows domain users with local administrator rights, typically users with assigned virtual desktops, to bypass processing, log on, and troubleshoot a desktop experiencing problems with Profile management.

If this setting is disabled or not configured on server operating systems, Profile management assumes that logons by domain users, but not local administrators, must be processed. On desktop operating systems, local administrator logons are processed.

By default this setting is disabled, and local administrator logons are not processed.

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, local administrator logons are not processed.

### Processed groups

This setting specifies which computer local groups and domain groups (local, global, and universal) are included in Profile management processing.

When enabled, Profile management processes only members of the specified user groups.

By default, this setting is disabled and members of all user groups are processed.

Specify domain groups in the form <DOMAIN NAME><GROUP NAME>.

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, members of all user groups are processed.

## Cross-platform policy settings

July 6, 2018

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The Cross-Platform section contains policy settings relating to configuring the Profile management cross-platform settings feature.

### Cross-platform settings user groups

This setting specifies the Windows user groups whose profiles are processed when the cross-platform settings feature is enabled.

By default, this setting is disabled and all user groups specified in the Processed Group policy setting are processed.

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 groups are processed.

### Enable cross-platform settings

This setting enables or disables the cross-platforms settings feature, that allows you to migrate users' profiles and roam them when a user connects to the same application running on multiple operating systems.

By default the cross-platform settings feature 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, no cross-platform settings are applied.

### Path to cross-platform definitions

This setting specifies the network location, as a UNC path, of the definition files copied from the download package.

Note: Users must have read access, and administrators write access, to this location and it must be either a Server Message Block (SMB) or Common Internet File System (CIFS) file share.

By default, no path is specified.

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 cross-platform settings are applied.

### Path to cross-platform settings store

This setting specifies the path to the cross-settings store, the folder in which users'cross-platform settings are saved. This path can be either a UNC path or a path relative to the home directory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Note: Users must have write access to the cross-settings store.

By default, this setting is disabled and the path Windows\PM_CP is used.

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.

### Source for creating cross-platform settings

This setting specifies a platform as the base platform if this setting is enabled for that platform's OU. Data from the base platform's profiles is migrated to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. This means you must decide which platform's profile data to use to seed the cross-platform settings store. This is referred to as the base platform.

When enabled, Profile management migrates the data from the single-platform profile to the store if the cross-platform settings store contains a definition file with no data, or if the cached data in a single-platform profile is newer than the definition's data in the store.

Important: If this setting 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 setting is disabled and Profile management does not migrate the data from the single-platform profile to the store.

## File system policy settings

July 6, 2018

The File System section contains policy settings for configuring which files and directories in a users profile are synchronized between the system where the profile is installed and the user store.

## Exclusions policy settings

July 6, 2018

The Exclusions section contains policy settings for configuring which files and directories in a users profile are excluded from the synchronization process.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Exclusion list - directories

This setting specifies a list of folders in the user profile that are ignored during synchronization.

Specify folder names as paths relative to the user profile (%USERPROFILE%).

By default, this setting is disabled and all folders in the user profile are synchronized.

Example: Desktop ignores the Desktop folder in the user profile

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 folders in the user profile are synchronized.

### Exclusion list - files

This setting specifies a list of files in the user profile that are ignored during synchronization.

By default, this setting is disabled and all files in the user profile are synchronized.

Specify file names as paths relative to the user profile (%USERPROFILE%). Note that wildcards are allowed and are applied recursively.

Example: Desktop\Desktop.ini ignores the file Desktop.ini in the Desktop folder

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 files in the user profile are synchronized.

## Synchronization policy settings

September 8, 2023

The Synchronization 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

This setting specifies any directories you want Profile management to include in the synchronization process that are located in excluded folders. By default, Profile management synchronizes everything in the user profile. It is not necessary to include subfolders of the user profile by adding them to this list. For more information, see Include and exclude items.

Paths on this list must be relative to the user profile.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Example: Desktop\exclude\include ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not

By default, this setting is disabled and no folders are specified.

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 non-excluded folders in the user profile are synchronized.

### Files to synchronize

This setting specifies any files you want Profile management to include in the synchronization process that are located in excluded folders. By default, Profile management synchronizes everything in the user profile. It is not necessary to include files in the user profile by adding them to this list. For more information, see Include and exclude items.

Paths on this list must be relative to the user profile. Relative paths are interpreted as being relative to the user profile. Wildcards can be used but are allowed only 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

By default, this setting is disabled and no files are specified.

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 non-excluded files in the user profile are synchronized.

### Folders to mirror

This setting specifies which folders relative to a user's profile root folder to mirror. Configuring this policy setting can help solve issues involving any transactional folder (also known as a referential folder), that is a folder containing 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. Be aware that, in these situations the "last write wins"so files in mirrored folders that have been modified in more than one session will be overwritten by the last update, resulting in loss of profile changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For example, you can mirror the Internet Explorer cookies folder so that Index.dat is synchronized with the cookies that it indexes.

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 should replace those 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 from the last session each time the user logs off so Index.dat stays up to date.

By default, this setting is disabled and no folders are mirrored.

If this setting 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.

## Folder redirection policy settings

July 6, 2018

The Folder Redirection 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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## AppData(Roaming) policy settings

July 6, 2018

The AppData(Roaming) section contains policy settings for specifying whether to redirect the contents 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

July 6, 2018

The Contacts section contains policy settings for specifying whether to redirect the contents 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

The Desktop section contains policy settings for specifying whether to redirect the contents 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

July 6, 2018

The Documents section contains policy settings for specifying whether to redirect the contents the Documents folder to a shared network location.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

February 21, 2019

The Downloads section contains policy settings that specify whether to redirect the contents 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

February 21, 2019

The Favorites section contains policy settings that specify whether to redirect the contents 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

July 6, 2018

The Links section contains policy settings that specify whether to redirect the contents the Links folder to a shared network location.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

The Music section contains policy settings that specify whether to redirect the contents 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

July 23, 2018

The Pictures section contains policy settings that specify whether to redirect the contents 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Saved Games policy settings

July 6, 2018

The Saved Games section contains policy settings that specify whether to redirect the contents 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

July 6, 2018

The Start Menu section contains policy settings that specify whether to redirect the contents 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

The Searches section contains policy settings that specify whether to redirect the contents 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

July 6, 2018

The Video section contains policy settings that specify whether to redirect the contents the Video folder to a shared network location.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

The Log 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 settings 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 (1MB).

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 may create significant network traffic, which may 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

The Profile handling 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 new profiles, as if in a 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.

### Path to the template profile

This setting specifies the path to the profile you want Profile management to use as a template to create new 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 new user profiles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 new 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 new 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 new 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 new 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

July 6, 2018

The Registry section contains policy settings that specify which registry keys are included or excluded from Profile management processing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Exclusion list

This setting specifies the list of registry keys in the HKCU hive excluded from Profile management processing when a user logs off.

When enabled, keys specified in this list are excluded from processing when a user logs off.

By default, this setting is disabled, and all registry keys in the HKCU hive are processed when a user logs 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, no registry keys are excluded from processing.

### Inclusion list

This setting specifies the list of registry keys in the HKCU hive included in Profile management processing when a user logs off.

When enabled, only keys specified in this list are processed when a user logs off.

By default, this setting is disabled, and all registry keys in the HKCU hive are processed when a user logs 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, all of HKCU is processed .

## Streamed user profiles policy settings

August 8, 2019

The Streamed user profiles section contains policy settings that specify how Profile management processes streamed user profiles.

### Always cache

This setting specifies whether or not 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 megabytes, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 To enable profile streaming exclusion.

### 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.

## Receiver policy settings

July 6, 2018

Note: Unless otherwise noted, "Receiver"refers to Citrix Receiver.

The Receiver section contains policy settings that specify a list of StoreFront addresses to push to Citrix Receiver for Windows running on the virtual desktop.

### StoreFront accounts list

This settings specifies a list of StoreFront stores administrators can choose to push to Citrix Receiver for Windows running on the virtual desktop. When creating a Delivery Group, administrators can select which stores to push to Citrix Receiver for Windows running on virtual desktops within that group.

By default, no stores are specified.

For each store, specify the following information as a semicolon-delimited entry:

- Store name. The name displayed to users of the store.
- Store URL. The URL for the store.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Store enabled state. Whether or not the store is available to users. This is either On or Off.
- Store description. The description displayed to users of the store.

For example: Sales Store;`https://sales.mycompany.com/Citrix/Store/discovery;On;Store` for Sales staff

## Virtual Delivery Agent policy settings

July 6, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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

July 6, 2018

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

August 12, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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):

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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 |
| 1 K | 270 MB |
| 40 K | 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

#### Enable monitoring of application failures on Desktop OS VDAs

By default, failures only from applications hosted on the Server OS VDAs are monitored. To monitor Desktop 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

January 31, 2020

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To add more than one executable, add each executable on a different line.

By default, no executables are specified.

## Configure COM Port and LPT Port Redirection settings using the registry

August 17, 2018

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 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.

| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Registry key | Description | Permitted values |
|---|---|---|
| AutoConnectClientLptPorts | Automatically connect LPT ports from the user device | 1 (Allow) or 0 (Prohibit) |

After configuring these settings, modify 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

July 6, 2018

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 Server 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 Desktop OS catalogs, use Configuration Manager to notify users. For Desktop 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

April 2, 2019

Managing a XenApp or XenDesktop 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 resource

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. It is the most comprehensive high availability feature Citrix offers for XenApp and XenDesktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Connection leasing

Citrix recommends trying Local Host Cache instead of connection leasing. Local Host Cache is a more powerful alternative.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

XenApp and XenDesktop 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 2, 2022

> **Note**
>
> Studio and Director do not support Citrix License Server VPX. For more information about Citrix License Server VPX, see the Citrix Licensing documentation.

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 below, 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 |
|---|---|---|
| XenApp | Platinum, Enterprise, Advanced | Concurrent |
| XenDesktop | Platinum, Enterprise, App, VDI | User/Device, Concurrent |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **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 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.

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 click **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 additional 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 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

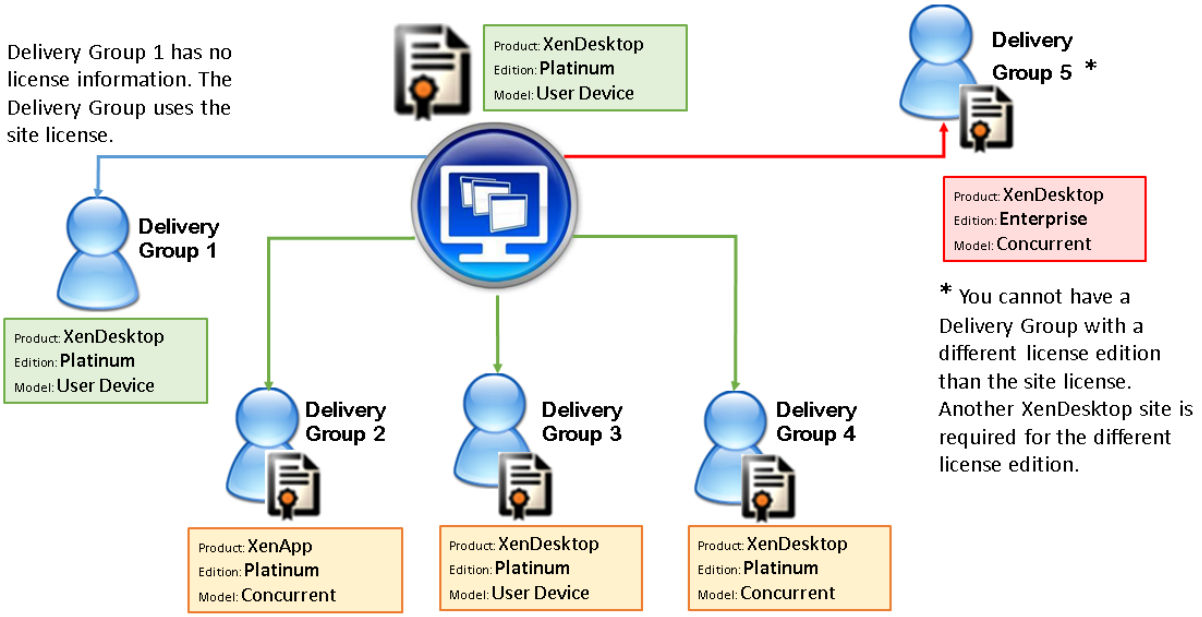
3. Select either **Edit licensing administrator group** or **Delete licensing administrator group** in the Actions pane.

## Multi-type licensing

November 16, 2018

Multi-type licensing supports consumption of different license types for Delivery Groups on a single XenApp or XenDesktop site. **Type** is a single combination of Product ID (XDT, MPS) and Model (UserDevice, Concurrent). The Delivery Groups must use the Product Edition set for the site.

If multi-type licensing is not configured, different license types can be used only when configured on entirely separate sites. The Delivery Groups use the site license.




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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.

### 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 | An enum (Concurrent or UserDevice) specifying the licensing model for the group. | If the feature toggle is disabled, attempting to set a property fails. |
| ProductCode | A text string of XDT (for XenDesktop) or MPS (for XenApp) specifying the licensing Product ID for the group. | If the feature toggle is disabled, attempting to set a property fails. |

### 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/.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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, apply the **Site level Site license**.

3. To change the license model, run the command **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–LicenseModel LicenseModel**.
4. To change the license product, run 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, for example, Premium and Advanced licenses.

6. To remove the license configuration, run 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 XenApp Platinum Concurrent" -ProductCode MPS -LicenseModel Concurrent**
2. We set the second Delivery Group for XenDesktop and Concurrent.
   **Set-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum Concurrent" -ProductCode XDT -LicenseModel Concurrent**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. We create and set the third Delivery Group for XenDesktop and UserDevice.
   **New-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum UserDevice" -PublishedName "MyDesktop"-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice**

### Special considerations

Multi-type licensing has different functionality than regular XenApp and XenDesktop licensing.

There are no alerts and notifications from Director or Studio:

- 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.

## Applications

October 29, 2018

### 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 Receiver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 information about:

- Delivery Groups, see the Create Delivery Groups article.
- Application Groups, see the Create Application Groups article.
- Tags, which you can add to applications; see the Tags article.

## 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Applications 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 an earlier

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

XenDesktop 7.x version, 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

Using these actions:

- **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 it 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

- Category/folder where application appears in Receiver (Delivery)
- Command line arguments; see Pass parameters to published applications section (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 section (Delivery)
- Name: the names seen by the user and by the administrator (Identification)
- Path to executable; see Pass parameters to published applications section (Location)
- Shortcut on user's desktop: enable or disable (Delivery)
- Visibility: limits which users can see the application in Citrix Receiver; 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 Receiver 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 two application limit settings; you can configure either or both:

- The maximum number of concurrent instances of an application by all users in the Delivery Group.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- One instance of the application per user in the Delivery Group

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.

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.

If application instances are also launched by methods other than Controller brokering (for example, while a Controller is in leased connection 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 application limits:

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 options listed below. When you are finished, click **OK** or **Apply**. (**OK** applies the change and closes the Edit Application Properties dialog box; **Apply** applies the change and leaves the dialog box open.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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. Tip: 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.)

## Universal Windows Platform Apps

June 30, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

XenApp and XenDesktop supports the use of Universal Windows Platform (UWP) apps with VDAs on Windows 10 and Windows Server 2016 machines. For information about UWP apps, see the following Microsoft documentation:

- What is a Universal Windows Platform (UWP) app?
- Distribute offline apps
- Guide to Universal Windows Platform (UWP) apps

The term Universal Apps is used throughout this article to refer to UWP apps.

### Requirements and limitations

Universal Apps are supported for VDAs on Windows 10 and Windows Server 2016 machines.

VDAs must be minimum version 7.11.

The following XenApp and XenDesktop features are either not supported or limited when using Universal 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 Universal Apps.
- Action Center remoting: Universal Apps can use the Action Center for displaying the messages in the session. Redirect these messages to the endpoint to display them to the user.

Launching Universal apps and non-Universal apps from same server is not supported for Windows 10 VDAs. For Windows Server 2016, Universal apps and non-Universal apps should be in separate Delivery Groups or Application Groups.

All Universal Apps installed on the machine are enumerated; therefore, Citrix recommends disabling user access to the Windows Store. This prevents the Universal Apps installed by one user from being accessed by a different user.

During sideloading, the Universal App is installed on the machine and is available for use for other users. When any other user launches the app, the app is installed. The OS then updates its AppX database to indicate "as installed"for the user launching the app.

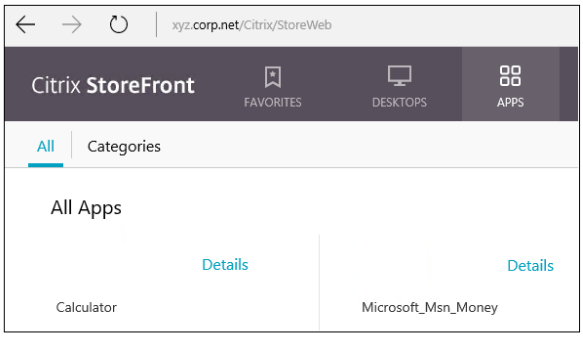
Graceful logoffs from a published Universal App that was launched in a seamless or fixed window might result in the session not closing, and the user being logged off. In such cases, several processes remaining in the session prevent the session from closing properly. To resolve this, determine which process is preventing the session from closing, and then add it to the "LogoffCheckSysModules"registry key value, following the guidance in CTX891671.

Application Display Names and Descriptions for Universal Apps might not have correct names. Edit and correct these properties when adding the applications to the Delivery Group.

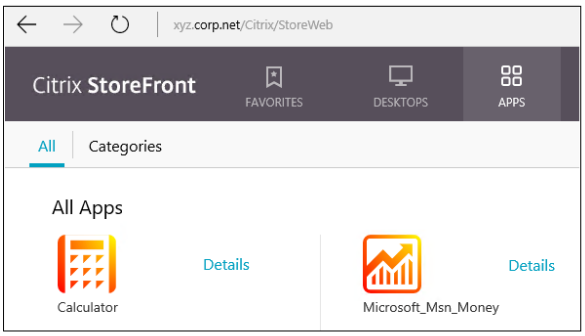
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Check the Known issues article for any additional issues.

Currently, several Universal 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, the Server Manager might also launch when a Univeral App is launched. To prevent this from occurring, you can disable Server Manager from auto-starting during logon with the HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon registry key. For details, see https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

### Install and publish Universal Apps

Support for Universal Apps is enabled by default.

To disable the use of Universal Apps on a VDA, add the registry setting **EnableUWASeamlessSupport** in HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle and set to **0**.

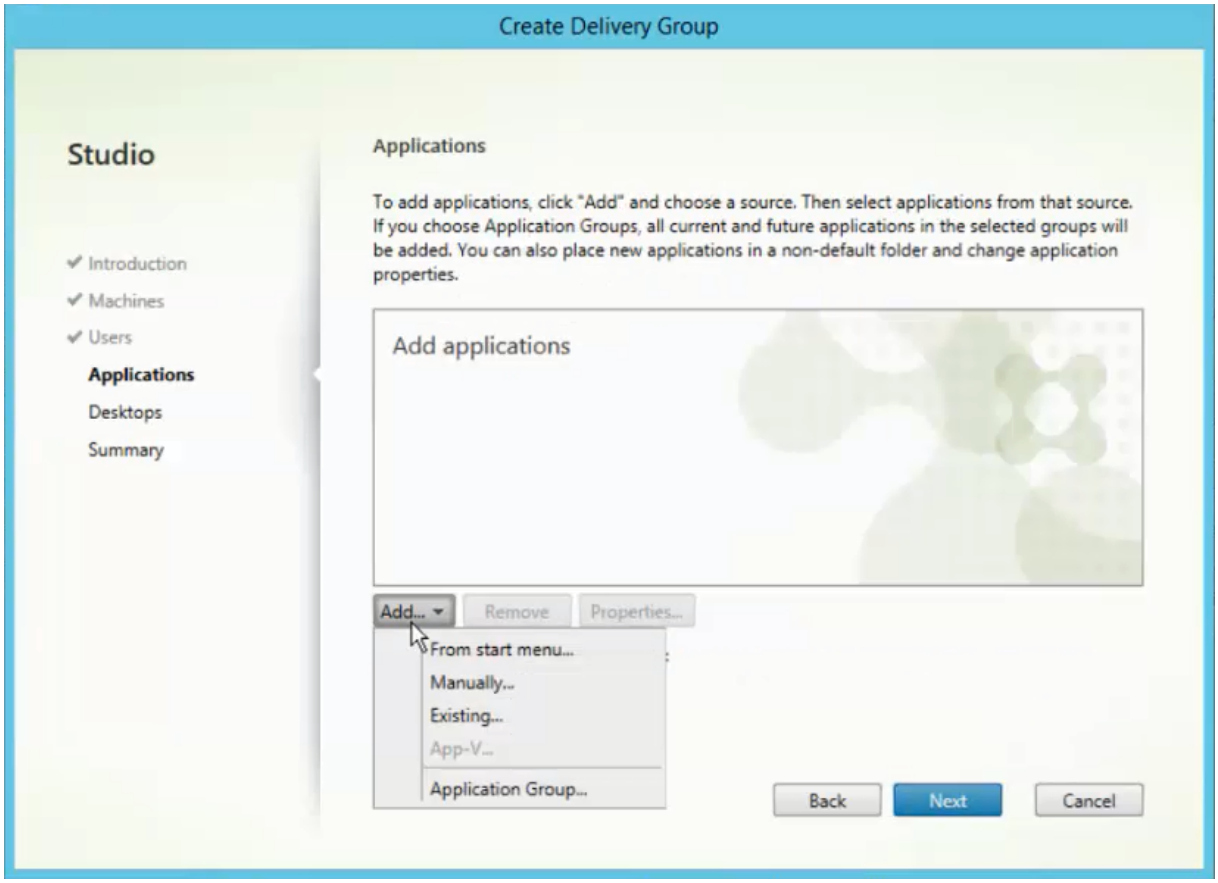
To install one or more Universal Apps on VDAs (or a master image), use one of the following methods:

- 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 https://docs.microsoft.com/en-us/microsoft-store/distribute-offline-apps?redirectedfrom=MSDN.
- Sideload the apps. For more information, see https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10?redirectedfrom=MSDN.

To add (publish) one or more Universal Apps in XenApp or XenDesktop:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

After the Universal Apps are installed on the machine, add the Universal Apps to a Delivery Group or Application Group. You can do this when you create a group, or later. On the Applications page of the wizard, select the **From Start menu** source.




When the applications list appears, select the check boxes of the Universal Apps you want to publish. Then click **Next**.

### Uninstall Universal Apps

When you uninstall a Universal 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

June 15, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp 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 XenApp or XenDesktop Site to no more than 50.

> **Note:**
>
> 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 NetScaler Gateway. The Site database should always be in the primary zone.

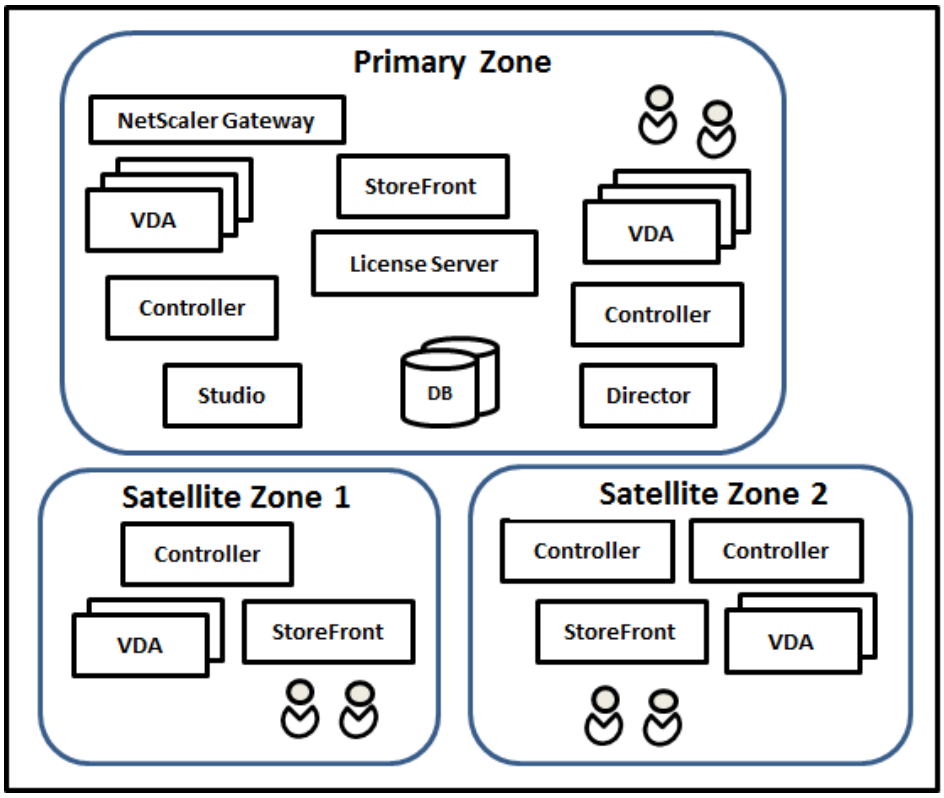
The primary zone should also have at least two Controllers for redundancy, and may have one or more VDAs with applications that are tightly-coupled with the database and infrastructure.

### Satellite zone

A satellite zone contains one or more VDAs, Controllers, StoreFront servers, and NetScaler 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.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- The 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 NetScaler 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 connection leasing 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 a zone which

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

is poorly connected with the current zone (for example, via a high-latency or low-bandwidth network), make sure you also move any associated host connection to the same zone.)
- Controllers in the primary zone keep connection leasing data for all zones. Controllers in satellite zones keep connection leasing data for their own zone and the primary zone, but not data for any other satellite zones.

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

> **Important:**
>
> To use the zone preference feature, you must be using minimum StoreFront 3.7 and NetScaler 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.

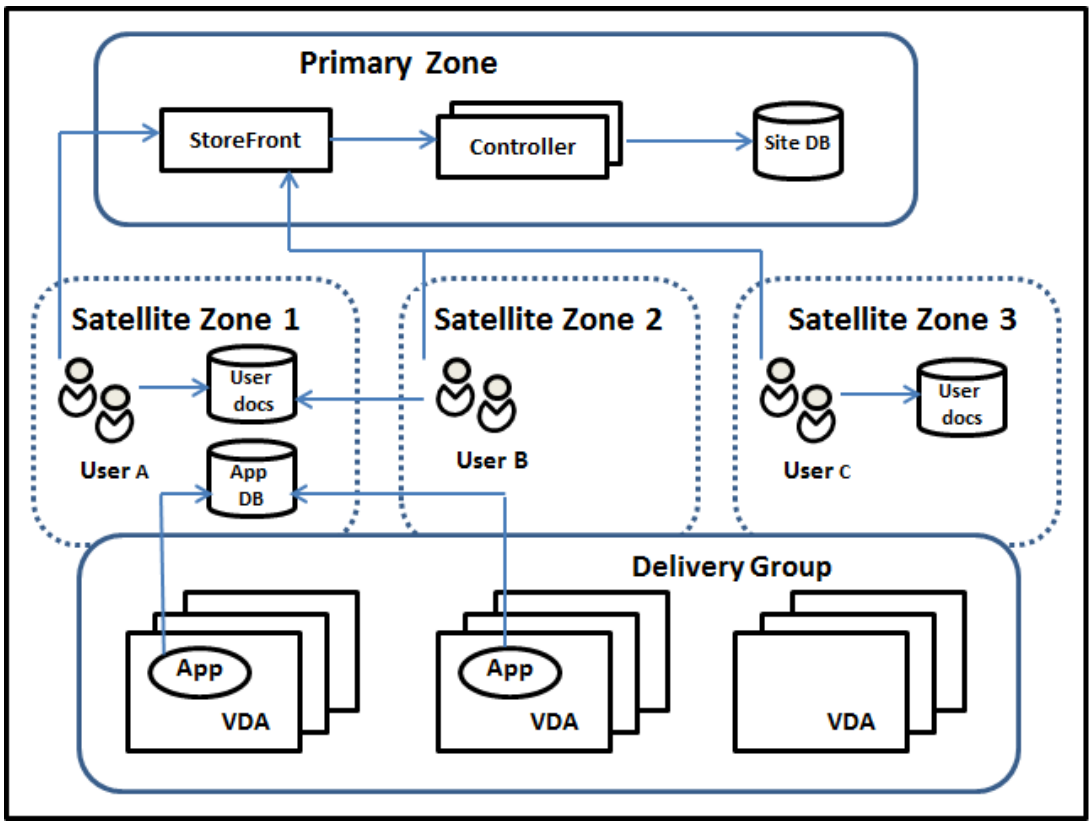
### How zone preference works

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 Receiver is running). This is referred to as the user location.

The following graphic shows an example multi-zone configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 Receiver endpoints: User A is using a device with Citrix Receiver 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:

- 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, as described in the next section.) When a user launches an application:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 Receiver 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 Receiver 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receiver on the endpoint device by the Citrix NetScaler Gateway through which that device is connecting. The NetScaler 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, so that the connection between them is low-latency and high-bandwidth.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.
  - NetScaler 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 XenApp or XenDesktop Site configuration. When a NetScaler 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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, NetScaler 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 NetScaler 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 Provisioning Services:** The Provisioning Services 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Then, use the Provisioning Services console to provision machines in that catalog. (If you create the catalog using the Provisioning Services 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If the Site contains no satellite zones, the primary zone is assumed and the zone selection box does not appear.

## Connections and resources

February 23, 2021

### 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 the Delegated Administration article.

### Where to find information about connection types

You can use the supported virtualization platforms to host and manage machines in your XenApp or XenDesktop 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 Hyper-V

- Microsoft System Center Virtual Machine Manager virtualization environments article.
- Microsoft documentation.

Microsoft Azure

- Microsoft Azure virtualization environments article.
- Microsoft documentation.

Microsoft Azure Resource Manager

- Microsoft Azure Resource Manager virtualization environments article.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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. You must also provide the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials.
- The credentials file for the root AWS account (retrieved from the AWS console) is not formatted the same as credentials files downloaded for standard AWS users. Therefore, Studio cannot use the file to populate the API key and secret key fields. Ensure that you are using AWS IAM credentials files.
- Dedicated hosts and the `tenancytype` PowerShell parameter used to specify a dedicated host for AWS connections are not supported in this version of XenApp and XenDesktop. Support for dedicated hosts was added at release 1811. See How to create machines in MCS using AWS Cloud for more information.

CloudPlatform

- 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.

Citrix XenServer

- Citrix XenServer documentation.
- When you create a connection, you must provide the credentials for a VM Power Admin or higher-level user.
- Citrix recommends using HTTPS to secure communications with XenServer. To use HTTPS, you must replace the default SSL certificate installed on XenServer; see CTX128656.
- You can configure high availability if it is enabled on the XenServer. Citrix recommends that you select all servers in the pool (from Edit High Availability) to allow communication with XenServer if the pool master fails.
- You can select a GPU type and group, or pass through, if the XenServer supports vGPU. The display indicates if the selection has dedicated GPU resources.

Nutanix Acropolis

- Nutanix virtualization environments article.
- Nutanix documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

VMware

- VMware virtualization environments article.
- VMware product documentation.

### Host storage

When provisioning machines, data is classified by type:

- Operating system (OS) data, which includes master images.
- Temporary data, which include 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 can 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 plug-ins.

Storing temporary data locally avoids having to traverse the network to access shared storage. This 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.

> **Note:**
>
> When using local storage on one or more XenServer hosts for temporary data storage, make sure that each storage location in the pool has a unique name. (To change a name in XenCenter, right-click the storage and edit the name property.)

#### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 that 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. See the Create Machine Catalogs article for details.

The hypervisor can also provide optimization technologies through read caching of the disk images locally; for example, XenServer offers IntelliCache. This can also reduce network traffic to the central storage.

#### Storage local to the hypervisor

The storage local to the hypervisor method stores data locally on the hypervisor. With this method, 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.

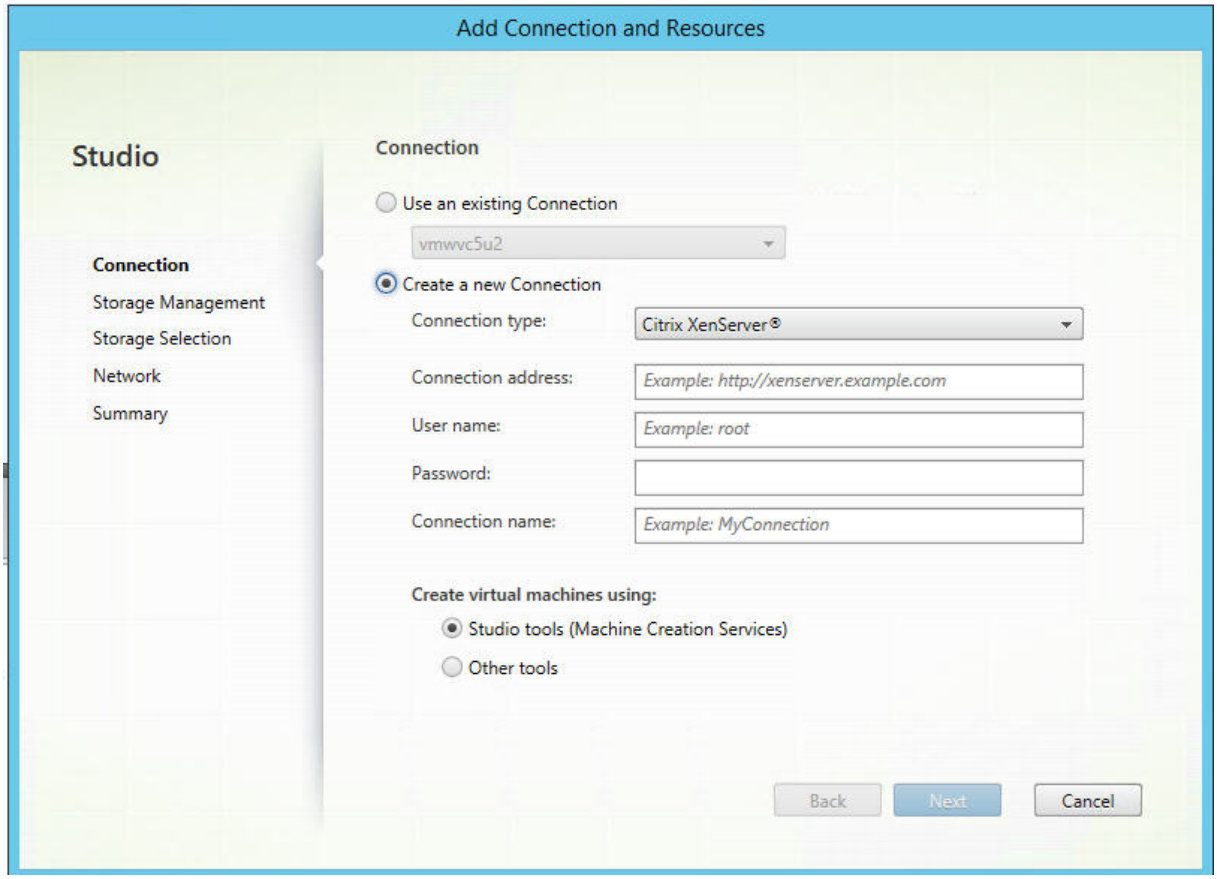
If you are creating a connection after you create the Site, start with step 1 below.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Important:**
>
> The host resources (storage and network) must be available before you create a connection.

- Select **Configuration > Hosting** in the Studio navigation pane.
- Select **Add Connections and Resources** in the Actions pane.
- 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



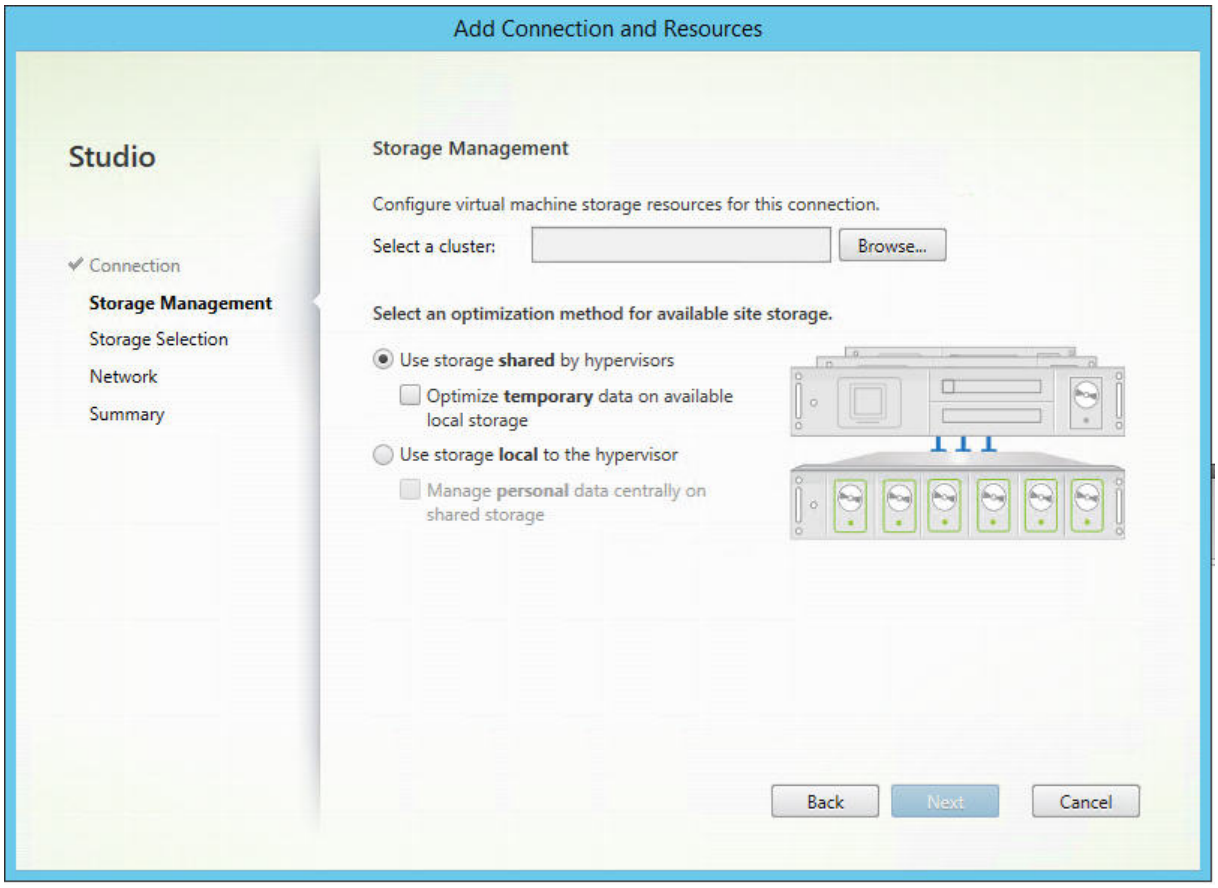

On the **Connection** page:

- To create a new connection select **Create a new Connection**. To create a connection based on the same host configuration as an existing connection, select **Use an existing Connection** and then choose the relevant connection
- Select 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 will appear in Studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Choose the tool you will use to create virtual machines: Studio tools (such as Machine Creation Services or Provisioning Services) 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.

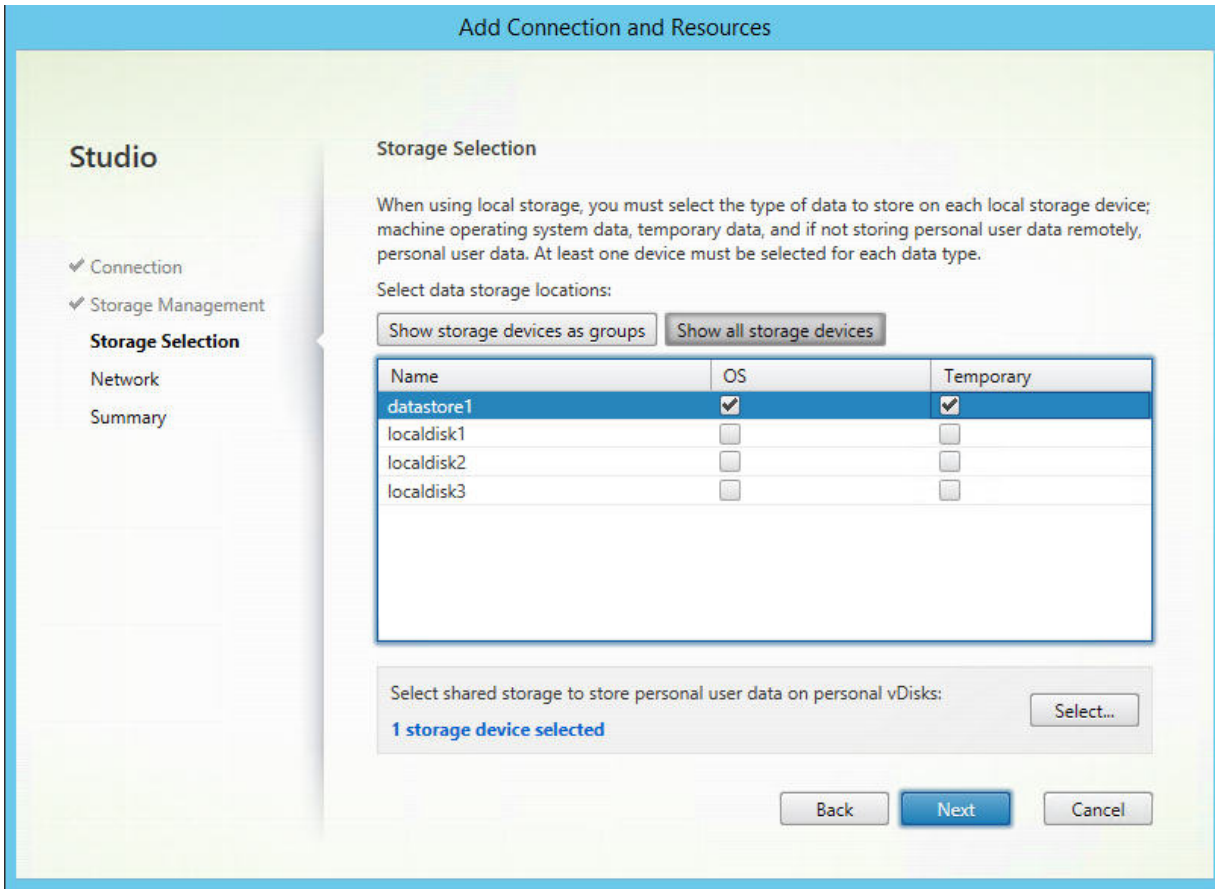
Select a storage management method: storage shared by hypervisors or storage local to the hypervisor.

- 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 will fail.
- If you choose storage local to the hypervisor, indicate if you want to manage personal data (personal vDisks) on shared storage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If you use shared storage on a XenServer hypervisor, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Use IntelliCache for XenServer 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 additional 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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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

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 will use.

#### Summary

Review your selections; if you want to make changes, use return to previous wizard pages. When you complete your review, 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 the Create Machine Catalogs article.

### Edit connection settings

Do not use this procedure to rename a connection or to create a new 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 will break 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 new 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- To change the connection address and credentials, select **Edit settings** and then enter the new information.
- To specify the high-availability servers for a XenServer connection, select **Edit HA servers**. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails.

**Advanced** page:

For a Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN connection type, which isused 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 generally 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.

**Note:** Enter information in the **Connection options** field only under the guidance of a Citrix Support representative.

### 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. Additionally, you can turn maintenance mode on or off for machines in Machine Catalogs or Delivery Groups.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Delete a connection

> **Caution:**
>
> Deleting a connection can result in the deletion of large numbers of machines and loss of data. Ensure that user data on affected machines is backed up or no longer required.

Before deleting a connection, ensure that:

- All users are logged off from the machines stored on the connection.
- No disconnected user sessions are running.
- Maintenance mode is turned on for pooled and dedicated machines.
- All machines in Machine Catalogs used by the connection are powered off.

A Machine Catalog becomes unusable when you delete a connection that 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 new search. You can either search by typing all or part of the machine name, or you can build an expression to use for an advanced search. To build an expression, click **Unfold**, and then select from the lists of properties and operators.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 may not be available, depending on the machine state and the connection host type.

- **Start:** Starts the machine if it is powered off or suspended.
- **Suspend:** Pauses the machine without shutting it down, and refreshes the list of machines.
- **Shut down:** Requests the operating system to shut down.
- **Force shut down:** Forcibly powers off the machine, and refreshes the list of machines.
- **Restart:** Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the desktop remains in its current state.
- **Enable maintenance mode:** Temporarily stops connections to a machine. Users cannot connect to a machine in this state. If users are connected, maintenance mode takes effect when they log off. (You can also turn maintenance mode on or off for all machines accessed through a connection, as described 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 will be 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 new machines.
- **Superseded**: The storage is being used only for existing machines. No new machines will be 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 new 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**.

### Use IntelliCache for XenServer connections

Using IntelliCache, hosted VDI deployments are more cost-effective because you can use a combination of shared storage and local storage. This enhances performance and reduces network traffic . The local storage caches the master image from the shared storage, which reduces the amount of reads on the shared storage. For shared desktops, writes to the differencing disks are written to local storage on the host and not to shared storage.

- 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 XenServer.

- When installing XenServer, select **Enable thin provisioning (Optimized storage for XenDesktop)**. Citrix does not support mixed pools of servers that have IntelliCache enabled and servers that do not. For more information, see the XenServer documentation.
- In XenApp and XenDesktop, IntelliCache is disabled by default. You can change the setting only when creating a XenServer connection; you cannot disable IntelliCache later. When you add a XenServer connection from Studio:
  - Select **Shared** as the storage type.
  - Select the **Use IntelliCache** check box.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 will be 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.

## Local Host Cache

February 11, 2021

To ensure that the XenApp and XenDesktop Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment, by following high availability best practices from Microsoft. (The Databases section in the System requirements article lists the SQL Server high availability features supported in XenApp and XenDesktop.) 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 XenApp or XenDesktop Site to continue when an outage occurs. An outage occurs when the connection between a Delivery Controller and the Site database fails. Local Host Cache engages when the site database is inaccessible for 90 seconds.

Local Host Cache is the most comprehensive high availability feature in XenApp and XenDesktop. It is a more powerful alternative to the connection leasing feature that was introduced in XenApp 7.6.

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; read on to learn how it works.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Note:**
>
> Although connection leasing is supported in version 7.15 LTSR, it will be removed in the following release.

### 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.

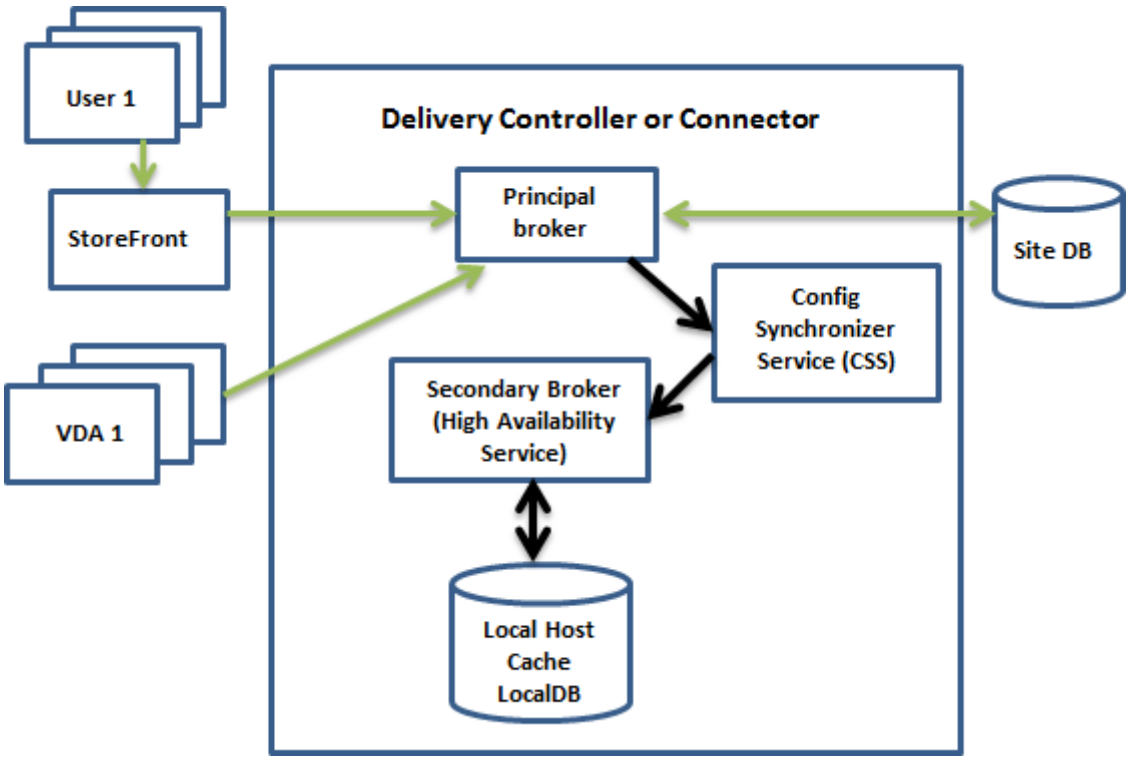
It also contains information for currently active connections that were established while the main database was unavailable:

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

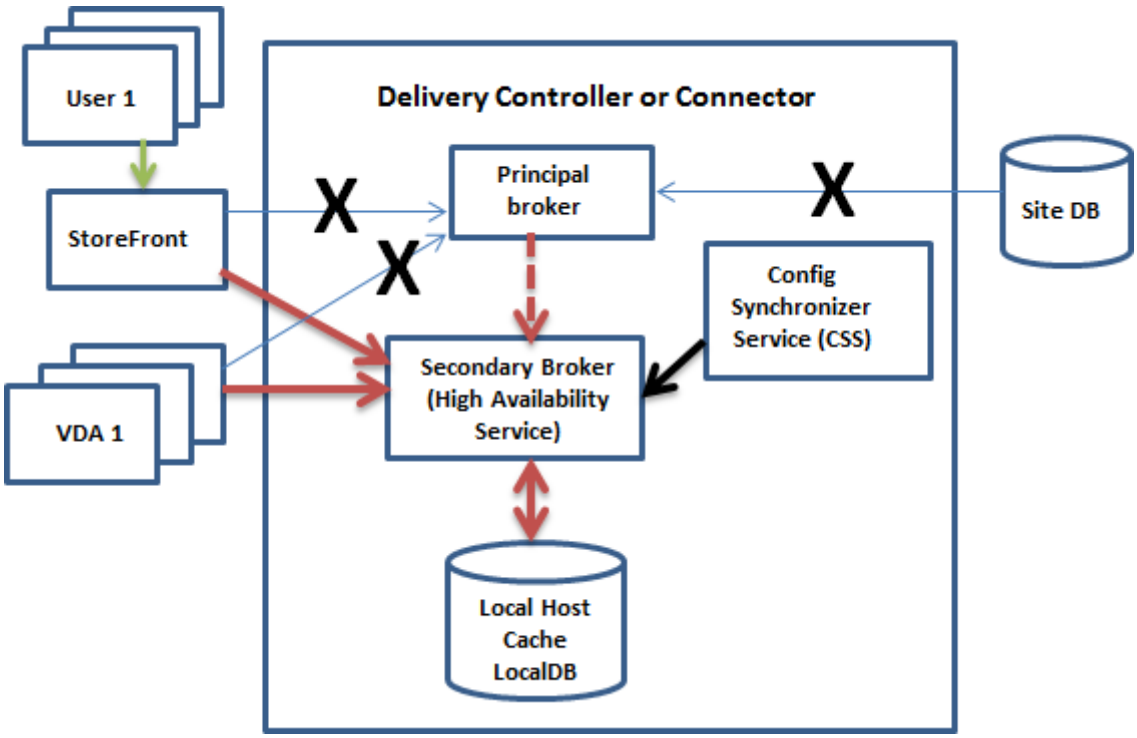



**During normal operations**:

- 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 every two minutes 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 principal broker uses the Citrix Config Synchronizer Service (CSS) to synchronize (copy) information to a *secondary broker* (Citrix High Availability Service) on the Controller. All broker configuration data is copied, not just items that have changed since the previous check. The secondary broker imports the data into a Microsoft SQL Server Express LocalDB database on the Controller. The CSS ensures that the information in the secondary broker's 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):

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**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 secondary broker (High Availability Service) to start listening for and processing connection requests (marked with a red dashed line in the graphic).
- When the outage begins, the secondary broker 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 secondary broker also gets current session information about that VDA.
- While the secondary broker 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 secondary broker 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 secondary broker removes any remaining VDA registrations from the previous outage, and resumes updating the LocalDB database with configuration changes received from the CSS.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Sites with multiple Controllers

Among its other tasks, the CSS routinely provides the secondary broker 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 secondary broker knows about all peer secondary brokers.

The secondary brokers 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 secondary broker will be in charge of brokering operations in the zone if an outage occurs. During the outage, all VDAs re-register with the elected secondary broker. The non-elected secondary brokers in the zone will actively reject incoming connection and VDA registration requests.

If an elected secondary broker fails during an outage, another secondary broker is elected to take over, and VDAs will re-register with the newly-elected secondary broker.

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

Local Host Cache is supported for server-hosted applications and desktops, and static (assigned) desktops; it is not supported for pooled VDI desktops (created by MCS or PVS).

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 or changes during an outage:**

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 (secondary) broker. Launches across zones (from a broker in one zone to a VDA in a different zone) are not supported during an outage.

By default, power-managed desktop VDAs in pooled Delivery Groups that have the `ShutdownDesktopsAfterU` property enabled are placed into maintenance mode when an outage occurs. You can change this default, to allow those desktops to be used during an outage. 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.

For the site, run the following PowerShell cmdlet:

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

For each affected Delivery Group, run the following PowerShell cmdlet:

```
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.

**RAM size:**

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:**

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 so 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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:**

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, the broker must have sufficient space 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:**

During an outage, one broker handles all the connections, so in Sites (or zones) that load balance among multiple Controllers during normal operations, the elected broker might need to handle many more requests than normal during an outage. Therefore, CPU demands will be higher. Every broker in the Site (zone) must be able to handle the additional load imposed by LocalDB and all of the affected VDAs, because the broker 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 broker, that broker 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"broker 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 with a different broker:

- An outage starts: When migrating from a principal broker to a secondary broker.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Broker failure during an outage: When migrating from a secondary broker that failed to a newly-elected secondary broker.
- 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
```

The interval cannot be eliminated entirely, no matter how quickly the VDAs register.

The time it takes to synchronize between brokers increases with the number of objects (such as VDAs, applications, groups). For example, synchronizing 5000 VDAs might take ten minutes or more to complete. See the "Monitor"section below for information about synchronization entries in the event log.

### 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 secondary broker 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 secondary broker.

Installation of this LocalDB database has no effect on whether or not you install SQL Server Express for use as the site database.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Default settings after XenApp or XenDesktop installation and upgrade

During a new installation of XenApp and XenDesktop, Local Host Cache is enabled by default. (Connection leasing is disabled by default.)

After an upgrade, the Local Host Cache setting is unchanged. For example, if Local Host Cache was enabled in the earlier version, it remains enabled in the upgraded version. If Local Host Cache was disabled (or not supported) in the earlier version, it remains disabled in the upgraded version.

### Enable and disable Local Host Cache

To enable Local Host Cache, enter:

```
Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled
 $false
```

This cmdlet also disables the connection leasing feature. Do not enable both Local Host Cache and connection leasing.

To determine whether Local Host Cache is enabled, enter:

```
Get-BrokerSite
```

Check that the LocalHostCacheEnabled property is True, and that the ConnectionLeasingEnabled property is False.

To disable Local Host Cache (and enable connection leasing), enter:

```
Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled
 $true
```

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 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.)
- In a Citrix Cloud scenario, the connector enters outage mode, regardless of the state of the connection to the control plane or primary zone.

### 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 (secondary broker).

- 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.
- 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 secondary broker (High Availability Service) is performing brokering operations.
- 3503: An outage has been resolved and normal operations have resumed.
- 3504: Indicates which secondary broker is elected, plus other brokers involved in the election.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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:** If a synchronization import fails, you can generate a report. This report stops at the object causing the error. This report feature affects synchronization speed, so Citrix recommends disabling it when not in use.

To enable and produce a CSS trace report, enter the following command:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

The HTML report is posted at `C:\\Windows\\ServiceProfiles\\NetworkService\\AppData\\Local\\Temp\\CitrixBrokerConfigSyncReport.html`.

After the report is generated, enter the following command to disable the reporting feature:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

**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

April 1, 2022

> **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 the feature in Studio by using the PowerShell SDK.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. Configure settings in Studio. (Use the Studio console or PowerShell).
3. Configure settings in StoreFront. (Use PowerShell).

### Enable the security key feature

By default, the feature is disabled. To enable it, use the Remote PowerShell SDK. For more information about the Remote PowerShell SDK, see SDKs and APIs.

To enable the feature, perform these steps:

1. Run the XenApp and XenDesktop Remote PowerShell SDK.
2. In a command window, run the following commands:
   - `Add-PSSnapIn Citrix*`. This command adds the Citrix snap-ins.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

### Configure settings in Studio

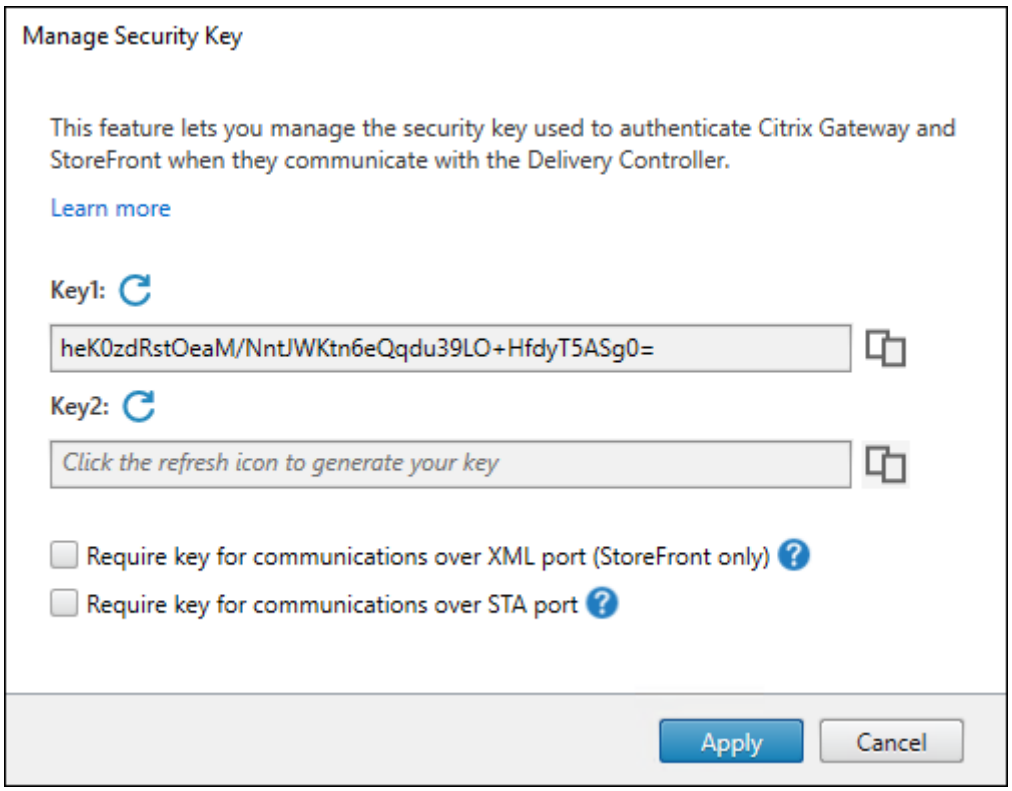
You can configure settings in Studio by using the Studio console or PowerShell.

#### Use the Studio console

After enabling the feature, navigate 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Run the XenApp and XenDeskop 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 the `Get-STFStoreServie` and `Set-STFStoreService` commands. For example:
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`
- To configure the key for communications over the STA port, use the `New-STFSecureTicketAuthority` command. For example:
  - `PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL > -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>`

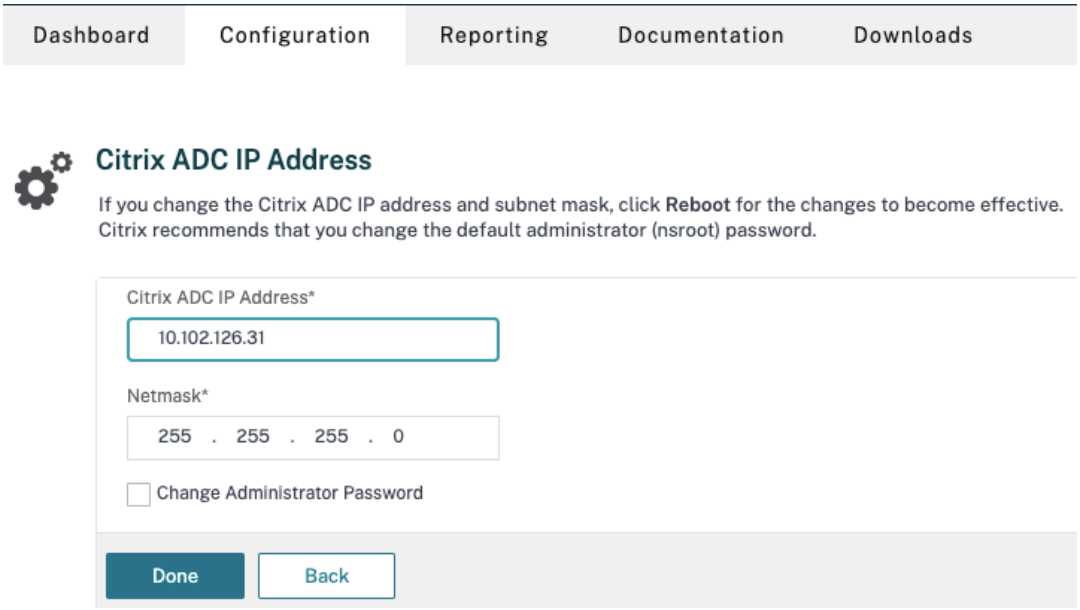
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

See the PowerShell command help for guidance and syntax.

### Configure settings in Citrix ADC

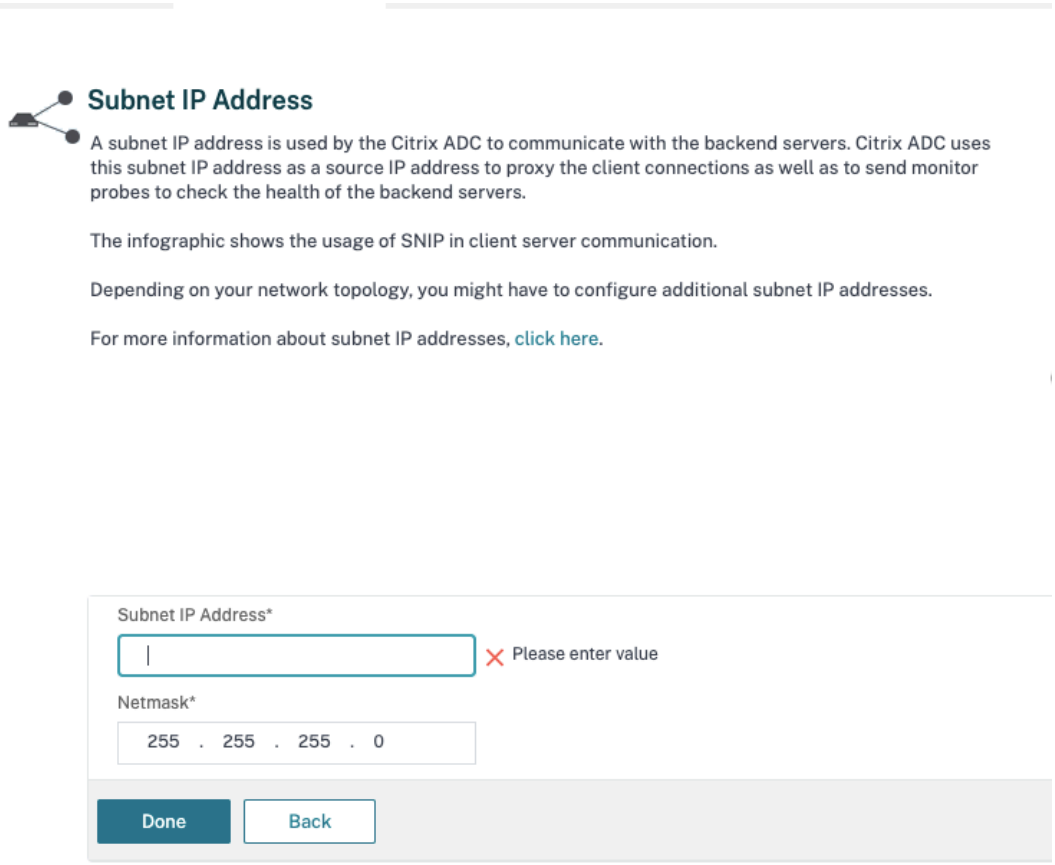
> **Note:**
>
> Configuring this feature in Citrix ADC is not required unless you use Citrix ADC as your gateway. If you use Citrix ADC, follow the steps below.

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.



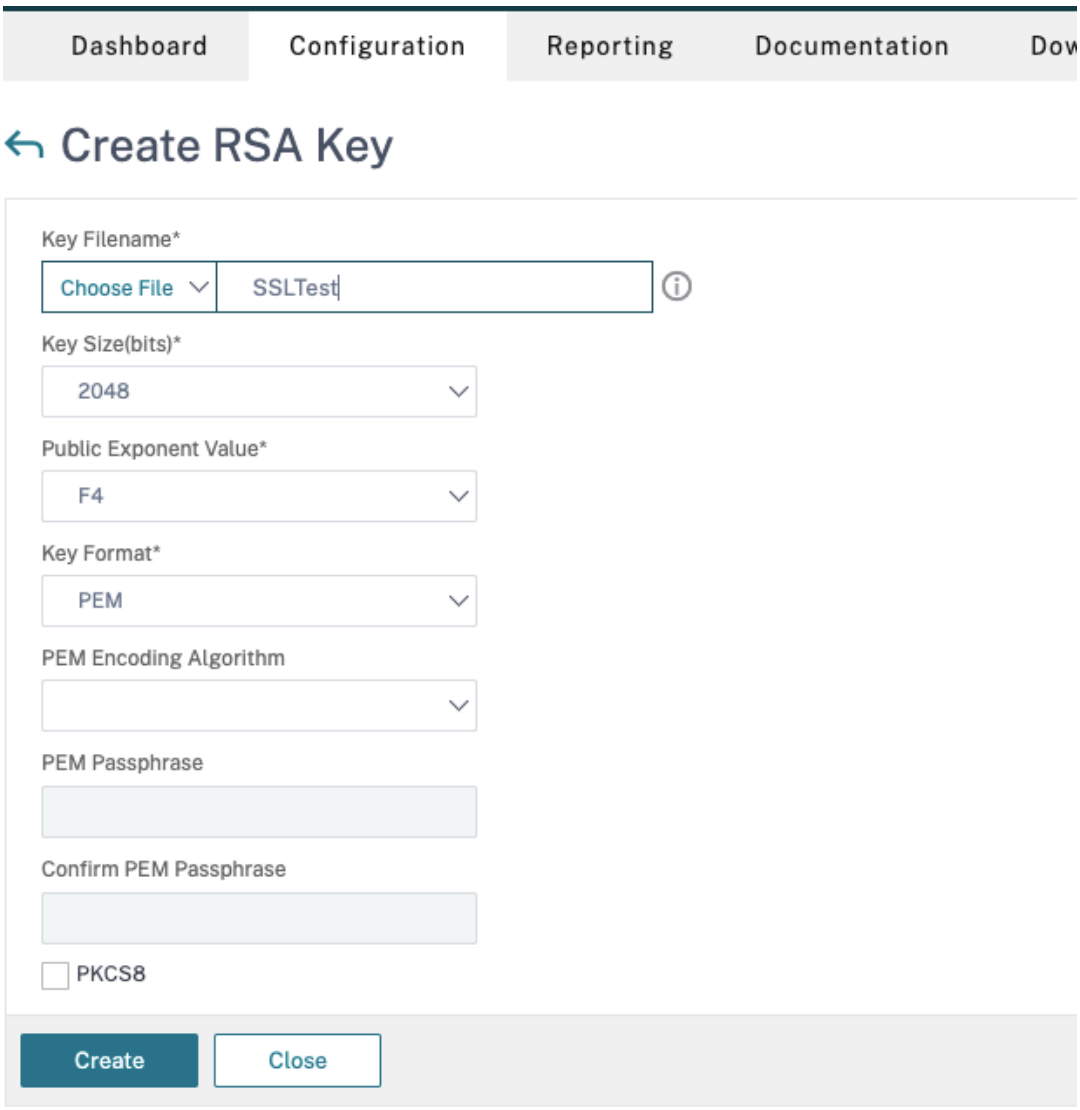

     - Subnet IP (SNIP) address for enabling communication between the Citrix ADC appliance and the back-end servers. For details, see Configuring Subnet IP Addresses.
     - Citrix Gateway virtual IP address and load balancer virtual IP address to log in to the ADC appliance for session launch. For details, see Create a virtual server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



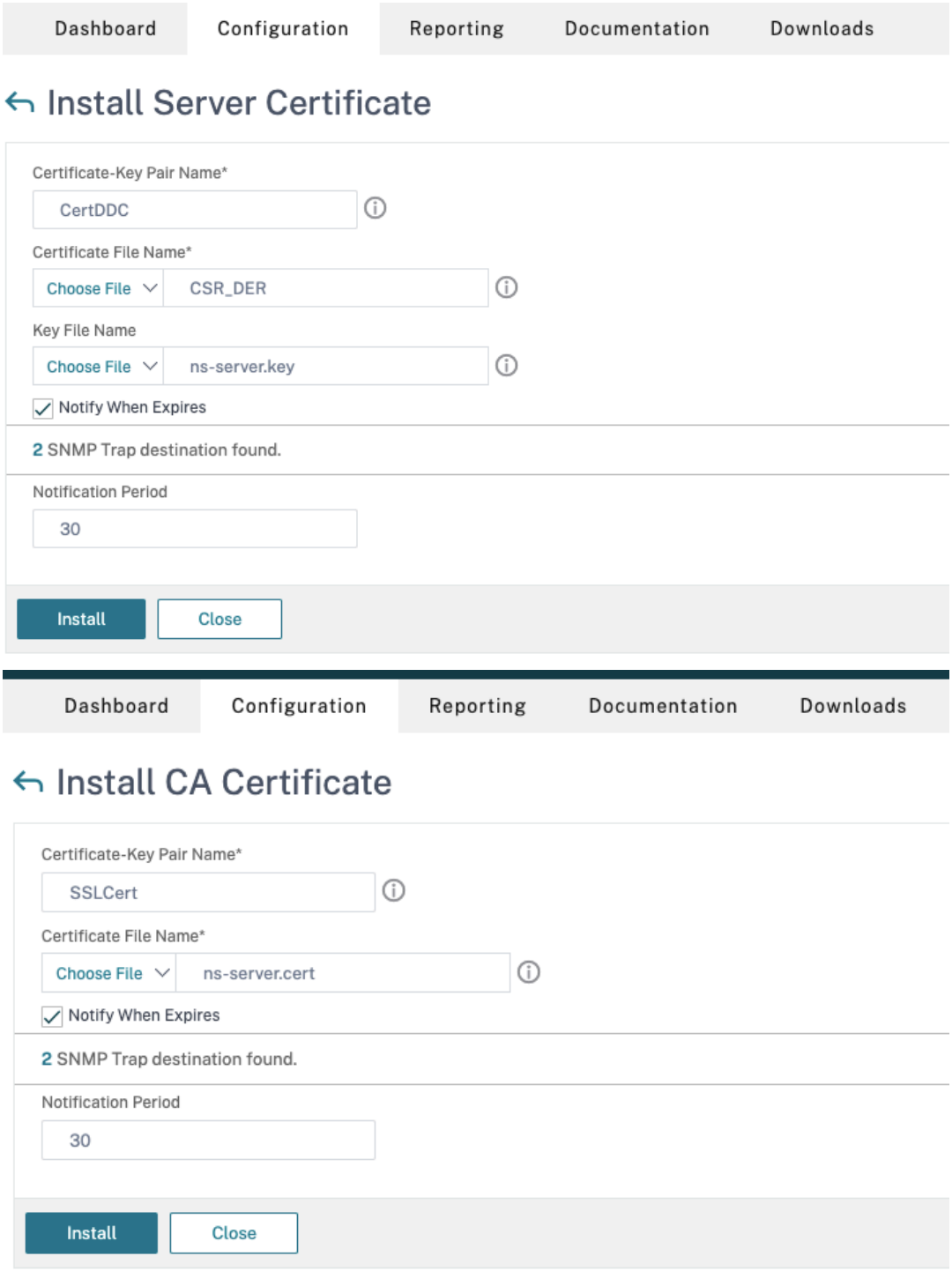

- The required modes and features in the Citrix ADC appliance are enabled.
  - To enable the modes, in the Citrix ADC GUI navigate to **System > Settings > Configure Mode**.
  - To enable the features, in the Citrix ADC GUI navigate to **System > Settings > Configure Basic Features**.
- Certificates related configurations are complete.
  - The Certificate Signing Request (CSR) is created. For details, see Create a certificate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



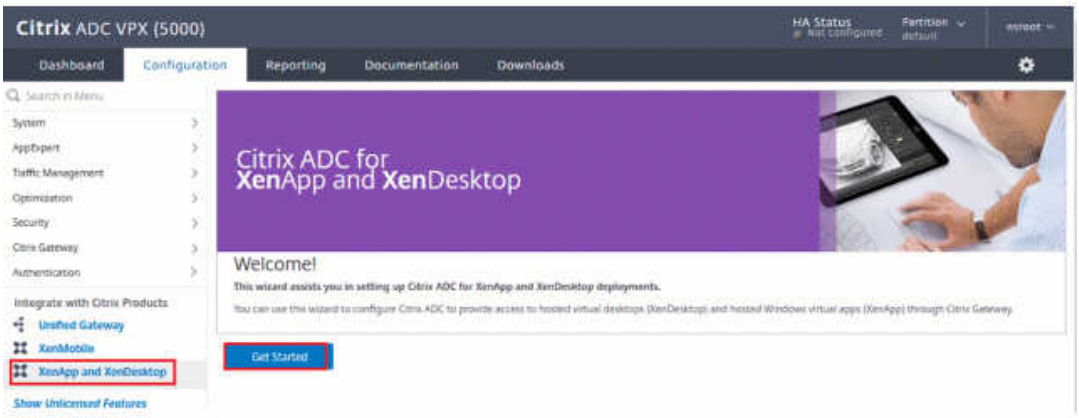

- The server and CA certificates and root certificates are installed. For details, see Install, link, and updates.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



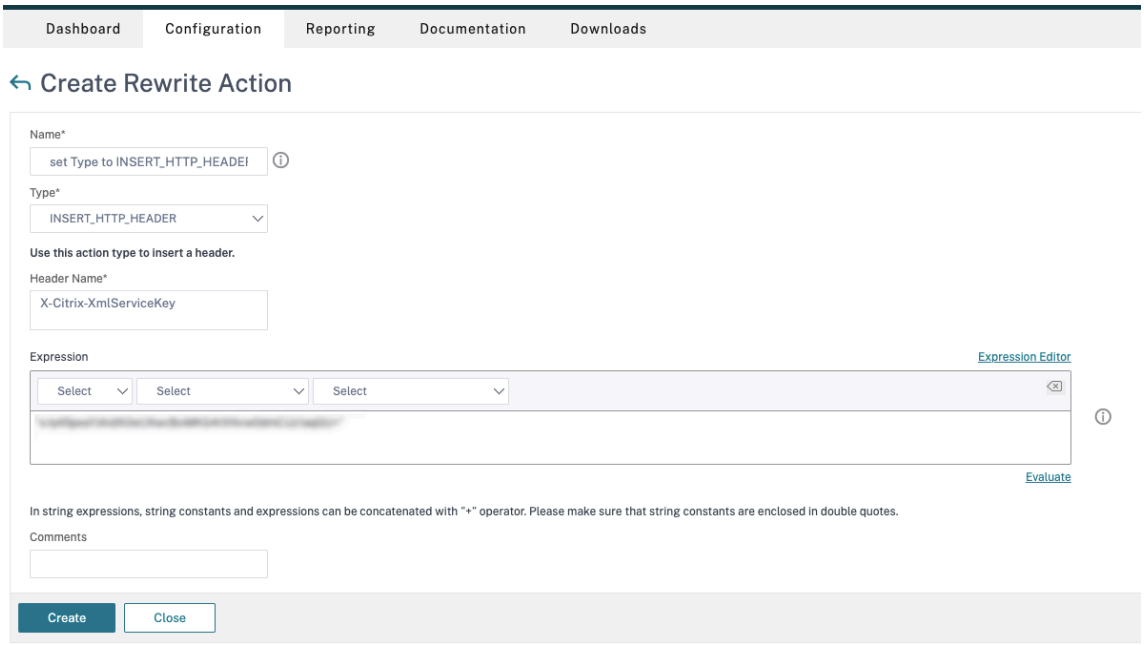

- A Citrix Gateway has been created for Citrix Virtual Desktops. Test the connectivity by clicking the **Test STA Connectivity** button to confirm that the virtual servers are online. For details, see Setting up Citrix ADC for Citrix Virtual Apps and Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



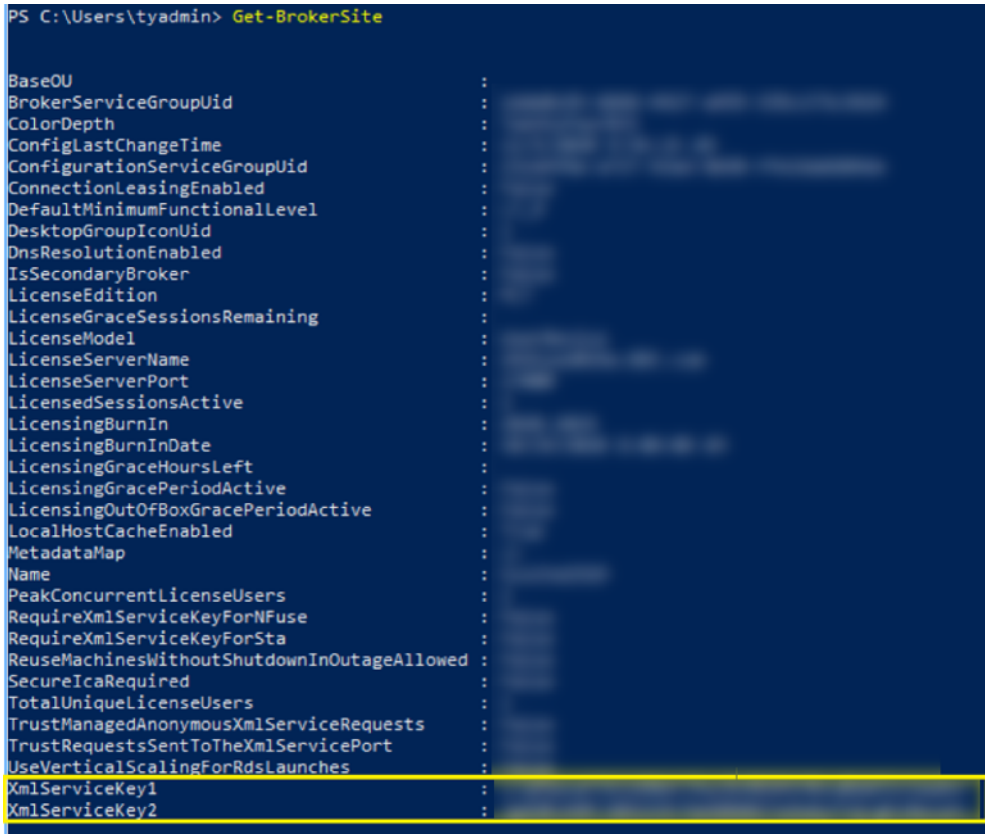

2. Add a rewrite action. For details, see Configuring a Rewrite Action.

   a) Navigate to **AppExpert > Rewrite > Actions**.
   b) Click **Add** to add a new rewrite action. You can name the action as "set Type to INSERT_HTTP_HEADER".




   a) In **Type**, select **INSERT_HTTP_HEADER**.
   b) In **Header Name**, enter X-Citrix-XmlServiceKey.
   c) In **Expression**, add <XmlServiceKey1 value> with the quotes. You can copy the XmlServiceKey1 value from your Desktop Delivery Controller configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

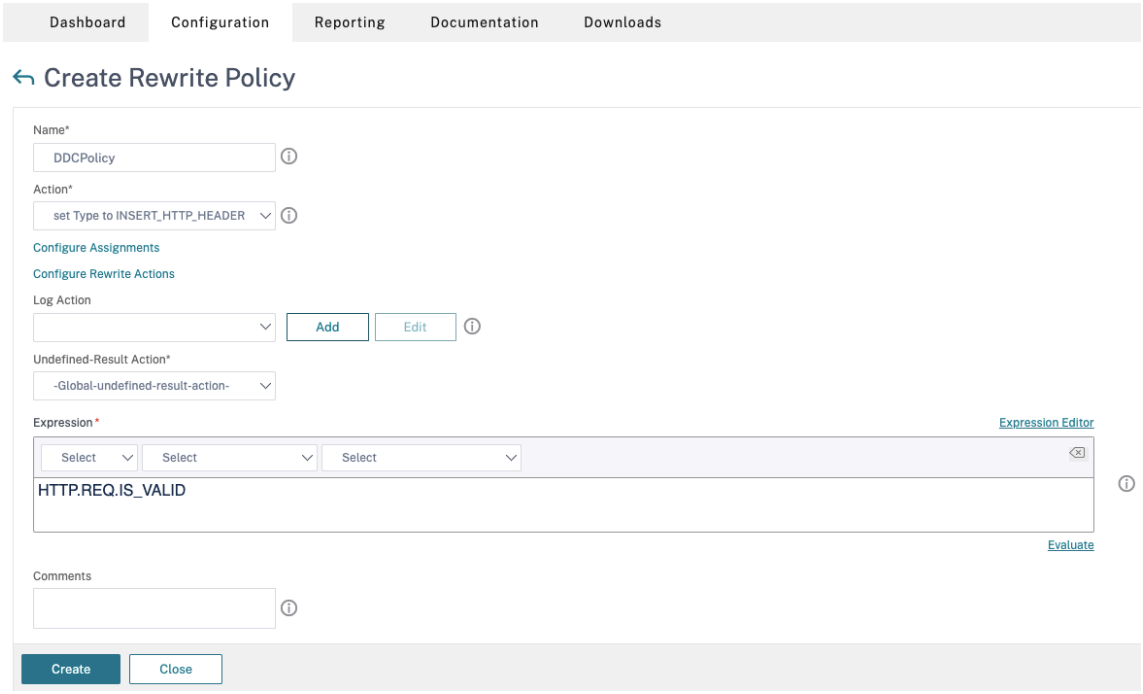



3. Add a rewrite policy. For details, see Configuring a Rewrite Policy.

   a) Navigate to **AppExpert > Rewrite > Policies**.

   b) Click **Add** to add a new policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




a) In **Action**, select the action created in the earlier step.
b) In **Expression**, add HTTP.REQ.IS_VALID.
c) Click **OK**.

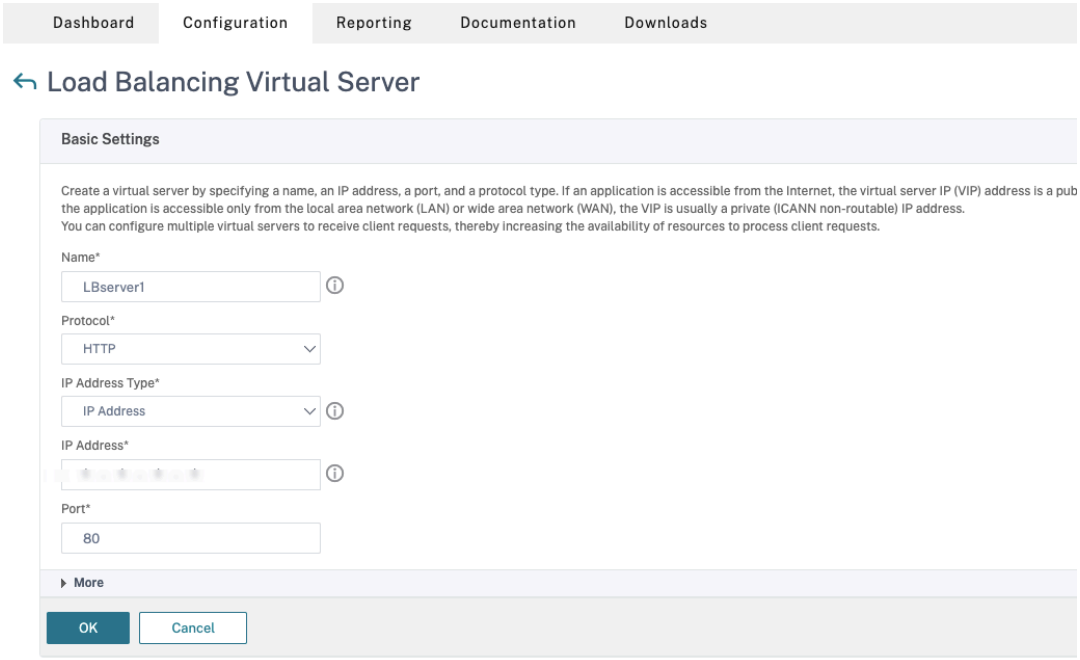
4. Set up load balancing. You must configure one load balancing virtual server per STA server. If not the sessions fail to launch.

   For details, see Set up basic load balancing.

   a) Create a load balancing virtual server.

      - Navigate to **Traffic Management > Load Balancing > Servers**.
      - In **Virtual Servers** page, click **Add**.

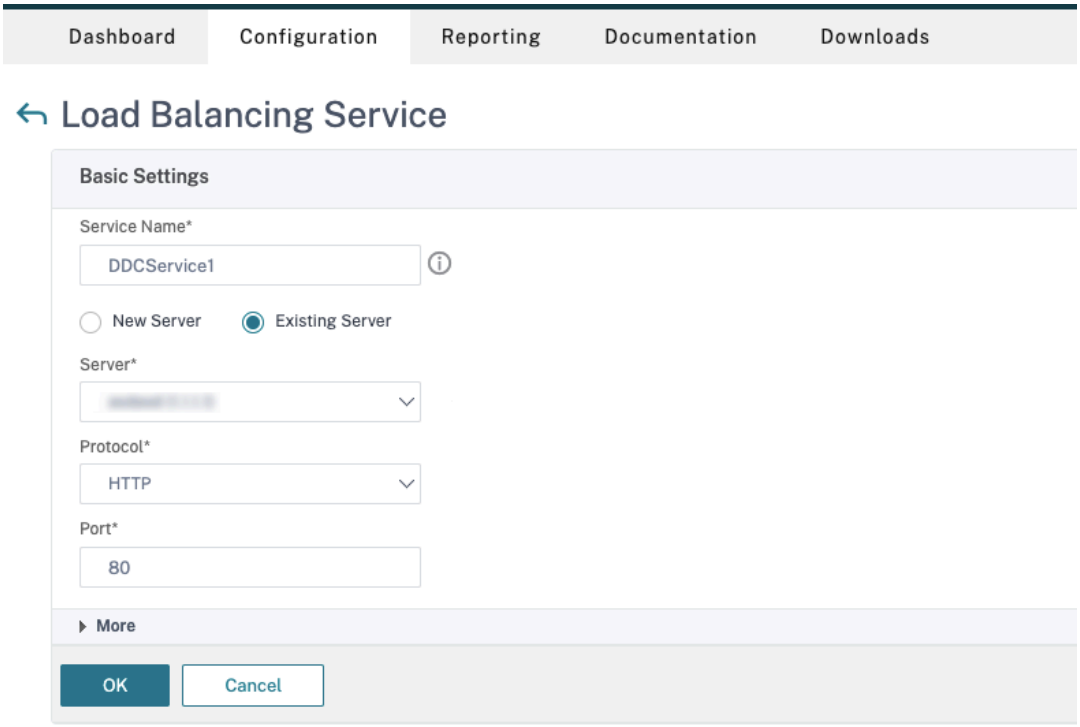
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




- In **Protocol**, select **HTTP**.
- Add the load balancing virtual IP address and in **Port** select **80**.
- Click **OK**.

b) Create a load balancing service.

- Navigate to **Traffic Management > Load Balancing > Services**.

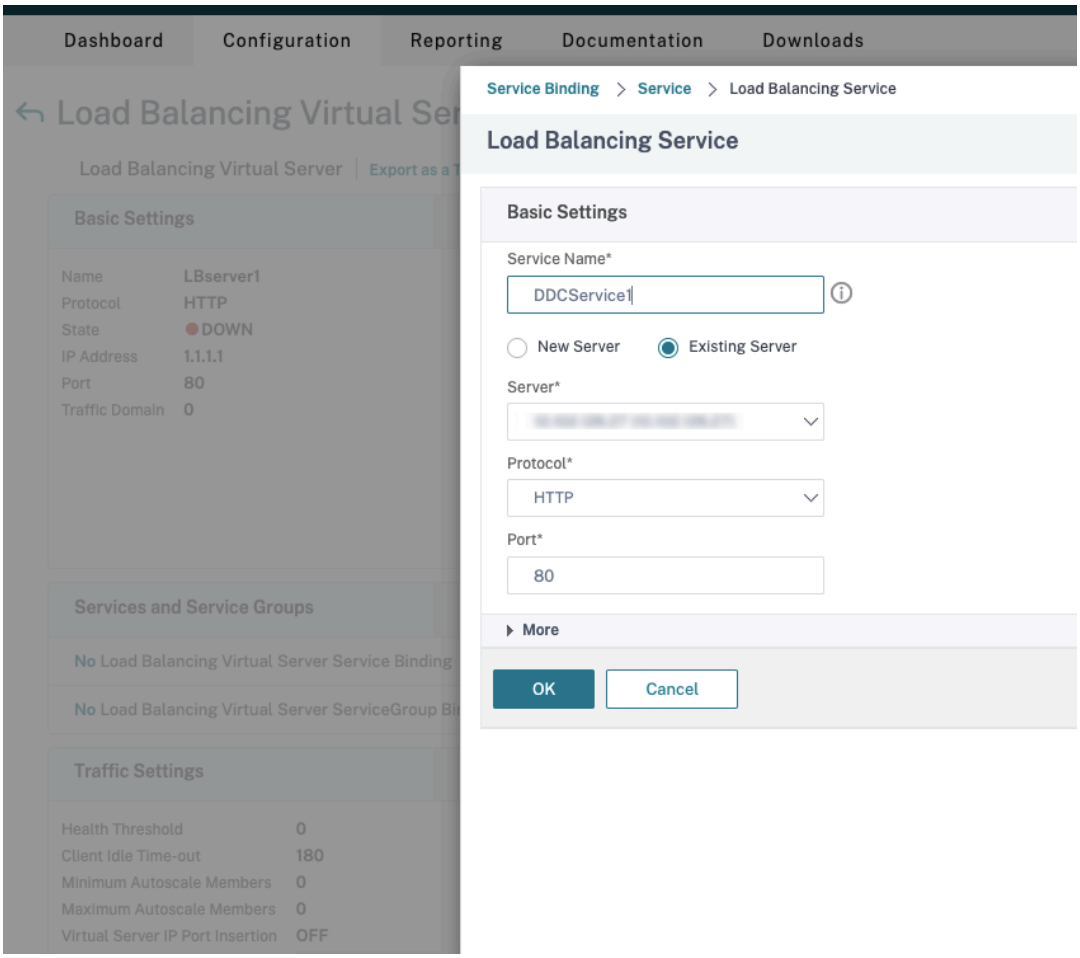



© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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**.

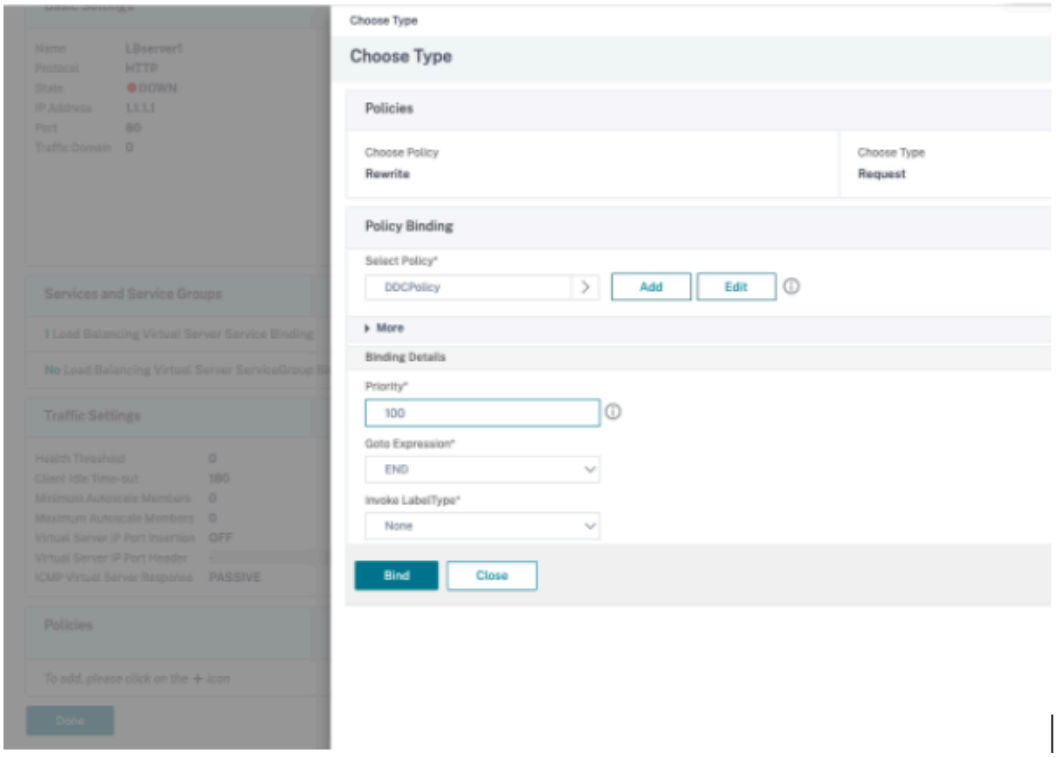



- In **Service Binding**, select the service created earlier.
- Click **Bind**.

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 **+**.

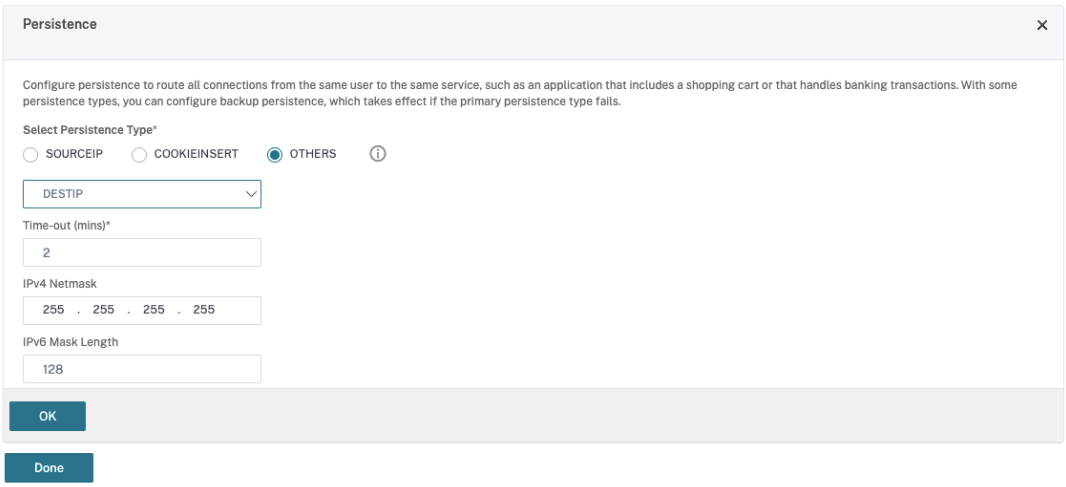
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




- 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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**.

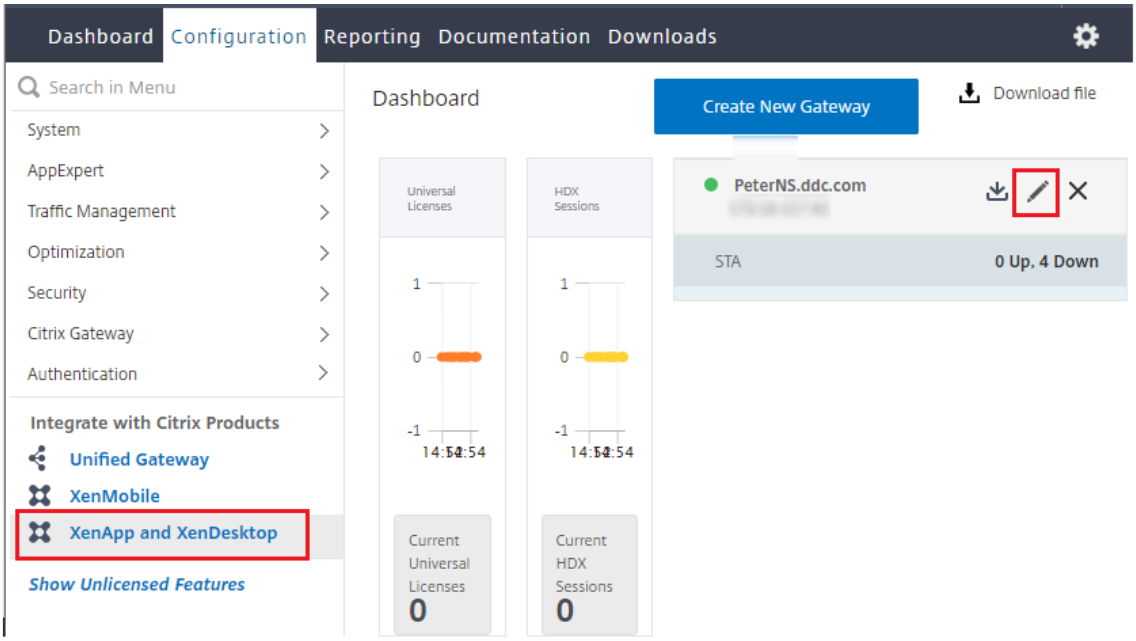
f) Repeat these steps for the other virtual server as well.

### 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.

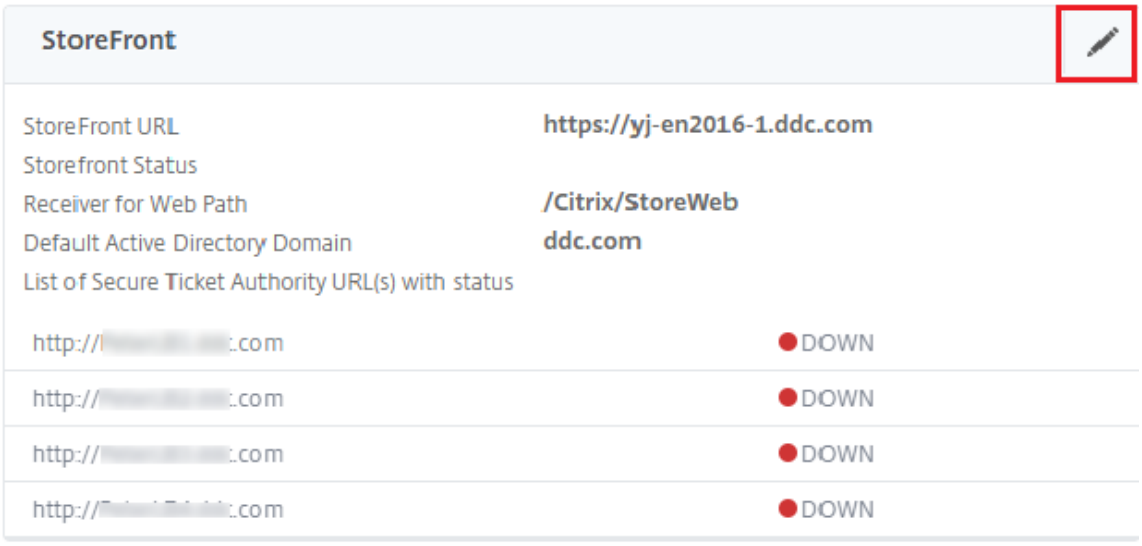
- Before the session launch, change the **Security Ticket Authority URL** of the gateway to use the FQDNs of the load balancing virtual servers.
- Ensure that the `TrustRequestsSentToTheXmlServicePort` parameter is set to False. By default, `TrustRequestsSentToTheXmlServicePort` parameter is set to False. 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, navigate 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.

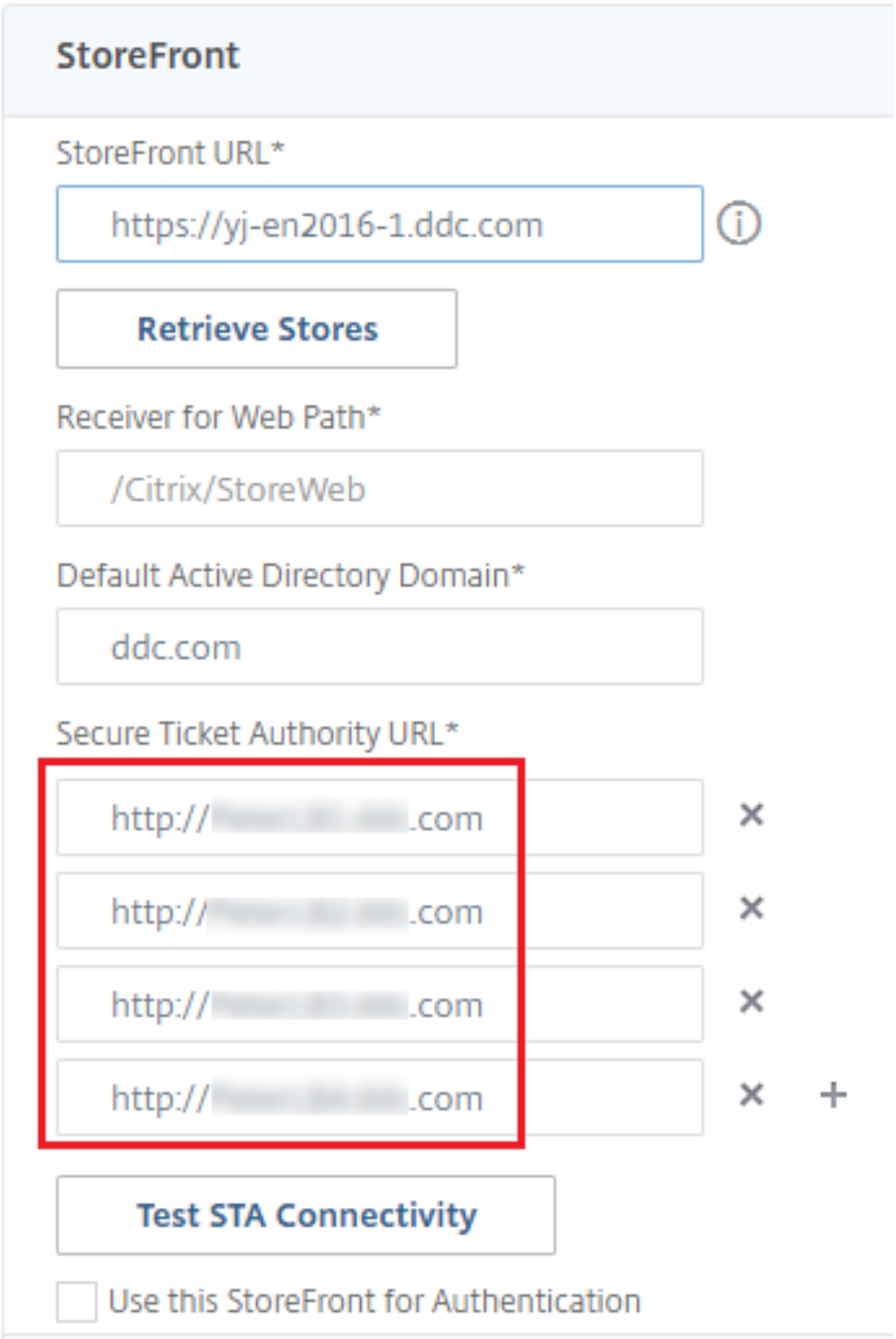
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




## Connection leasing

April 23, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Important:**
>
> Local Host Cache (LHC) is the preferred XenApp and XenDesktop high availability solution, instead of connection leasing. See Local Host Cache for details.

- In this release, during a new installation of XenApp and XenDesktop, connection leasing is disabled by default.
- Connection leasing will no longer be provided, beginning with the Current Release following this XenApp and XenDesktop 7.15 Long Term Service Release.

To ensure that the Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment by following high availability best practices from Microsoft. However, network issues and interruptions may prevent Delivery Controllers from accessing the database, resulting in users not being able to connect to their applications or desktop.

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available.

Although users may have a large number of published resources available, they often use only a few of them regularly. When you enable connection leasing, each Controller caches user connections to those recently used applications and desktops during normal operations (when the database is available).

The leases generated on each Controller are uploaded to the Site database for periodic synchronization to other Controllers on the Site. In addition to leases, each Controller's cache holds application, desktop, icon, and worker information. The lease and related information is stored on each Controller's local disk. If the database becomes unavailable, the Controller enters leased connection mode and "replays"the cached operations when a user attempts to connect or reconnect to a recently used application or desktop from StoreFront.

Connections are cached for a lease period of two weeks. So, if the database becomes unavailable, the desktops and applications that the user launched in the previous two weeks remain accessible to that user through StoreFront. However, desktops and applications that have not been launched during the previous two-week lease period are not accessible when the database is unavailable. For example, if a user last launched an application three weeks ago, its lease has expired, and that user cannot launch that application if the database becomes unavailable now. Leases for long-running active or disconnected application or desktop sessions are extended so that they are not considered expired.

By default, connection leasing affects the entire Site; however, you can revoke all leases for specific users, which prevents them from accessing any applications or desktops when the Controller is in leased connection mode. Several other registry settings apply on a Controller basis.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Considerations and limitations

While connection leasing can improve connection resiliency and user productivity, there are considerations related to the availability, operation, and performance of other features.

Connection leasing is supported for server-hosted applications and desktops, and static (assigned) desktops; it is not supported for pooled VDI desktops or for users who have not been assigned a desktop when the database becomes unavailable.

When the Controller is in leased connection mode:

- Administrators cannot use Studio, Director, or the PowerShell console.
- Workspace Control is not available. When a user logs on to Citrix Receiver, sessions do not automatically reconnect; the user must relaunch the application.
- If a new lease is created immediately before the database becomes unavailable, but the lease information has not yet been synchronized across all Controllers, the user might not be able to launch that resource after the database becomes unavailable.
- Server-hosted application and desktop users may use more sessions than their configured session limits. For example:
  - A session may not roam when a user launches it from one device (connecting externally through NetScaler Gateway) when the Controller is not in leased connection mode and then connects from another device on the LAN when the Controller is in leased connection mode.
  - Session reconnection may fail if an application launches just before the database becomes unavailable; in such cases, a new session and application instance are launched.
- Static (assigned) desktops are not power-managed. VDAs that are powered off when the Controller enters leased connection mode remain unavailable until the database connection is restored, unless the administrator manually powers them on.
- If session prelaunch and session linger are enabled, new prelaunch sessions are not started. Prelaunched and lingering sessions will not be ended according to configured thresholds while the database is unavailable.
- Load management within the Site may be affected. Server-based connections are routed to the most recently used VDA. Load evaluators (and especially, session count rules) may be exceeded.
- The Controller will not enter leased connection mode if you use SQL Server Management Studio to take the database offline. Instead, use one of the following Transact-SQL statements:
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Either statement cancels any pending transactions and causes the Controller to lose its connection with the database. The Controller then enters leased connection mode.

When connection leasing is enabled, there are two brief intervals during which users cannot connect or reconnect: (1) from the time the database becomes unavailable to when the Controller enters leased connection mode, and (2) from the time the Controller changes from leased connection mode to when database access is fully restored and the VDAs have re-registered.

If you configure a nondefault session roaming value, session reconnection reverts to its default value when a Controller enters leased connection node. For details, see Connection leasing and session roaming.

See the Zones article for information about where connection leasing data is kept.

### Configure and deploy

When configuring your deployment to accommodate connection leasing:

- VDAs must be at minimum version 7.6, and the Machine Catalogs and Delivery Groups that use those machines must be at that minimum level (or a later supported version).
- The Site database size requirements will increase.
- Each Controller needs additional disk space for the cached lease files.

You can turn connection leasing off or on from the PowerShell SDK or the Windows registry. From the PowerShell SDK, you can also remove current leases. The following PowerShell cmdlets affect connection leasing; see the cmdlet help for details.

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false - Turns connection leasing on or off. Default = $true
- Get-BrokerServiceAddedCapability - Outputs "ConnectionLeasing"for the local Controller.
- Get-BrokerLease - Retrieves either all or a filtered set of current leases.
- Remove-BrokerLease - Marks either one or a filtered set of leases for deletion.
- Update-BrokerLocalLeaseCache –Updates the connection leasing cache on the local Controller. The data is resynchronized during the next synchronization.

## Virtual IP and virtual loopback

April 4, 2019

Note: These features are valid only for supported Windows server machines. They do not apply to Windows desktop OS machines.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp 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 XenApp 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**How Microsoft Remote Desktop (RD) IP virtualization works**

- Virtual IP addressing must be enabled on the Microsoft server.

  For example, in a Windows Server 2008 R2 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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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:

- Preferred loopback is supported only on Windows Server 2008 R2 and Windows Server 2012 R2.
- Use preferred loopback only if both Virtual IP and virtual loopback are enabled; otherwise, you may have unintended results.
- Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Run regedit on the servers where the applications reside.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\V for 32-bit machines)
- Name: PreferLoopback, Type: REG_DWORD, Data: 1

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <list of processes>

## Delivery Controllers

June 30, 2022

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 should always have 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. Additional 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.

(In the documentation for earlier XenApp and XenDesktop 7.x releases, information about VDA registration was included in this article. That information has been enhanced and now resides in the article linked above.)

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Note:**
>
> 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 executing 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 will 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. **Important:** If you plan to generate scripts that will 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; it removes the Controller from the database so that it can no longer be used to broker connections 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 are offered the option of generating 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 very 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 currently located (the old Site), select **Configuration > Controllers** in the Studio navigation pane and then select the Controller you want to move.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. Select **Remove Controller** in the Actions pane. If you do not have the correct database roles and permissions, you are offered the option of generating 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 Provisioning Services or is an existing image, you can move a VDA to another Site (from Site 1 to Site 2) when upgrading, or when moving 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. **Important:** 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); it 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.

For information about how to use the Group Policy Editor, see the Citrix policies documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# VDA registration

February 10, 2021

## 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 XenApp and XenDesktop deployment, VDAs register with Controllers. In a XenApp and XenDesktop 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 or Cloud Connectors, the VDA might reject session launches that were brokered by an unlisted Controller or Cloud Connector. 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.

XenApp and XenDesktop automatically test the connectivity to configured Controllers or Cloud Connectors during VDA installation. Errors are displayed if a Controller or Cloud Connector cannot be

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

reached. If you ignore a warning that a Controller or Cloud Connector cannot be contacted (or when you do not specify addresses during VDA installation), 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.

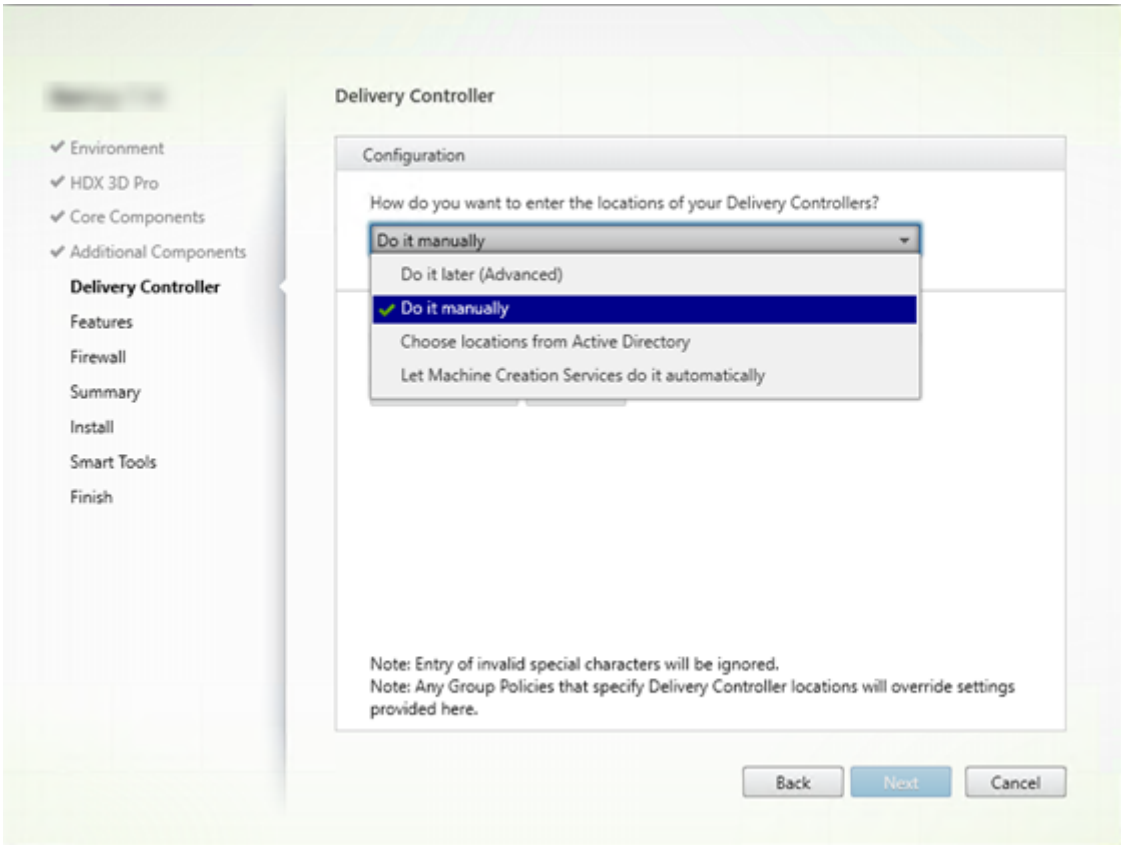
There are several methods for configuring Controller or Cloud Connector addresses on a VDA.

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Policy-based (LGPO\GPO)

Citrix recommends using GPO for initial VDA registration. It has the highest priority. (Although auto-update was listed previously as the highest priority, 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)`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 more 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 plan to use only MCS to provision VMs, you can instruct MCS to set up the list of Controllers or Cloud Connectors. This feature is compatible with auto-update: MCS injects the list of Controllers or Cloud Connectors into the `Personality.ini` file during initial provisioning (when creating the machine catalog). Auto-update keeps the list up-to-date.

This method is not recommended for use in large environments. You can use this method if you:

- Have a small environment
- Will not move VDAs between sites
- Use only MCS to provision VMs
- Don't want to use Group Policy

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.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 PVS to provision machines, except for PVS 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 or Cloud Connector has been added or removed since the last check, or if a policy change occurred that affects VDA registration, the Controller or Cloud Connector sends an updated list to its registered VDAs and the cache is updated. The VDA accepts connections from all the Controllers or Cloud Connectors 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 or Cloud Connector was removed from the site), the VDA re-registers, choosing among the Controllers or Cloud Connectors in the ListOfDDCs.

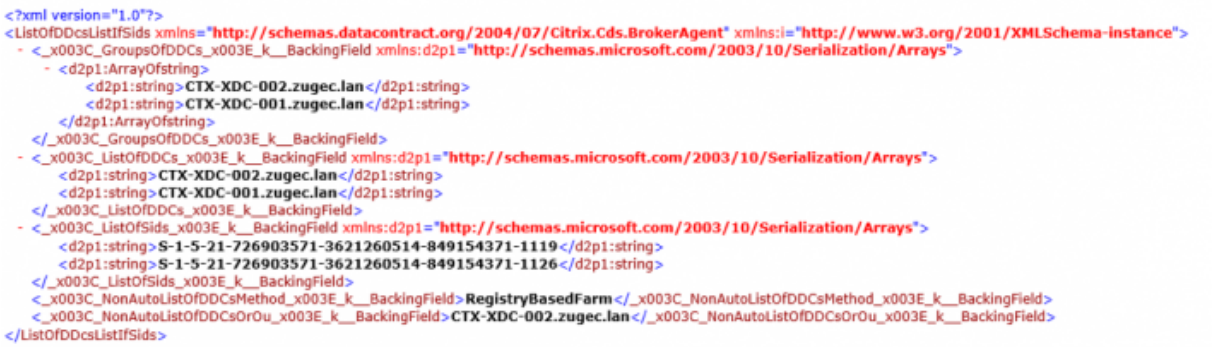
For example:

- 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 the 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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. 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

#### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 the 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: https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/
- Mutual authentication using Kerberos: https://docs.microsoft.com/en-us/windows/win32/ad/mutual-authentication-using-kerberos?redirectedfrom=MSDN

#### 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

You might want to process Controllers or Cloud Connectors in groups. With groups, one group is 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.

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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### 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 will 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.

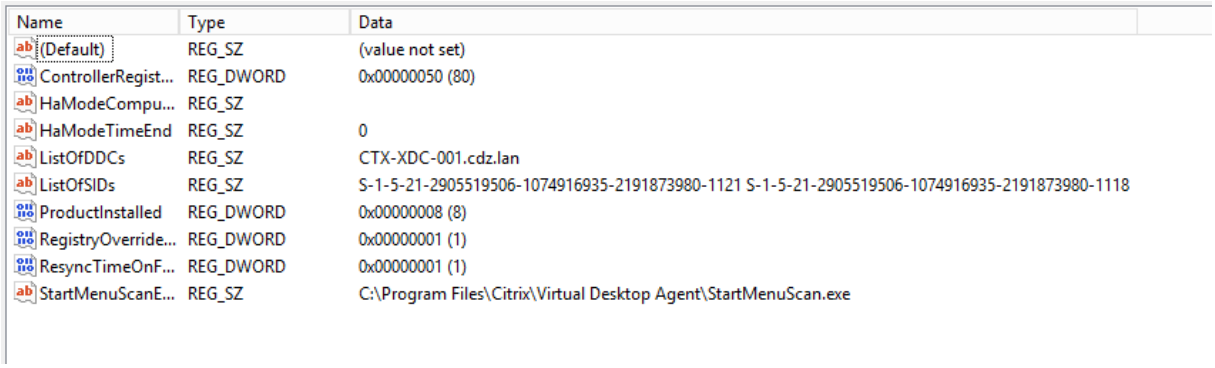
- **Separate roles for Controllers:** Before zones were introduced in XenApp and XenDesktop 7.7, the ListOfSIDs was manually configured when only a subset of Controllers was used for registration. For example, if you were using XDC-001 and XDC-002 as XML brokers, and XDC-003 and XDC-004 for VDA registration, you specified all Controllers in the ListOfSIDs, and XDC-003 and XDC-004 in the ListOfDDCs. This is not a typical or recommended configuration and is not used 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 prepopulating the ListOfSIDs, the resolution from DNS names to SIDs might 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



| 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 are expected to be"machine, review the **Troubleshoot** tab in the details pane for possible causes and recommended corrective actions.

For more information about functional levels, see *VDA versions and functional levels* section in Create Machine Catalogs.

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

October 29, 2018

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.

Use the following features to optimize the reliability of sessions, reduce inconvenience, downtime,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

The Logon interval section describes how to change the default setting.

You can also log a user off of a session, disconnect a session, and configure session prelaunch and linger; see the Manage Delivery Groups article.

### 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 Receiver 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 NetScaler 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Receiver 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 Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, Citrix Receiver 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 Receiver 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 Receiver. Citrix Receiver submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions.

Cookies are not used if you enable the Auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Citrix Receiver attempts to reconnect automatically.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For maximum protection of user credentials and sessions, use encryption for all communication between clients and the Site.

Disable Auto Client Reconnect on Citrix Receiver for Windows by using the icaclient.adm file. For more information, see the documentation for your Citrix Receiver 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 Receiver.
- 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 Receiver 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.

> **Note:**
>
> 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.
- **Reconnecting:** After logging on to the server, users can reconnect to all of their desktops or applications at any time by clicking Reconnect. By default, Reconnect opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect to open only those desktops or applications that the user disconnected from previously.
- **Logging off:** For users opening desktops or applications through StoreFront, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.
- **Disconnecting:** Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Workspace control is available only for Citrix Receiver 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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; see Connection leasing and session roaming below.

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 settings

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Connection leasing and session roaming

If you're not familiar with connection leasing, see the Connection leasing article.

When a Controller enters leased connection mode, session reconnection reverts to its default value, reconnecting the user to only one of the active or disconnected sessions for the desktop or application.

For additional security, if you configured a nondefault session roaming value, and have multiple users who share the same logon credentials on multiple devices, consider disabling the connection leasing feature for the Delivery Group that includes that user account.

Why? In this scenario, one session is shared among all devices. This could be undesirable if, for example, one person has sensitive information displayed that is not meant to be seen by someone else who reconnects with the same credentials while the Controller is in leased connection mode.

Disabling connection leasing in the entitlement policy eliminates this possibility: a user will not be able to see the session of another user with the same logon, even when the Controller is in leased connection mode. Other entitlement policies can remain as-is; individual user accounts can use the connection leasing functionality through separate entitlements.

To disable connection leasing in an entitlement policy, add the "LeasingBehavior Disallowed"property to the entitlement policy cmdlet. If you disable connection leasing, you must manually delete any launch leases that have already been created and cached for that entitlement policy; otherwise, users will still be able to reconnect during a database outage.

### 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.

> **Note:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> This setting applies only to VMs with desktop (workstation) VDAs; Microsoft controls the logon timeout on machines with server VDAs.

## Use Search in Studio

July 23, 2018

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.

   Note: 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 drop-down list of search properties; you can perform an advanced search by building an expression from the properties in the drop-down list.

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

January 5, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 additional 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.

See below for details and examples of using a tag restriction.

- 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 the "Create multiple restart schedules for machines in a Delivery Group"section in the Manage Delivery Groups article.

- Tailor the application (assignment) of Citrix policies to a subset of 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 of the Create Policy wizard, select that tag and also the **Enable** checkbox. You can also add a tag to a Delivery Group and then apply a Citrix policy to that group. For details, see the Create policies article. (Note that the Studio interface for adding a tag to a machine has changed since the blog post was published.)

You can apply tags to the following items:

- Machines
- Applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

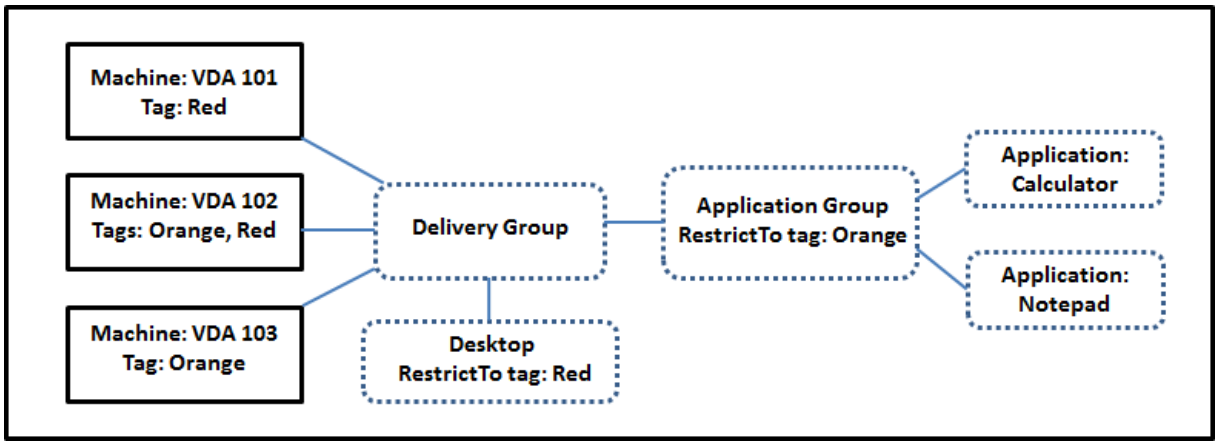
A tag restriction involves several steps:

- 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

This example introduces a simple layout that 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

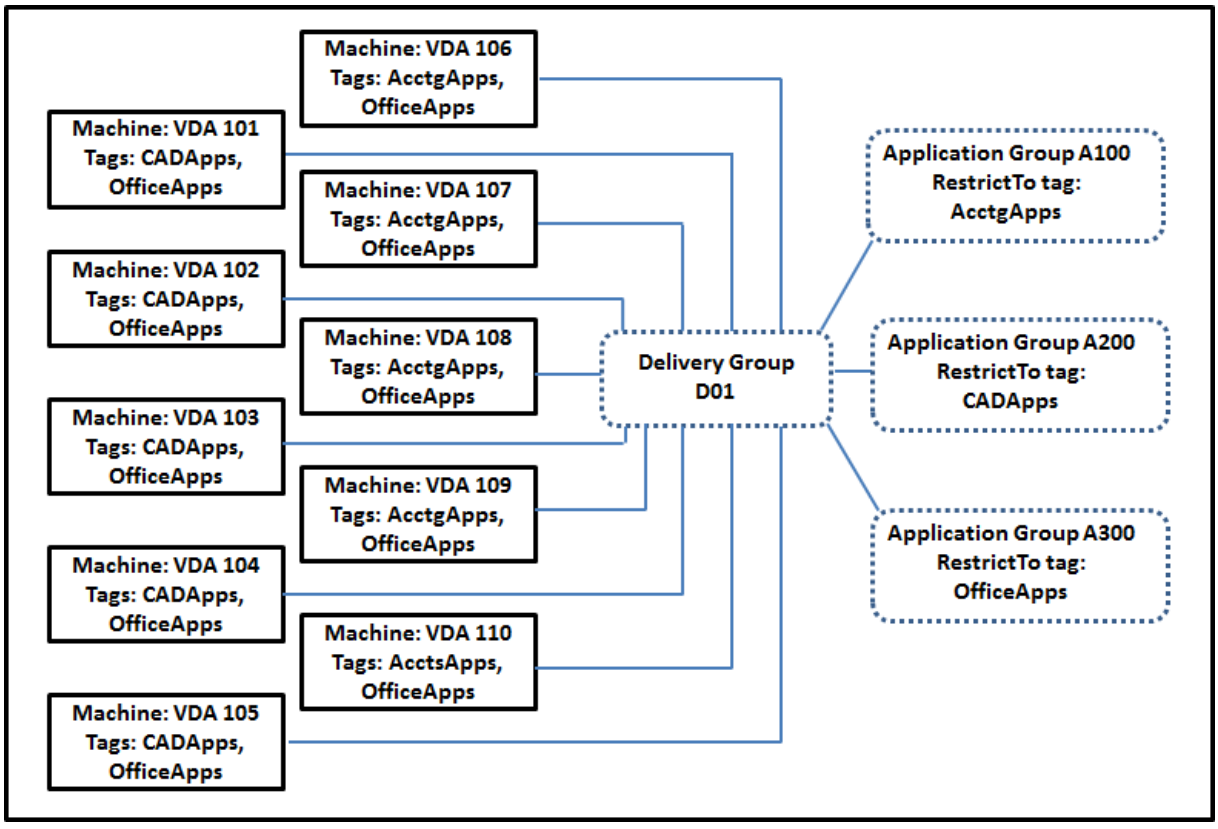
- The desktop in the shared Delivery Group was created with a tag restriction named "Red," so that desktop can be launched only on machines in that Delivery Group that have the tag "Red": VDA 101 and 102.
- The Application Group was created with the "Orange" tag restriction, so each of its applications (Calculator and Notepad) can be launched only on machines in that Delivery Group that have the tag "Orange": VDA 102 and 103.

Note that machine VDA 102 has both tags (Red and Orange), so it can be considered for launching the applications and the desktop.

**Example 2**

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.

(The "How to configure example 2" section shows the steps used to create and apply the tags, and then configure the tag restrictions in this example.)




This example uses ten 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 ten machines (VDA 101-110)

Only ten 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 the Create policies article for details.

Tag restrictions are configured when you create or edit desktops in Delivery Groups, and when you create and edit Application Groups. For complete information about creating and editing groups, see the following articles:

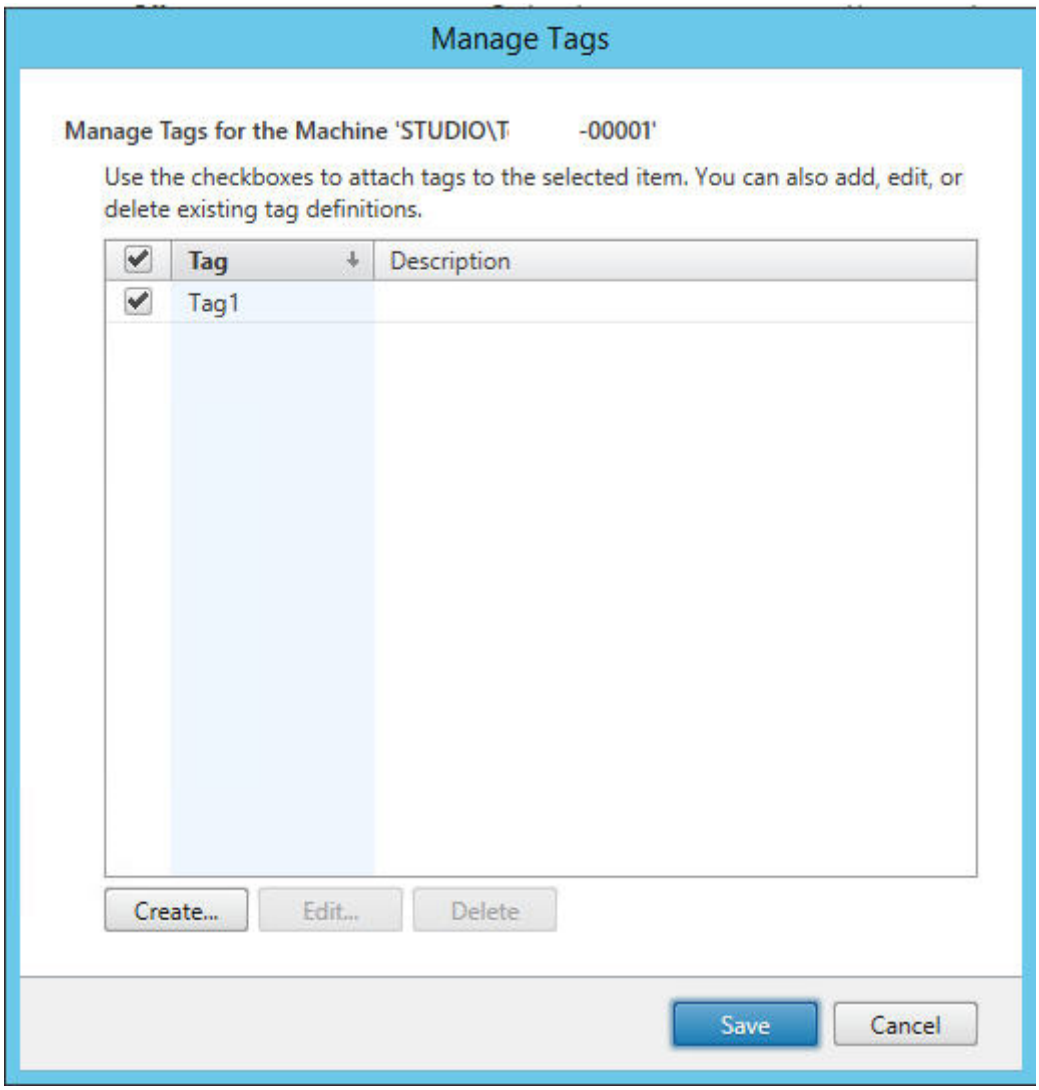
- Create Delivery Groups
- Manage Delivery Groups
- Create Application Groups
- Manage Application Groups

### Use the Manage Tags dialogs in Studio

In Studio, select the items you want to apply a tag to (one or more 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The following actions are available from the Manage Tags dialog box. Be sure to review the Cautions section.

**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. **Note:** 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 will affect all the selected machines.

If you attempt to add a tag to one or more machines, and that tag is currently used as a restriction in an Application Group, you are warned that the action could result in making those machines available

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

for launch. If that's what you intended, proceed.

**To remove one or more tags:**

Clear the check box next to the tag name. **Note:** 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), clearing the check box will remove the tag from all the selected machines.

If you attempt to remove a tag from a machine that is using that tag as a restriction, a warning message will be displayed, indicating that could affect which machines are considered for launch. If that's what you intended, proceed.

**To edit a tag:**

Select a tag and then click **Edit**. Enter a new name and/or description. 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. You must 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**.

**Tip:** 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 below.

### Manage tag restrictions

Configuring a tag restriction is a multi-step process: You first create the tag and add/apply it to machines. Then, you add the restriction to the Application Group or the desktop.

**Create and apply the tag:**

Create the tag and then add (apply) it to the machines that will be affected by the tag restriction, using the **Manage Tags** actions described above.

**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 dropdown.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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 dropdown or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

**To add a tag restriction to a desktop:**

Create or edit a Delivery Group. 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 dropdown.

**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 dropdown or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

### Cautions when adding, removing, or deleting tags from items

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 when configuring an Application Group or a desktop, which will limit launch consideration to only machines in specified Delivery Groups that have that tag.

If you attempt to add a tag to one or more machines after that tag has been configured as a tag restriction for a desktop or an Application Group, Studio warns you that adding that tag might make the machines available for launching additional applications or desktops. If that is what you intended, proceed. If not, you can 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 will display 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 remove it as a restriction by editing the group. (If you were allowed to delete a tag that's used as a restriction in an Application Group, that could 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 currently 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

All machines may not have the same sets of applications. A user may 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 will affect the next machine restart cycle. It will not affect any restart cycles that is in progress while the changes are being made. (See the Mange Delivery Groups article.)

### 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 above.

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** and then 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), and then 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** and then 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, and then close the dialog box.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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. The Create Application Group wizard launches.
2. On the **Delivery Groups** page of the wizard, select Delivery Group D01. Select **Restrict launches to machines with tag** and then select the AcctgApps tag from the dropdown.
3. Complete the wizard, specifying the accounting users and the accounting applications. (When adding the application, choose the "From Start menu"source, which will search 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.

### More information

Blog post: How to assign desktops to specific servers.

## IPv4/IPv6 support

October 29, 2018

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.

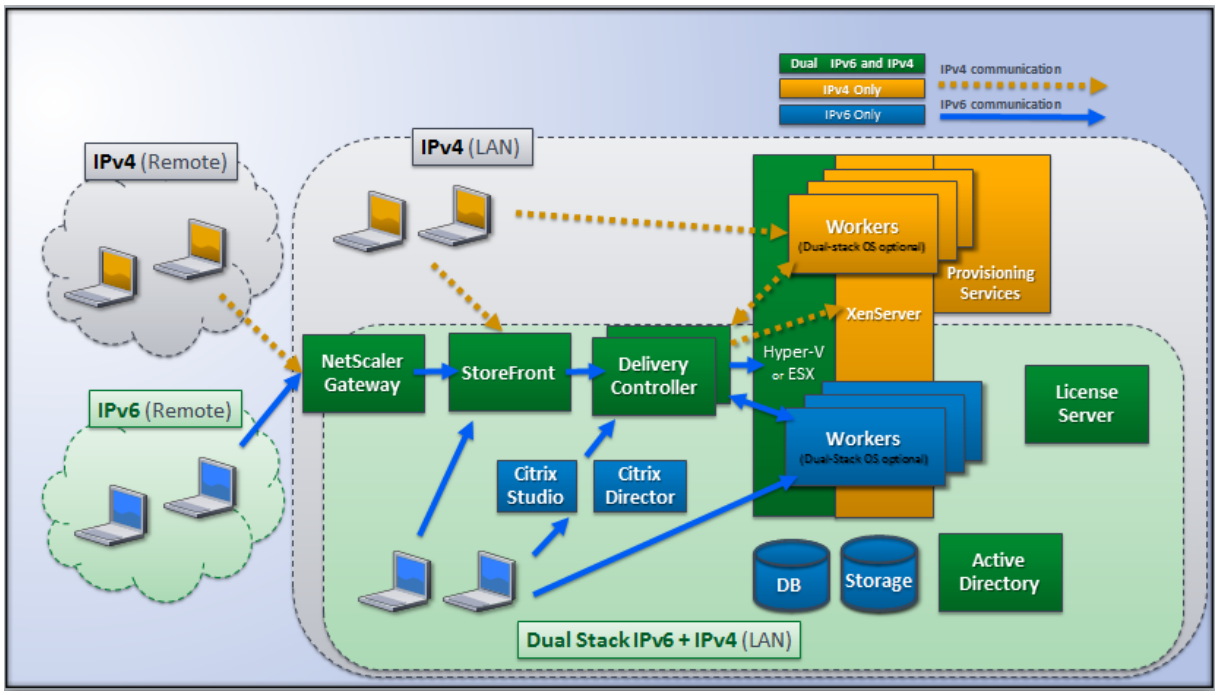
When the Only use IPv6 Controller registration policy setting is enabled, VDAs register with a Delivery Controller for incoming connections using an IPv6 address.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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:

- Provisioning Services
- XenServer Version 6.x
- 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.

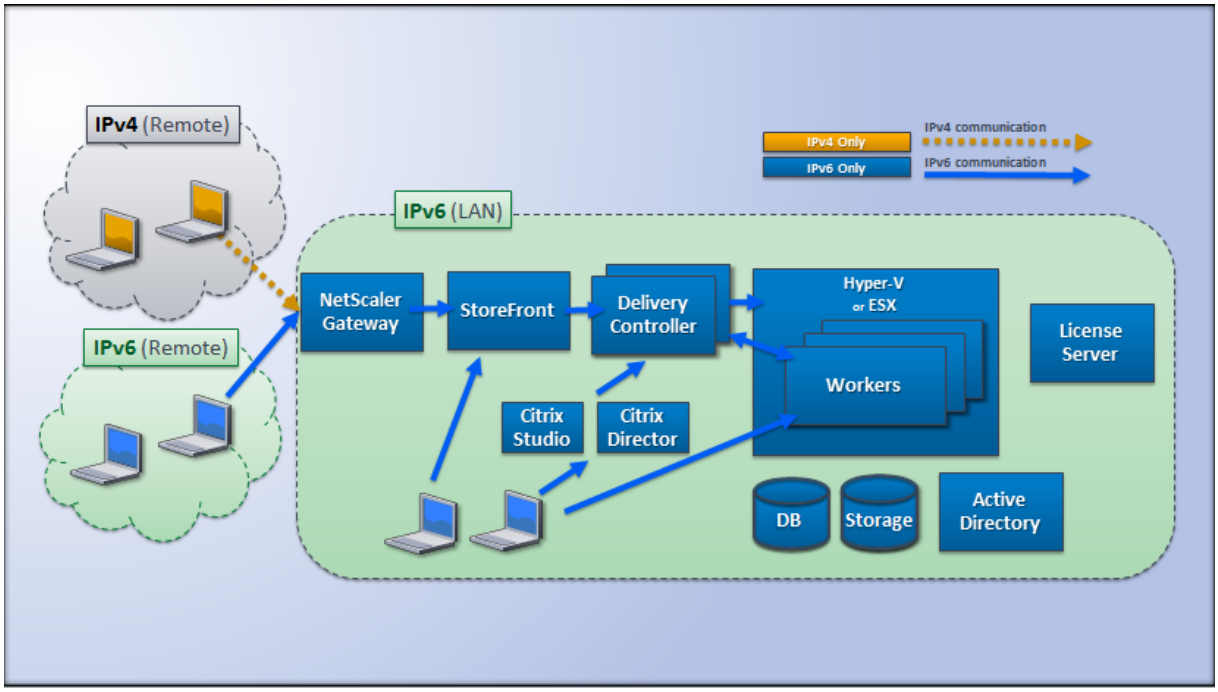
#### Pure IPv6 deployment

The following figure illustrates a pure IPv6 deployment. In this scenario:

- The components are running on operating systems configured to support an IPv6 network.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Important:** 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

May 11, 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 XenApp and XenDesktop 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 XenApp and XenDesktop 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. XenApp and XenDesktop 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 XenApp and XenDesktop policy setting.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Provisioning Services 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 Desktop 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 Server OS machines that are created with Machine Creation Services
- **Both provisioned and dedicated** –Examples are Desktop OS machines with a static assignment but without a Personal vDisk that are created with Provisioning Services
- **Both provisioned and shared** –Examples are Desktop OS machines with a random assignment that are created with Provisioning Services and desktops without Personal vDisks that are created with VDI-in-a-Box

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp 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 XenApp and XenDesktop 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.

Note: 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Folder | Redirected in Windows 8? | Redirected in Windows Server 2008? |
|---|---|---|
| Links | Yes | No |
| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

## Citrix Insight Services

February 8, 2021

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).

The features offered by Citrix Insight Services continue to grow and evolve, and now form an integral part of Citrix Smart Tools. Citrix Smart Tools enables you to automate deployment tasks, health checks, and power management. For information about the technologies, see the Citrix Smart Tools documentation.

All information uploaded to Citrix is used for troubleshooting and diagnostic purposes, as well as 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.citrix.com/about/legal/privacy.html

This XenApp and XenDesktop release supports the following tools and technologies.

- XenApp and XenDesktop install and upgrade analytics
- Citrix Customer Experience Improvement Program
- Citrix Smart Tools
- Citrix Call Home (part of Citrix Smart Tools)
- Citrix Scout

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 will be 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.

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:

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0

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 (CEIP)

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 XenApp or XenDesktop 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 XenApp or XenDesktop deployment:

- If you upgrade from a version that did not support CEIP, you are asked if you want to participate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- If you upgrade from a version that supported CEIP, and participation was enabled, CEIP will be enabled in the upgraded Site.
- If you upgrade from a version that supported CEIP, and participation was disabled, CEIP will be disabled in the upgraded Site.
- If you upgrade form 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 will be 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:

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0

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 Provisioning Services, AppDNA, Citrix License Server, Citrix Receiver for Windows, Universal Print Server, and Session Recording. See their documentation for details about installation and participation default values.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Citrix Smart Tools

You can enable Smart Tools access when you install a Delivery Controller.

The option to enable Smart Tools access (and participate in Call Home, if it is not already enabled) is selected by default. Click **Connect**. A browser window opens and navigates automatically to a Smart Services web page, where you enter your Citrix Cloud account credentials. (If you don't have a Citrix Cloud account, simply enter your Citrix account credentials, and a new Citrix Cloud account is automatically created for you.) After you're authenticated, a certificate is silently installed in the Smart Tools Agent directory.

To use the Smart Tools technologies, see the Smart Tools documentation.

### Citrix Call Home

When you install certain components and features in XenApp or XenDesktop, 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 XenApp and XenDesktop, 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). 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 XenApp and XenDesktop 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

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 these key datapoints: 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 bassis (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.

### 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 won't appear.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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 and connect to Citrix Smart Tools. There are three options:

- Connect to Citrix Smart Tools, which includes the Call Home functionality via the Smart Tools agent. This is the default and recommended option. If you choose this option, the Smart Tools agent is configured. (The Smart Tools agent is installed, regardless of whether this option is selected.)
- Participate only in Call Home, but do not connect to Smart Tools. If you choose this option, the Smart Tools agent is installed, but not configured. Call Home functionality is provided through the Citrix Telemetry Service and Citrix Insight Services.
- Do not connect to Smart Tools or participate in Call Home.

When you're installing a Controller, you will not be able to 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, the page will ask only about Smart Tools. If you're already enrolled in Call Home and the Smart Agent is already installed, the wizard page won't appear.

For information about Smart Tools, see the Smart Tools documentation.

### 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
```

To confirm that scheduled uploads are enabled, enter Get-CitrixCallHome. It should return IsEnabled=True and IsMasterImage=False.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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. It should return IsEnabled=True and IsMasterImage=True.

### Create a custom schedule

Ceate 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}

### Cancel scheduled uploads

After you cancel scheduled uploads, you can still upload diagnostic data using PowerShell cmdlets.

Disable-CitrixCallHome

To confirm that scheduled uploads are disabled, enter Get-CitrixCallHome. It should return IsEnabled=False and IsMasterImage=False.

### Examples

The following cmdlet creates a schedule to bundle and upload data at 11:20 every evening. Note that 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

To confirm the schedule, enter Get-CitrixCallHomeSchedule, In the above example,it should return StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily.

The following cmdlet creates a schedule to bundle and upload data at 11:20 every Wednesday evening.

$timespan –New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To confirm the schedule, enter Get-CitrixCallHomeSchedule, In the above example, it should return StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

### 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.

**Step 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.

**Step 2.** In PowerShell, run **netsh winhttp import proxy source=ie**.

```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

**Step 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 below.

TelemetryService.exe - Notepad

File Edit Format View Help

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
                <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
    </startup>
    <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
        <dependentAssembly>
          <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
          <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
        </dependentAssembly>
        <probing privatePath="TelemetryModule" />
      </assemblyBinding>
    </runtime>
<system.net>
<defaultProxy>
<proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
</defaultProxy>
</system.net>

</configuration>
```

**Step 4.** Restart the Telemetry Service.

Run the Call Home cmdlets in PowerShell.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Manually collect and upload diagnostic information

You can use the CIS web site 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 web site:

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. Then, at a later time, 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 may 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>]

### 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 <String>] [<CommonParameters>]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Parameter | Description |
| --- | --- |
| 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 will be 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’; ‘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 <PSCredential> -Path <String> [<CommonParameters>]

The Path parameter specifies the location of the previously-saved bundle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 for PVS VDAs, which was noted at 2:30 PM for Citrix Support case 123456. In addition to the Call Home data, the file "c:\Diagnostics\ExtraData.zip"will be incorporated into the uploaded bundle.

C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip"-Description "Registration failures with PVS VDAs"-IncidentTime "14:30"-SRNumber 123456 -Name "RegistrationFailure-021812016"-Collect "{'wmi':{'enabled':false}}"-UploadHeader "{'key1':'value1'}"-AppendHeaders "{'key2':'value2'}"

The following cmdlet saves Call Home data related to Citrix Support case 223344, noted at 8:15 AM. The data will be 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

The following cmdlet uploads the data bundle you saved earlier.

$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip

### Citrix Scout

For full details, see Citrix Scout.

## Citrix Scout

August 17, 2021

### Introduction

Citrix Scout collects diagnostics that can be used for proactive maintenance in your XenApp and XenDesktop deployment. Citrix offers comprehensive, automated analysis through Citrix Insight Services. You can also use Scout to troubleshoot issues, either on your own or with guidance from Citrix Support. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Scout offers three main procedures:

- **Collect:** Runs a one-time diagnostics collection on machines you select in a Site. Then, you either upload the file containing the collection 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. Then, Scout collects other diagnostics and uploads the file containing the trace and the collection 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 containing each collection is automatically uploaded to Citrix.

The graphical interface described in this article is the primary way to use Scout. Alternatively, you can use the PowerShell interface to configure one-time or scheduled diagnostic collections and uploads. See Call Home.

Where to run Scout:

- In an on-premises XenApp and XenDesktop deployment, run Scout from a Delivery Controller to capture diagnostics from one or more Virtual Delivery Agents (VDAs) and Delivery Controllers. You can also run Scout from a VDA to collect local diagnostics.
- In a Citrix Cloud environment that uses the XenApp and XenDesktop Service, run Scout from a VDA to collect local diagnostics.

#### 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 troubleshooting common issues such as VDA registrations and application/desktop launches. No other Event Tracing for Windows (ETW) information is collected.

Collected information includes:

- Registry entries created by XenApp and XenDesktop 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.

About trace information:

- The trace information is compressed as it is collected, maintaining a small footprint on the machine.
- On each machine, the Citrix Telemetry Service retains a maximum of 10 MB of compressed recent trace information, with a maximum time limit of eight days.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Traces are held in memory to avoid IOPs on provisioned machines.
- The trace buffer uses a circular mechanism to retain traces in memory.

For a list of the datapoints that Scout collects, see Scout key datapoints.

### Prerequisites and considerations

Permissions

- 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.
- Use **Run as administrator** when launching Scout.

For each machine from which you collect diagnostics:

- 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.
- To set a schedule for diagnostic collection, the machine must be running a Scout version provided with XenApp and XenDesktop 7.14 or a later supported version.

Scout runs verification tests on the machines you select to ensure these requirements are met.

#### Verification tests

Before a diagnostic collection starts, verification tests run automatically for each selected machine. These tests ensure that the requirements listed above are met. If a test fails for a machine, Scout displays a message, with suggested corrective actions.

| Error message | Corrective action |
| --- | --- |
| Scout cannot reach this machine | Ensure that the machine is powered-on. Ensure that the network connection is working properly. (This can include verifying that your firewall is properly configured.) Ensure that file and printer sharing is turned on. See the Microsoft documentation for instructions. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Error message | Corrective action |
| --- | --- |
| 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. |

**Version compatibility**

This version of Scout (3.x) is intended to be run on (minimum) XenApp and XenDesktop 7.14 Controllers and VDAs.

An earlier version of Scout is provided with earlier XenApp and XenDesktop deployments. 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 XenApp and XenDesktop 7.14 (minimum) | Yes | Yes |
| Support XenDesktop 5.x, 7.1 to 7.13 | Yes | No |
| Support XenApp 6.x, 7.5 to 7.13 | Yes | No |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Feature | Scout 2.23 | Scout 3.0 |
|---|---|---|
| Allow collection of diagnostic data | Up to 10 machines at once (by default) | Unlimited (subject to resources 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 telemetry installed) |

#### Install

By default, Scout is installed automatically as part of the Citrix Telemetry Service when you install 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 XenApp or XenDesktop ISO.

#### 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 is not visible. You simply enter your account credentials. After Citrix validates the credentials, you are allowed to 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 entering your Citrix Cloud credentials, the token is displayed. Copy the token and then paste it into Scout. You are then allowed to continue in the

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Scout wizard.

The token is stored locally on the machine where you're running Scout. If you want to use that token the next time you select **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, or you can specify the proxy server's IP address and port number.

### 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.

**Step 1. Launch Scout.**

From the machine's Start menu: **Citrix > Citrix Scout**. On the opening page, click **Collect**.

**Step 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**.

Scout automatically launches verification tests on each machine you selected, 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 will not be collected from that machine.

When the verification tests complete, click **Continue**.

**Step 3. Collect diagnostics from machines.**

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 comp;leted collection are retained. 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**.
- If a collection for a machine succeeds and you want 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, do not click **Back**. If you click that button and confirm the prompt, the collection is lost.

When the collection completes, click **Continue**.

**Step 4. Save or upload the collection.**

Choose whether to upload the file containing the collected diagnostics 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 from Citrix; see CTX136396 for Citrix Insight Services, or Smart Tools support.

Click **Done** to return to the Scout opening page. You do not need to complete any further steps in this procedure.

**Step 5. Authenticate for uploads and optionally specify proxy.**

Review Upload authorization for details of this process.

- If you have not previously authenticated through Scout, continue with this step.
- If you previously authenticated through Scout, the stored authorization token is used by default. If this is OK with you, choose this option and click **Continue**. You are not prompted for credentials for this collection; continue with Step 6.
- If you previously authenticated, but want to reauthorize and have a new token issued, click **Change/Reauthorize** and continue with this step.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 will 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**.

**Step 6. Provide information about the upload.**

Enter upload details:

- The name field contains the default name for the file that will contain the collected diagnostics. This should suffice for most collections, although you can change the name. (If you delete the default name and leave the name field empty, the default name will be 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.

### Trace and reproduce

The Trace and Reproduce procedure comprises selecting machines, starting a trace on those machines, reproduce issues on those machines, completing the diagnostics collection, and then uploading the file containing the traces and collection 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.

**Step 1. Launch Scout.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

From the machine's Start menu: **Citrix > Citrix Scout**. On the opening page, click **Trace & Reproduce**.

**Step 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, and then click **Continue**.

Scout launches verification tests on each of the machines you selected, ensuring 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 will not be collected from that machine.

When the verification tests complete, click **Continue**.

**Step 3. 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.

**Step 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 retained. 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**.
- If a collection for a machine succeeds and you want to collect diagnostics again from a machine, click **Collect Again** in that machine's Action column. The newer collection overwrites the earlier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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, do not click the **Back** button. If you click that button and confirm the prompt, the collection is lost.

When the collection completes, click **Continue**.

**Step 5. Save or upload the collection.**

Choose whether to upload the file containing the collected diagnostics to Citrix, or save it on the local machine.

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, or Citrix Smart Tools.

Click **Done** to return to the Scout opening page. You do not need to complete any further steps in this procedure.

**Step 6. Authenticate for uploads and optionally specify proxy.**

Review Upload authorization for details of this process.

- If you have not previously authenticated through Scout, continue with this step.
- If you previously authenticated through Scout, the stored authorization token is used by default. If this is OK with you, choose this option and click **Continue**. You are not prompted for credentials for this collection; continue with Step 7.
- If you previously authenticated, but want to reauthorize and have a new token issued), 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 will 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

When you're done, click **Continue**.

**Step 7. Provide information about the upload.**

Enter upload details:

- The name field contains the default name for the file that will contain the collected diagnostics. This should suffice for most collections, although you can change the name. (If you delete the default name and leave the name field empty, the default name will be 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 lik 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

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.)

**Step 1. Launch Scout.**

From the machine's Start menu: **Citrix > Citrix Scout**. On the opening page, click **Schedule**.

**Step 2. Select machines.**

The Select machines page lists all the VDAs and Controllers in the Site. You can filter the display by machine name.

When you installed VDAs and Controllers using the graphical interface, you were offered the opportunity to participate in Call Home. For details, see Citrix Call Home. (Call Home includes scheduling functionality equivalent to Scout.) 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.

Keep in mind that although you enabled/disabled Call Home on a per-machine basis, setting a schedule in Scout uses the same commands, but affects all the machines you select.

Select the check box next to each machine you want to collect diagnostics from, and then click **Continue**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Scout launches verification tests on each of the machines you selected, ensuring 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 (or traces) will not 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**.

**Step 3. Set schedule.**

Indicate when you want diagnostics to be collected. Remember: The schedule affects all the selected machines.

- To configure a weekly schedule for the selected machines, click **Weekly**. Choose the day of the week and enter the time of day (24-hour clock) when the diagnostics collection will begin.
- To configure a daily schedule for the selected machines, click **Daily**. Enter the time of day (24-hour clock) when the diagnostics collection will 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**.

**Step 4. Authenticate for uploads and optionally specify 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 will 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**.

Review the configured schedule. Click **Done** to return to the Scout opening page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

When each scheduled collection occurs, each selected machine's Windows application log contains entries about the collection and upload.

## Monitor

October 29, 2018

Administrators and help-desk personnel can monitor XenApp and XenDesktop 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.

### Session Recording

Session Recording allows you to record the on-screen activity of any user's session, over any type of connection, from any server running XenApp subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications —such as financial operations and healthcare patient information systems —supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

For details, see the Session Recording articles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Configuration Logging

Configuration Logging is a feature that 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 interface 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 Desktop Machines
- Failed Server Machines

For details about how to enable and configure Configuration Logging, see the Configuration Logging article. The Director articles describe how to view logged information from that tool.

### Event logs

XenApp and XenDesktop services log events that occur. Event logs can be used to monitor and troubleshoot operations.

For details, see the Event logs article. Individual feature articles might also contain event information.

## Session Recording 7.15

September 29, 2019

Session Recording allows you to record the on-screen activity of any user session hosted on a VDA for Server OS or Desktop OS, over any type of connection, subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording provides flexible policies to trigger recordings of application and desktop sessions automatically. Session Recording enables IT personnel to monitor and examine user activity of application and desktop sessions, and therefore supports internal controls for regulatory compliance and

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

### Benefits

**Enhanced security through logging and monitoring**. Session Recording allows organizations to record on-screen user activity for applications that deal with sensitive information. The approach is especially critical in regulated industries such as healthcare and finance. Where personal information that must not be recorded is involved, policy controls allow selective recording.

**Powerful activity monitoring**. Session Recording captures and archives screen updates, including mouse activity and the visible output of keystrokes in secured video recordings to provide a record of activity for specific users, applications, and servers.

Session Recording is not designed or intended to contribute to the collection of evidence for legal proceedings. Citrix recommends that organizations using Session Recording use other techniques for evidence collection, such as conventional video records combined with traditional text-based eDiscovery tools.

**Faster problem resolution**. When users call with a problem that is hard to reproduce, help desk support staff can enable recording of user sessions. When the issue recurs, Session Recording provides a time-stamped visual record of the error, which can then be used for faster troubleshooting.

## Get started with Session Recording

March 17, 2020

After you perform the following steps, you can begin recording and reviewing XenApp and XenDesktop sessions.

1. Become familiar with the Session Recording components.
2. Select the deployment scenario for your environment.
3. Verify the installation requirements.
4. Install the Windows roles and features prerequisites.
5. Install Session Recording.
6. Configure the Session Recording components to permit recording and viewing of sessions.

Session Recording consists of five components:

- **Session Recording Agent.** A component installed on each VDA for Server OS or Desktop OS to enable recording. It is responsible for recording session data.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Session Recording Server.** A server that hosts:
  - The Broker. An IIS 6.0+ hosted Web application that handles the search queries and file download requests from the Session Recording Player, handles policy administration requests from the Session Recording Policy Console, and evaluates recording policies for each XenApp and XenDesktop session.
  - The Storage Manager. A Windows service that manages the recorded session files received from each Session Recording-enabled computer running XenApp and XenDesktop.
  - Administrator Logging. An optional subcomponent installed with the Session Recording Server to log the administration activities. All the logging data is stored in a separate SQL Server database named **CitrixSessionRecordingLogging** by default. You can customize the database name.
- **Session Recording Player.** A user interface that users access from a workstation to play recorded XenApp and XenDesktop session files.
- **Session Recording Database.** A component that manages the SQL Server database for storing recorded session data. When this component is installed, it creates a database named **CitrixSessionRecording** by default. You can customize the database name.
- **Session Recording Policy Console.** A console used to create policies to specify which sessions are recorded.

This illustration shows the Session Recording components and their relationship with each other:

In the deployment example illustrated here, the Session Recording Agent, Session Recording Server, Session Recording Database, Session Recording Policy Console, and Session Recording Player all reside behind a security firewall. The Session Recording Agent is installed on a VDA for Server OS or Desktop OS. A second server hosts the Session Recording Policy Console, a third server acts as the Session Recording Server, and a fourth server hosts the Session Recording Database. The Session Recording Player is installed on a workstation. A client device outside the firewall communicates with the VDA for Server OS on which the Session Recording Agent is installed. Inside the firewall, the Session Recording Agent, Session Recording Policy Console, Session Recording Player, and Session Recording Database all communicate with the Session Recording Server.

## Plan your deployment

March 17, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Limitations and caveats

Session Recording does not support Desktop Composition Redirection (DCR) display mode. By default, Session Recording disables DCR in a session if the session is to be recorded by recording policy. You can configure this behavior in Session Recording Agent properties.

Session Recording does not support the Framehawk display mode. Sessions in Framehawk display mode cannot be recorded and played back correctly. Sessions recorded in Framehawk display mode might not contain the sessions' activities.

Session Recording cannot record the Lync webcam video when using the HDX RealTime Optimization Pack.

Depending upon your environment, you can deploy the Session Recording components in different scenarios.

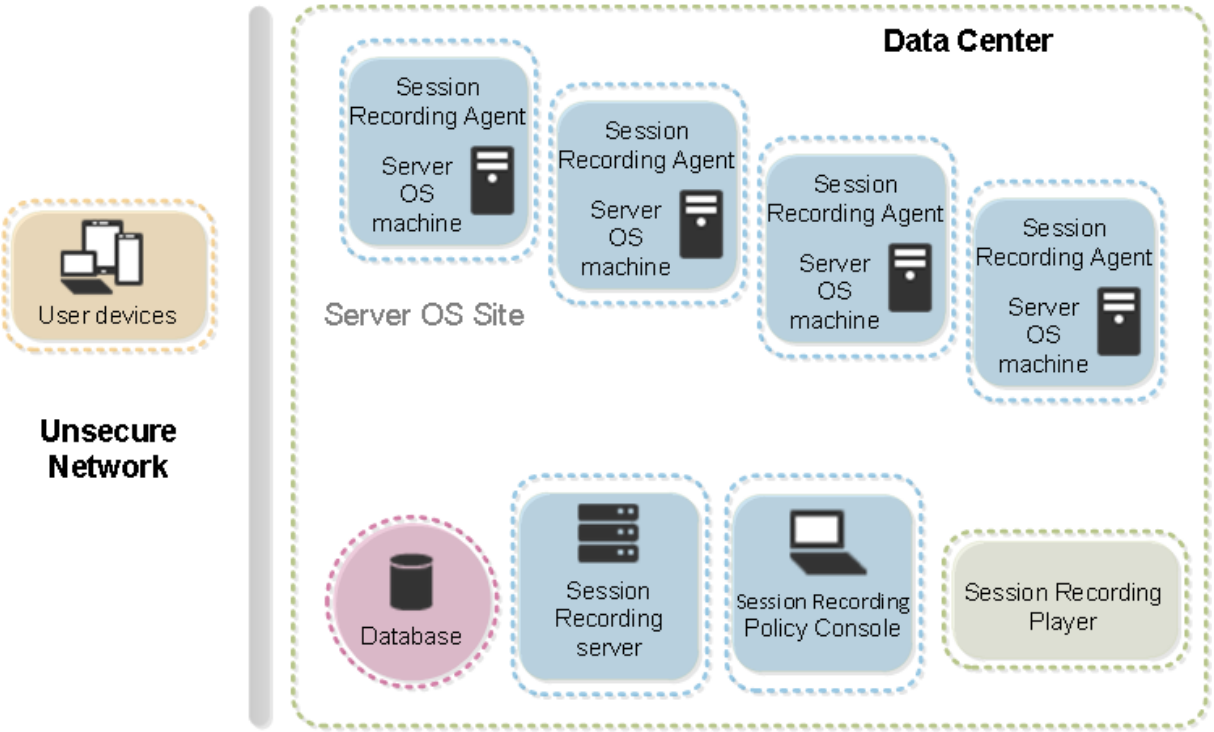
A Session Recording deployment is not limited to a single site. Except the Session Recording Agent, all components are independent of the server site. For example, you can configure multiple sites to use a single Session Recording Server.

Alternatively, if you have a large site with many agents and plan to record many graphically intense applications (for example, AutoCAD applications), or you have many sessions to record, a Session Recording Server can experience a high performance demand. To alleviate performance issues, you can install multiple Session Recording Servers on different machines and point the Session Recording Agents to the different machines. Keep in mind that an agent can point to only one server at a time.

### Suggested server site deployment

Use this type of deployment for recording sessions for one or more Sites. The Session Recording Agent is installed on each VDA for Server OS in a Site. The Site resides in a data center behind a security firewall. The Session Recording Administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) are installed on other servers and the Session Recording Player is installed on a workstation, all behind the firewall but not in the data center.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Important deployment notes

- To enable Session Recording components to communicate with each other, install them in the same domain or across trusted domains that have a transitive trust relationship. The system cannot be installed on a workgroup or across domains that have an external trust relationship.
- Considering its intense graphical nature and memory usage when playing back large recordings, We do not recommend installing the Session Recording Player as a published application.
- The Session Recording installation is configured for TLS/HTTPS communication. Ensure that you install a certificate on the Session Recording Server and that the root certificate authority (CA) is trusted on the Session Recording components.
- If you install the Session Recording Database on a standalone server running SQL Server 2016 Express Edition, SQL Server 2014 Express Edition, SQL Server 2012 Express Edition, or SQL Server 2008 R2 Express Edition, the server must have TCP/IP protocol enabled and SQL Server Browser service running. These settings are disabled by default, but they must be enabled for the Session Recording Server to communicate with the database. For information about enabling these settings, see the Microsoft articles Enable TCP/IP Network Protocol for SQL Server and SQL Server Browser Service.
- Consider the effects of session sharing when planning your Session Recording deployment. Session sharing for published applications can conflict with Session Recording policy rules for published applications. Session Recording matches the active policy with the first published application that a user opens. After the user opens the first application, any subsequent applica-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tions opened during the same session continue to follow the policy that is in force for the first application. For example, if a policy states that only Microsoft Outlook should be recorded, the recording commences when the user opens Outlook. However, if the user opens a published Microsoft Word second (while Outlook is running), Word also is recorded. Conversely, if the active policy does not specify that Word should be recorded, and the user launches Word before Outlook (which should be recorded, according to the policy), Outlook is not recorded.

- Though you can install the Session Recording Server on a Delivery Controller, we do not recommend you do so because of performance issues.
- You can install the Session Recording Policy Console on a Delivery Controller.
- You can install both the Session Recording Server and Session Recording Policy Console on the same system.
- Ensure that the NetBIOS name of the Session Recording Server does not exceed the limit of 15 characters (Microsoft has a 15-character limit on the host name length).
- PowerShell 5.1 or later is required for custom event logging. Upgrade PowerShell if you install the Session Recording Agent on Windows Server 2012 R2 that has PowerShell 4.0 installed. Failure to comply can cause failed API calls.

## Security recommendations

March 17, 2020

Session Recording is deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is simple and security features such as digital signing and encryption can be configured optionally.

Communication between Session Recording components is achieved through Internet Information Services (IIS) and Microsoft Message Queuing (MSMQ). IIS provides the web services communication link between Session Recording components. MSMQ provides a reliable data transport mechanism for sending recorded session data from the Session Recording Agent to the Session Recording Server.

> **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.

Consider these security recommendations when planning your deployment:

- Ensure that you properly isolate the different administrator roles in the corporate network, in the Session Recording system, or on individual machines. By not doing so, security threats that

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

can impact the system functionality or abuse the system might occur. We recommend that you assign different administrator roles to different persons or accounts. Do not allow general session users to have administrator privileges to the VDA system.

  - XenApp and XenDesktop administrators do not grant VDA local administrator role to any users of published apps or desktops. If the local administrator role is a requirement, protect the Session Recording Agent components by using Windows mechanisms or third-party solutions.
  - Separately assign the Session Recording database administrator and Session Recording policy administrator.
  - We recommend that you do not assign VDA administrator privileges to general session users, especially when using Remote PC Access.
  - Session Recording Server local administration account must be strictly protected.
  - Control access to machines where the Session Recording Player is installed. If a user is not authorized for the Player role, do not grant that user local administrator role for any player machine. Disable anonymous access.
  - We recommend using a physical machine as a storage server for Session Recording.

- Session Recording records session graphics activities without regard to the sensitivity of the data. Under certain circumstances, sensitive data (including but not limited to user credentials, privacy information, and third-party screens) might be recorded unintentionally. Take the following measures to prevent risks:

  - Disable core memory dump for VDAs unless for specific troubleshooting cases.

    To disable core memory dump:

    1. Right-click **My Computer**, and then select **Properties**.
    2. Click the **Advanced** tab, and then under **Startup and Recovery**, click **Settings**.
    3. Under **Write Debugging Information**, select **(none)**.

    See the Microsoft article at https://support.microsoft.com/en-us/kb/307973.

  - Session owners notify attendees that online meetings and remote assistance software might be recorded if a desktop session is being recorded.

  - Ensure that logon credentials or security information does not appear in all local and Web applications published or used inside the corporation. Otherwise, they are recorded by Session Recording.

  - Close any application that might expose sensitive information before switching to a remote ICA session.

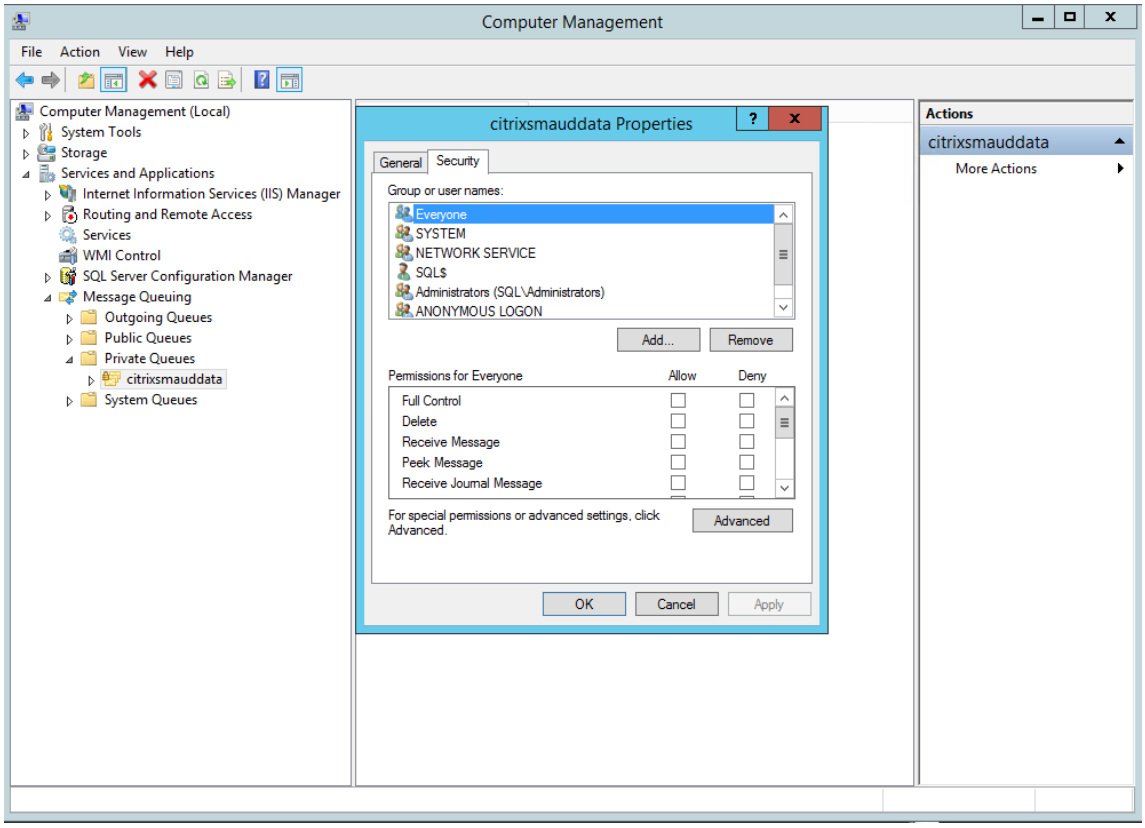
  - We recommend only automatic authentication methods (for example, single sign on, smartcard) for accessing published desktops or Software as a Service (SaaS) applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Session Recording relies on certain hardware and hardware infrastructure (for example, corporate network devices, operation system) to function properly and to meet security needs. Take measures at the infrastructure levels to prevent damage or abuse to those infrastructures and make the Session Recording function secure and reliable.
  - Properly protect and keep network infrastructure supporting Session Recording available.
  - We recommend using a third-party security solution or Windows mechanism to protect Session Recording components. Session Recording components include:
    - On the Session Recording Server
      - Processes: SsRecStoragemanager.exe and SsRecAnalyticsService.exe
      - Services: CitrixSsRecStorageManager and CitrixSsRecAnalyticsService
      - All files in Session Recording Server installation folder
      - Registry key values within HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server
    - On the Session Recording Agent
      - Process: SsRecAgent.exe
      - Service: CitrixSmAudAgent
      - All files in Session Recording Agent installation folder
      - Registry key values within HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent
- Set the access control list (ACL) for Message Queuing (MSMQ) on the Session Recording Server to restrict VDA or VDI machines that can send MSMQ data to the Session Recording Server and prevent unauthorized machines from sending data to the Session Recording Server.

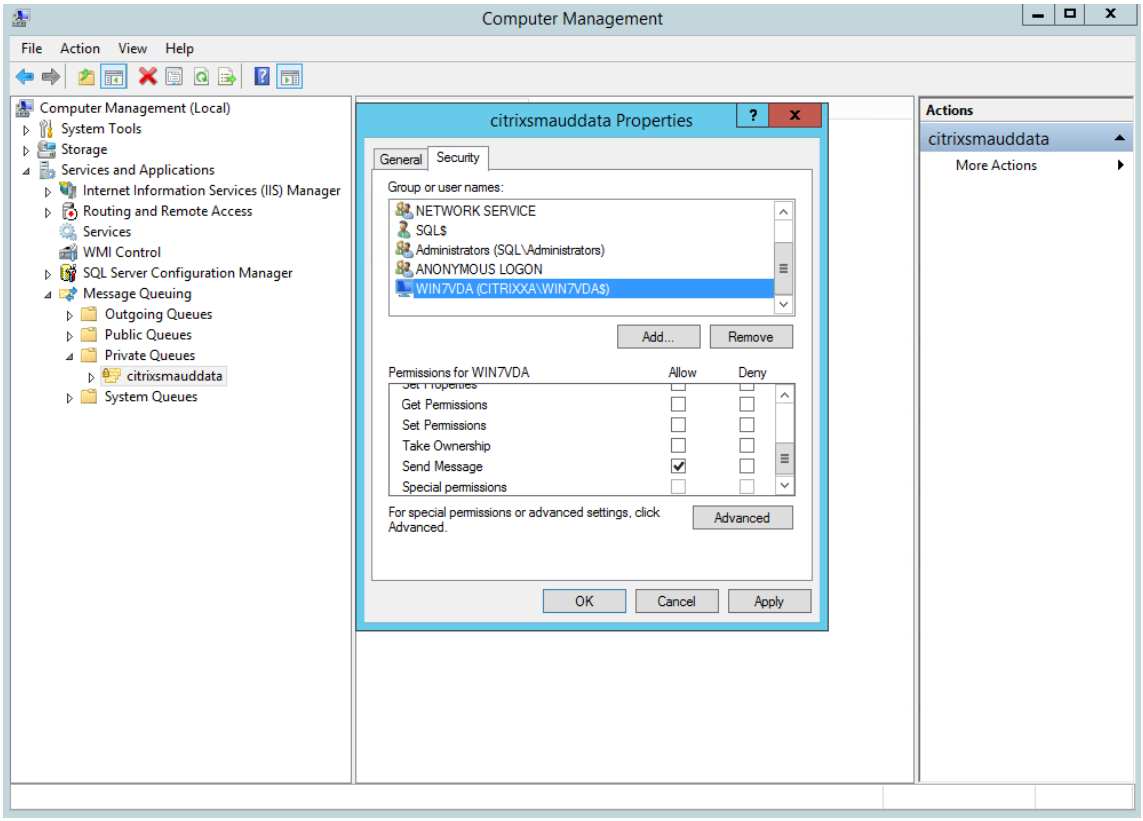
1. Install server feature Directory Service Integration on each Session Recording Server and VDA or VDI machine where Session Recording is enabled. Then restart the Message Queuing service.
2. From the Windows **Start** menu on each Session Recording Server, open **Administrative Tools** > **Computer Management**.
3. Open **Services and Applications** > **Message Queuing** > **Private Queues**.
4. Click the private queue **citrixsmauddata** to open the **Properties** page and select the **Security** tab.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




5. Add the computers or security groups of the VDAs that send MSMQ data to this server and grant them the **Send Message** permission.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




- Properly protect the event log for the Session Record Server and Session Recording Agents. We recommend using a Windows or third-party remote logging solution to protect the event log or redirect the event log to the remote server.
- Ensure that servers running the Session Recording components are physically secure. If possible, lock these computers in a secure room to which only authorized personnel can gain direct access.
- Isolate servers running the Session Recording components on a separate subnet or domain.
- Protect the recorded session data from users accessing other servers by installing a firewall between the Session Recording Server and other servers.
- Keep the Session Recording Administration Server and SQL database up to date with the latest security updates from Microsoft.
- Restrict non-administrators from logging on to the administration machine.
- Strictly limit who is authorized to make recording policy changes and view recorded sessions.
- Install digital certificates, use the Session Recording file signing feature, and set up TLS communications in IIS.
- Set up MSMQ to use HTTPS as its transport. The way is to set the MSMQ protocol listed in **Session Recording Agent Properties** to HTTPS. For more information, see Troubleshoot MSMQ.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Use TLS 1.1 or TLS 1.2 (recommended) and disable SSLv2, SSLv3, TLS 1.0 on the Session Recording Server and Session Recording Database. For more information, see the Microsoft article at https://support.microsoft.com/default.aspx?scid=kb;en-us;187498.

  Disable RC4 cipher suites for TLS on the Session Recording Server and Session Recording Database:

1. Using the Microsoft Group Policy Editor, navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **SSL Configuration Settings**.
2. Set the **SSL Cipher Suite Order** policy to **Enabled**. By default, this policy is set to **Not Configured**.
3. Remove any RC4 cipher suites.

- Use playback protection. Playback protection is a Session Recording feature that encrypts recorded files before they are downloaded to the Session Recording Player. By default, this option is enabled and is in **Session Recording Server Properties**.
- Follow NSIT guidance for cryptographic key lengths and cryptographic algorithms.
- Configure TLS 1.2 support for Session Recording.

  - We recommend using TLS 1.2 as the communication protocol to ensure the end-to-end security of the Session Recording components.

    **To configure TLS 1.2 support of Session Recording:**

    1. Log on to the machine hosting the Session Recording Server. Install the proper SQL Server client component and driver, and set strong cryptography for .NET Framework (version 4 or later).

    1. Install the Microsoft ODBC Driver 11 (or a later version) for SQL Server.
    2. Apply the latest hotfix rollup of .NET Framework.
    3. Install `ADO.NET - SqlClient` based on your version of .NET Framework. For more information, see https://support.microsoft.com/en-us/kb/3135244.
    4. Add a DWORD value SchUseStrongCrypto = 1 under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319.
    5. Restart the machine.

    2. Log on to the machine hosting the Session Recording Policy Console. Apply the latest hotfix rollup of .NET Framework and set strong cryptography for .NET Framework (version 4 or later). The method for setting strong cryptography is same as substeps 1-d and 1-e. You can omit these steps if you choose to install the Session Recording Policy Console on the same computer as the Session Recording Server.

To configure the TLS 1.2 support for SQL Server with versions earlier than 2016, see https://support.microsoft.com/en-us/kb/3135244. To use TLS 1.2, configure HTTPS as the communication protocol for the Session Recording components.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For information about configuring the Session Recording security features, see Configuring Security Features of Session Recording.

## Scalability considerations

March 24, 2020

Session Recording is a highly scalable system that handles thousands or tens of thousands of sessions. Installing and running Session Recording requires few extra resources beyond what is necessary to run XenApp and XenDesktop. However, if you plan to use Session Recording to record a large number of sessions or if the sessions you plan to record can result in large session files (for example, graphically intense applications), consider the performance of your system when planning your Session Recording deployment.

This article explains how Session Recording achieves high scalability and how you can get the most out of your recording system at a lowest cost.

### Why Session Recording scales well

There are two major reasons that Session Recording scales well compared with competitive products:

- Small file size

  A recorded session file made with Session Recording is highly compact. It is many orders of magnitude smaller than an equivalent video recording made with solutions that screen-scrape. The network bandwidth, disk space, and disk IOPS required to transport and store each Session Recording file is typically at least 10 times less than an equivalent video file.

  The small size of recorded session files means faster and smoother rendering of video frames. Recordings are also completely lossless and have no pixelation that is common in most compact video formats. Text in recordings is easy to read during playback as it is in the original sessions. To maintain small file sizes, Session Recording does not record key frames within the files.

- Low processing required to generate files

  A recorded session file contains the ICA protocol data for a session that is extracted virtually in its native format. This means the file captures the ICA protocol data stream that is used to communicate with Citrix Workspace app. There is no need to run expensive transcoding or encoding software components to change the format of data in real time. The low amount of processing is also important for VDA scalability and ensures the end-user experience is maintained when many sessions are recorded from the same VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Moreover, only those ICA virtual channels that are capable of being played back are recorded, which results in a further optimization. For example, the printer and client drive mapping channels are not recorded because they can generate high volumes of data without any benefit in video playback.

### Estimate data input and processing rates

The Session Recording Server is the central collection point for recorded session files. Each machine that is running a multi-session OS VDA with Session Recording enabled sends recorded session data to the Session Recording Server. Session Recording can handle high volumes of data and can tolerate bursts and faults, but there are physical limits on how much data any one server can handle.

Consider how much data you will be sending to each Session Recording Server and how quickly the servers can process and store this data. The rate at which your system can store incoming data must be higher than the data input rate.

To estimate your data input rate, multiply the number of sessions recorded by the average size of each recorded session and divide by the time for which you are recording sessions. For example, you might record 5,000 Microsoft Outlook sessions of 20 MB each over an 8-hour work day. In this case, the data input rate is approximately 3.5 Mbps. (5,000 sessions times 20 MB divided by 8 hours, divided by 3,600 seconds per hour.) A typical Session Recording Server connected to a 100 Mbps LAN with sufficient disk space to store the recorded data is capable of processing data at around 5.0 Mbps based on the physical limits imposed by disk and network IOPS. This is the processing rate. In the example, the processing rate (5.0 Mbps) is higher than the input rate (3.5 Mbps), so recording the 5,000 Outlook sessions is feasible.

Note that the amount of data per session varies greatly depending on what is being recorded, while other factors such as the screen resolution, color depth, and graphics mode also have impacts. A session running a CAD package where graphics activity is constantly high likely generates a much larger recording than a session in which the end user sends and receives emails in Microsoft Outlook. Therefore, recording the same number of CAD sessions can generate an extremely high input rate and require the use of more Session Recording Servers.

### Bursts and faults

The previous example assumes a very simple uniform throughput of data but does not explain how the system deals with short periods of higher activity, known as bursts. A burst might occur when all users log on at the same time in the morning, known as the 9 o'clock rush, or when they receive the same email in their Outlook inbox at once. The 5.0 Mbps processing rate of the Session Recording Server is highly inadequate at dealing with this sudden demand.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The Session Recording Agent running on each VDA uses Microsoft Message Queuing (MSMQ) to send recorded data to the Storage Manager running on the central Session Recording Server. The data is sent in a store-and-forward manner similar to how an email is delivered between the sender, mail server, and the receiver. If the Session Recording Server or the network cannot handle the high rate of data in a burst, the recorded session data is temporarily stored until the backlog of data messages is cleared. The data message might be temporarily stored in the outgoing queue on the VDA if the network is congested, or stored on the Session Recording Server's receiving queue if the data has traversed the network but the Storage Manager is still busy processing other messages.

MSMQ also serves as a fault tolerance mechanism. If the Session Recording Server goes down or the link is broken, recorded data is held in the outgoing queue on each VDA. When the fault is rectified, all queued data is sent together. The use of MSMQ also allows you to take a Session Recording Server offline for upgrade or maintenance without interrupting the recording of existing sessions and losing data.

The main limitation of MSMQ is that disk space for the temporary storage of data messages is finite. This limits how long a burst, fault, or maintenance event can last before data is eventually lost. The overall system can continue after data loss, but in this situation, individual recordings have chunks of data missing. A file with missing data is still playable but only up to the point where data was first lost. Note the following:

- Adding more disk space to each server, especially the Session Recording Server, and making it available to MSMQ can increase the tolerance to bursts and faults.
- It is important to configure the Message Life setting for each Session Recording Agent to an appropriate level (on the **Connections** tab in Session Recording Agent Properties). The default value of 7,200 seconds (two hours) means that each recorded data message has two hours to reach the Storage Manager before it is discarded and recording files are damaged. With more disk space available (or fewer sessions to record), you can choose to increase this value. The maximum value is 365 days.

The other limitation with MSMQ is that when data backlogs, there is extra disk IOPS in the queue to read and write data messages. Under normal conditions, the Storage Manager receives and processes data from the network directly without the data message ever being written to disk. Storing the data involves a single write operation to disk that appends the recorded session file. When data is backlogged, the disk IOPS is tripled: each message must be written to disk, read from disk, and written to file. As the Storage Manager is heavily IOPS bound, the processing rate of the Session Recording Server drops until the backlog of messages is cleared. To mitigate the effects of this extra IOPS, adopt the following recommendations:

- Ensure that the disk on which MSMQ stores messages is different from the recording file storage folders. Even though IOPS bus traffic is tripled, the drop in the true processing rate is never as severe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Have planned outages at off-peak times only. Depending on budget constraints, follow recognized approaches to building high availability servers. The approaches include the use of UPS, dual NICs, redundant switches, and hot swappable memory and disks.

### Design for spare capacity

The data rate of recorded session data is unlikely to be uniform, bursts and faults might occur, and the clearing of message backlogs is expensive in IOPS. For this reason, design each Session Recording Server with plenty of spare capacity. Adding more servers or improving the specification of existing servers, as described in later sections, always gains you extra capacity. The general rule of thumb is to run each Session Recording server at a maximum of 50% of its total capacity. In the earlier example, if the server is capable of processing 5.0 Mbps, target the system to run only at 2.5 Mbps. Instead of recording 5,000 Outlook sessions that generate 3.5 Mbps on one Session Recording Server, reduce this to 3,500 sessions that generate only about 2.5 Mbps.

### Backlogs and live playback

Live playback is when a reviewer opens a session recording for playback while the session is still active. During live playback, the Session Recording Agent responsible for the session switches to a streaming mode for that session, and recording data is sent immediately to the Storage Manager without internal buffering. Because the recording file is constantly updated, the Player can continue to be fed with the latest data from the live session. However, data sent from the Agent to the Storage Manager is through MSMQ, so the queuing rules described earlier apply. A problem can occur in this scenario. When MSMQ is backlogged, the new recorded data available for live playback is queued like all other data messages. The reviewer can still play the file, but viewing latest live recorded data is delayed. If live playback is an important feature for reviewers, ensure a low probability of backlog by designing spare capacity and fault tolerance into your deployment.

### XenApp and XenDesktop scalability

Session Recording never reduces session performance and never stops sessions in response to recorded data backlogs. Maintaining the end-user experience and single-server scalability is paramount in the design of the Session Recording system. If the recording system becomes irreversibly overloaded, recorded session data is discarded. Extensive scalability testing by Citrix reveals that the impact of recording ICA sessions on the performance and scalability of XenApp and XenDesktop servers is low. The size of the impact depends on the platform, memory available, and the graphical nature of the sessions being recorded. With the following configuration, you can expect a single-server scalability impact of between 1% and 5%. In other words, if a server can host 100 users without Session Recording installed, it can host 95–99 users after installation:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 64-bit server with 8 GB RAM running a multi-session OS VDA
- All sessions running Office productivity applications, such as Outlook and Excel
- The use of applications is active and sustained
- All sessions are recorded as configured by the Session Recording policies

If fewer sessions are recorded or session activity is less sustained and more sporadic, the impact is less. In many cases, the scalability impact is negligible and user density per server remains the same. As mentioned earlier, the low impact is due to the simple processing requirements of the Session Recording components installed on each VDA. Recorded data is simply extracted from the ICA session stack and sent as-is to the Session Recording Server through MSMQ. There is no expensive encoding of data.

There is a minor overhead of using Session Recording even when no sessions are recorded. Although the impact is low, if you are sure that no sessions will ever be recorded from a particular server, you can disable recording on that server. Removing Session Recording is one way of doing this. A less invasive approach is to clear the **Enable session recording for this VDA machine** check box on the **Session Recording** tab in Session Recording Agent Properties. If session recording is required in future, reselect this check box.

### Measuring throughput

There are various ways to measure throughput of recorded session data from the sending VDA to the receiving Session Recording Server. One of the simplest and most effective approaches is to observe the size of files that are recorded, and the rate at which disk space on the Session Recording Server is being consumed. The volume of data written to disk closely reflects the volume of network traffic being generated. The Windows Performance Monitor tool (perfmon.exe) has a range of standard system counters that can be observed in addition to some counters provided by Session Recording. Counters can be used to measure throughput, and identify bottlenecks and system problems. The following table outlines some of the most useful performance counters.

| Performance Object | Counter Name | Description |
|---|---|---|
| Citrix Session Recording Agent | Active Recording Count | Indicates the number of sessions that are currently being recorded on a particular VDA. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Performance Object | Counter Name | Description |
| --- | --- | --- |
| Citrix Session Recording Agent | Bytes read from the Session Recording Driver | The number of bytes read from the kernel components responsible for acquiring session data. Useful for determining how much data a single VDA generates for all sessions recorded on that server. |
| Citrix Session Recording Storage Manager | Active Recording Count | Similar to the Citrix Session Recording Agent counter except for the Session Recording Server. Indicates the total number of sessions currently being recorded for all servers. |
| Citrix Session Recording Storage Manager | Message bytes/sec | The throughput of all recorded sessions. Can be used to determine the rate at which the Storage Manager is processing data. If MSMQ is backlogged with messages, the Storage Manager runs at full speed. This value can be used to indicate the maximum processing rate of the Storage Manager. |
| LogicalDisk | Disk Write Bytes/sec | Can be used to measure disk write-through performance. This is important in achieving high scalability for the Session Recording Server. Performance of individual drives can also be observed. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Performance Object | Counter Name | Description |
| --- | --- | --- |
| MSMQ Queue | Bytes in Queue | This counter can be used to determine the amount of data backlogged in the CitrixSmAudData message queue. If this value increases over time, the rate of recorded data received from the network is greater than the rate at which the Storage Manager can process data. This counter is useful for observing the effect of data bursts and faults. |
| MSMQ Queue | Message in Queue | Similar to the Bytes in Queue counter but measures the number of messages. |
| Network Interface | Bytes Total/sec | Can be measured on both sides of the link to observe how much data is generated when sessions are recorded. When measured on the Session Recording Server, this counter indicates the rate at which incoming data is received. Contrasts with the Citrix Session Recording Storage Manager/Message bytes/sec counter that measures the processing rate of data. If network rate is greater than this value, messages build in the message queue. |
| Processor | % Processor Time | Worth monitoring even though CPU is unlikely to be a bottleneck. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Session Recording Server hardware

You can increase the capacity of your deployment by carefully selecting the hardware used for the Session Recording Server. You have two choices: scaling up (by increasing the capacity of each server) or scaling out (by adding more servers). In making either of the choices, your aim is to increase scalability at a lowest cost.

### Scaling up

When examining a single Session Recording Server, consider the following best practices to ensure optimal performance for available budgets. The system is dependent on IOPS. This ensures a high throughput of recorded data from the network onto the disk. So it is important to invest in appropriate network and disk hardware. For a high-performance Session Recording Server, a dual CPU or dual core CPU is recommended but little is gained from any higher specification. 64-bit processor architecture is recommended but an x86 processor type is also suitable. 4 GB of RAM is recommended but again there is little benefit from adding more.

### Scaling out

Even with the best scaling up practices, there are limits to performance and scalability that can be reached with a single Session Recording Server when recording a large number of sessions. It might be necessary to add extra servers to meet the load. You can install more Session Recording Servers on different machines to have the Session Recording Servers work as a load balancing pool. In this type of deployment, the Session Recording Servers share the storage and the database. To distribute the load, point the Session Recording Agents to the load balancer that is responsible for the workload distribution.

## Network capacity

A 100 Mbps network link is suitable for connecting a Session Recording Server. A Gb Ethernet connection might improve performance, but does not result in 10 times greater performance than a 100 Mbps link. In practice, the gain in throughput is significantly less.

Ensure that network switches used by Session Recording are not shared with third-party applications that might compete for available network bandwidth. Ideally, network switches are dedicated for use with the Session Recording Server. If network congestion proves to be the bottleneck, a network upgrade is a relatively inexpensive way to increase the scalability of the system.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Storage

Investment in disk and storage hardware is the single most important factor in server scalability. The faster that data can be written to disk, the higher the performance of the overall system. When selecting a storage solution, take more note of the write performance than the read performance.

Store data on a set of local disks controlled either as RAID by a local disk controller or as a SAN.

> **Note:**
>
> Storing data on a NAS based on file-based protocols such as SMB, CIFS, or NFS has serious performance and security implications. Never use this configuration in a production deployment of Session Recording.

For a local drive setup, aim for a disk controller with built-in cache memory. Caching allows the controller to use elevator sorting during write-back, which minimizes disk head movement and ensures write operations are completed without waiting for the physical disk operation to complete. This can improve write performance significantly at a minimal extra cost. Caching does however raise the problem of data loss after a power failure. To ensure the integrity of data and the file system, consider a battery backup facility for the caching disk controller, which ensures that, if power is lost, the cache is maintained and data is written to disk when power is eventually restored.

Consider using a suitable RAID storage solution. There are many RAID levels available depending on performance and redundancy requirements. The following table specifies each of the RAID levels and how applicable each standard is to Session Recording.

| RAID Level | Type | Minimum Number of Disks | Description |
|---|---|---|---|
| RAID 0 | Striped set without parity | 2 | Provides high performance but no redundancy. Loss of any disk destroys the array. This is a low cost solution for storing recorded session files where the impact of data loss is low. Easy to scale up performance by adding more disks. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| RAID Level | Type | Minimum Number of Disks | Description |
| --- | --- | --- | --- |
| RAID 1 | Mirrored set without parity | 2 | No performance gain over one disk, making it a relatively expensive solution. Use this solution only if a high level of redundancy is required. |
| RAID 3 | Striped set with dedicated parity | 3 | Provides high write performance with redundancy characteristics similar to RAID 5. RAID 3 is recommended for video production and live streaming applications. As Session Recording is this type of application, RAID 3 is most highly recommended but it is not common. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| RAID Level | Type | Minimum Number of Disks | Description |
| --- | --- | --- | --- |
| RAID 5 | Striped set with distributed parity | 3 | Provides high read performance with redundancy but at the cost of slower write performance. RAID 5 is the most common for general purpose usages. But due to the slow write performance, RAID 5 is not recommended for Session Recording. RAID 3 can be deployed at a similar cost but with significantly better write performance. |
| RAID 10 | Mirrored set and striped set | 4 | Provides performance characteristics of RAID 0 with redundancy benefits of RAID 1. An expensive solution that is not recommended for Session Recording. |

RAID 0 and RAID 3 are the most recommended RAID levels. RAID 1 and RAID 5 are popular standards but are not recommended for Session Recording. RAID 10 does provide some performance benefits but is too expensive for the additional gain.

Decide on the type and specification of disk drives. IDE/ATA drives and external USB or Firewire drives are not suitable for use in Session Recording. The main choice is between SATA and SCSI. SATA drives provide reasonably high transfer rates at a reduced cost per MB compared with SCSI drives. However, SCSI drives provide better performance and are more common in server deployments. Server RAID solutions mostly support SCSI drives but some SATA RAID products are now available. When evaluating the specifications of disk drive products, consider the rotational speed of disk and other performance characteristics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Because the recording of thousands of sessions per day can consume significant amounts of disk space, you must choose between overall capacity and performance. From the earlier example, recording 5,000 Outlook sessions over an 8-hour work day consumes about 100 GB of storage space. To store 10 days' worth of recordings (that is, 50,000 recorded session files), you need 1,000 GB (1 TB). This pressure on disk space can be eased by shortening the retention period before archiving or deleting old recordings. If 1 TB of disk space is available, a seven-day retention period is reasonable, ensuring disk space usage remains around 700 GB, with 300 GB remaining as a buffer for busy days. In Session Recording, the archiving and deleting of files is supported with the ICLDB utility and has a minimum retention period of two days. You can schedule a background task to run once a day at some off-peak time. For more information about the ICLDB commands and archiving, see Manage your database records.s

The alternative to using local drive and controllers is to use a SAN storage solution based on block-level disk access. To the Session Recording Server, the disk array appears as a local drive. SANs are more expensive to set up, but as the disk array is shared, SANs do have the advantage of simplified and centralized management. There are two main types of SAN: Fibre Channel and iSCSI. iSCSI is essentially SCSI over TCP/IP and is gaining popularity over Fibre Channel since the introduction of Gb Ethernet.

### Database scalability

The Session Recording Database requires Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, or Microsoft SQL Server 2008 R2. The volume of data sent to the database is small because the database stores only metadata about the recorded sessions. The files of the recorded sessions themselves are written to a separate disk. Typically, each recorded session requires only about 1 KB of space in the database, unless the Session Recording Event API is used to insert searchable events to the session.

The Express Editions of Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, and Microsoft SQL Server 2008 R2 impose a database size limitation of 10 GB. At 1 KB per recording session, the database can catalog about 4,000,000 sessions. Other editions of Microsoft SQL Server have no database size restrictions and are limited only by available disk space. As the number of sessions in the database increases, performance of the database and speed of searches diminishes only negligibly.

If you are not making customizations through the Session Recording Event API, each recorded session generates four database transactions: two when recording starts, one when the user logs on to the session being recorded, and one when recording ends. If you use the Session Recording Event API to customize sessions, each searchable event recorded generates one transaction. Because even the most basic database deployment can handle hundreds of transactions per second, the processing load on the database is unlikely to be stressed. The impact is light enough that the Session Recording

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Database can run on the same SQL Server as other databases, including the XenApp or XenDesktop data store database.

If your Session Recording deployment requires many millions of recorded sessions to be cataloged in the database, follow Microsoft guidelines for SQL Server scalability.

## Install, upgrade, and uninstall Session Recording

October 29, 2018

This chapter details how to install Session Recording by using the XenApp/XenDesktop installer. It contains the following sections:

Installation checklist

Install the Session Recording Administration components

Configure Director to use the Session Recording Server

Install the Session Recording Agent

Install the Session Recording Player

Automate installations

Upgrade Session Recording

Uninstall Session Recording

### Installation checklist

As of version 7.14, you can install the Session Recording components by using the XenApp/XenDesktop installer.

Before you start the installation, complete this list:

| ☒ | Step |
| --- | --- |
| | Select the machines on which you want to install each Session Recording component and ensure that each computer meets the hardware and software requirements for the component or components to be installed on it. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| | Step |
|---|---|
| | Use your Citrix account credentials to access the XenApp and XenDesktop download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.<br>To use the TLS protocol for communication between the Session Recording components, install the correct certificates in your environment.<br>Install any hotfixes required for the Session Recording components. The hotfixes are available from the Citrix Support.<br>Configure Director to create and activate the Session Recording policies. For more information, see Configure Director to use the Session Recording Server. |

**Note:**

- Citrix recommends that you divide the published applications into separate Delivery Groups based on your recording policies because session sharing for published applications can conflict with active policies if they are in the same Delivery Group. Session Recording matches the active policy with the first published application that a user opens.
- If you are planning to use Machine Creation Services (MCS) or Provisioning Services, prepare a unique QMId. Failure to comply can cause recording data losses.
- SQL Server requires that TCP/IP is enabled, the SQL Server Browser service is running, and Windows Authentication is used.
- To use HTTPS, configure server certificates for TLS/HTTPS.
- Ensure that users under **Local Users and Groups** > **Groups** > **Users** have write permission to the C:\windows\Temp folder.

### Install the Session Recording Administration components

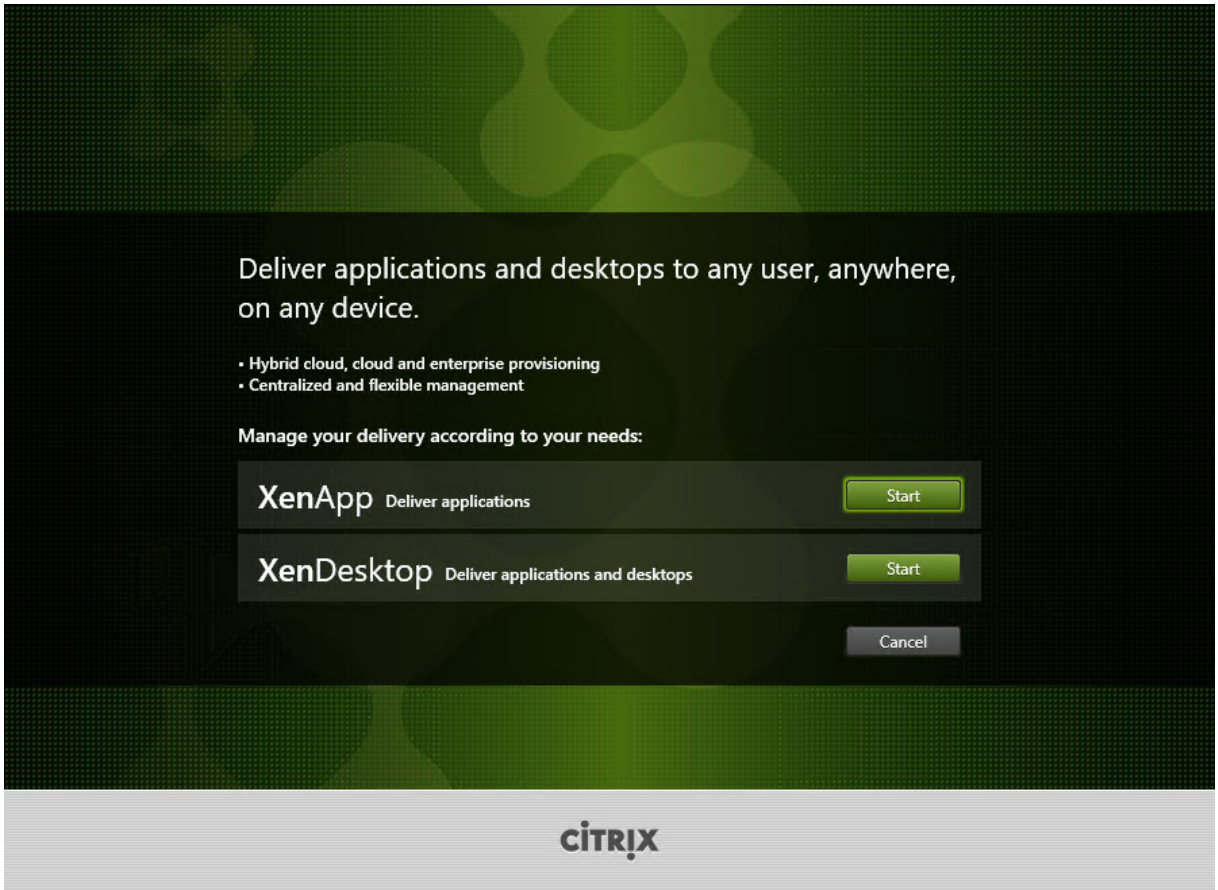
Citrix recommends you install the Session Recording Administration, Session Recording Agent, and Session Recording Player components on separate servers. The Session Recording Administration components include the Session Recording Database, Session Recording Server, and Session Recording Policy Console. You can choose which of these components to install on a server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 1: Download the product software and launch the wizard**

1. If you have not downloaded the XenApp and XenDesktop ISO yet, use your Citrix account credentials to access the XenApp and XenDesktop download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.
2. Use a local administrator account to log on to the machine where you are installing the Session Recording Administration components. 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.

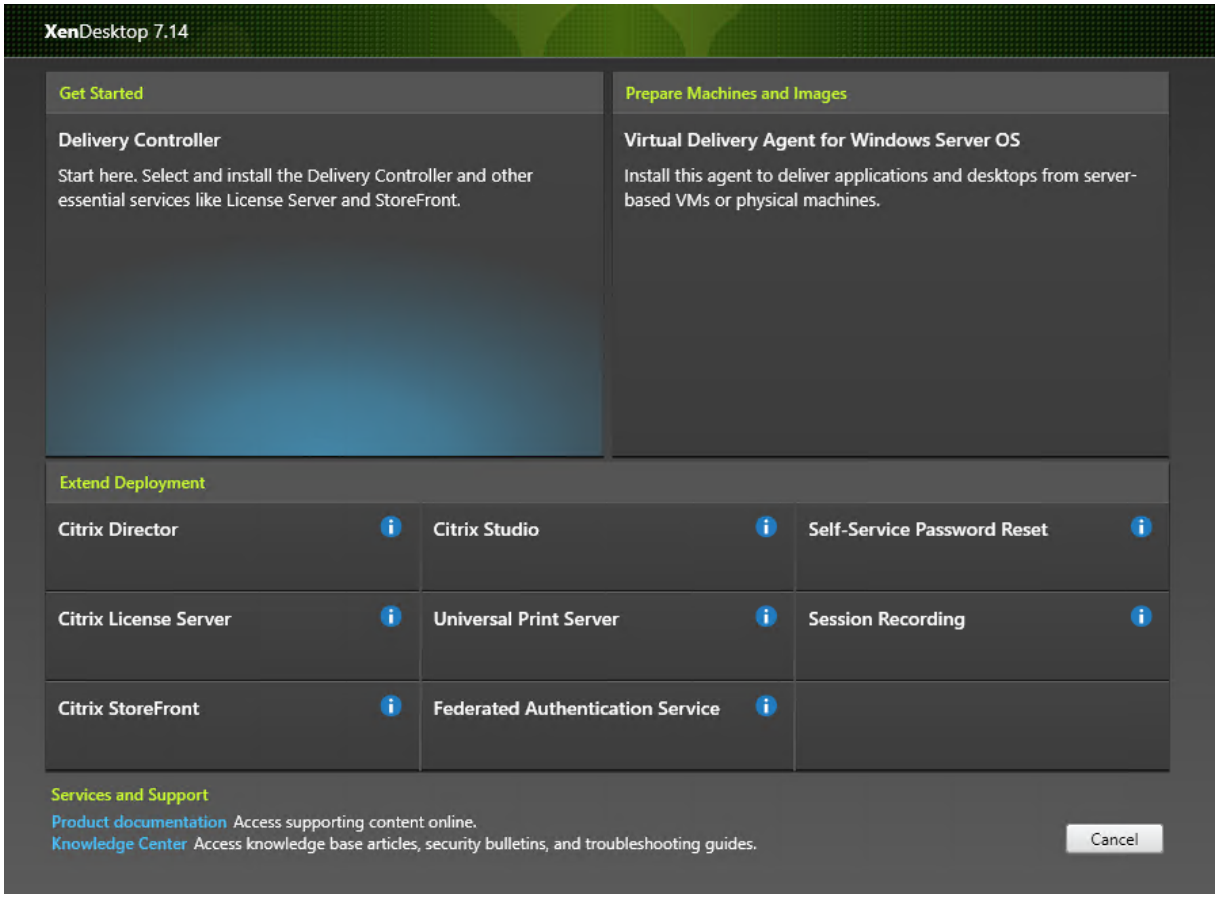
**Step 2: Choose which product to install**




Click **Start** next to the product to install: **XenApp** or **XenDesktop**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

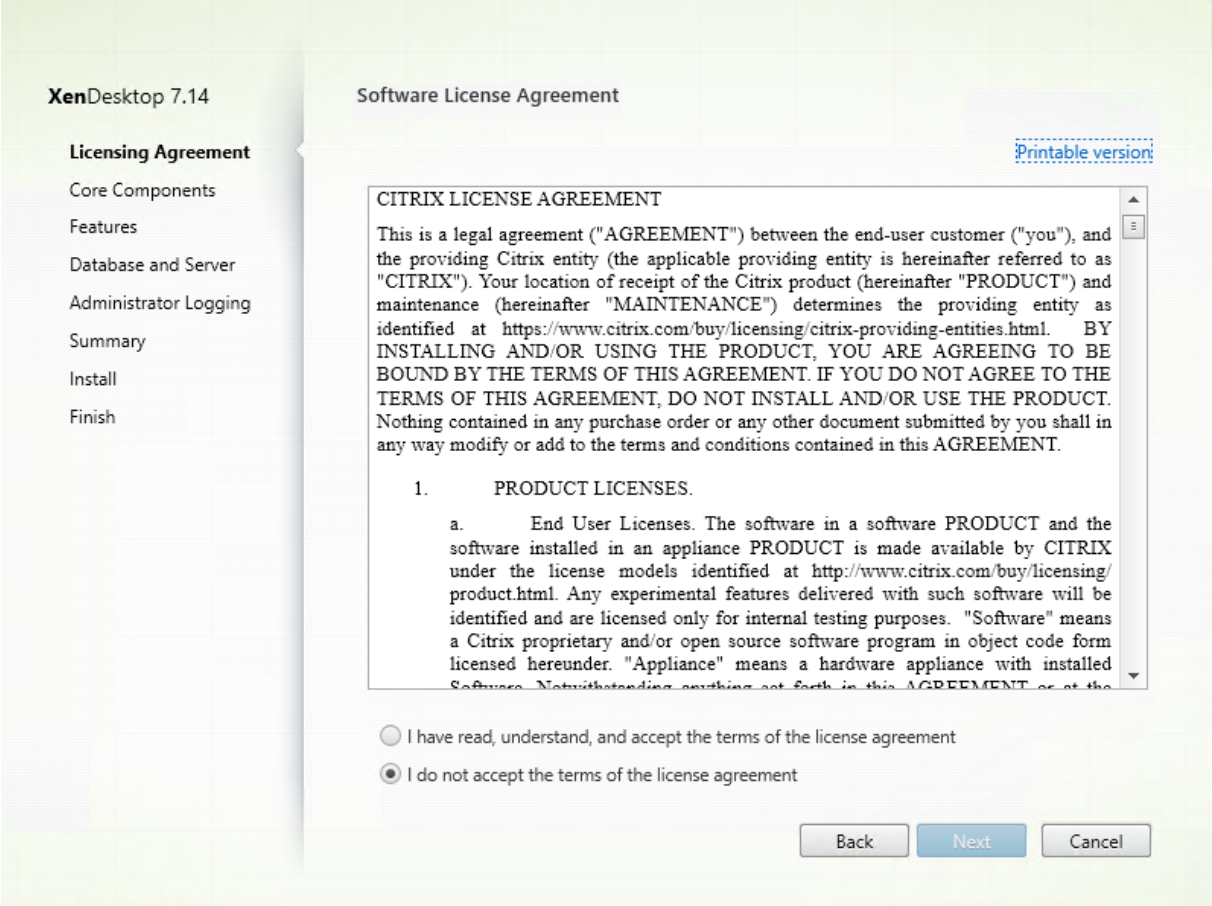
### Step 3: Select Session Recording




Select the **Session Recording** entry.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

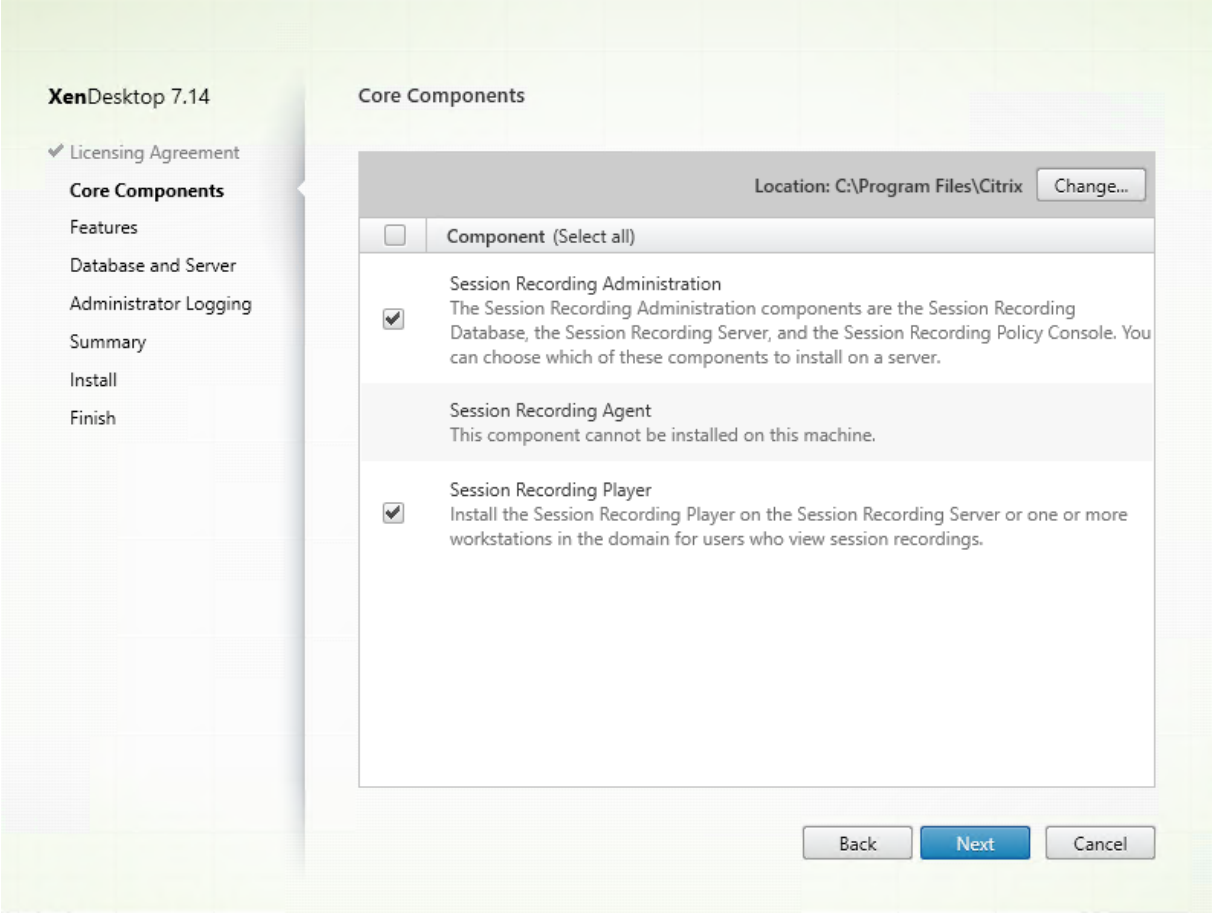
### Step 4: Read and accept the license agreement




On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 5: Select the components to install and the installation location**

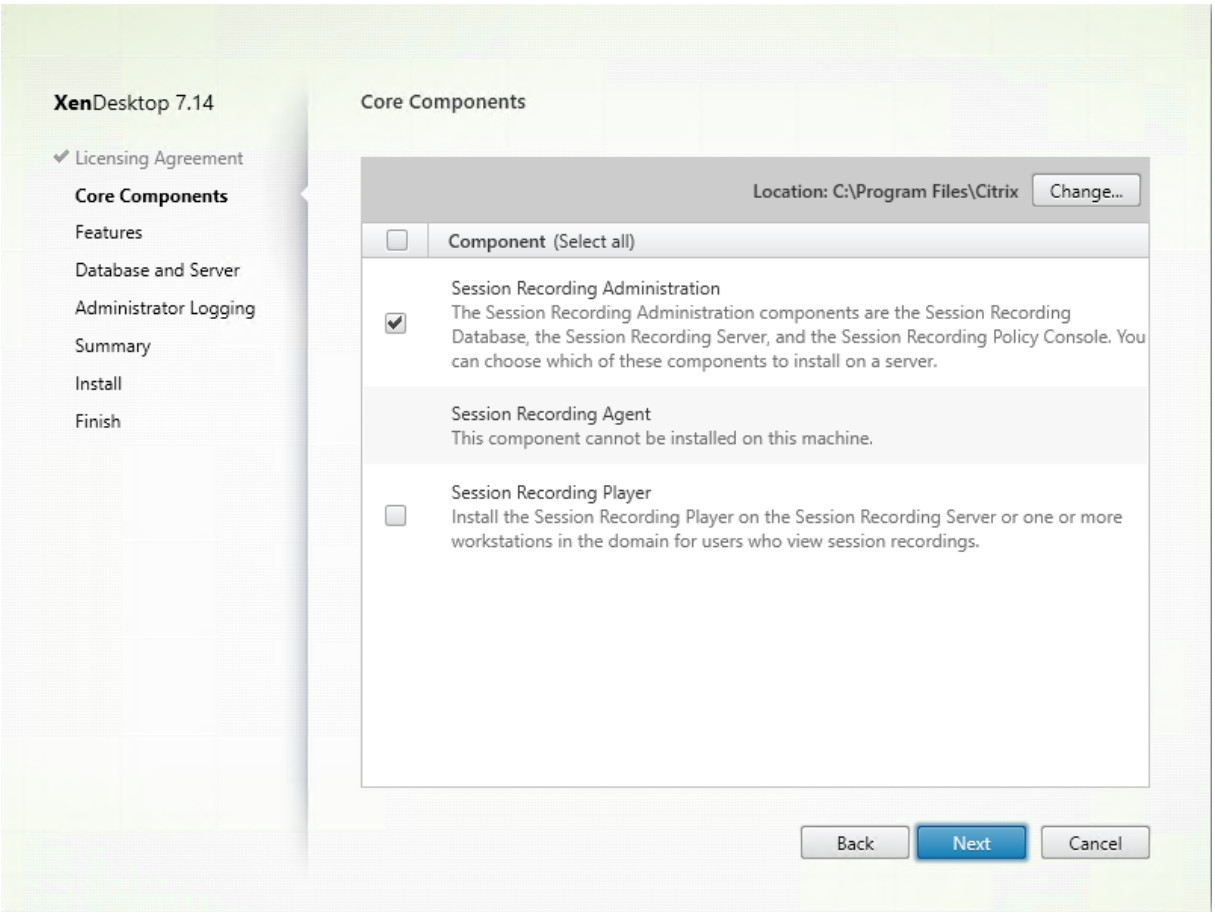



On the **Core Components** page:

- **Location**: By default, components are installed in C:\Program Files\Citrix. The default location works for most deployments. You can specify a custom installation location.
- **Component**: By default, all the check boxes next to the components that can be installed are selected. The installer knows whether it is running on a Desktop OS or a Server OS. It allows the Session Recording Administration components to be installed on a Server OS only, and it does not allow the Session Recording Agent to be installed on a machine that has no VDA installed in advance. If you install the Session Recording Agent on a machine that has no VDA installed in advance, The **Session Recording Agent** option is unavailable.

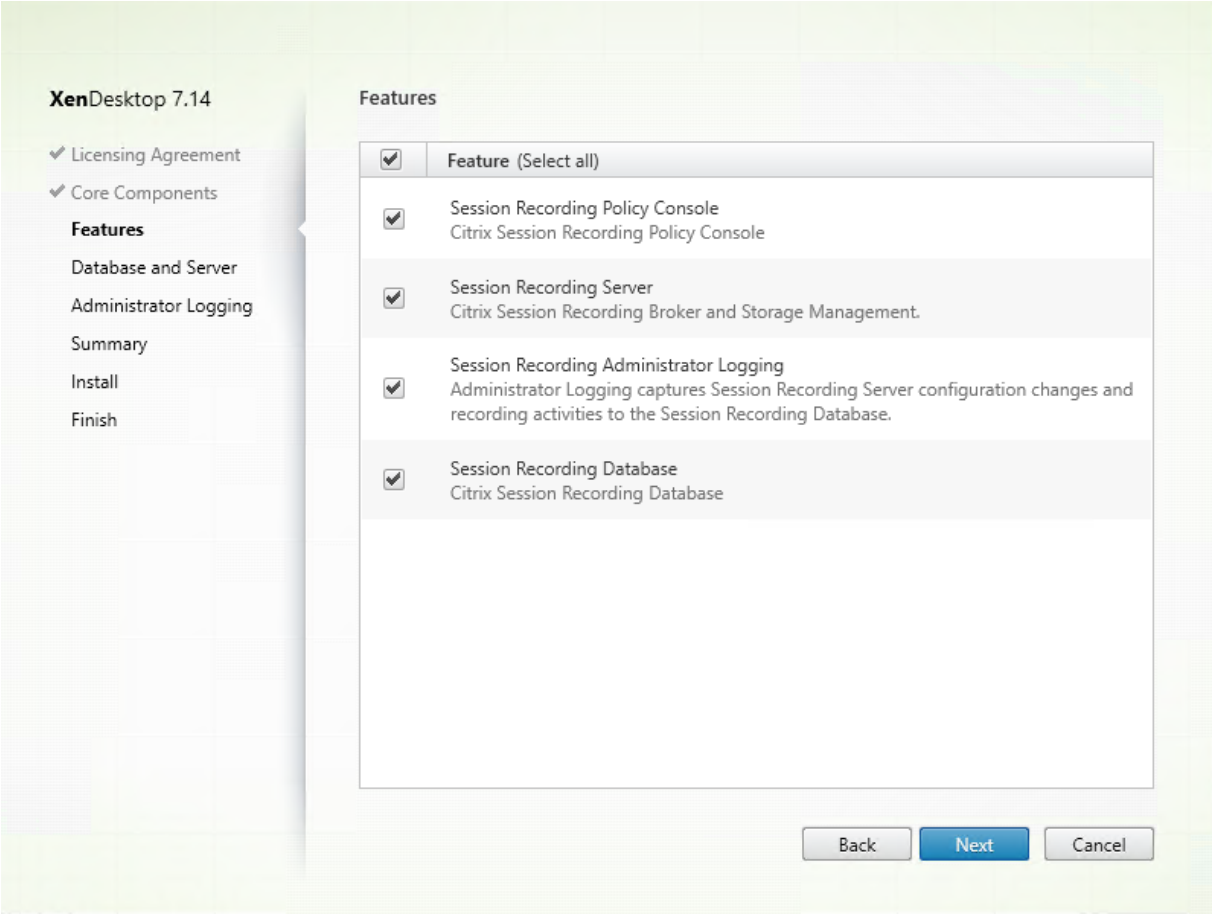
Select **Session Recording Administration** and click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 6: Select the features to install**




On the **Features** page:

- By default, all the check boxes next to the features that can be installed are selected. Installing all these features on a single server is fine for a proof of concept. However, for a large production environment, Citrix recommends you install the Session Recording Policy Console on a separate server and the Session Recording Server, Session Recording Administrator Logging and Session Recording Database on another separate server. Note that the Session Recording Administrator Logging is an optional subfeature of the Session Recording Server. You must select the Session Recording Server before you can select the Session Recording Administrator Logging.
- To add another feature on the same server after you select and install a feature or features on it, you can only run the msi package but cannot run the installer again.

Select the feature or features you want to install and click **Next**.

**Step 6.1: Install the Session Recording Database** **Note:** Session Recording Database is not an actual database. It is a component responsible for creating and configuring the required databases in the Microsoft SQL Server instance during installation. Session Recording supports three solutions for

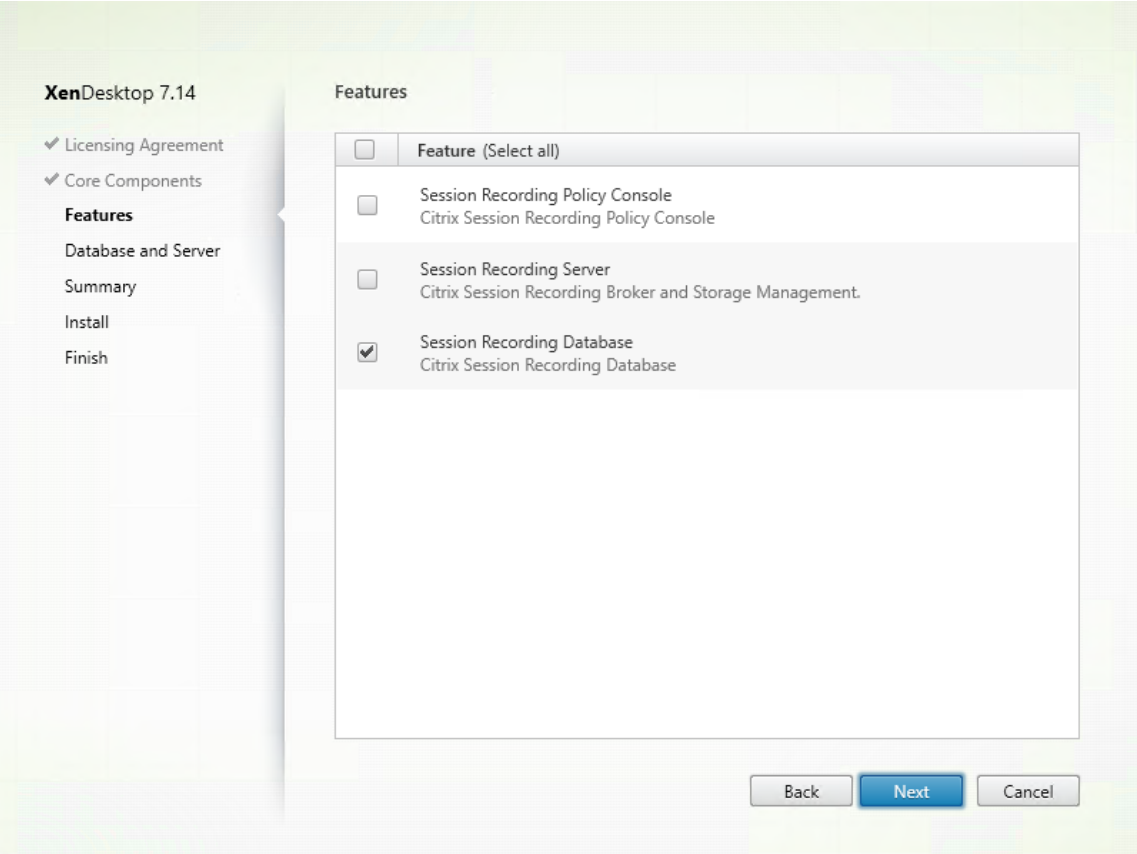
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

database high availability based on Microsoft SQL Server. For more information, see Install Session Recording with database high availability.

There are typically three types of deployments for the Session Recording Database and Microsoft SQL Server:

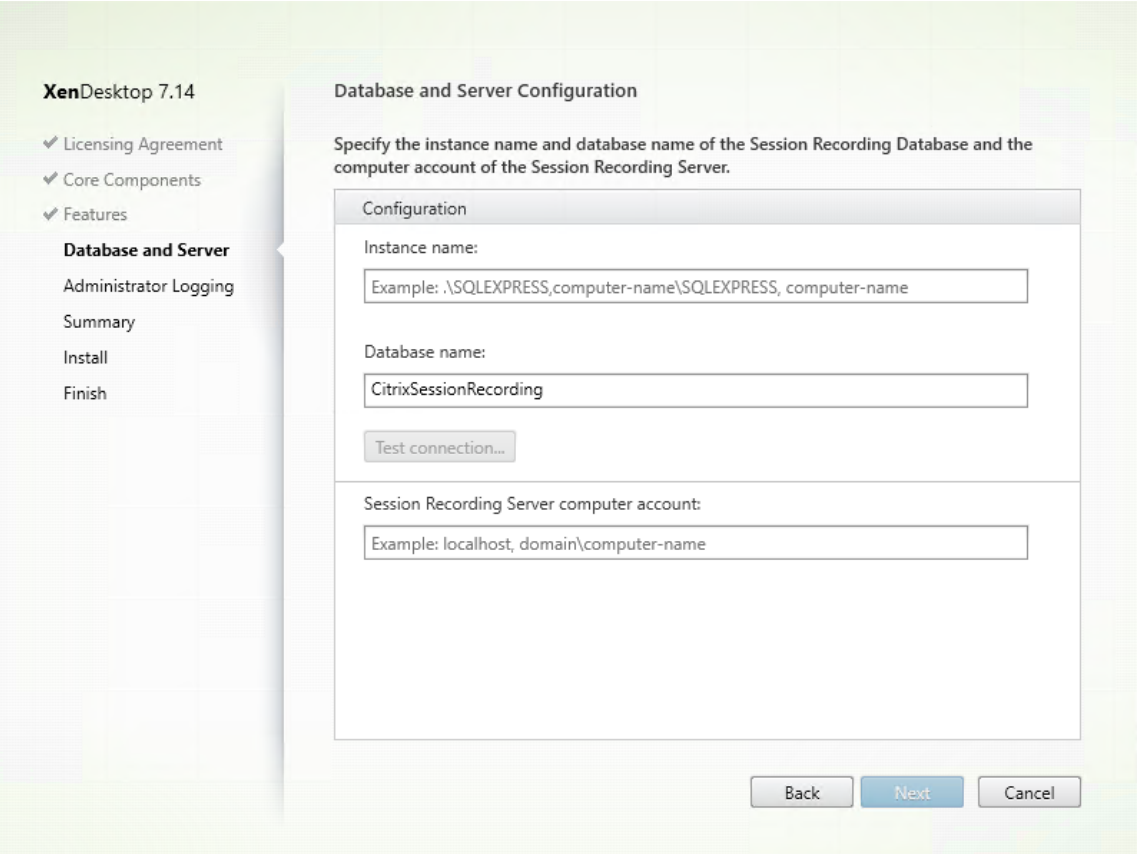
- Deployment 1: Install the Session Recording Server and Session Recording Database on the same machine and the Microsoft SQL Server on a remote machine. (**Recommended**)
- Deployment 2: Install the Session Recording Server, Session Recording Database, and Microsoft SQL Server on the same machine.
- Deployment 3: Install the Session Recording Server on a machine and install both the Session Recording Database and Microsoft SQL Server on another machine. (**Not recommended**)

1. On the **Features** page, select **Session Recording Database** and click **Next**.




2. On the **Database and Server Configuration** page, specify the instance name and database name of the Session Recording Database and the computer account of the Session Recording Server. Click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




On the **Database and Server Configuration** page:

- **Instance name**: If the database instance is not a named instance as you configured when you set up the instance, you can use only the computer name of the SQL Server. If you have named the instance, use computer-name\instance-name as the database instance name. To determine the server instance name you are using, run **select @@servername** on the SQL Server. The return value is the exact database instance name. If your SQL server is configured to be listening on a custom port (other than the default port 1433), set the custom listener port by appending a comma to the instance name. For example, type **DXSBC-SRD-1,2433** in the **Instance name** text box, where 2433, following the comma, denotes the custom listener port.
- **Database name**: Type a custom database name in the **Database name** text box or use the default database name preset in the text box. Click **Test connection** to test the connectivity to the SQL Server instance and the validity of the database name.

> **Important:**
>
> A custom database name must contain only A-Z, a-z, and 0-9, and cannot exceed 123 characters.

- You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
- Or, use the SessionRecordingAdministrationx64.msi package (unzip the ISO file, and you can find this msi package under …\x64\Session Recording). During the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Enter the correct credentials and then click **OK** to continue the installation.

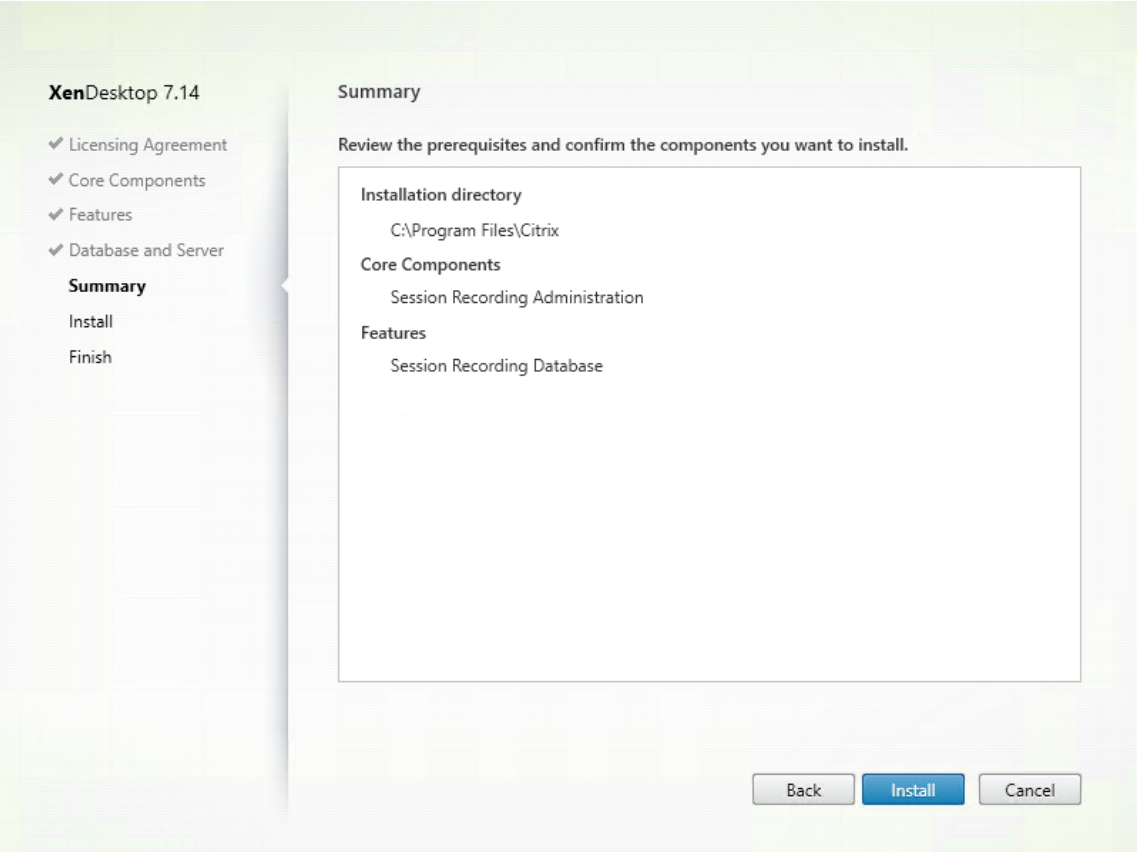
  The installation creates the new Session Recording Database and adds the machine account of the Session Recording Server as **db_owner**.

- **Session Recording Server computer account**
  - **Deployments 1 and 2**: Type **localhost** in the **Session Recording Server computer account** field.
  - **Deployment 3**: Type the name of the computer hosting the Session Recording Server in the format of domain\computer-name. The Session Recording Server computer account is the user account for accessing the Session Recording Database.

  **Note:** Attempts to install the Session Recording Administration components can fail with error code 1603 when a domain name is set in the **Session Recording Server computer account** field. As a workaround, type **localhost** or NetBIOS domain name\machine name in the **Session Recording Server computer account** field.

3. Review the prerequisites and confirm the installation.

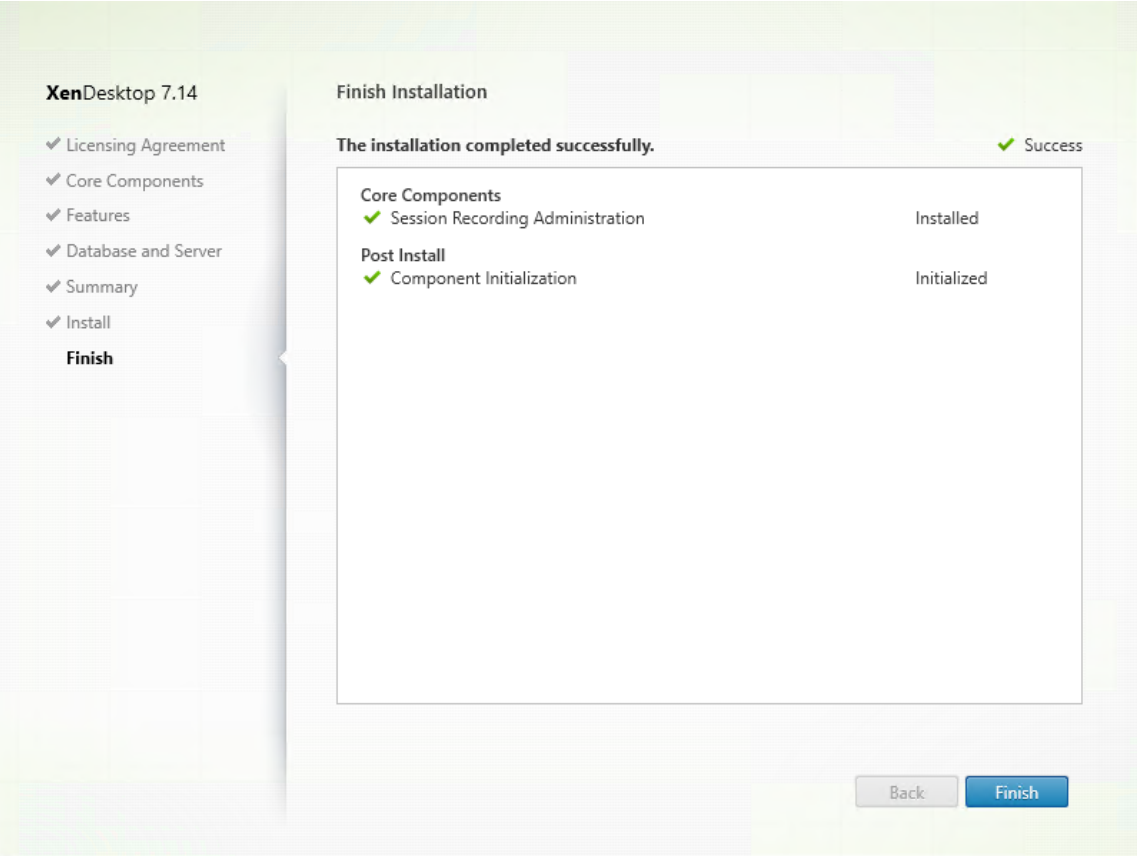
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes. Or, click **Install** to start the installation.

4. Complete the installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



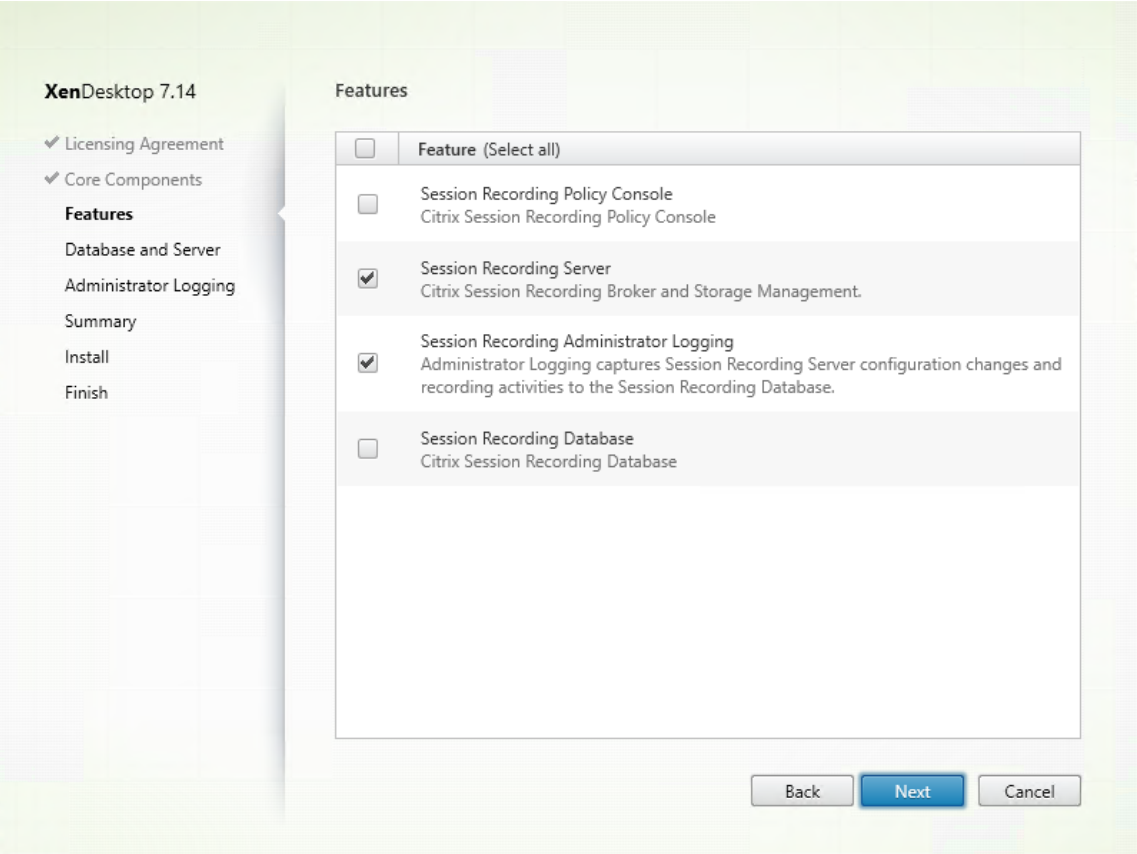

The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording Database.

### Step 6.2: Install the Session Recording Server

1. On the **Features** page, select **Session Recording Server** and **Session Recording Administrator Logging**. Click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

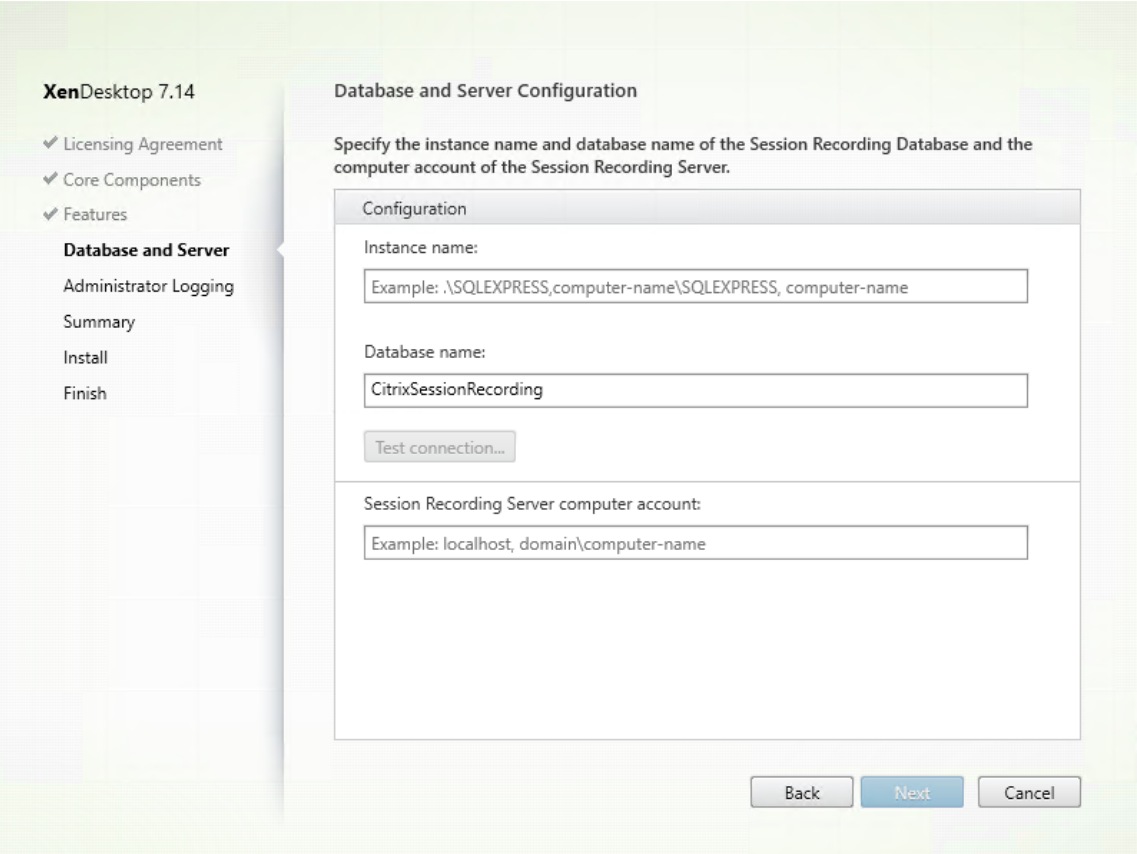



**Note:**

- The Session Recording Administrator Logging is an optional subfeature of the Session Recording Server. You must select the Session Recording Server before you can select the Session Recording Administrator Logging.
- Citrix recommends you install the Session Recording Administrator Logging together with the Session Recording Server at the same time. If you don't want the Administrator Logging feature to be enabled, you can disable it on a later page. However, if you choose not to install this feature at the beginning but want to add it later, you can only manually add it by using the SessionRecordingAdministrationx64.msi package.

2. On the **Database and Server Configuration** page, specify the configurations.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



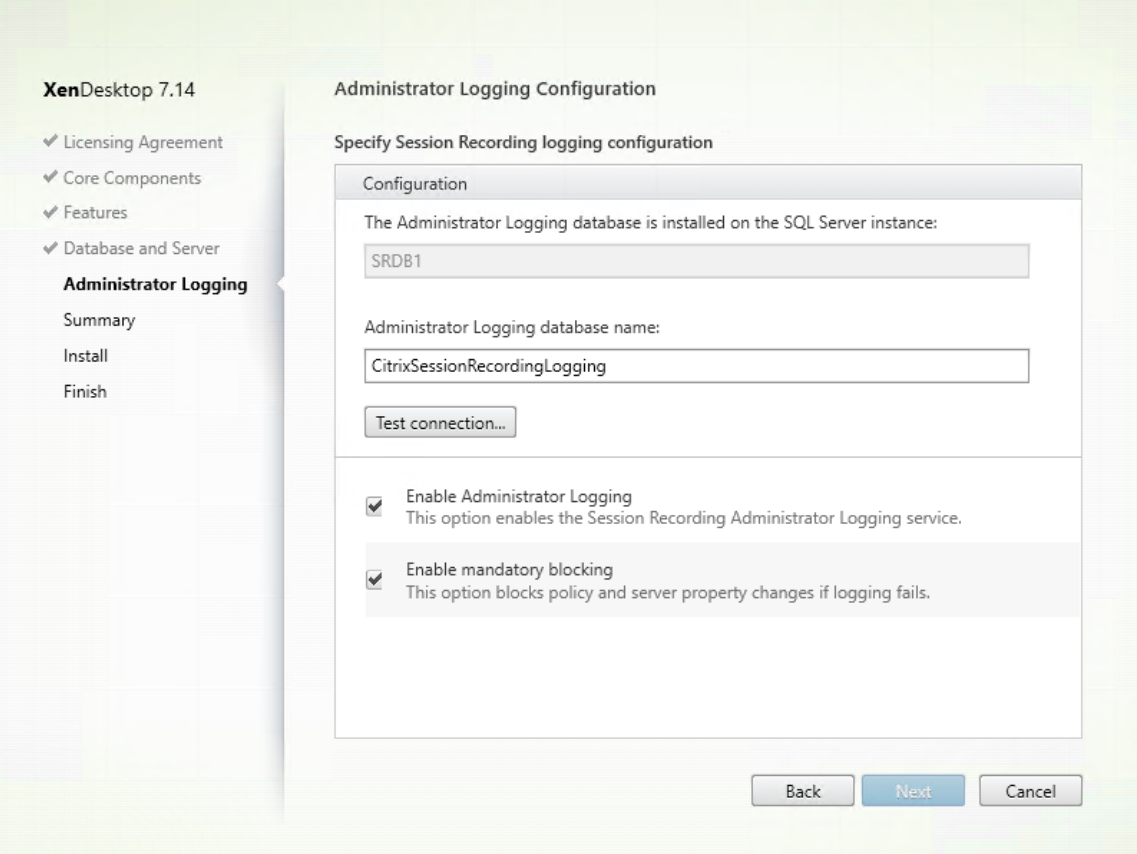

On the **Database and Server Configuration** page:

- **Instance name**: Type the name of your SQL Server in the **Instance name** text box. If you are using a named instance, type computer-name\instance-name; otherwise, type computer-name only. If your SQL server is configured to be listening on a custom port (other than the default port 1433), set the custom listener port by appending a comma to the instance name. For example, type **DXSBC-SRD-1,2433** in the **Instance name** text box, where 2433, following the comma, denotes the custom listener port.
- **Database name**: Type a custom database name in the **Database name** text box or use the default database name **CitrixSessionRecording** that is preset in the text box.
- You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:
  - Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
  - Or, use the SessionRecordingAdministrationx64.msi package to install the Session Recording Server. During the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Enter the correct credentials and then click **OK** to continue the installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- After typing the correct instance name and database name, click **Test connection** to test the connectivity to the Session Recording Database.
- Enter the Session Recording Server computer account, and then click **Next**.

3. On the **Administration Logging Configuration** page, specify configurations for the Administration Logging feature.




On the **Administration Logging Configuration** page:

- **The Administration Logging database is installed on the SQL Server instance**: This text box is not editable. The SQL Server instance name of the Administration Logging database is automatically grabbed from the instance name that you typed on the **Database and Server Configuration** page.
- **Administrator Logging database name**: If you choose to install the Session Recording Administrator Logging feature, type a custom database name for the Administrator Logging database in this text box or use the default database name **CitrixSessionRecordingLogging** that is preset in the text box.
  **Note:** The Administrator Logging database name must be different from the Session Recording Database name that is set in the **Database name** text box on the previous, **Database and Server Configuration** page.
- After typing the Administrator Logging database name, click **Test connection** to test the

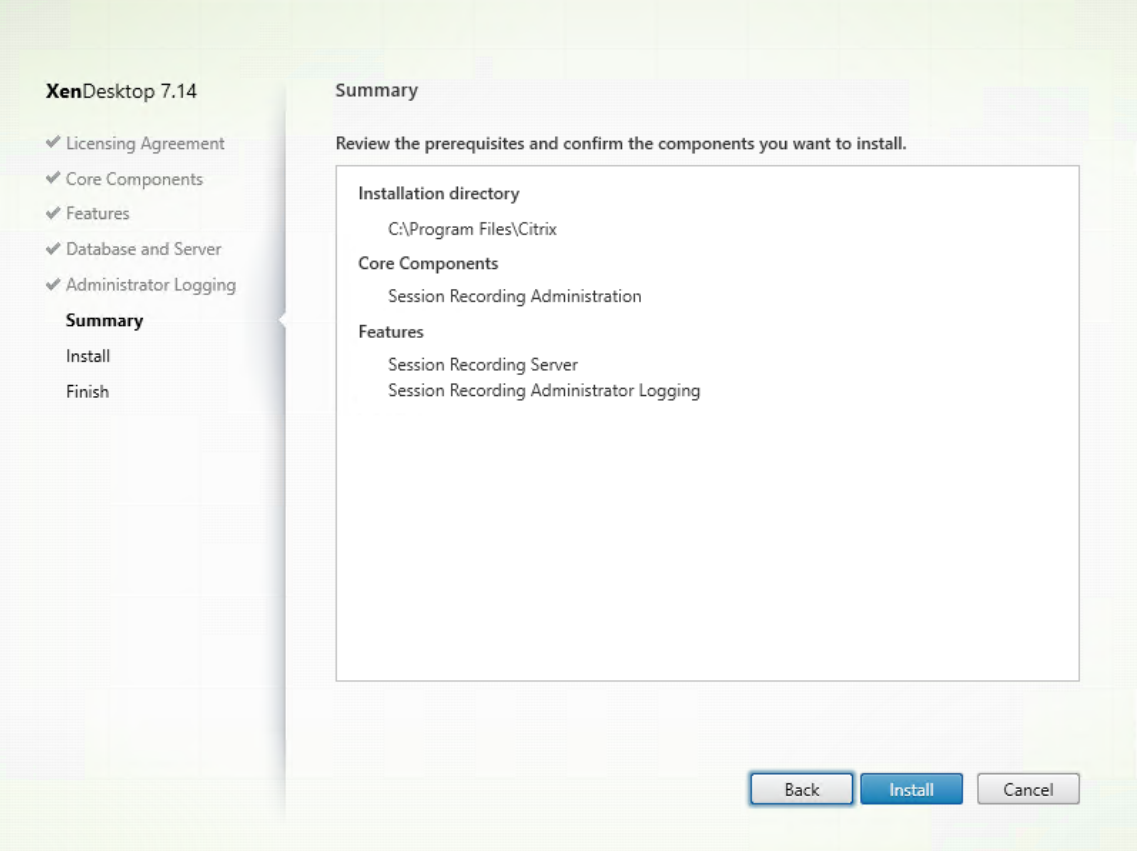
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

connectivity to the Administrator Logging database.

- **Enable Administration Logging**: By default, the Administration Logging feature is enabled. You can disable it by clearing the check box.
- **Enable mandatory blocking**: By default, mandatory blocking is enabled. the normal features might be blocked if logging fails. You can disable mandatory blocking by clearing the check box.

Click **Next** to continue the installation.

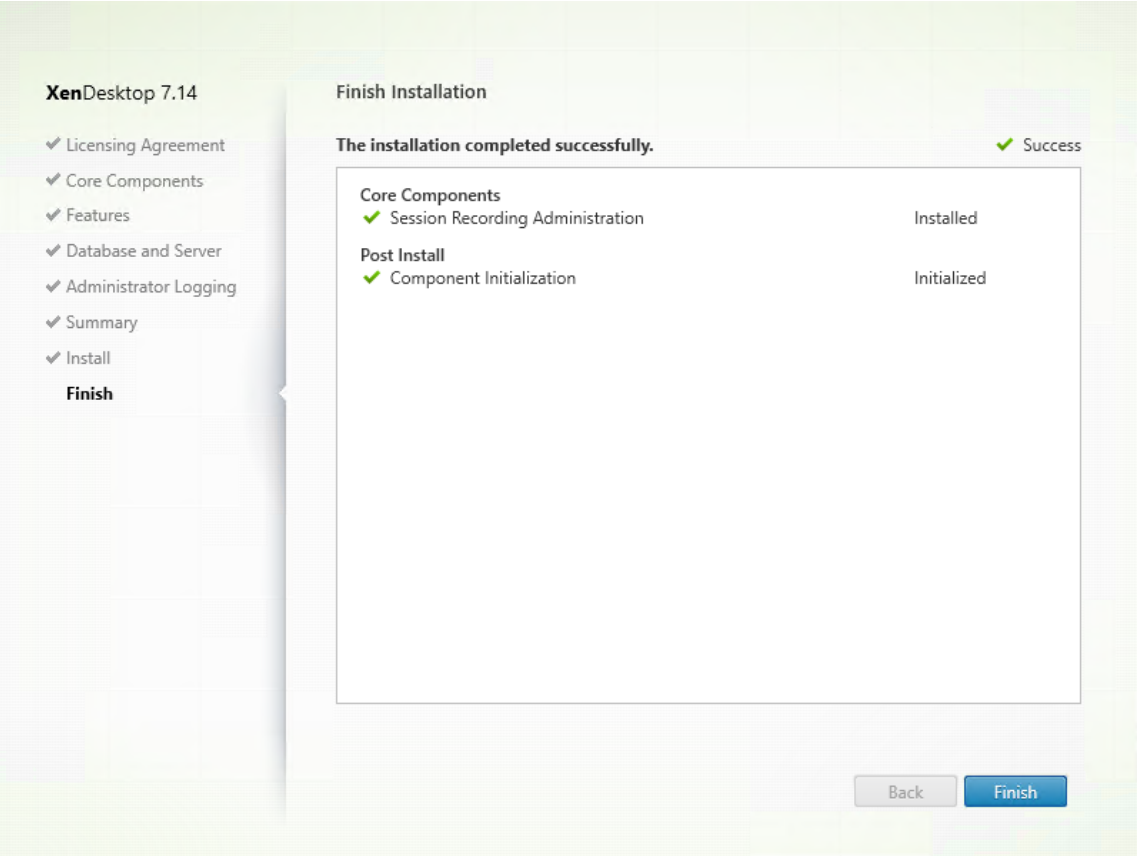
4. Review the prerequisites and confirm the installation.




The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes. Or, click **Install** to start the installation.

5. Complete the installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

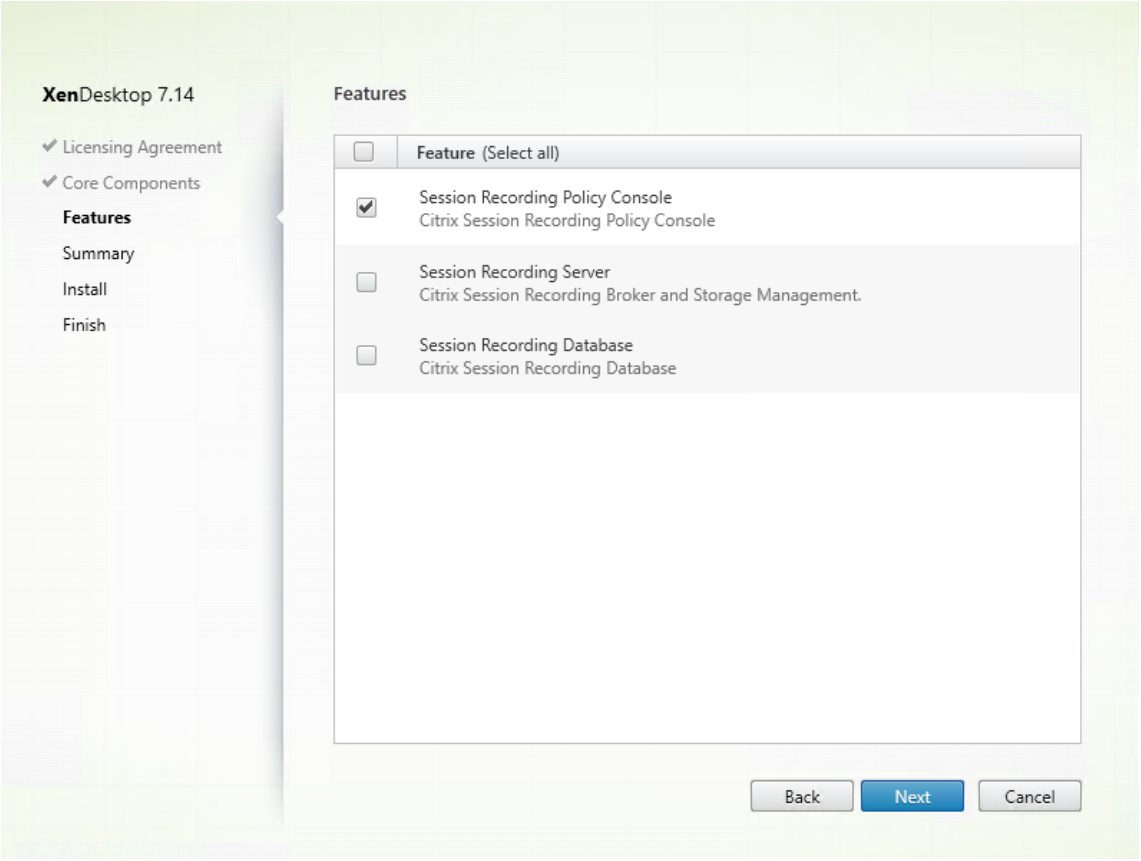
Click **Finish** to complete the installation of the Session Recording Server.

**Note:** The Session Recording Server default installation uses HTTPS/TLS to secure communications. If TLS is not configured in the default IIS site of the Session Recording Server, use HTTP. To do so, cancel the selection of SSL in the IIS Management Console by navigating to the Session Recording Broker site, opening the SSL settings, and clearing the **Require SSL** check box.

### Step 6.3: Install the Session Recording Policy Console

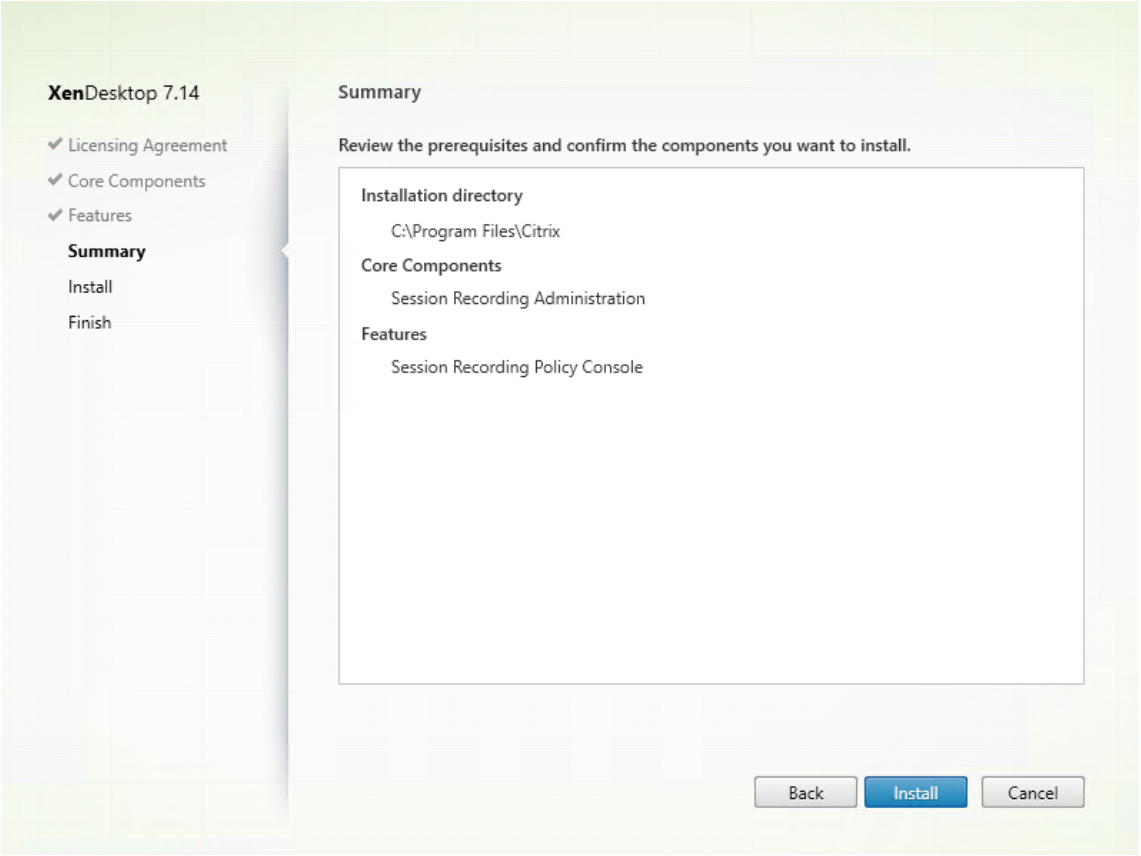
1. On the **Features** page, select **Session Recording Policy Console** and click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




2. Review the prerequisites and confirm the installation.

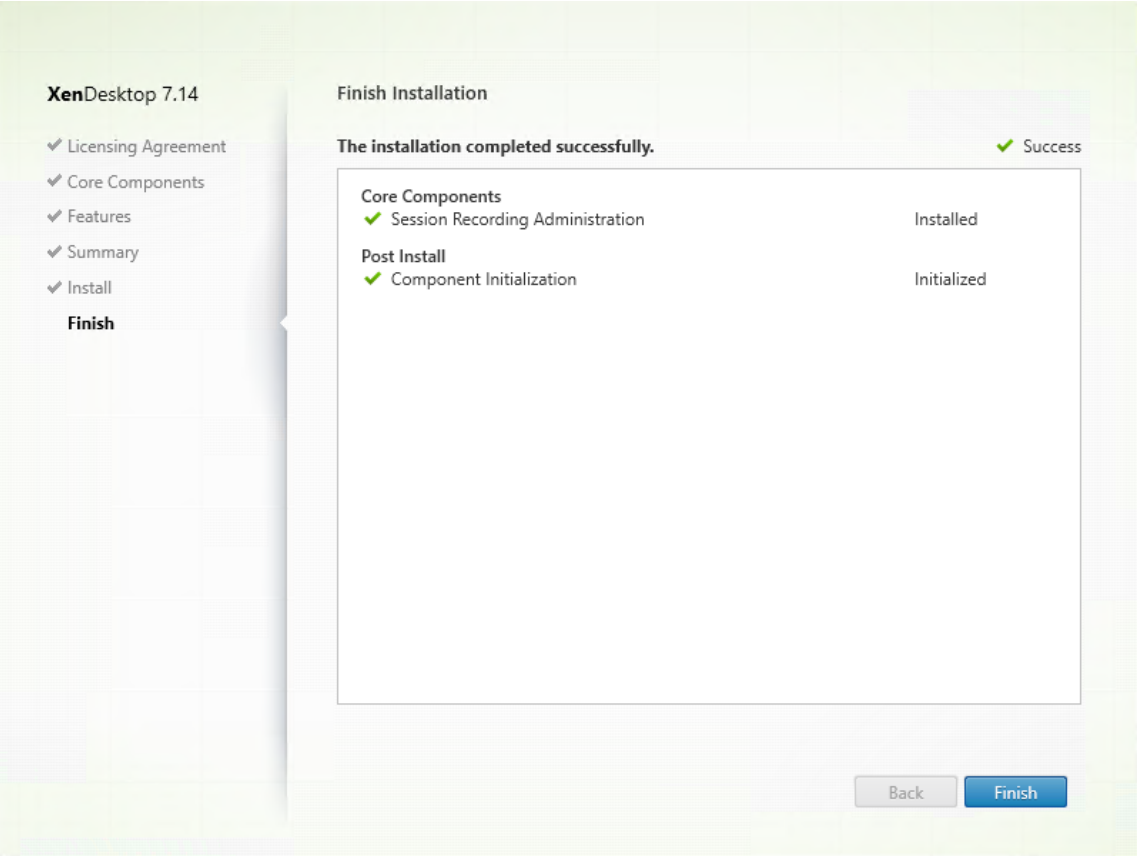
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes. Or, click **Install** to start the installation.

3. Complete the installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The **Finish Installation** page shows green check marks for all the prerequisites and component that have been installed and initialized successfully.

Click **Finish** to complete your installation of the Session Recording Policy Console.

#### Step 7: Install Broker_PowerShellSnapIn_x64.msi

**Important:** To use the Session Recording Policy Console, you must have the Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) installed. The snap-in cannot be automatically installed by the installer. Locate the snap-in on the XenApp/XenDesktop ISO (\layout\image-full\x64\Citrix Desktop Delivery Controller) and follow the instructions for installing it manually. Failure to comply can cause an error.

### Configure Director to use the Session Recording Server

You can use the Director console to create and activate the Session Recording policies.

1. For an HTTPS connection, install the certificate to trust the Session Recording Server in the Trusted Root Certificates of the Director server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. To configure the Director server to use the Session Recording Server, run the **C:\inetpub\wwwroot\Director\ /configsessionrecording** command.
3. Enter the IP address or FQDN of the Session Recording Server and the port number and connection type (HTTP/HTTPS) that the Session Recording Agent uses to connect to the Session Recording Broker on the Director server.

## Install the Session Recording Agent

You must install the Session Recording Agent on the VDA or VDI machine on which you want to record sessions.

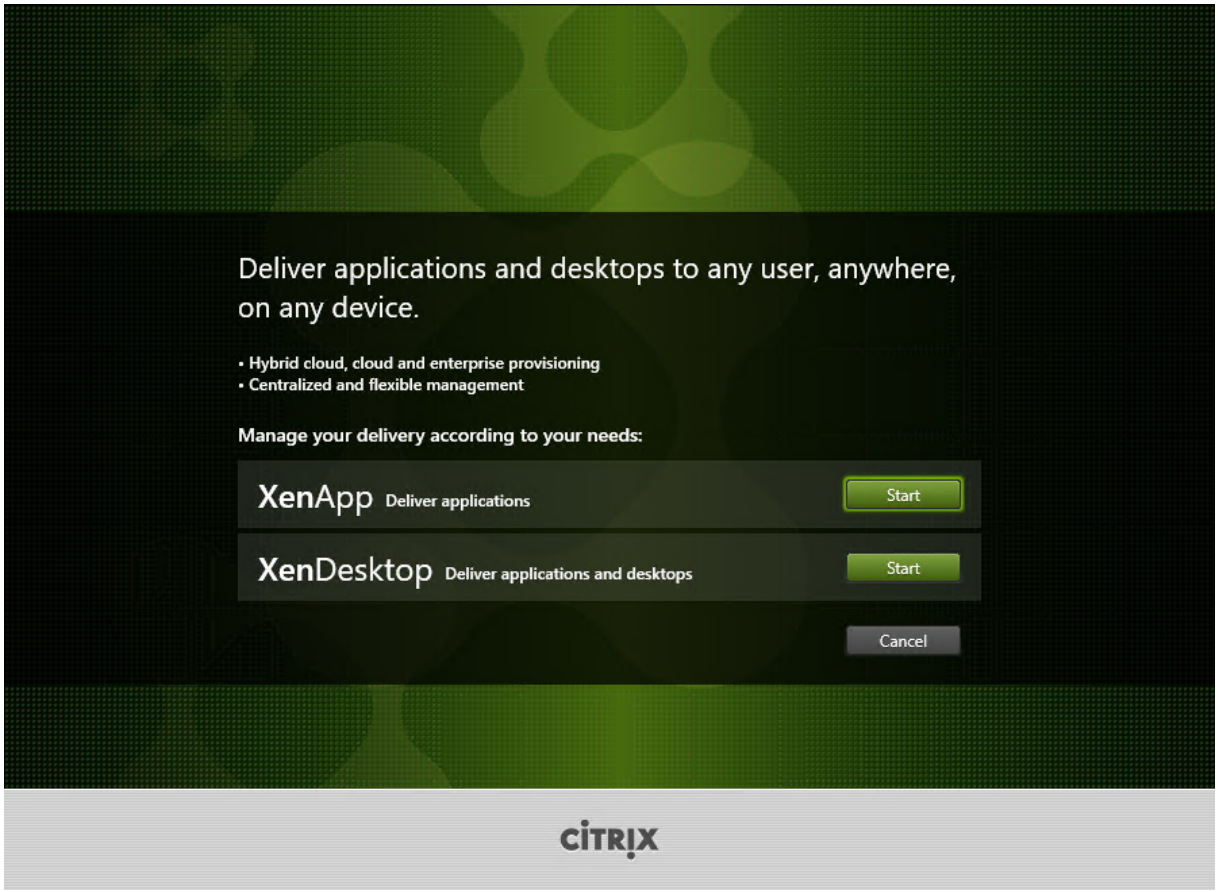
### Step 1: Download the product software and launch the wizard

Use a local administrator account to log on to the machine where you are installing the Session Recording Agent component. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

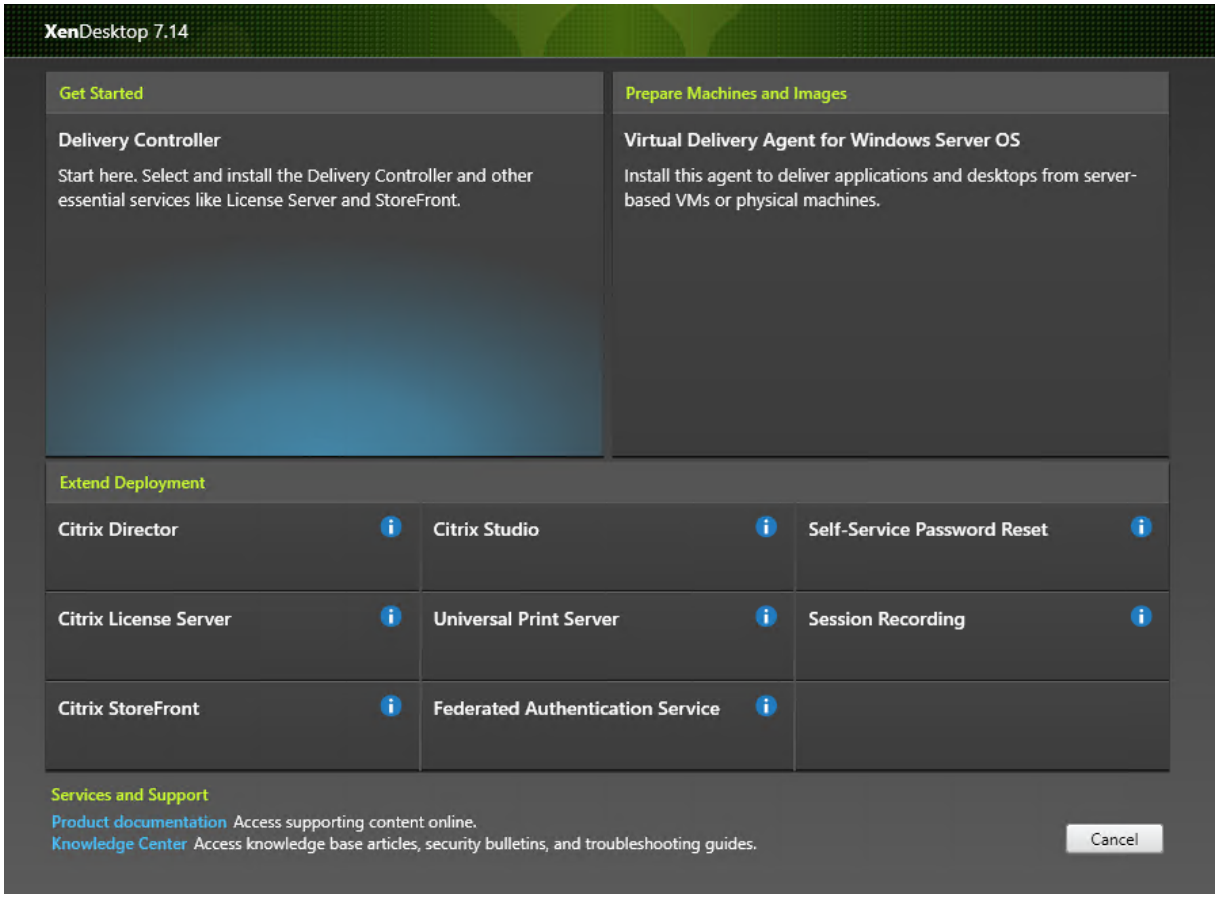
**Step 2: Choose which product to install**




Click **Start** next to the product to install: **XenApp** or **XenDesktop**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

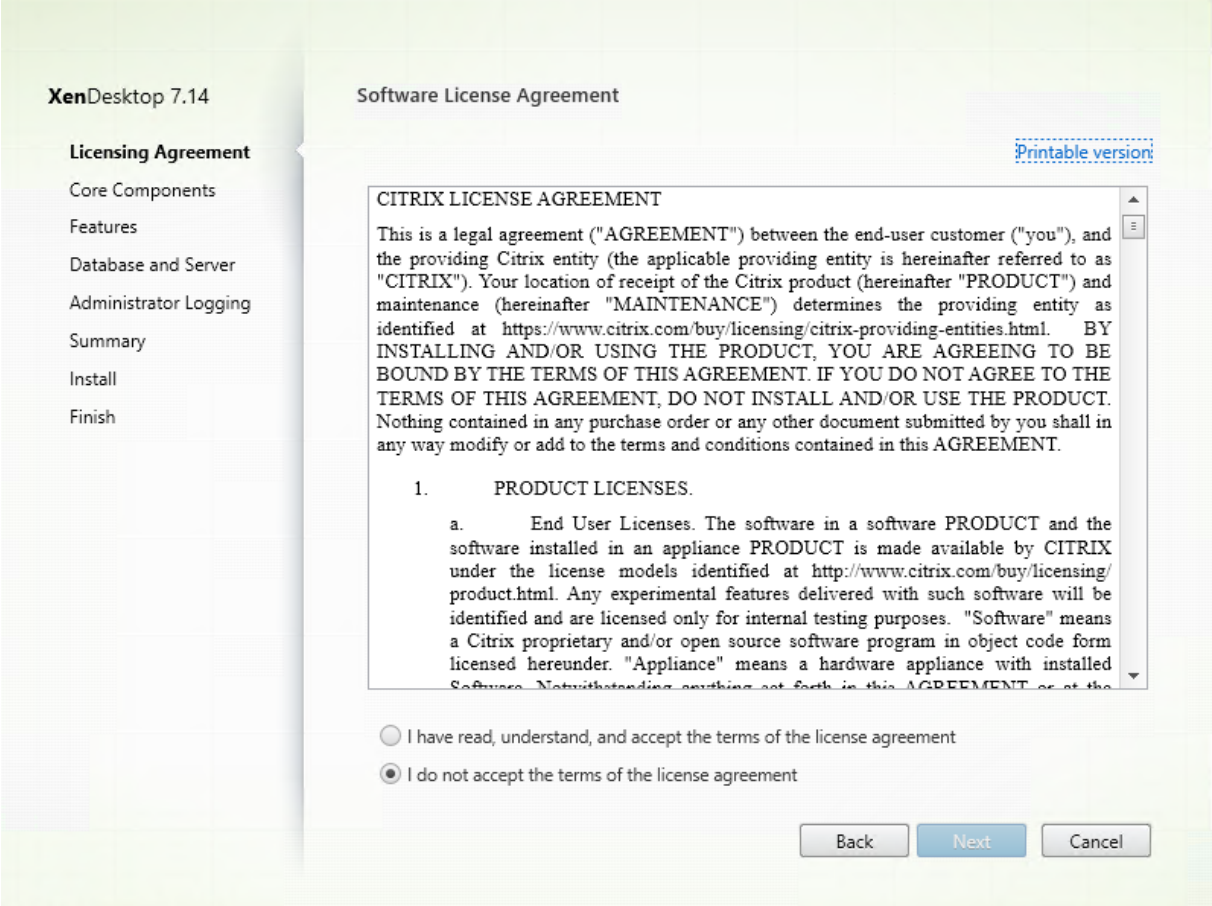
### Step 3: Select Session Recording




Select the **Session Recording** entry.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

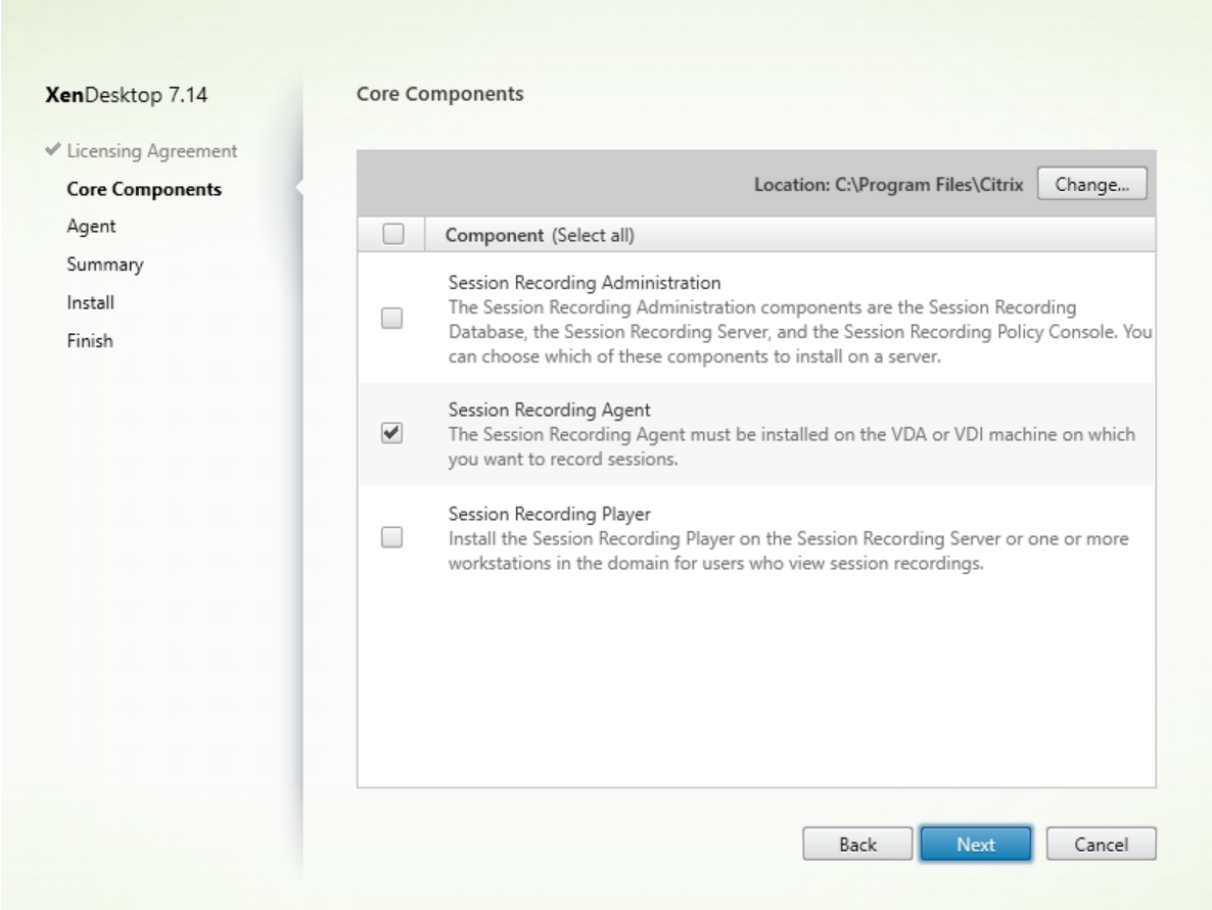
**Step 4: Read and accept the license agreement**




On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

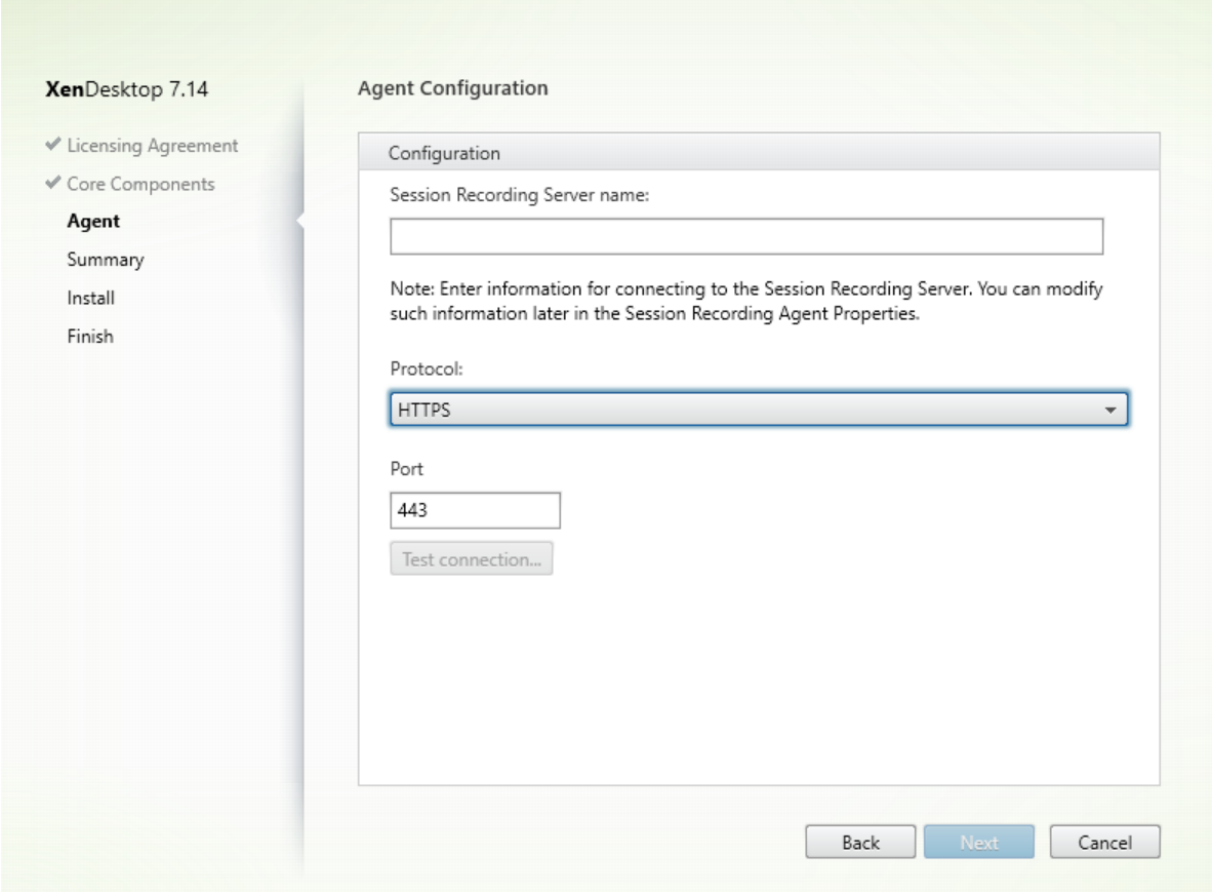
**Step 5: Select the component to install and the installation location**




Select **Session Recording Agent** and click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Step 6: Specify the Agent configuration



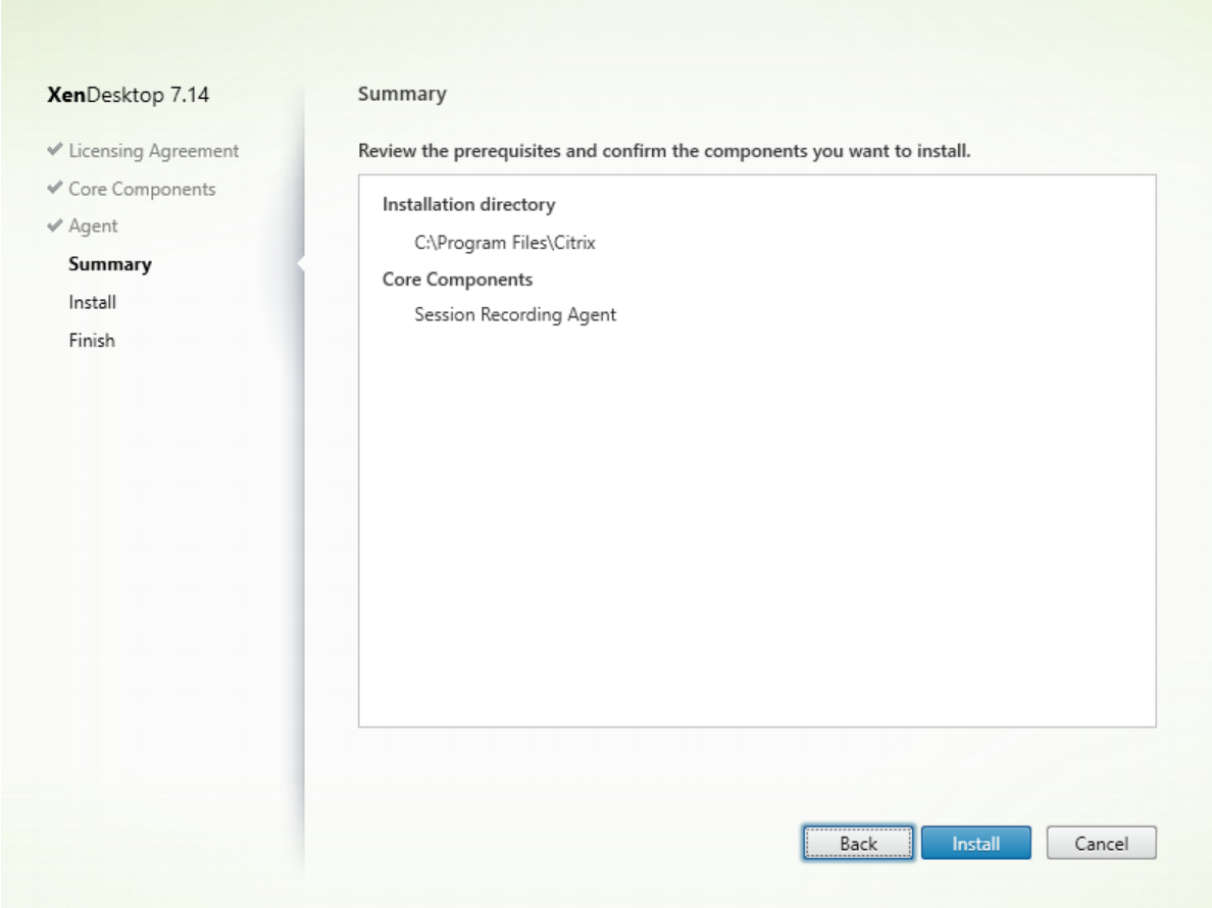

On the **Agent Configuration** page:

- If you have installed the Session Recording Server in advance, enter the name of the computer where you installed the Session Recording Server and the protocol and port information for the connection to the Session Recording Server. If you have not installed Session Recording yet, you can modify such information later in **Session Recording Agent Properties**.

**Note:** There is a limitation with the test connection function of the installer. It does not support the "HTTPS requires TLS 1.2"scenario. If you use the installer in this scenario, test connection fails but you can ignore the failure and click **Next** to continue the installation. It does not affect normal functioning.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

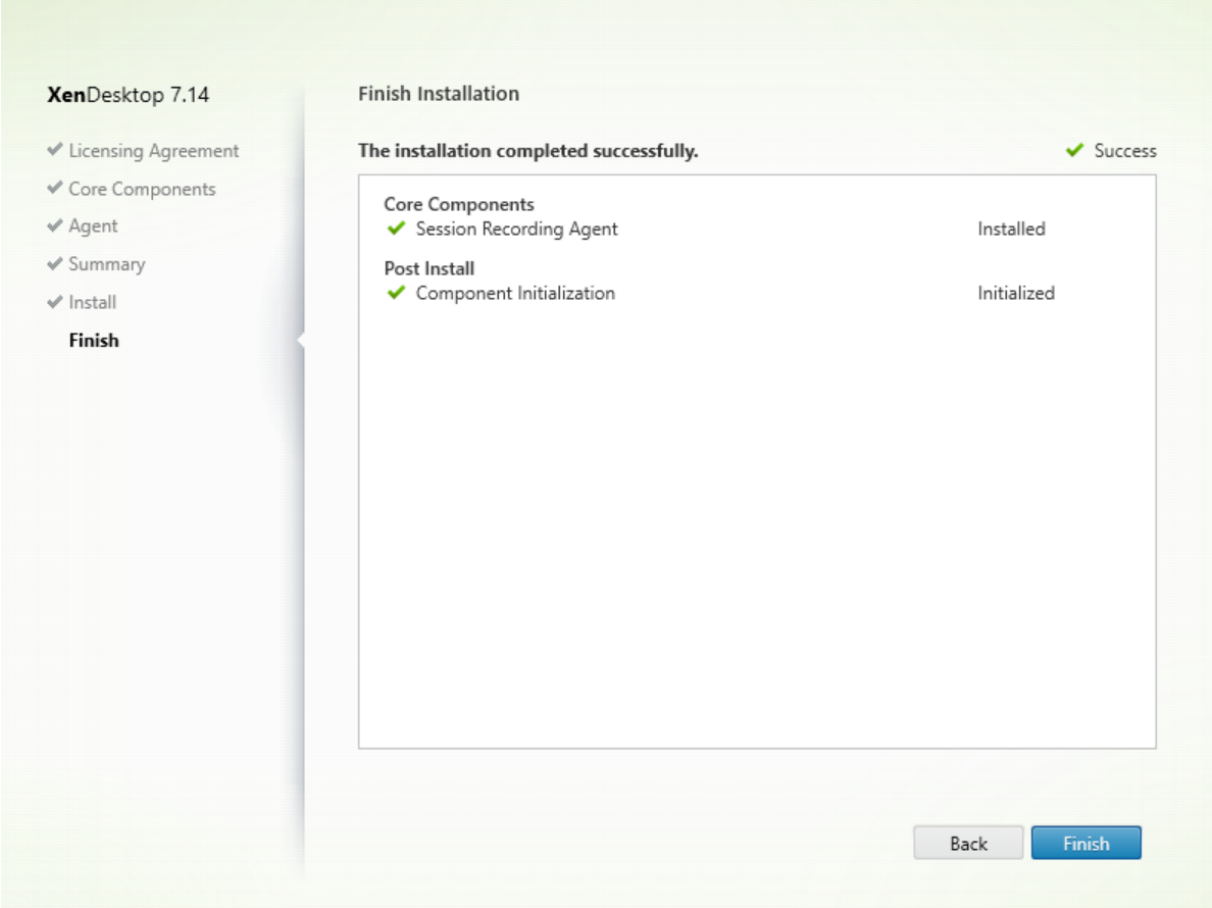
**Step 7: Review the prerequisites and confirm the installation**




The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes. Or, click **Install** to start the installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 8: Complete the installation**




The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording Agent.

**Note:** When Machine Creation Services (MCS) or Provisioning Services (PVS) creates multiple VDAs with the configured master image and Microsoft Message Queuing (MSMQ) installed, those VDAs can have the same QMId under certain conditions. This might cause various issues, for example:

- Sessions might not be recorded even if the recording agreement is accepted.
- The Session Recording Server might not be able to receive session logoff signals and consequently, sessions might always be in Live status.

As a workaround, create a unique QMId for each VDA and it differs depending on the deployment methods.

No extra actions are required if Desktop OS VDAs with the Session Recording agent installed are created with PVS 7.7 or later and MCS 7.9 or later in the static desktop mode that is, for example, configured to make all changes persistent with a separate Personal vDisk or the local disk of your VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For Server OS VDAs created with MCS or PVS and Desktop OS VDAs that are configured to discard all changes when a user logs off, use the GenRandomQMID.ps1 script to modify the QMId on system startup. Modify the power management strategy to ensure that enough VDAs are running before user logon attempts.

To use the GenRandomQMID.ps1 script, do the following:

1. Make sure that the execution policy is set to **RemoteSigned** or **Unrestricted** in PowerShell.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

2. Create a scheduled task, set the trigger as on system startup, and run with the SYSTEM account on the PVS or MCS master image machine.
3. Add the command as a startup task.

   ```
   powershell .exe -file C:\\GenRandomQMID.ps1
   ```

**Summary of the GenRandomQMID.ps1 script:**

1. Remove the current QMId from the registry.
2. Add SysPrep = 1 to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters.
3. Stop related services, including CitrixSmAudAgent and MSMQ.
4. To generate a random QMId, start the services that stopped previously.

```
# Remove old QMId from registry and set SysPrep flag for MSMQ
Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\
    MachineCache -Name QMId -Force
Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "
    SysPrep" -Type DWord -Value 1
# Get dependent services
\$depServices = Get-Service -name MSMQ -dependentservices | Select -
    Property Name
# Restart MSMQ to get a new QMId
Restart-Service -force MSMQ
# Start dependent services
if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        \$startMode = Get-WmiObject win32\_service -filter \"NAME = '\$
            \(\$depService.Name)'\" | Select -Property StartMode
        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name
         }


 }

 }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Install the Session Recording Player

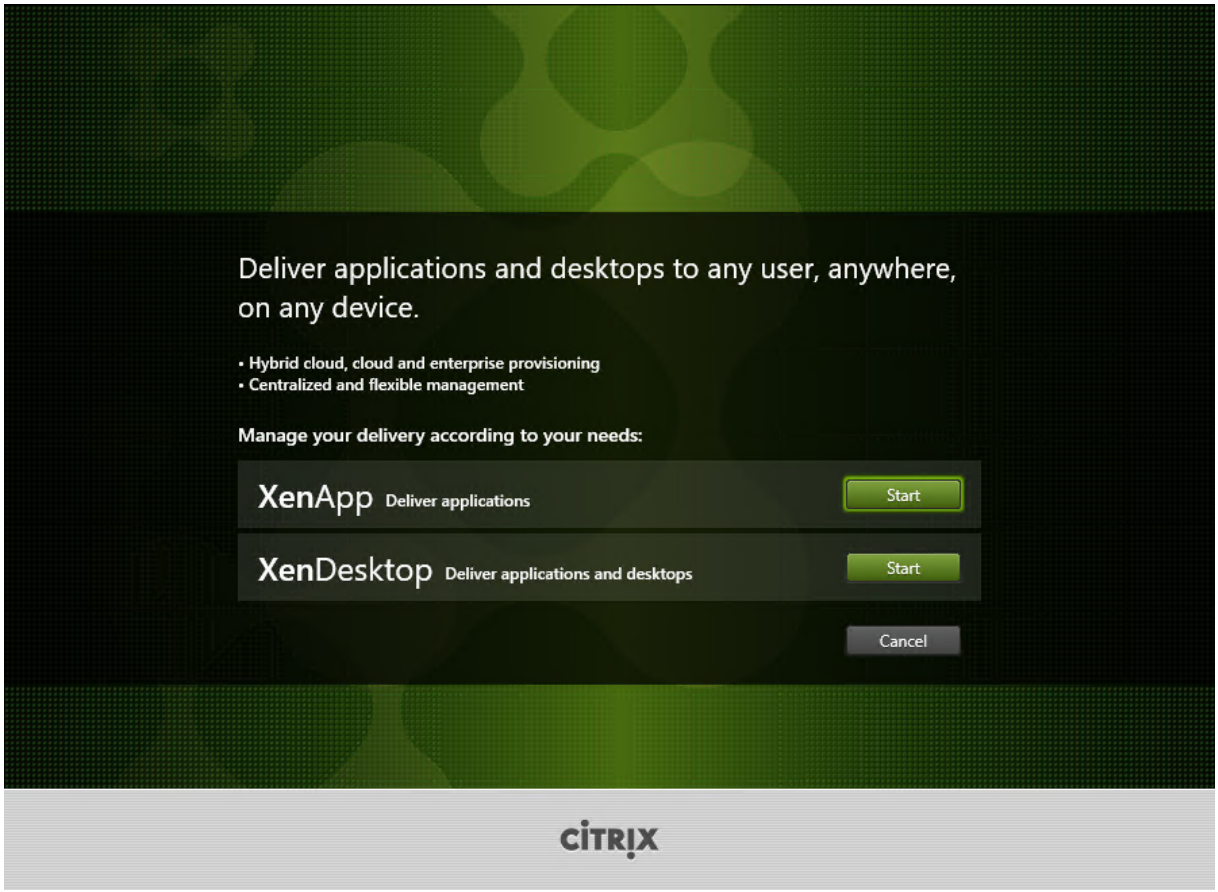
Install the Session Recording Player on the Session Recording Server or one or more workstations in the domain for users who view session recordings.

### Step 1: Download the product software and launch the wizard

Use a local administrator account to log on to the machine where you are installing the Session Recording Player component. 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.

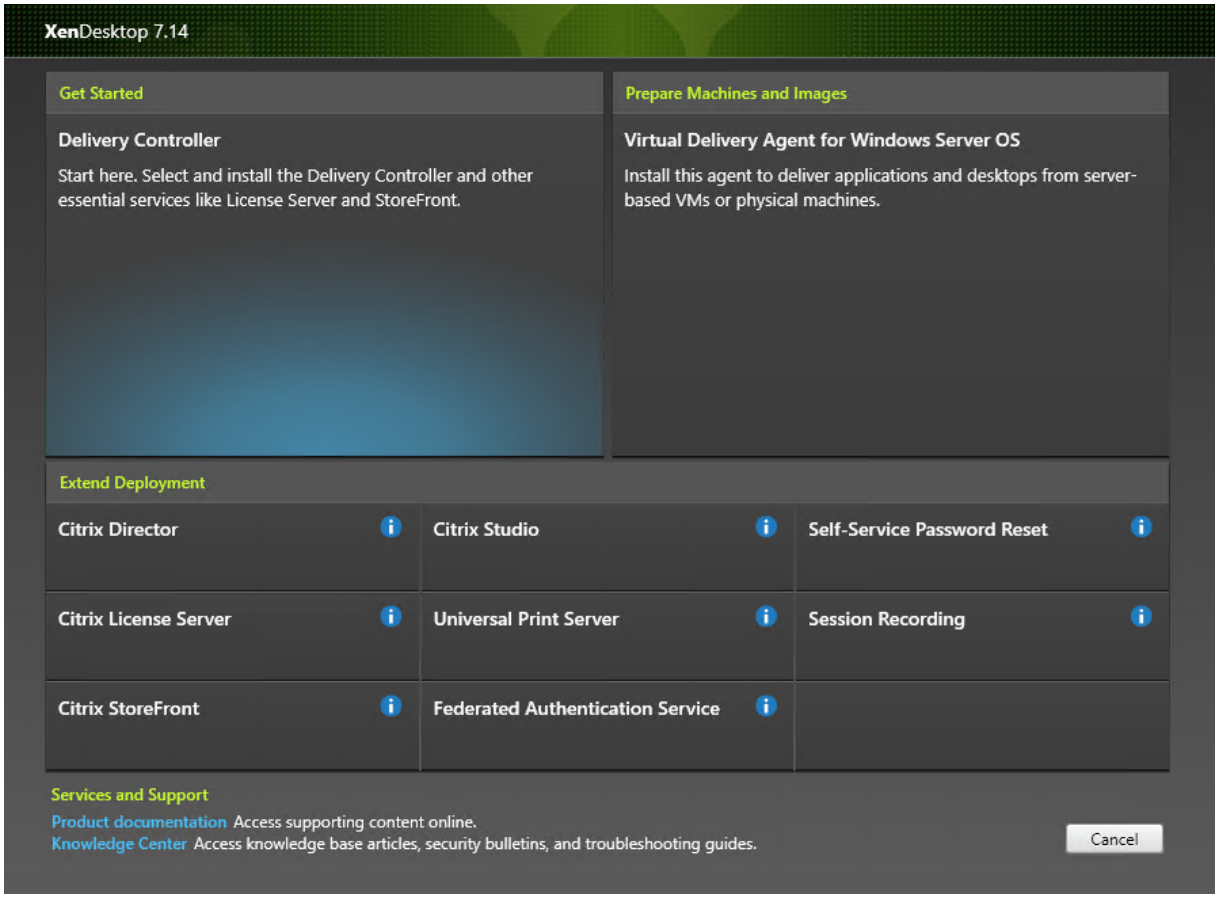
### Step 2: Choose which product to install




Click **Start** next to the product to install: **XenApp** or **XenDesktop**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

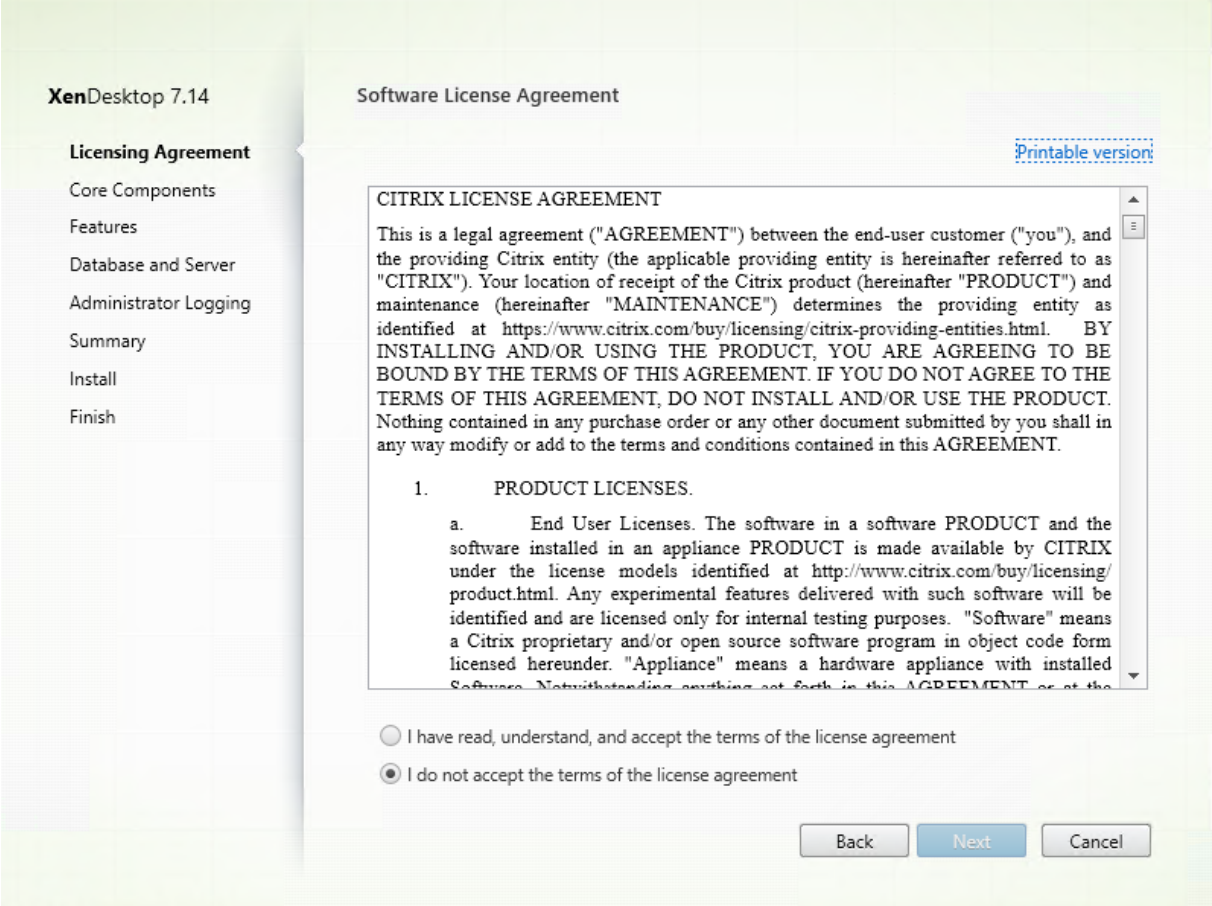
### Step 3: Select Session Recording




Select the **Session Recording** entry.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

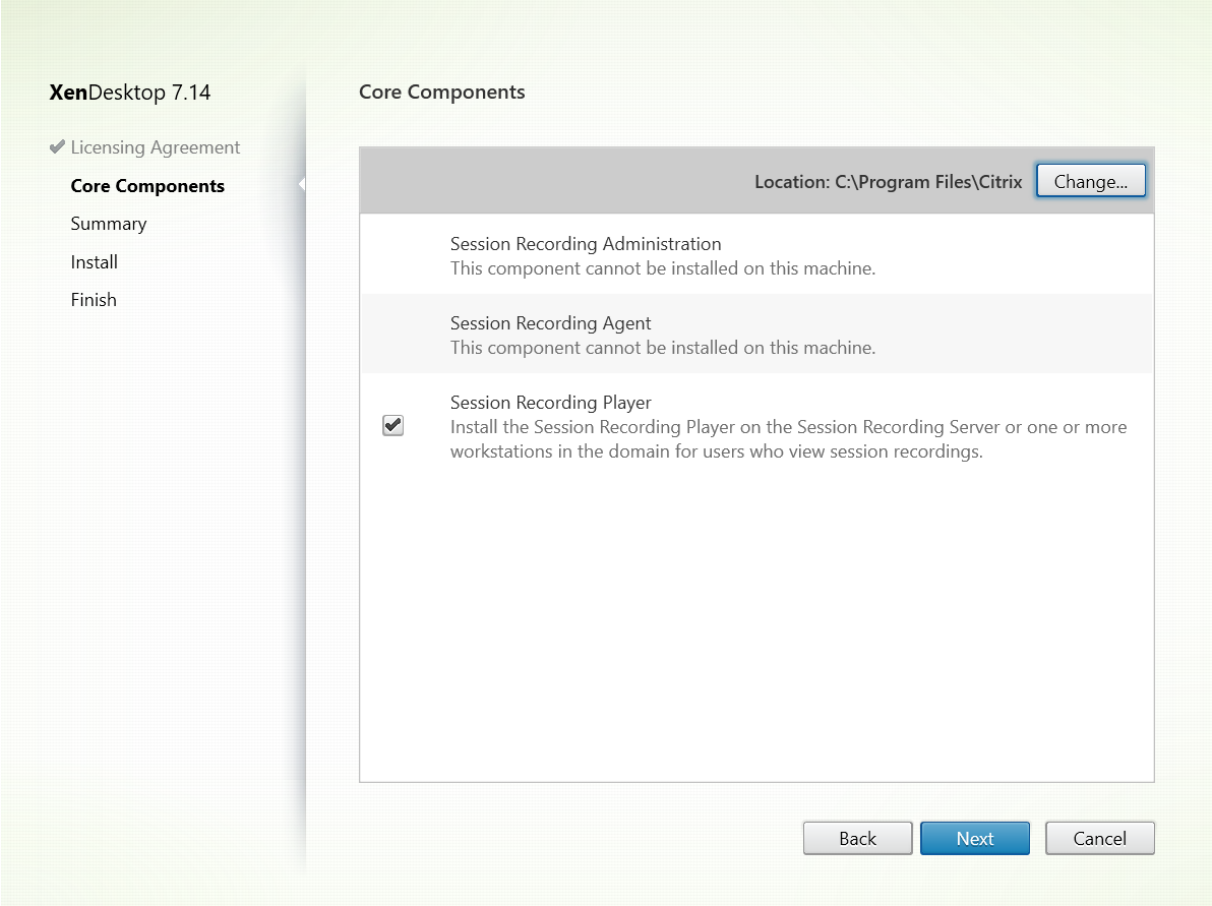
### Step 4: Read and accept the license agreement




On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

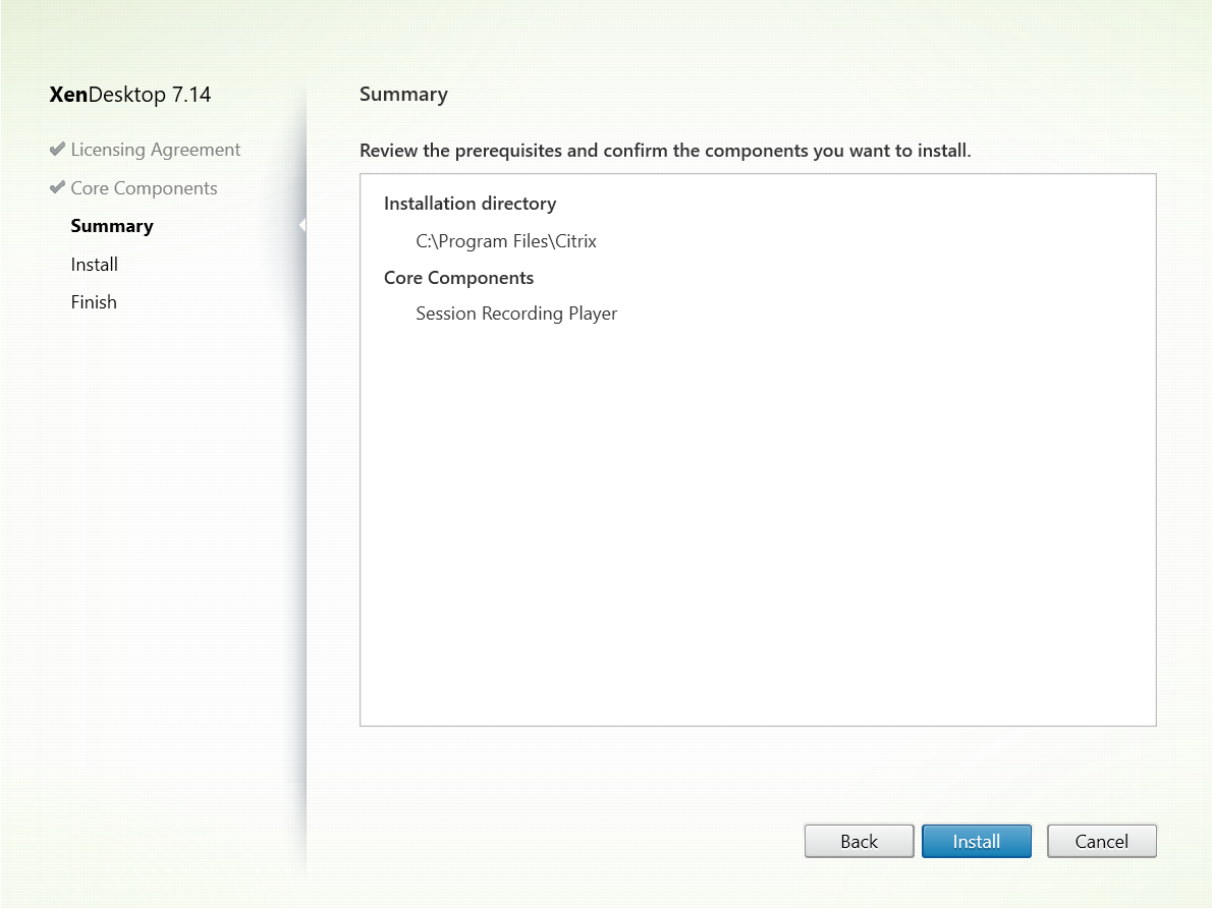
### Step 5: Select the component to install and the installation location




Select **Session Recording Player** and click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

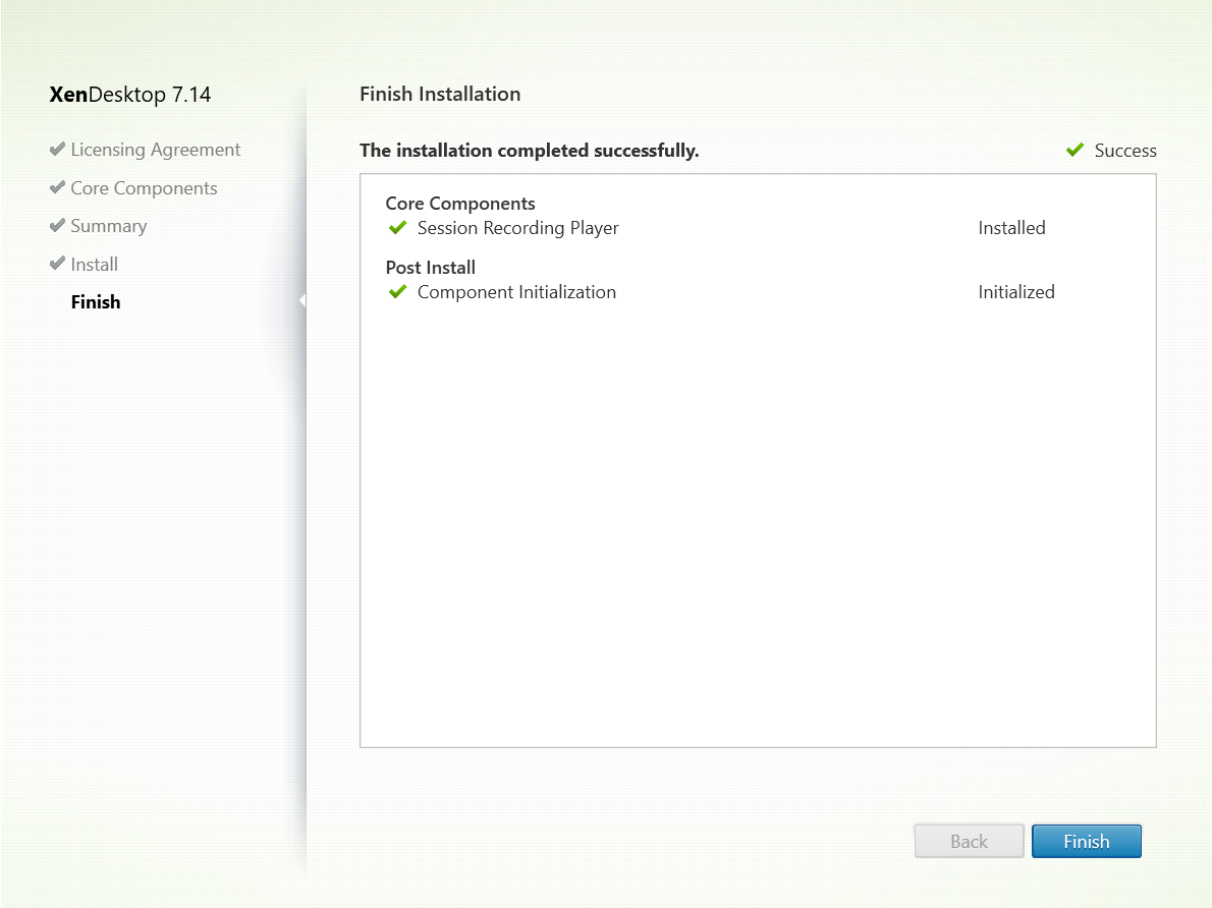
### Step 6: Review the prerequisites and confirm the installation




The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes. Or, click **Install** to start the installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Step 7: Complete the installation**




The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording Player.

## Automate installations

To install the Session Recording Agent on multiple servers, write a script that uses silent installation.

The following command line installs the Session Recording Agent and creates a log file to capture the installation information.

**For 64-bit systems:**

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVER-NAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKER-PORT=yourbrokerport

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**Note**: The SessionRecordingAgentx64.msi file in the XenApp/XenDesktop ISO is under \layout\image-full\x64\Session Recording.

**For 32-bit systems:**

msiexec /i SessionRecordingAgent.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

**Note:** The SessionRecordingAgent.msi file in the XenApp/XenDesktop ISO is under \layout\image-full\x86\Session Recording.

where:

**yourservername** is the NetBIOS name or FQDN of the computer hosting the Session Recording Server. If not specified, this value defaults to **localhost**.

**yourbrokerprotocol** is HTTP or HTTPS that Session Recording Agent uses to communicate with Session Recording Broker. If not specified, this value defaults to HTTPS.

**yourbrokerport** is the port number that Session Recording Agent uses to communicate with Session Recording Broker. If not specified, this value defaults to zero, which directs Session Recording Agent to use the default port number for your selected protocol: 80 for HTTP or 443 for HTTPS.

**/l*v** specifies verbose logging.

***yourinstallationlog*** is the location of your installation log file.

**/q** specifies the quiet mode.

### Upgrade Session Recording

You can upgrade certain deployments to later versions without having to first set up new machines or Sites. You can upgrade from Session Recording 7.6 (or later) to the latest release of Session Recording.

**Notes:**

- When you upgrade Session Recording Administration from 7.6 to 7.13 or later and choose **Modify** in Session Recording Administration to add the Administrator Logging service, the SQL Server instance name does not appear on the **Administrator Logging Configuration** page. The following error message appears when you click **Next**: `Database connection test failed. Please enter correct Database instance name.` As a workaround, add the read permission for localhost users to the following SmartAuditor Server registry folder: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Attempts to upgrade the Session Recording Database might fail when you have only this component installed on a machine. In this case, check whether the following registry entries exist under HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\SmartAuditor\Database. If not, manually add the entries before upgrading.

| Key name | Key type | Key value |
|---|---|---|
| SmAudDatabaseInstance | String | The instance name of your Session Recording Database |
| DatabaseName | String | The database name of your Session Recording Database |

#### Requirements, preparation, and limitations

**Note:** You cannot upgrade from a Technology Preview version.

- You must use the Session Recording installer's graphical or command-line interface to upgrade the Session Recording components on the machine where you installed the components.
- Before beginning any upgrade activity, back up the database named CitrixSessionRecording in the SQL Server instance, so that you can restore it if any issues are discovered after the database upgrade.
- In addition to being a domain user, you must be a local administrator on the machines where you are upgrading the Session Recording components.
- If the Session Recording Server and Session Recording Database are not installed on the same server, you must have the database role permission to upgrade the Session Recording Database; otherwise, you can
  - Ask the database administrator to assign the **securityadmin** and **dbcreator** server role permissions for the upgrade. After the upgrade completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
  - Or, use the SessionRecordingAdministrationx64.msi package to upgrade. During the msi upgrade, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Enter the correct credentials and then click **OK** to continue the upgrade.
- If you do not plan to upgrade all the Session Recording Agents at the same time, Session Recording Agent 7.6.0 (or later) can work with the latest (current) release of Session Recording Server. However, some new features and bug fixes might not take effect.
- Any sessions launched during the upgrade of Session Recording Server are not recorded.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

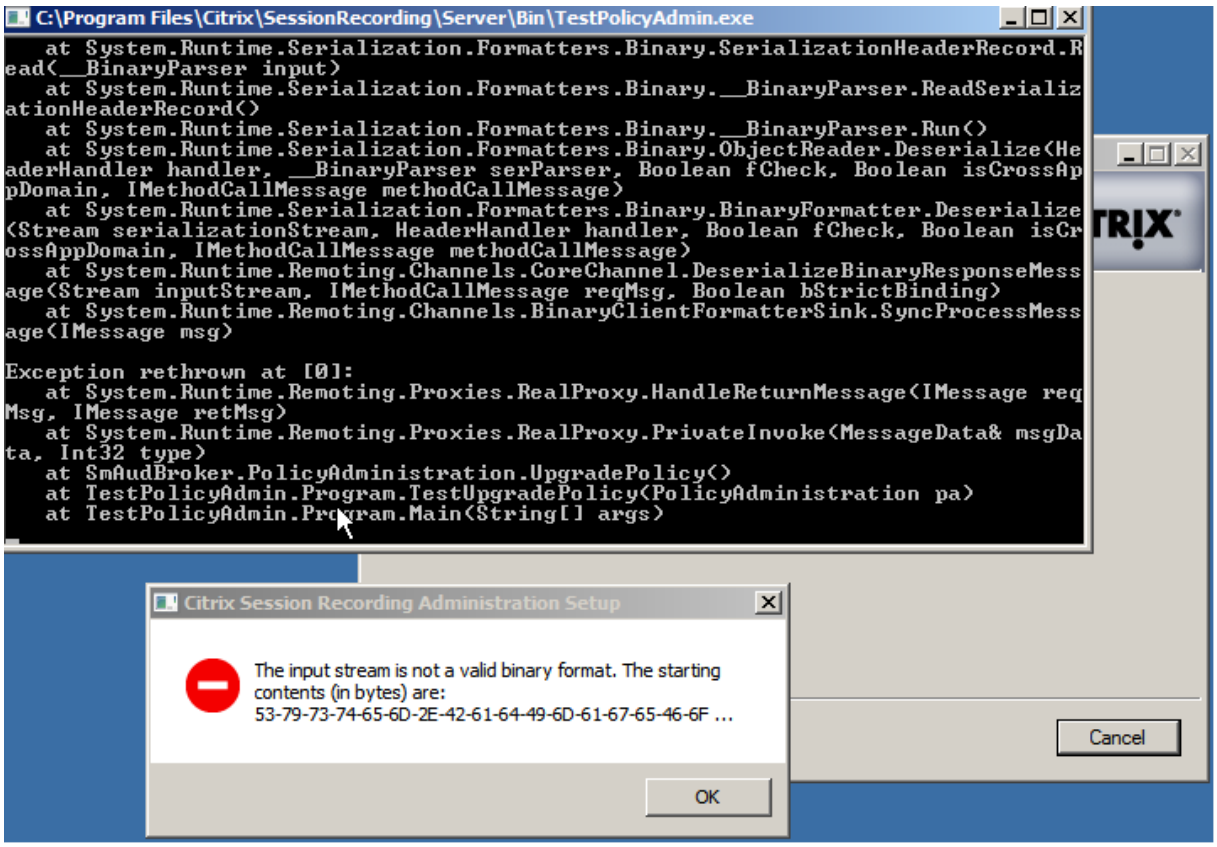
- The **Graphics Adjustment** option in Session Recording Agent Properties is enabled by default after a fresh installation or upgrade to keep compatible with the Desktop Composition Redirection mode. You can disable this option manually after a fresh installation or upgrade.
- The Administrator Logging feature is not installed after you upgrade Session Recording from a previous release that doesn't contain this feature. To add this new feature, modify the installation after the upgrade.
- If there are live recording sessions when the upgrade process starts, there is very little chance that the recording can be completed.
- Review the upgrade sequence below, so that you can plan and mitigate potential outages.

**Upgrade sequence**

1. If the Session Recording Database and Session Recording Server are installed on different servers, stop the Session Recording Storage Manager service manually on the Session Recording Server, and then upgrade the Session Recording Database first.
2. Ensure that the Session Recording Broker is running with the IIS service. Upgrade the Session Recording Server. If the Session Recording Database and Session Recording Server are installed on the same server, the Session Recording Database will also be upgraded.
3. The Session Recording service is back online automatically when the upgrade of the Session Recording Server is completed.
4. Upgrade the Session Recording Agent (on the master image).
5. Upgrade the Session Recording Policy Console with or after the Session Recording Server.
6. Upgrade the Sessoin Recording Player.

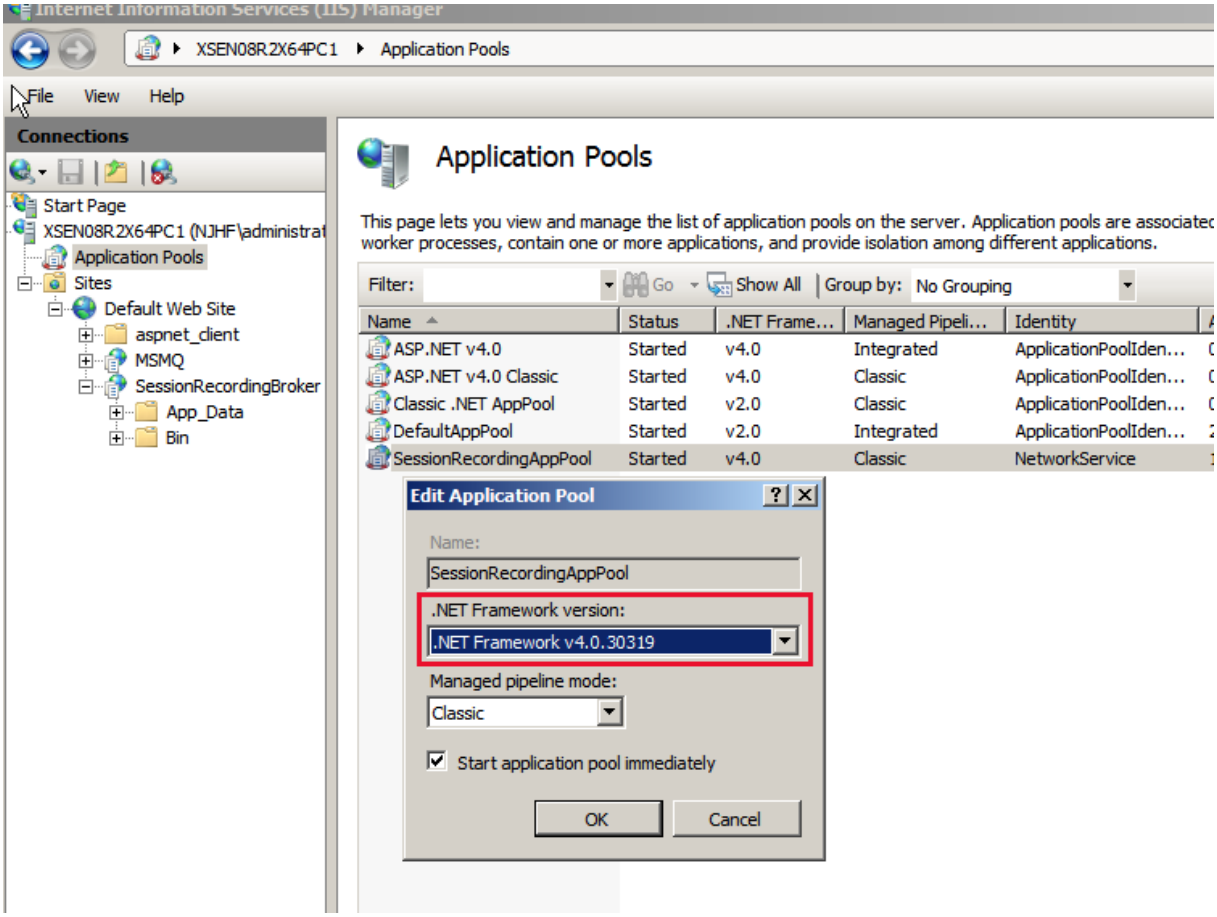
**Note:** The following error might occur when you upgrade the Session Recording Administration component on Windows Server 2008 R2.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




In this case, change the “.NET Framework version”for “SessionRecordingAppPool”to “.NET Framework v4”in IIS and do the upgrade again.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Uninstall Session Recording

**To remove the Session Recording components from a server or workstation, use the uninstall or remove programs option available from the Windows Control Panel.** To remove the Session Recording Database, you must have the same **securityadmin** and **dbcreator** SQL Server role permissions as when you installed it.

For security reasons, the Administrator Logging Database is not removed after the components are uninstalled.

## Configure Session Recording

May 25, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

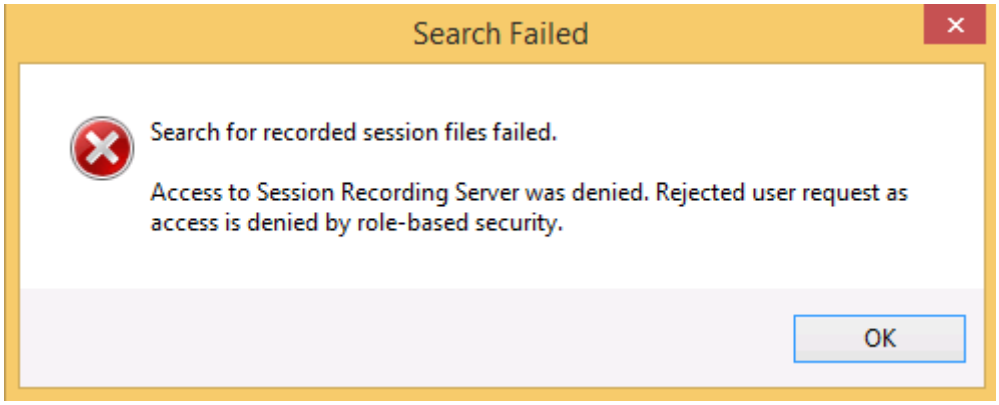
## Configure Session Recording to play and record sessions

After you install the Session Recording components, perform the following steps to configure Session Recording to record XenApp or XenDesktop sessions and allow users to view them:

- Authorize users to play recordings
- Authorize users to administer recording policies
- Set an active recording policy to record sessions
- Configure custom policies
- Configure the Session Recording Player to connect to the Session Recording Server

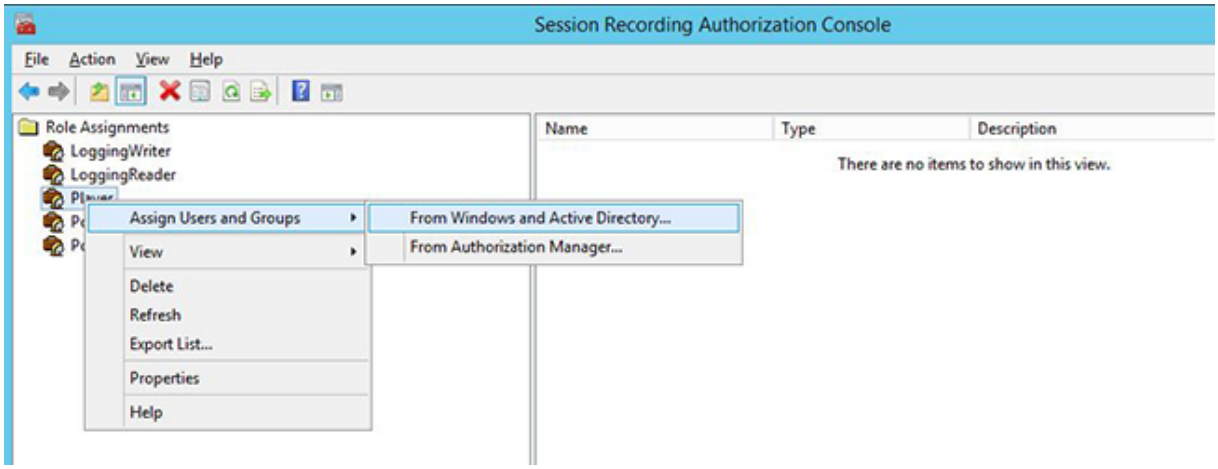
### Authorize users to play recorded sessions

When you install Session Recording, no user has the permission to play recorded sessions. You must assign the permission to each user, including the administrator. A user without the permission to play recorded sessions receives the following error message when trying to play a recorded session:




1. Log on as an administrator to the computer hosting the Session Recording Server.
2. Start the Session Recording Authorization Console.
3. In the Session Recording Authorization Console, select Player.
4. Add the users and groups you want to authorize to view recorded sessions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Authorize users to administer recording policies

When you install Session Recording, domain administrators grant the permission to control the recording policies by default. You can change the authorization setting.

1. Log on as an administrator to the machine hosting the Session Recording Server.
2. Start the Session Recording Authorization Console and select PolicyAdministrators.
3. Add the users and groups who can administer recording policies.

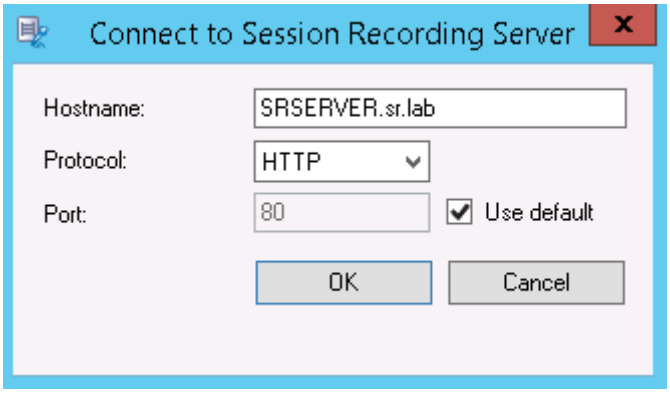
### Set the active recording policy to record sessions

The active recording policy specifies a session recording behavior on all VDAs or VDIs that have the Session Recording Agent installed and connected to the Session Recording Server. When you install Session Recording, the active recording policy is **Do not record**. Sessions cannot be recorded until you change the active recording policy.

**Important:** A policy can contain many rules, but only one active policy can be running at a time.

1. Log on as an authorized Policy Administrator to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If the **Connect to Session Recording Server** dialog box appears, ensure that the name of the computer hosting the Session Recording Server, the protocol, and the port number are correct.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




4. In the Session Recording Policy Console, expand **Recording Policies** to display the recording policies available, with a check mark indicating which policy is active:
    - **Do not record**. The default policy. If you do not specify another policy, no sessions are recorded.
    - **Record everyone with notification**. If you choose this policy, all sessions are recorded. A window appears to notify each recording occurrence.
    - **Record everyone without notification**. If you choose this policy, all sessions are recorded. No window appears to notify recording occurrence.
5. Select the policy you want to make active.
6. From the menu bar, choose **Action** > **Activate Policy**.

Session Recording allows you to create your own recording policy. When you create recording policies, they appear in the **Recording Policies** folder of the Session Recording Policy Console.

The generic recording policy might not fit your requirements. You can configure policies and rules based on users, VDA and VDI servers, Delivery Groups, and applications. For more information about custom policies, see Create custom recording policies.

**Note:** The Administrator Logging feature of Session Recording allows you to log the recording policy changes. For more information, see Log administration activities.

### Configure the Session Recording Player

Before a Session Recording Player can play sessions, you must configure it to connect to the Session Recording Server that stores the recorded sessions. Each Session Recording Player can be configured with the ability to connect to multiple Session Recording Servers, but can connect to only one Session Recording Server at a time. If the Player is configured with the ability to connect to multiple Session Recording Servers, users can change which Session Recording Server the Player connects to by selecting a check box on the **Connections** tab at **Tools** > **Options**.

1. Log on to the workstation where the Session Recording Player is installed.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. Start the Session Recording Player.
3. From the Session Recording Player menu bar, choose **Tools** > **Options**.
4. On the **Connections** tab, click **Add**.
5. In the **Hostname** field, type the name or IP address of the computer hosting the Session Recording Server and select the protocol. By default, Session Recording is configured to use HTTPS/SSL to secure communications. If SSL is not configured, select HTTP.
6. To configure the Session Recording Player with the ability to connect to multiple Session Recording Servers, repeat Steps 4 and 5 for each Session Recording Server.
7. Ensure that you select the check box for the Session Recording Server you want to connect to.

#### Configure the connection to the Session Recording Server

The connection between the Session Recording Agent and the Session Recording Server is typically configured when the Session Recording Agent is installed. To configure this connection after the Session Recording Agent is installed, use Session Recording Agent Properties.

1. Log on to the server where the Session Recording Agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. Click the **Connections** tab.
4. In the **Session Recording Server** field, type the FQDN of the Session Recording Server.

   > **Note:**
   >
   > To use Message Queuing over HTTPS (TCP is used by default), type an FQDN in the **Session Recording Server** field. Otherwise, session recording fails.

5. In the **Session Recording Storage Manager message queue** section, select the protocol that is used by the Session Recording Storage Manager to communicate and modify the default port number if necessary.

   > **Note:**
   >
   > To use Message Queuing over HTTP and HTTPS, install all the IIS recommended features.

6. In the **Message life** field, accept the default 7,200 seconds (two hours) or type a new value for the number of seconds each message is retained in the queue if there is a communication failure. After this period of time elapses, the message is deleted and the file is playable until the point where the data is lost.
7. In the **Session Recording Broker** section, select the communication protocol that the Session Recording Broker uses to communicate and modify the default port number if necessary.
8. When prompted, restart the **Session Recording Agent Service** to accept the changes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Grant access rights to users

July 18, 2018

> **Important:**
>
> For security reasons, grant users only the rights they need to perform specific functions, such as viewing recorded sessions.

You grant rights to Session Recording users by assigning them to roles using the Session Recording Authorization Console on the Session Recording Server. Session Recording users have three roles:

- **Player.** Grants the right to view recorded XenApp sessions. There is no default membership in this role.
- **PolicyQuery.** Allows the servers hosting the Session Recording Agent to request recording policy evaluations. By default, authenticated users are members of this role.
- **PolicyAdministrator.** Grants the right to view, create, edit, delete, and enable recording policies. By default, administrators of the computer hosting the Session Recording Server are members of this role.

Session Recording supports users and groups defined in Active Directory.

### Assign users to roles

1. Log on to the computer hosting the Session Recording Server, as an administrator or as a member of the Policy Administrator role.
2. Start the Session Recording Authorization Console.
3. Select the role to which you want to assign users.
4. From the menu bar, choose **Action** >**Assign Windows Users and Groups**.
5. Add the users and groups.

Any changes made to the console take effect during the update that occurs once every minute.

## Create and activate recording policies

December 1, 2020

Use the Session Recording Policy Console to create and activate policies that determine which sessions are recorded.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Important:**
>
> To use the Session Recording Policy Console, you must have the Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) installed. The snap-in cannot be automatically installed by the installer. Locate the snap-in on the XenApp and XenDesktop ISO (\layout\image-full\x64\Citrix Desktop Delivery Controller) and follow the instructions for installing it manually. Failure to comply can cause an error.
>
> **Tip:**
>
> You can edit the registry to prevent recording file losses in case that your Session Recording Server might fail unexpectedly. Log on as an administrator to the machine where you installed the Session Recording Agent, open the Registry Editor, and add a DWORD value `DefaultRecordActionOnError =1` under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`.

You can activate system policies available when Session Recording is installed or create and activate your own custom policies. Session Recording system policies apply a single rule to all users, published applications, and servers. Custom policies specifying which users, published applications, and servers are recorded.

The active policy determines which sessions are recorded. Only one policy is active at a time.

### System policies

Session Recording provides these system policies:

- **Do not record**. This is the default policy. If you do not specify another policy, no sessions are recorded.
- **Record everyone with notification**. If you choose this policy, all sessions are recorded. A pop-up window appears to notify recording occurrence.
- **Record everyone without notification**. If you choose this policy, all sessions are recorded. No pop-up window appears to notify recording occurrence.

System policies cannot be modified or deleted.

### Activate a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a **Connect to Session Recording Server** pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. In the Session Recording Policy Console, expand **Recording Policies**.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose **Action** > **Activate Policy**.

### Create custom recording policies

When you create your own policy, you make rules to specify which users and groups, published applications, and servers have their sessions recorded. A wizard within the Session Recording Policy Console helps you create rules. To obtain the list of published applications and servers, you must have the site administrator read permission. Configure that on this site's Delivery Controller.

For each rule you create, you specify a recording action and rule criteria. The recording action applies to sessions that meet the rule criteria.

For each rule, choose one recording action:

- **Do not record**. (Choose **Disable session recording** in the **Rules** wizard.) This recording action specifies that sessions meeting the rule criteria are not recorded.
- **Record with notification**. (Choose **Enable session recording with notification** in the **Rules** wizard.) This recording action specifies that sessions meeting the rule criteria are recorded. A pop-up window appears to notify recording occurrence.
- **Record without notification**. (Choose **Enable session recording without notification** in the **Rules** wizard.) This recording action specifies that sessions meeting the rule criteria are recorded. Users are unaware that they are being recorded.

For each rule, choose at least one of the following items to create the rule criteria:

- **Users or Groups**. Creates a list of users or groups to which the recording action of the rule applies.
- **Published Resources**. Creates a list of published applications or desktops to which the recording action of the rule applies. In the **Rules** wizard, choose the XenApp and XenDesktop site or sites on which the applications or desktops are available.
- **Delivery Groups or Machines**. Creates a list of Delivery Groups or machines to which the recording action of the rule applies. In the **Rules** wizard, choose the location of the Delivery Groups or machines.
- **IP Address or IP Range**. Creates a list of IP addresses or ranges of IP addresses to which the recording action of the rule applies. On the **Select IP Address and IP Range** screen, add a valid IP address or IP range for which recording is enabled or disabled.

**Note:** The Session Recording Policy Console supports configuring multiple criteria within a single rule. When a rule applies, both the "AND"and the "OR"logical operators are used to compute the final action. Generally speaking, the "OR"operator is used between items within a criterion, and the "AND"

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

operator is used between separate criteria. If the result is true, the Session Recording policy engine takes the rule's action. Otherwise, it goes to the next rule and repeats the process.

When you create more than one rule in a recording policy, some sessions might match the criteria for more than one rule. In these cases, the rule with the highest priority is applied to the sessions.

The recording action of a rule determines its priority:

- Rules with the **Do not record** action have the highest priority
- Rules with the **Record with notification** action have the next highest priority
- Rules with the **Record without notification** action have the lowest priority

Some sessions might not meet any rule criteria in a recording policy. For these sessions, the recording action of the policies fallback rule applies. The recording action of the fallback rule is always **Do not record**. The fallback rule cannot be modified or deleted.

To configure custom policies, do the following:

1. Log on as an authorized Policy Administrator to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console and select **Recording Policies** in the left pane. From the menu bar, choose **Action** > **Add New Policy**.
3. Right-click the **New policy** and select **Add Rule**.
4. Select a recording option - In the **Rules** wizard, select **Disable session recording**, **Enable Session Recording with notification** (or **without notification**), and then click **Next**.
5. Select the rule criteria - You can choose one or any combination of the options:
   **Users or Groups**
   **Published resources**
   **Delivery Groups or Machines**
   **IP Address or IP Range**
6. Edit the rule criteria - To edit, click the underlined values. The values are underlined based on the criteria you chose in the previous step.
   **Note:** If you choose the **Published Resources** underlined value, the **Site Address** is the IP address, a URL, or a machine name if the Controller is on a local network. The **Name of Application** list shows the display name.
7. Follow the wizard to finish the configuration.

### Use Active Directory groups

Session Recording allows you to use Active Directory groups when creating policies. Using Active Directory groups instead of individual users simplifies the creation and management of rules and policies. For example, if users in your company's finance department are contained in an Active Directory

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

group named Finance, you can create a rule that applies to all members of this group by selecting the Finance group in the **Rules** wizard when creating the rule.

### White list users

You can create Session Recording policies ensuring that the sessions of some users in your organization are never recorded. This is called *white listing* these users. White listing is useful for users who handle privacy-related information or when your organization does not want to record the sessions of a certain class of employees.

For example, if all managers in your company are members of an Active Directory group named Executive, you can ensure that these users' sessions are never recorded by creating a rule that disables session recording for the Executive group. While the policy containing this rule is active, no sessions of members of the Executive group are recorded. The sessions of other members of your organization are sessions recorded based on other rules in the active policy.

### Use IP address or IP range rule criteria

You can use client IP addresses as rule criteria for policy matching. For example, if you want to record sessions from clients with specific IP addresses or within an IP range, use the **Rules** wizard to create a rule that applies only to those clients.

### Create a new policy

**Note:** When using the **Rules** wizard, you might be prompted to "click on underlined value to edit" when no underlined value appears. Underlined values appear only when applicable. If no underline values appear, ignore the step.

1. Log on to the server where Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a **Connect to Session Recording Server** pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click **OK**.
4. In the Session Recording Policy Console, select **Recording Policies**.
5. From the menu, choose **Add New Policy**. A policy called **New Policy** appears in the left pane.
6. Right-click the new policy and choose **Rename** from the menu.
7. Type a name for the policy you are about to create and press **Enter** or click anywhere outside the new name.
8. Right-click the policy, choose **Add New Rule** from the menu to launch the **Rules** wizard.
9. Follow the instructions to create the rules for this policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Modify a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a **Connect to Session Recording Server** pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click **OK**.
4. In the Session Recording Policy Console, expand **Recording Policies**.
5. Select the policy you want to modify. The rules for the policy appear in the right pane.
6. To add a new rule, modify a rule, or delete a rule:
    - From the menu bar, choose **Action** >**Add New Rule**. If the policy is active, a pop-up window appears requesting confirmation of the action. Use the **Rules** wizard to create a new rule.
    - Select the rule you want to modify, right-click, and choose **Properties**. Use the **Rules** wizard to modify the rule.
    - Select the rule you want to delete, right-click, and choose **Delete Rule**.

### Delete a policy

**Note:** You cannot delete a system policy or a policy that is active.

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a **Connect to Session Recording Server** pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click **OK**.
4. In the Session Recording Policy Console, expand **Recording Policies**.
5. In the left pane, select the policy you want to delete. If the policy is active, you must activate another policy.
6. From the menu bar, choose **Action** > **Delete Policy**.
7. Select **Yes** to confirm the action.

**Note:** Limitation regarding prelaunched application sessions:

- If the active policy tries to match an application name, the applications launched in the prelaunched session are not matched, which results in the session not being recorded.
- If the active policy records every application, when a user logs on to Citrix Receiver for Windows (at the same time that a prelaunched session is established), a recording notification appears and the prelaunched (empty) session and any applications to be launched in that session going forward are recorded.

As a workaround, publish applications in separate Delivery Groups according to their recording policies. Do not use an application name as a recording condition. This ensures that prelaunched sessions can be recorded. However, notifications still appear.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Understand rollover behavior

When you activate a policy, the previously active policy remains in effect until the user's session ends. However, sometimes the new policy takes effect when the file rolls over. Files roll over when they have reached the maximum size. For more information about the maximum file size for recordings, see Specify file size for recordings.

The following table details what happens when you apply a new policy while a session is being recorded and a rollover occurs:

| If the previous policy was | And the new policy is | After a rollover, the policy will be |
|---|---|---|
| Do not record | Any other policy | No change. The new policy takes effect only when the user logs on to a new session. |
| Record without notification | Do not record | Recording stops. |
| Record without notification | Record with notification | Recording continues and a notification message appears. |
| Record with notification | Do not record | Recording stops. |
| Record with notification | Record without notification | Recording continues. No message appears the next time a user logs on. |

## Create notification messages

February 13, 2019

If the active recording policy specifies that users are notified when their sessions are recorded, a pop-up window appears displaying a notification message after the users type their credentials. The default notification message is `"Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs."` The users can click **OK** to dismiss the window and continue their sessions.

The default notification message appears in the language of the operating system of the computers hosting the Session Recording Server.

You can create custom notifications in languages you choose; however, you can have only one notification message for each language. Your users see notification messages in the languages of their

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

preferred local settings.

### Create a new notification message

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Notifications** tab.
4. Click **Add**.
5. Choose the language for the message and type the new message. You can create only one message for each language.

After accepting and activating, the new message appears in the Language-specific notification messages box.

**Note:** The Administrator Logging feature of Session Recording allows you to log the Session Recording server policy changes. For more information, see Log administration activities.

## Disable or enable recording

November 12, 2019

You install the Session Recording Agent on each VDA for Server OS for which you want to record sessions. Within each agent is a setting that enables recording for the server on which it is installed. After recording is enabled, Session Recording evaluates the active recording policy that determines which sessions are recorded.

When you install the Session Recording Agent, recording is enabled. Citrix recommends that you disable Session Recording on servers that are not recorded because they experience a small impact on performance, even if no recording takes place.

### Disable or enable recording on a server

1. Log on to the server where the Session Recording Agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. Under **Session Recording**, select or clear the **Enable session recording for this Server OS VDA** check box to specify whether or not sessions can be recorded for this server.
4. When prompted, restart the Session Recording Agent Service to accept the change.

**Note:** When you install Session Recording, the active policy is
**Do not record** (no sessions are recorded on any server). To begin recording, use the Session Recording Policy Console to activate a different policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Enable custom event recording

Session Recording allows you to use third-party applications to insert custom data, known as events, into recorded sessions. These events appear when the session is viewed using the Session Recording Player. They are part of the recorded session file and cannot be modified after the session is recorded.

For example, an event might contain the following text: "User opened a browser."Each time a user opens a browser during a session that is being recorded, the text is inserted into the recording at that point. When the session is played using the Session Recording Player, the viewer can locate and count the times that the user opened a browser by noting the number of markers that appear in the Events and Bookmarks list in the Session Recording Player.

To insert custom events into recordings on a server:

- Use **Session Recording Agent Properties** to enable a setting on each server where you want to insert custom events. You must enable each server separately. You cannot globally enable all servers in a site.
- Write applications built on the Event API that runs within each user's XenApp session (to inject the data into the recording).

The Session Recording installation includes an event recording COM application (API) that allows you to insert text from third-party applications into a recording. You can use the API from many programming languages including Visual Basic, C++, or C#. For more information, see Citrix article CTX226844. The Session Recording Event API .dll is installed as part of the Session Recording installation. You can find it at C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll.

To enable custom event recording on a server, do the following:

1. Log on to the server where the Session Recording Agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. In **Session Recording Agent Properties**, click the **Recording** tab.
4. Under **Custom event recording**, select the **Allow third party applications to record custom data on this server** check box.

## Enable or disable live session playback and playback protection

October 10, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Enable or disable live session playback

Using Session Recording Player, you can view a session after or while it is being recorded. Viewing a session that is being recorded is similar to seeing actions happening live. However, there is actually a delay of one to two seconds when the data propagates from the XenApp or XenDesktop server.

Some functionality is not available when you view sessions that are not recorded completely:

- A digital signature cannot be assigned until recording is complete. If digital signing is enabled, you can view live playback sessions, but they are not digitally signed and you cannot view certificates until the session is completed.
- Playback protection cannot be applied until recording is complete. If playback protection is enabled, you can view live playback sessions, but they are not encrypted until the session is completed.
- You cannot cache a file until recording is complete.

By default, live session playback is enabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Playback** tab.
4. Select or clear the **Allow live session playback** check box.

### Enable or disable playback protection

As a security precaution, Session Recording automatically encrypts recorded files that are downloaded for viewing in the Session Recording Player. This playback protection prevents recorded files from being copied and viewed by anyone other than the user who downloaded the file. The files cannot be played back on another workstation or by another user. Encrypted files are identified with an `.icle` extension. Unencrypted files are identified with an `.icl` extension. The files remain encrypted while they reside in `%localAppData%\Citrix\SessionRecording\Player\Cache` on the Session Recording Player until an authorized user opens them.

We recommend that you use HTTPS to protect the transfer of data.

By default, playback protection is enabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Playback** tab.
4. Select or clear the **Encrypt session recording files downloaded for playback** check box.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Enable and disable digital signing

July 18, 2018

If you install certificates on the computers on which the Session Recording components are installed, you can enhance the security of your Session Recording deployment by assigning digital signatures to Session Recording.

By default, digital signing is disabled. After you select the certificate to sign the recordings, Session Recording grants the read permission to the Session Recording Storage Manager Service.

### Enable digital signing

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Signing** tab.
4. Browse to the certificate that enables secure communication among the computers on which the Session Recording components are installed.

### Disable digital signing

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Signing** tab.
4. Click **Clear**.

## Specify where recordings are stored

October 18, 2018

Use Session Recording Server Properties to specify where recordings are stored and where archived recordings are restored for playback.

**Note:** To archive files or restore deleted files, use the ICLDB command.

### Specify directories for storing recordings

By default, recordings are stored in the drive:**\SessionRecordings** directory of the computer hosting the Session Recording Server. You can change the directory where the recordings are stored, add addi-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tional directories to load-balance across multiple volumes, or make use of additional space. Multiple directories in the list indicate that recordings are load-balanced across the directories. You can add a directory multiple times. Load balancing cycles through the directories.

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Storage** tab.
4. Use the **File storage directories** list to manage the directories where recordings are stored.

After you select the directories, Session Recording grants its service with Full Control permission to these directories.

You can create file storage directories on the local drive, the SAN volume, or a location specified by a UNC network path. Network mapped drive letters are not supported. Do not use Session Recording with Network-Attached Storage (NAS), due to serious performance and security problems associated with writing recording data to a network drive.

### Specify a directory for restoring archived recordings for playback

By default, archived recordings are restored in the drive:**\SessionRecordingsRestore** directory of the computer hosting the Session Recording Server. You can change the directory.

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Storage** tab.
4. In the **Restore directory for archived files** field, type your directory for restoring archived recordings.

## Specify file size for recordings

October 29, 2018

As recordings grow in size, the files can take longer to download and react more slowly when you use the seek slider to navigate during playback. To control file size, specify a threshold limit for a file. When the recording reaches this limit, Session Recording closes the file and opens a new one to continue recording. This action is called a rollover.

**Important:** The rollover setting does not apply to VDI desktop sessions for XenDesktop 7.8 and Session Recording Agent. In those cases, each recording file has a maximum size of 1GB and activities are not recorded after the limit is reached.

You can specify two thresholds for a rollover:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **File size.** When the file reaches the specified number of megabytes, Session Recording closes the file and opens a new one. By default, files roll over after reaching 50 megabytes; however, you can specify a limit from 10 megabytes to one gigabyte.
- **Duration.** After the session records for the specified number of hours, the file is closed and a new file is opened. By default, files roll over after recording for 12 hours; however, you can specify a limit from one to 24 hours.

Session Recording checks both fields to determine which event occurs first to determine when to roll over. For example, if you specify 17MB for the file size and six hours for the duration and the recording reaches 17MB in three hours, Session Recording reacts to the 17MB file size to close the file and open a new one.

To prevent the creation of many small files, Session Recording does not roll over until at least one hour elapses (this is the minimum number that you can enter) regardless of the value specified for the file size. The exception to this rule is if the file size surpasses one gigabyte.

### Specify the maximum file size for recordings

1. Log on to the computer hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Rollover** tab.
4. Enter an integer between 10 and 1,024 to specify the maximum file size in megabytes.
5. Enter an integer between 1 and 24 to specify the maximum recording duration in hours.

## Log administration activities

October 29, 2018

Session Recording Administrator Logging logs the following activities:

- Changes to recording policies on Session Recording Policy Console or Citrix Director.
- Changes in Session Recording Server Properties.
- Downloads of recordings in Session Recording Player.
- Recording a session by Session Recording after policy query.
- Unauthorized attempts to access the Administrator Logging service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **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.

### Disable or enable Administrator Logging

After installation, you can disable or enable the Session Recording Administrator Logging feature in Session Recording Server Properties.

1. As an administrator, log on to the server where Session Recording Administrator Logging is installed.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. Click the **Logging** tab.

When Session Recording Administrator Logging is disabled, no new activities are logged. You can query the existing logs from the web-based UI.

When **mandatory blocking** is enabled, the following activities are blocked if the logging fails. A system event is also logged with an Event ID 6001:

- Changes to recording policies on Session Recording Policy Console or Citrix Director.
- Changes in Session Recording Server Properties.

The recording of sessions is not impacted by the mandatory blocking setting.

### Grant access rights to users

For security reasons, grant users only the rights they need to perform specific functions, such as querying logs of Administrator Logging.

You grant rights to the users by assigning them to roles using Session Recording Authorization Console on the Session Recording Server. Administrator Logging has two roles:

- **LoggingWriter**. Grants the right to write the Administrator Logging logs. By default, local administrators and Network Service are members of this role.

  **Note:** Modifying the default **LoggingWriter** membership might cause log writing failure.

- **LoggingReader.** Grants the right to query the Administrator Logging logs. There is no default membership in this role.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### To assign users to roles

1. As an administrator, log on to the computer hosting the Session Recording Server.
2. Start **Session Recording Authorization Console**.
3. Select the role to which you want to assign users.
4. From the menu bar, choose **Action** > **Assign Windows Users and Groups**.
5. Add users and groups.

Any changes made to the console take effect during the update that occurs once every minute.

### Configure an Administrator Logging service account

By default, Administrator Logging is running as a web application in Internet Information Services (IIS), and its identity is Network Service. To enhance the security level, you can change the identity of this web application to a service account or a specific domain account.

1. As an administrator, log on to the computer hosting the Session Recording Server.
2. In IIS Manager, click **Application Pools.**
3. In **Application Pools**, right-click **SessionRecordingLoggingAppPool** and choose **Advanced Settings**.
4. Change the attribute **identity** to the specific account that you want to use.
5. Grant the **db_owner** permission to the account for the database **CitrixSessionRecordingLogging** on Microsoft SQL Server.
6. Grant the read permission to the account for the registry key at **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\S**

### Disable or enable the recording action logging

By default, Administrator Logging logs every recording action after the policy query completes. This might generate a large amount of loggings. To improve the performance and save the storage, disable this kind of logging in Registry.

1. As an administrator, log on to the computer hosting the Session Recording Server.
2. Open the Registry Editor.
3. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
4. Set the value of **EnableRecordingActionLogging** to:

   **0**: disable the recording action logging

   **1**: enable the recording action logging

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Query Administrator Logging data

Session Recording provides a web-based UI to query all the Administrator Loggings.

On the computer hosting the Session Recording Server:

1. From the **Start** menu, choose **Session Recording Administrator Logging**.
2. Enter the credentials of a **LoggingReader** user.

On other computers:

1. Open a web browser and visit the web page for Administrator Logging.

   **For HTTPS:** `https://servername/SessionRecordingLoggingWebApplication/`, where *servername* is the name of the computer hosting the Session Recording Server.

   **For HTTP:** `http://servername/SessionRecordingLoggingWebApplication/`, where *servername* is the name of the computer hosting the Session Recording Server.

2. Enter the credentials of a **LoggingReader** user.

## Install Session Recording with database high availability

March 11, 2021

Session Recording supports the following solutions for database high availability based on Microsoft SQL Server. The databases can automatically fail over when the hardware or software of a principal or primary SQL Server fails, which ensures that Session Recording continues to work as expected.

- Always On Availability Groups

The Always On Availability Groups feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. Introduced in SQL Server 2012, Always On Availability Groups maximizes the availability of a set of user databases for an enterprise. Always On Availability Groups requires that the SQL Server instances reside on the 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.

- SQL Server clustering

The Microsoft SQL clustering technology allows one server to automatically take over the tasks and responsibilities of the server that has failed. However, setting up this solution is complicated and the automatic failover is typically slower than alternatives such as SQL Server database mirroring. For more information, see https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/windows/always-on-failover-cluster-instances-sql-server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- SQL Server database mirroring

Database mirroring ensures that an automatic failover occurs in seconds if the active database server fails. This solution is more expensive than the other two solutions because full SQL Server licenses are required on each database server. You cannot use the SQL Server Express edition in a mirrored environment. For more information, see https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/database-mirroring-sql-server.

### Methods for installing Session Recording with database high availability

To install Session Recording with database high availability, do either of the following:

- Install the Session Recording Server components first and then configure database high availability for the created databases.
  You can install the Session Recording Administration components with databases configured to be installed on the prepared SQL Server instance and then configure database high availability for the created databases.
  - For Always On Availability Groups and clustering, you must manually change the SQL Server instance name to the name of the availability group listener or SQL Server network in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance.
  - For database mirroring, you must manually add the failover partners for databases in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner and HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner
- Configure database high availability for empty databases first and then install the Session Recording Administration components.
  You can create two empty databases as the Session Recording Database and the Administrator Logging Database in the expected primary SQL Server instance and configure high availability. Then enter the SQL Server instance name when installing the Session Recording Server components:
  - To use the Always On Availability Groups solution, enter the name of your availability group listener.
  - To use the database mirroring solution, enter the name of your principal SQL Server.
  - To use the clustering solution, enter the network name of your SQL Server.

## View recordings

October 29, 2018

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Use Session Recording Player to view, search, and bookmark recorded XenApp or XenDesktop sessions.

If sessions are recorded with the live playback feature enabled, you can view sessions that are in progress, with a delay of a few seconds, as well as sessions that are completed.

Sessions that have a longer duration or larger file size than the limits configured by your Session Recording administrator appear in more than one session file.

**Note:** A Session Recording administrator must grant users the right to access the recorded sessions of VDAs for Server OS. If you are denied access to viewing sessions, contact your Session Recording administrator.

When Session Recording Player is installed, the Session Recording administrator typically sets up a connection between the Session Recording Player and a Session Recording Server. If this connection is not set up, the first time you perform a search for files, you are prompted to set it up. Contact your Session Recording administrator for setup information.

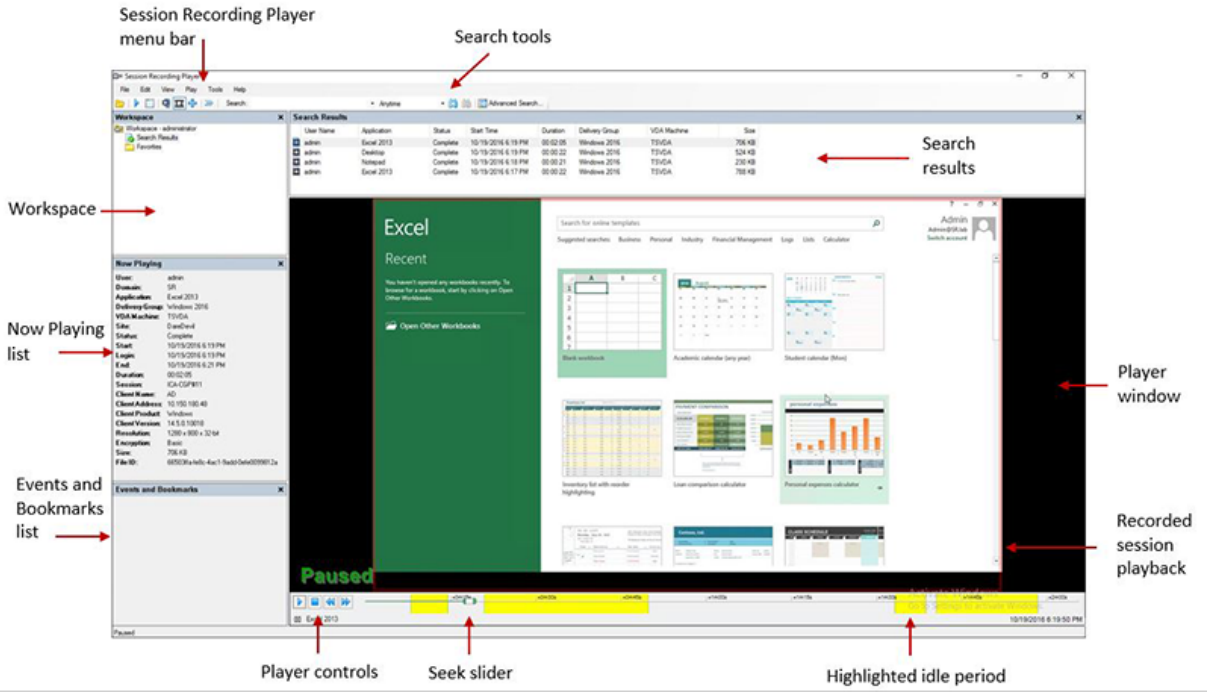
### Launch the Session Recording Player

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.

   The Session Recording Player appears.

This illustration shows the Session Recording Player with callouts indicating its major elements. The functions of these elements are described throughout the following articles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




### Display or hide window elements

The Session Recording Player has window elements that toggle on and off.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View**.
4. Choose the elements that you want to display. Selecting an element causes it to appear immediately. A check mark indicates that the element is selected.

### Change Session Recording Servers

If the Session Recording administrator sets up your Session Recording Player with the ability to connect to multiple Session Recording Servers, you can select the Session Recording Server that the Session Recording Player connects to. The Session Recording Player can connect to only one Session Recording Server at a time.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections** .
4. Select the Session Recording Server to which you want to connect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Open and play recordings

August 17, 2021

You can open session recordings in Session Recording Player in three ways:

- Perform a search using the Session Recording Player. Recorded sessions that meet the search criteria appear in the search results area.
- Access recorded session files directly from your local disk drive or a shared drive.
- Access recorded session files from a Favorites folder

When you open a file that was recorded without a digital signature, a warning message appears telling you that the origin and integrity of the file were not verified. If you are confident of the integrity of the file, click **Yes** in the warning window to open the file.

**Note:** The Administrator Logging feature of Session Recording allows you to log the downloads of recordings in the Session Recording Player. For more information, see Log administration activities.

## Open and play a recording in the search results area

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Perform a search.
4. If the search results area is not visible, select **Search Results** in the Workspace pane.
5. In the search results area, select the session you want to play.
6. Do any of the following:
    - Double-click the session.
    - Right-click and select **Play**.
    - From the **Session Recording Player** menu bar, choose **Play** > **Play**.

## Open and play a recording by accessing the file

The name of a recorded session file begins with "i_", which is followed by a unique alphanumeric file ID and then the .icl or .icle file extension. The .icl extension denotes the recordings without playback protection applied; the .icle extension denotes the recordings with playback protection applied. Recorded session files are saved in a folder that incorporates the date the sessions were recorded. For example, the file for a session recorded on December 22, 2014, is saved in folder path 2014\12\22.

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. Do any of the following:

    - From the **Session Recording Player** menu bar, choose **File** > **Open** and browse for the file.
    - Using Windows Explorer, navigate to the file and drag the file into the **Player** window.
    - Using Windows Explorer, navigate to and double-click the file.
    - If you created Favorites in the Workspace pane, select **Favorites** and open the file from the Favorites area in the same way you open files from the search results area.

### Use favorites

Creating the Favorites folders allows you to quickly access recordings that you view frequently. These Favorites folders reference recorded session files that are stored on your workstation or on a network drive. You can import and export these files to other workstations and share these folders with other Session Recording Player users.

**Note**: Only users with access rights to the Session Recording Player can download the recorded session files associated with the Favorites folders. Contact your Session Recording administrator for the access rights.

To create a Favorites subfolder:

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. In the **Session Recording Player** window, select the **Favorites** folder in your Workspace pane.
4. From the menu bar, choose **File** > **Folder** > **New Folder**. A new folder appears under the **Favorites** folder.
5. Type the folder name, then press **Enter** or click anywhere to accept the new name.

Use the other options that appear in the **File** > **Folder** menu to delete, rename, move, copy, import, and export the folders.

## Play recorded sessions

October 29, 2018

After you open a recorded session in the Session Recording Player, you can navigate through the recorded sessions using these methods:

- Use the player controls to play, stop, pause, and increase or decrease playback speed.
- Use the seek slider to move forward or backward.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If you have inserted markers into the recording or if the recorded session contains custom events, you can also navigate through the recorded session by going to those markers and events.

**Note:**

- During playback of a recorded session, a second mouse pointer might appear. The second pointer appears at the point in the recording when the user navigated within Internet Explorer and clicked an image that was originally larger than the screen but was scaled down automatically by Internet Explorer. While only one pointer appears during the session, two might appear during playback.
- This version of Session Recording does not support SpeedScreen Multimedia Acceleration for XenApp or the Flash quality adjustment policy setting for XenApp. When this option is enabled, playback displays a black square.
- Session Recording cannot record the Lync webcam video when using the HDX RealTime Optimization Pack.
- When you record a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance.
- You cannot record Windows 7 desktop sessions correctly when **Legacy Graphics Mode** is enabled by the XenDesktop site policy and **Disk-based Caching** is enabled by the Citrix Receiver for Windows policy. Those recordings show a black screen.
  As a workaround, disable **Disk-based Caching** with GPO on the machines where you installed Citrix Receiver for Windows. For more information about disabling **Disk-based Caching**, see CTX123169.
- Session Recording does not support the Framehawk display mode. Sessions in Framehawk display mode cannot be recorded and played back correctly. Sessions recorded in Framehawk display mode might not contain the sessions' activities.

### Use player controls

You can click the player controls in the lower part of the Player window or access them by choosing **Play** from the **Session Recording Player** menu bar. Use Player controls to:

| Player Control | Function |
|---|---|
| | Plays the selected session file. |
| | Pauses playback. |
| | Stops playback. If you click **Stop**, then **Play**, the recording restarts at the beginning of the file. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Player Control | Function |
| --- | --- |
| | Halves the current playback speed down to a minimum of one-quarter normal speed. |
| | Doubles the current playback speed up to a maximum of 32 times normal speed. |

### Use the seek slider

Use the seek slider in the lower part of the Player window to jump to a different position within the recorded session. You can drag the seek slider to the point in the recording you want to view or click anywhere on the slider bar to move to that location.

You can also use the following keyboard keys to control the seek slider:

| Key | Seek action |
| --- | --- |
| Home | Seeks to the beginning. |
| End | Seeks to the end. |
| Right Arrow | Seeks forward five seconds. |
| Left Arrow | Seeks backward five seconds. |
| Move mouse wheel one notch down | Seeks forward 15 seconds. |
| Move mouse wheel one notch up | Seeks backward 15 seconds. |
| Ctrl + Right Arrow | Seeks forward 30 seconds. |
| Ctrl + Left Arrow | Seeks backward 30 seconds. |
| Page Down | Seeks forward one minute. |
| Page Up | Seeks backward one minute. |
| Ctrl + Move mouse wheel one notch down | Seeks forward 90 seconds. |
| Ctrl + Move mouse wheel one notch up | Seeks backward 90 seconds. |
| Ctrl + Page Down | Seeks forward six minutes. |
| Ctrl + Page Up | Seeks backward six minutes. |

To adjust the speed of the seek slider: From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Player** and drag the slider to increase or decrease the seek response time. A faster response

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

time requires more memory. The response might be slow depending on the size of the recordings and your machine's hardware.

### Change the playback speed

You can set Session Recording Player to play recorded sessions in exponential increments from one-quarter normal playback speed to 32 times normal playback speed.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play** > **Play Speed**.
4. Choose a speed option.

The speed adjusts immediately. A number indicating the increased or decreased speed appears below the Player window controls. Text indicating the exponential rate appears briefly in green in the Player window.

### Highlight the idle periods of recorded sessions

Idle periods of a recorded session are the portions in which no action takes place. The Session Recording Player can highlight the idle periods of recorded sessions when played back. The option is **On** by default.

Note that idle periods are not highlighted when playing back the live sessions with Session Recording Player.

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View** > **Idle Periods** and check or uncheck the option box.

### Skip over spaces where no action occurred

Fast review mode allows you to set Session Recording Player to skip the portions of recorded sessions in which no action takes place. This setting saves time for playback viewing; however, it does not skip animated sequences such as animated mouse pointers, flashing cursors, or displayed clocks with second hand movements.

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play** > **Fast Review Mode**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The option toggles on and off. Each time you choose it, its status appears briefly in green in the Player window.

## Use events and bookmarks

October 29, 2018

You can use events and bookmarks to help you navigate through recorded sessions.

Events are inserted to sessions as they are recorded, using the Event API and a third-party application. Events are saved as part of the session file. You cannot delete or alter them using the Session Recording Player.

Bookmarks are markers you insert to a recorded session during session playback using the Session Recording Player. After insertion, bookmarks are associated with the recorded session until you delete them, but they are not saved as part of the session file. Bookmarks are stored as separate ".iclb"files in the **Bookmarks** cache folder on the Session Recording Player, for example, C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks, with the same file names as the ".icl"recording files. If you want to play back a recording file with bookmarks on another Player, copy the ".iclb"files to the **Bookmarks** cache folder on that Player. By default, each bookmark is labeled with the text "Bookmark,"but you can change this to any text annotation up to 128 characters long.

Events and bookmarks appear as dots in the lower part of the Player window. Events appear as yellow dots; bookmarks appear as blue dots. Moving the mouse over these dots displays the text label associated with them. You can also display the events and bookmarks in the **Events and Bookmarks** list of the Session Recording Player. They appear in this list with their text labels and the times in the recorded session at which they appear, in chronological order.

You can use events and bookmarks to help you navigate through recorded sessions. By going to an event or bookmark, you can skip to the point in the recorded session where the event or bookmark is inserted.

### Display events and bookmarks in the list

The **Events and Bookmarks** list displays the events and bookmarks inserted in the recorded session that is currently playing. It can show events only, bookmarks only, or both.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. Move the mouse pointer to the **Events and Bookmarks** list area and right-click to display the menu.
4. Choose **Show Events Only**, **Show Bookmarks Only**, or **Show All**.

### Insert a bookmark

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing the recorded session to which you want to add a bookmark.
4. Move the seek slider to the position where you want to insert the bookmark.
5. Move the mouse pointer into the Player window area and right-click to display the menu.
6. Add a bookmark with the default **Bookmark** label or create an annotation:
    - To add a bookmark with the default **Bookmark** label, choose **Add Bookmark**.
    - To add a bookmark with a descriptive text label that you create, choose **Add Annotation**. Type the text label you want to assign to the bookmark, up to 128 characters. Click **OK**.

### Add or change an annotation

After a bookmark is created, you can add an annotation to it or change its annotation.

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the events and bookmarks list is displaying bookmarks.
5. Select the bookmark in the **Events and Bookmarks** list and right-click to display the menu.
6. Choose **Edit Annotation**.
7. In the window that appears, type the new annotation and click **OK**.

### Delete a bookmark

1. Log on to the workstation where Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the events and bookmarks list is displaying bookmarks.
5. Select the bookmark in the events and bookmarks list and right-click to display the menu.
6. Choose **Delete**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Go to an event or bookmark

Going to an event or bookmark causes the Session Recording Player to go to the point in the recorded session where the event or bookmark is inserted.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing a session recording containing events or bookmarks.
4. Go to an event or bookmark:
    - In the lower part of the Player window, click the dot representing the event or bookmark to go to the event or bookmark.
    - In the **Events and Bookmarks** list, double-click the event or bookmark to go to it. To go to the next event or bookmark, select any event or bookmark from the list, right-click to display the menu, and choose **Seek to Bookmark**.

## Change the playback display

October 29, 2018

Options allow you to change how recorded sessions appear in the Player window. You can pan and scale the image, show the playback in full screen, display the Player window in a separate window, and display a red border around the recorded session to differentiate it from the Player window background.

### Display the Player window in full screen

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View** > **Player Full Screen**.
4. To return to the original size, press ESC or F11.

### Display the Player window in a separate window

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View** > **Player in Separate Window**. A new window appears containing the Player window. You can drag and resize the window.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. To embed the Player window in the main window, choose **View** >**Player in Separate Window**, or press **F10**.

### Scale the session playback to fit the Player window

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play** >**Panning and Scaling** > **Scale to Fit**.

    - **Scale to Fit (Fast Rendering)** shrinks images while providing good quality. Images are drawn quicker than using the High Quality option but the images and texts are not sharp. Use this option if you are experiencing performance issues when using the High Quality mode.
    - **Scale to Fit (High Quality)** shrinks images while providing high quality. Using this option can cause the images to be drawn more slowly than the Fast Rendering option.

### Pan the image

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play** > **Panning and Scaling** > **Panning**. The pointer changes to a hand and a small representation of the screen appears in the top right of the Player window.
4. Drag the image. The small representation indicates where you are in the image.
5. To stop panning, choose one of the scaling options.

### Display a red border around Session Recording

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Player**.
4. Select the **Show border around session recording** check box.
   **Tip:** If the **Show border around session recording** check box is not selected, you can temporarily view the red border by clicking and holding down the left mouse button while the pointer is in the Player window.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Cache recorded session files

April 26, 2019

Each time you open a recorded session file, the Session Recording Player downloads the file from the location where the recordings are stored. If you download the same files frequently, you can save download time by caching the files on your workstation. Cached files are stored on your workstation in this folder:

```
userprofile\\AppData\\Local\\Citrix\\SessionRecording\\Player\\Cache
```

You can specify how much disk space is used for the cache. When the recordings fill the specified disk space, Session Recording deletes the oldest, least used recordings to make room for new recordings. You can empty the cache at any time to free up disk space.

### Enable caching

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Cache**.
4. Select the **Cache downloaded files on local machine** check box.
5. If you want to limit the amount of disk space used for caching, select the **Limit amount of disk space to use** check box and specify the number of megabytes to be used for cache.
6. Click **OK**.

### Empty caches

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Cache**.
4. Select the **Cache downloaded files on local machine** check box.
5. In the Session Recording Player, choose **Tools** > **Options** > **Cache**.
6. Click **Purge Cache** and **OK** to confirm the action.

## Search for recordings

October 29, 2018

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The Session Recording Player allows you to perform quick and advanced searches and to specify options that apply to all searches. Results of searches appear in the search results area of the Session Recording Player.

> **Note:**
>
> To display all available recorded sessions, up to the maximum number of sessions that might appear in a search, perform a search without specifying any search parameters.

### Perform a quick search

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Define your search criteria:
    - Enter a search criterion in the **Search** field.
    - Move the mouse pointer over the **Search** label to display a list of parameters to use as a guideline.
    - Click the arrow to the right of the **Search** field to display the text for the last 64 searches you performed.
    - Use the drop-down list to the right of the **Search** field to select a period or duration specifying when the session was recorded.
4. Click the binocular icon to the right of the drop-down list to start the search.

### Perform an advanced search

Advanced searches might take up to 20 seconds to return results containing more than 150,000 entities. Citrix recommends using more accurate search conditions such as a date range or user to reduce the result number.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. In the **Session Recording Player** window, click **Advanced Search** on the tool bar or choose **Tools** > **Advanced Search**.
4. Define your search criteria on the tabs of the **Advanced Search** dialog box:
    - **Common** allows you to search by domain or account authority, site, group, VDA for Server OS, application, or file ID.
    - **Date/Time** allows you to search date, day of week, and time of day.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Events** allows you to search for Citrix-defined and custom events that are inserted to the sessions.
- **Other** allows you to search by session name, client name, client address, and recording duration. It also allows you to specify, for this search, the maximum number of search results displayed and whether or not archived files are included in the search.
  When you specify search criteria, the query you are creating appears in the pane at the bottom of the dialog box.

5. Click **Search** to start the search.

   You can save and retrieve advanced search queries. Click **Save** in the **Advanced Search** dialog box to save the current query. Click **Open** in the **Advanced Search** dialog box to retrieve a saved query. Queries are saved as files with an .isq extension.

### Set search options

The Session Recording Player search options allow you to limit the maximum number of session recordings that appear in search results and to specify whether or not search results include archived session files.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Search**.
4. In the **Maximum result to display** field, type the number of search results you want to display. A maximum of 500 results can be displayed.
5. To set whether or not archived files are included in searches, select or clear **Include archived files**.

## Troubleshoot Session Recording

March 11, 2021

The troubleshooting information contains solutions to some issues you might encounter during and after installing the Session Recording components:

- Components failing to connect to each other
- Sessions failing to record
- Problems with the Session Recording Player or Session Recording Policy Console
- Issues involving your communication protocol

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **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.

### Session Recording Agent cannot connect

When the Session Recording Agent cannot connect, the **Exception caught while sending poll messages to Session Recording Broker** event message is logged, followed by the exception text. The exception text provides reasons why the connection failed. The reasons include:

- **The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel.** This exception means that the Session Recording Server is using a certificate that is signed by a CA that the server on which the Session Recording Agent resides does not trust, or have a CA certificate for. Alternatively, the certificate might have expired or been revoked.

  Resolution: Verify that the correct CA certificate is installed on the server hosting the Session Recording Agent or use a CA that is trusted.

- **The remote server returned an error: (403) forbidden.** This is a standard HTTPS error displayed when you attempt to connect using HTTP (nonsecure protocol). The computer hosting the Session Recording Server rejects the connection because it accepts only secure connections.

  Resolution: Use Session Recording Agent Properties to change the Session Recording Broker protocol to **HTTPS**.

**The Session Recording Broker returned an unknown error while evaluating a record policy query. Error code 5 (Access Denied). For more information, see the Event log on the Session Recording Server.** This error occurs when sessions are started and a request for a record policy evaluation is made. The error is a result of the Authenticated Users group (this is the default member) being removed from the Policy Query role of the Session Recording Authorization Console.

Resolution: Add the Authenticated Users group back into this role, or add each server hosting each Session Recording Agent to the PolicyQuery role.

**The underlying connection was closed. A connection that was expected to be kept alive was closed by the server.** This error means that the Session Recording Server is down or unavailable to accept requests. This could be due to IIS being offline or restarted, or the entire server might be offline.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Resolution: Verify that the Session Recording Server is started, IIS is running on the server, and the server is connected to the network.

### Installation of Session Recording Server components fails

The installation of the Session Recording Server components fails with error codes 2503 and 2502.
Resolution:
Check the access control list (ACL) of folder C:\windows\Temp to ensure that the Local Users and Groups have write permission for this folder. If not, manually add write permission.

### Session Recording Server cannot connect to the Session Recording Database

When the Session Recording Server cannot connect to the Session Recording Database, you might see a message similar to one of the following:

**Event Source:**

**A network-related or instance-specific error occurred while establishing a connection to SQL Server**. This error appears in the applications event log with ID 2047 in the Event Viewer of the computer hosting the Session Recording Server.

**Citrix Session Recording Storage Manager Description: Exception caught while establishing database connection.** This error appears in the applications event log in the Event Viewer of the computer hosting the Session Recording Server.

**Unable to connect to the Session Recording Server. Ensure that the Session Recording Server is running.** This error message appears when you launch the Session Recording Policy Console.

Resolution:

- The Express Edition of Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014, or Microsoft SQL Server 2016 is installed on a stand-alone server and does not have the correct services or settings configured for Session Recording. The server must have TCP/IP protocol enabled and SQL Server Browser service running. See the Microsoft documentation for information about enabling these settings.
- During the Session Recording installation (administration portion), incorrect server and database information was given. Uninstall the Session Recording Database and reinstall it, supplying the correct information.
- The Session Recording Database Server is down. Verify that the server has connectivity.
- The computer hosting the Session Recording Server or the computer hosting the Session Recording Database Server cannot resolve the FQDN or NetBIOS name of the other. Use the ping command to verify the names can be resolved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Check the firewall configuration on the Session Recording Database to ensure that the SQL Server connections are allowed. For more information, see the Microsoft article at https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access.

**Logon failed for user 'NT_AUTHORITY\ANONYMOUS LOGON'.** This error message means that the services are logged on incorrectly as .\administrator.

Resolution: Restart the services as local system user and restart the SQL services.

### Sessions are not recording

If your application sessions are not recording successfully, start by checking the application event log in the Event Viewer on the VDA for Server OS that runs the Session Recording Agent and Session Recording Server. This might provide valuable diagnostic information.

If sessions are not recording, these issues might be the cause:

- **Component connectivity and certificates**. If the Session Recording components cannot communicate with each other, this can cause session recordings to fail. To troubleshoot recording issues, verify that all components are configured correctly to point to the correct computers and that all certificates are valid and correctly installed.
- **Non-Active Directory domain environments**. Session Recording is designed to run in a Microsoft Active Directory domain environment. If you are not running in an Active Directory environment, you might experience recording issues. Ensure that all Session Recording components are running on computers that are members of an Active Directory domain.
- **Session sharing conflicts with the active policy.** Session Recording matches the active policy with the first published application that a user opens. Subsequent applications opened during the same session continue to follow the policy that is in force for the first application. To prevent session sharing from conflicting with the active policy, publish the conflicting applications on separate VDAs for Server OS.
- **Recording is not enabled.** By default, installing the Session Recording Agent on a VDA for Server OS enables the server for recording. Recording will not occur until an active recording policy is configured to allow this.
- **The active recording policy does not permit recording.** For a session to be recorded, the active recording policy must permit the sessions for the user, server, or published application to be recorded.
- **Session Recording services are not running.** For sessions to be recorded, the Session Recording Agent service must be running on a VDA for Server OS and the Session Recording Storage Manager service must be running on the computer hosting the Session Recording Server.
- **MSMQ is not configured.** If MSMQ is not correctly configured on the server running the Session Recording Agent and the computer hosting the Session Recording Server, recording problems

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

might occur.

### Unable to view live session playback

If you experience difficulties when viewing recordings using the Session Recording Player, the following error message might appear:

**Download of recorded session file failed. Live session playback is not permitted. The server has been configured to disallow this feature.** This error indicates that the server is configured to disallow the action.

Resolution: In **Session Recording Server Properties**, choose the **Playback** tab and select the **Allow live session playback** check box.

### Recordings are corrupt or incomplete

- If recordings are corrupted or incomplete when you view them using the Session Recording Player, you might also see warnings in the Event logs on the Session Recording Agent.

  **Event Source**: Citrix Session Recording Storage Manager

  **Description**: Data lost while recording file <icl file name>

  This usually happens when Machine Creation Services (MCS) or Provisioning Services (PVS) is used to create VDAs with a master image configured and Microsoft Message Queuing (MSMQ) installed. In this condition, the VDAs have the same QMId for MSMQ.

  As a workaround, create a unique QMId for each VDA. For more information, see Step 8 in the **Install the Session Recording Agent** section of Install, upgrade, and uninstall Session Recording.

- Session Recording Player might report an internal error with this message - "**The file being played has reported that an internal system error (error code: 9) occurred during its original recording. The file can still be played up to the point that the recording error occurred**" when playing back a certain recording file.

  This is usually caused by insufficient Session Recording Agent buffer size when recording graphic intensive sessions.

  As a workaround, change the registry value of HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmA to a higher one in the Session Recording Agent, and then restart the machine.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Test connection of the database instance failed when installing the Session Recording Database or Session Recording Server

When you install the Session Recording Database or Session Recording Server, the test connection fails with the error message **Database connection test failed. Please correct Database instance name** even if the database instance name is correct.

In this case, make sure that the current user has the public SQL Server role permission to correct the permission limitation failure.

### Administrator Logging

In Windows Server 2008 R2 SP1, before you install the Administrator Logging feature, install **.Net Framework 3.5 Features** > **WCF Activation** > **HTTP Activation**, and then install .Net Framework 4.5 or a later version. Ensure that you don't install these two requirements in reverse order. If you fail to comply, Administrator Logging might not work as expected. You might experience operation blocking when trying to change Session Recording configurations with the Server Properties Console or update Session Recording policies with Policy Console with mandatory logging enabled.

To resolve this issue:

1. Open the Internet Information Services (IIS) Manager and navigate to the **Application Pools** node.
2. Right-click **SessionRecordingLoggingAppPool** and open the **Basic Settings** dialog box.
3. Change the .NET Framework version to .NET Framework v4.0.

## Verify component connections

July 23, 2018

During the setup of Session Recording, the components might not connect to other components. All the components communicate with the Session Recording Server (Broker). By default, the Broker (an IIS component) is secured using the IIS default website certificate. If one component cannot connect to the Session Recording Server, the other components might also fail when attempting to connect.

The Session Recording Agent and Session Recording Server (Storage Manager and Broker) log connection errors in the applications event log in the Event Viewer of the computer hosting the Session Recording Server, while the Session Recording Policy Console and Session Recording Player display connection error messages on screen when they fail to connect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Verify that the Session Recording Agent is connected

1. Log on to the server where the Session Recording Agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. In **Session Recording Agent Properties**, click **Connection**.
4. Verify that the value for the Session Recording Server is the correct server name of the computer hosting the Session Recording Server.
5. Verify that the server given as the value for the Session Recording Server can be contacted by your VDA for Server OS.

**Note:** Check the application event log for errors and warnings.

### Verify that the Session Recording Server is connected

**Caution: Using Registry Editor can cause serious problems that might require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.**

1. Log on to the computer hosting the Session Recording Server.
2. Open the Registry Editor.
3. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Verify that the value of **SmAudDatabaseInstance** correctly references the Session Recording Database you installed on your SQL Server instance.

### Verify that the Session Recording Database is connected

1. Using a SQL Management tool, open your SQL instance that contains the Session Recording Database you installed.
2. Open the Security permissions of the Session Recording Database.
3. Verify that the Session Recording Computer Account has access to the database. For example, if the computer hosting the Session Recording Server is named **SsRecSrv** in the MIS domain, the computer account in your database must be configured as **MIS\SsRecSrv$**. This value is configured during the Session Recording Database installation.

### Test IIS connectivity

Testing connections to the Session Recording Server IIS site by using a Web browser to access the Session Recording Broker webpage can help you determine whether problems with communication between Session Recording components stem from misconfigured protocol configuration, certification issues, or problems starting Session Recording Broker.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To verify IIS connectivity for the Session Recording Agent:

1. Log on to the server where the Session Recording Agent is installed.
2. Open a Web browser and type the following address:
    - For HTTPS: `https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, where *servername* is the name of the computer hosting the Session Recording Server.
    - For <HTTP: `http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, where *servername* is the name of the computer hosting the Session Recording Server.
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

To verify IIS connectivity for the Session Recording Player:

1. Log on to the workstation where the Session Recording Player is installed.
2. Open a Web browser and type the following address:
    - For HTTPS: `https://servername/SessionRecordingBroker/Player.rem?wsdl`, where *servername* is the name of the computer hosting the Session Recording Server.
    - For HTTP: `http://servername/SessionRecordingBroker/Player.rem?wsdl`, where *servername* is the name of the computer hosting the Session Recording Server.
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

To verify IIS connectivity for the Session Recording Policy Console:

1. Log on to the server where the Session Recording Policy Console is installed.
2. Open a Web browser and type the following address:
    - For HTTPS: `https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, where *servername* is the name of the computer hosting the Session Recording Server.
    - For HTTP: `http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, where *servername* is the name of the computer hosting the Session Recording Server.
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

If you see an XML document within your browser, it verifies that the computer running the Session Recording Policy Console is connected to the computer hosting the Session Recording Server using the configured protocol.

### Troubleshoot certificate issues

If you are using HTTPS as your communication protocol, the computer hosting the Session Recording Server must be configured with a server certificate. All component connections to the Session Recording Server must have root certificate authority (CA). Otherwise, attempted connections between the components fail.

You can test your certificates by accessing the Session Recording Broker webpage as you would when testing IIS connectivity. If you are able to access the XML page for each component, the certificates are configured correctly.

Here are some common ways certificate issues cause connections to fail:

- **Invalid or missing certificates.** If the server running the Session Recording Agent does not have a root certificate to trust the server certificate and cannot trust and connect to the Session Recording Server over HTTPS, causing connectivity to fail, verify that all components trust the server certificate on the Session Recording Server.
- **Inconsistent naming.** If the server certificate assigned to the computer hosting the Session Recording Server is created using an FQDN, all connecting components must use the FQDN when connecting to the Session Recording Server. If a NetBIOS name is used, configure the components with a NetBIOS name for the Session Recording Server.
- **Expired certificates.** If a server certificate expired, connectivity to the Session Recording Server through HTTPS fails. Verify the server certificate assigned to the computer hosting the Session Recording Server is valid and has not expired. If the same certificate is used for the digital signing of session recordings, the event log of the computer hosting the Session Recording Server provides error messages that the certificate expired or warning messages when it is about to expire.

## Search for recordings using the Player fails

October 29, 2018

If you experience difficulties when searching for recordings using the Session Recording Player, the following error messages might appear:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Search for recorded session files failed. The remote server name could not be resolved: servername.** The **servername** is the name of the server to which the Session Recording Player is attempting to connect. The Session Recording Player cannot contact the Session Recording Server. Two possible reasons are an incorrectly typed server name or that the DNS cannot resolve the server name.

  Resolution: From the Player menu bar, choose **Tools** > **Options** > **Connections** and verify that the server name in the **Session Recording Servers** list is correct. If it is correct, from a command prompt, run the ping command to see if the name can be resolved. When the Session Recording Server is down or offline, the search for recorded session files failed error message is **Unable to contact the remote server**.

- **Unable to contact the remote server.** This error occurs when the Session Recording Server is down or offline.

  Resolution: Verify that the Session Recording Server is connected.

- **Access denied.** An access denied error can occur if the user was not given permission to search for and download recorded session files.

  Resolution: Assign the user to the Player role using the Session Recording Authorization Console.

- **Access denied when the Player role is assigned.** This error occurs when you install the Session Recording Player on the same machine with the Session Recording Server, and you have enabled UAC. When you assign the Domain Admins or Administrators user group as the Player role, a non-built-in administrator user who is included in that group might fail to pass the role-based check when searching recording files with the Session Recording Player.

  Resolutions:

  - Run Session Recording Player as administrator.
  - Assign specific users as Player role rather than the entire group.
  - Install Session Recording Player in a separate machine rather than Session Recording Server.

- **Search for recorded session files failed. The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel.** This exception is caused by the Session Recording Server using a certificate that is signed by a CA that the client device does not trust or have a CA certificate for.

  Resolution: Install the correct or trusted CA certificate workstation where the Session Recording Player is installed.

- **The remote server returned an error: (403) forbidden.** This error is a standard HTTPS error that occurs when you attempt to connect using HTTP (nonsecure protocol). The server rejects

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

the connection because, by default, it is configured to accept only secure connections.

Resolution: From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections**. Select the server from the **Session Recordings Servers** list, and click **Modify**. Change the protocol from **HTTP** to **HTTPS**.

### Troubleshoot MSMQ

If a notification message is given but the viewer cannot find recordings after a search in the Session Recording Player, there is a problem with MSMQ. Verify that the queue is connected to the Session Recording Server (Storage Manager). Use a Web browser to test for connection errors (if you are using HTTP or HTTPS as your MSMQ communication protocol).

To verify that the queue is connected:

1. Log on to the server hosting the Session Recording Agent and view the outgoing queues.
2. Verify that the queue to the computer hosting the Session Recording Server has a connected state.
    - If the state is **waiting to connect**, there are messages in the queue, and the protocol is HTTP or HTTPS (corresponding to the protocol selected on the **Connections** tab in **Session Recording Agent Properties**), perform Step 3.
    - If the state is **connected** and there are no messages in the queue, there might be a problem with the server hosting the Session Recording Server. Skip Step 3 and perform Step 4.
3. If there are messages in the queue, open a Web browser and type the following address:
    - For HTTPS: `https://servername/msmq/private$/CitrixSmAudData`, where *servername* is the name of the computer hosting the Session Recording Server.
    - For HTTP: `http://servername/msmq/private$/CitrixSmAudData`, where *servername* is the name of the computer hosting the Session Recording Server.

    If the page returns an error such as **The server only accepts secure connections**, change the MSMQ protocol listed in **Session Recording Agent Properties** to HTTPS. If the page reports a problem with the website security certificate, there might be a problem with a trust relationship for the TLS secure channel. In that case, install the correct CA certificate or use a CA that is trusted.
4. If there are no messages in the queue, log on to the computer hosting the Session Recording Server and view private queues. Select **citrixsmauddata**. If there are messages in the queue (Number of Messages Column), verify that the Session Recording StorageManager service is started. If it is not, restart the service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Change your communication protocol

October 29, 2018

For security reasons, Citrix does not recommend using HTTP as a communication protocol. The Session Recording installation is configured to use HTTPS. To use HTTP instead of HTTPS, you must change several settings.

## Use HTTP as the communication protocol

1. Log on to the computer hosting the Session Recording Server and disable secure connections for Session Recording Broker in IIS.
2. Change the protocol setting from HTTPS to HTTP in **Session Recording Agent Properties** on each server where the Session Recording Agent is installed:
    a) Log on to each server where the Session Recording Agent is installed.
    b) From the **Start** menu, choose **Session Recording Agent Properties**.
    c) In **Session Recording Agent Properties**, choose the **Connections** tab.
    d) In the **Session Recording Broker** area, select **HTTP** from the **Protocol** drop-down list and click **OK** to accept the change. If you are prompted to restart the service, click **Yes**.
3. Change the protocol setting from HTTPS to HTTP in the Session Recording Player settings:
    a) Log on to each workstation where the Session Recording Player is installed.
    b) From the **Start** menu, choose **Session Recording Player**.
    c) From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections**, select the server, and choose **Modify**.
    d) Select **HTTP** from the **Protocol** drop-down list and click **OK** twice to accept the change and exit the dialog box.
4. Change the protocol setting from HTTPS to HTTP in the Session Recording Policy Console:
    a) Log on to the server where the Session Recording Policy Console is installed.
    b) From the **Start** menu, choose **Session Recording Policy Console**.
    c) Select **HTTP** from the **Protocol** drop-down list and click **OK** to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording Policy Console.

## Revert to HTTPS as the communication protocol

1. Log on to the computer hosting the Session Recording Server and enable secure connections for the Session Recording Broker in IIS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. Change the protocol setting from HTTP to HTTPS in **Session Recording Agent Properties** on each server where the Session Recording Agent is installed:
    a) Log on to each server where the Session Recording Agent is installed.
    b) From the **Start** menu, choose **Session Recording Agent Properties**.
    c) In **Session Recording Agent Properties**, choose the **Connections** tab.
    d) In the **Session Recording Broker** area, select **HTTPS** from the **Protocol** drop-down list and click **OK** to accept the change. If you are prompted to restart the service, click **Yes**.
3. Change the protocol setting from HTTP to HTTPS in the Session Recording Player settings:
    a) Log on to each workstation where the Session Recording Player is installed.
    b) From the **Start** menu, choose **Session Recording Player**.
    c) From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections**, select the server, and choose **Modify**.
    d) Select **HTTPS** from the **Protocol** drop-down list and click **OK** twice to accept the change and exit the dialog box.
4. Change the protocol setting from HTTP to HTTPS in the Session Recording Policy Console:
    a) Log on to the server where the Session Recording Policy Console is installed.
    b) From the **Start** menu, choose **Session Recording Policy Console**.
    c) Select **HTTPS** from the **Protocol** drop-down list and click **OK** to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording Policy Console.

## Manage your database records

February 13, 2019

The ICA Log database (ICLDB) utility is a database command-line utility used to manipulate the session recording database records. This utility is installed during the Session Recording installation in the drive:\Program Files\Citrix\SessionRecording\Server\Bin directory at the server hosting the Session Recording Server software.

### Quick reference chart

The following table lists the commands and options that are available for the ICLDB utility. Type the commands using the following format:

icldb [version | locate | dormant | import | archive | remove | removeall] command-options [/l] [/f] [/s] [/?]

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

> **Note:**
>
> More extensive instructions are available in the help associated with the utility. To access the help, from a command prompt, type drive:**\Program Files\Citrix\SessionRecording\Server\Bin** directory, type **icldb /?**. To access help for specific commands, type **icldb *command* /?**.

| Command | Description |
| --- | --- |
| archive | Archives the session recording files older than the retention period specified. Use this command to archive files. |
| dormant | Displays or counts the session recording files that are considered dormant. Dormant files are session recordings that were not completed due to data loss. Use this command to verify if you suspect that you are losing data. You can check whether the session recording files are becoming dormant for the entire database, or only recordings made within the specified number of days, hours, or minutes. |
| import | Imports session recording files to the Session Recording database. Use this command to rebuild the database if you lose database records. Also, use this command to merge databases (if you have two databases, you can import the files from one of the databases). |
| locate | Locates and displays the full path to a session recording file using the file ID as the criteria. Use this command when you are looking for the storage location of a session recording file. It is also one way to verify if the database is up-to-date with a specific file. |
| remove | Removes the references to session recording files from the database. Use this command (with caution) to clean up the database. Specify the retention period to be used as the criteria. You can also remove the associated physical file. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Command | Description |
| --- | --- |
| removeall | Removes all of the references to session recording files from the Session Recording Database and returns the database to its original state. The actual physical files are not deleted; however you cannot search for these files in the Session Recording Player. Use this command (with caution) to clean up the database. Deleted references can be reversed only by restoring from your backup. |
| version | Displays the Session Recording Database schema version. |
| /l | Logs the results and errors to the Windows event log. |
| /f | Forces the command to run without prompts. |
| /s | Suppresses the copyright message. |
| /? | Displays help for the commands. |

### Archive session recording files

To maintain an adequate level of spare disk capacity in the recording storage locations, archive session recording files regularly. Depending on the amount of disk space available and the typical size of session recording files, archiving intervals differ. Session recording files must be older than two days from the start date before a session recording file can be archived. This rule is to prevent any live recordings from being archived before they become complete.

Two methods are available when you archive session recordings. The database record for a session recording file can be updated to have a status of archived while the session recording file remains in the recording storage location. This method can be used to reduce the search results in the Player. The other method is to update the database record for a session recording file to the status of archived and also move the session recording file from the recording storage location to another location for backup to alternative media. When the ICLDB utility moves session recording files, the files are moved to the specified directory where the original file folder structure of year/month/day no longer exists.

The session recording record in the Session Recording Database contains two fields associated with archiving: the archive time representing the current date and time a session recording was archived; the archive note, an optional text note that might be added by the administrator during archiving. The two fields indicate a session recording has been archived and the time of archiving.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

In the Session Recording Player, any archived session recordings show a status of Archived and the date and time of archiving. Session recordings that have been archived might still be played if the files have not been moved. If a session recording file was moved during archiving, a file not found error is displayed. The session recording file must be restored before the session can be played. To restore a session recording, provide the administrator with the File ID and Archive Time of the session recording from the recording Properties dialog box in the Session Recording Player. Restoring archived files is discussed further in the following Restore session recording files section.

The **archive** command of the ICLDB utility has several parameters that are described as follows:

- **/RETENTION:<days>** - The retention period in days for session recordings. Recordings older than the number of days specified are marked as archived in the Session Recording Database. The retention period must be an integer number greater than or equal to 2 days.
- **/LISTFILES** –Lists the full path and file name of session recording files as they are being archived. This is an optional parameter.
- **/MOVETO:<directory>** - The directory to which you physically move archived session recording files. The specified directory must exist. This is an optional parameter. If no directory is specified, files remain in their original storage location.
- **/NOTE:<note>** - A text note that is added to the database record for each session recording archived. Ensure that the note is enclosed with double quotes. This is an optional parameter.
- **/L** –Logs the results and errors to the Windows event log of the number of session recording files archived. This is an optional parameter.
- **/F** –Forces the archive command to run without prompts. This is an optional parameter.

**To archive session recordings in the Session Recording Database and physically move session recording files**

1. Log on to the server where the Session Recording Server is installed as a local administrator.
2. Start a command prompt.
3. Change from the current working directory to the Bin directory of the Session Recording Server installation path (<Session Recording Server Installation Path>/Server/Bin).
4. Run the **ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /MOVETO:<directory> /NOTE:<note> /L** command where **days** is the retention period for session recording files, **directory** is the directory where archived session recording files are moved to, and **note** is the text note that is added to the database record for each session recording file being archived. Enter **Y** to confirm the archive.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**To only archive session recordings in the Session Recording Database**

1. Log on to the server where the Session Recording Server is installed as a local administrator.
2. Start a command prompt.
3. Change from the current working directory to the Bin directory of the Session Recording Server installation path (<Session Recording Server Installation Path>/Server/Bin).
4. Run the **ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /NOTE:<note> /L** command where **days** is the retention period for session recordings and **note** is the text note that is added to the database record for each session recording being archived. Enter **Y** to confirm the archive.

## Restore session recording files

Restoration of session recording files is required when you want to view a session recording that was archived in the Session Recording Database and the file has been moved from the recording storage location. Archived session recordings that were not moved from the recording storage location during archiving are still accessible in the Session Recording Player.

Two methods are available for restoring session recording files that have been moved. Copy the required session recording file to the restore directory for archived files, or import the required session recording file back to the Session Recording Database by using the ICLDB utility. Citrix recommends the first method for restoring archived session recording files. Remove archived files copied to the restore directory for archived files when you no longer need them.

The Session Recording Broker utilizes the **Restore directory for archived files** when a session recording file is not found in its original storage location. This case occurs when the Session Recording Player requests a session recording file for playback. The Session Recording Broker first attempts to find the session recording file in the original storage location. If the file is not found in the original storage location, the Session Recording Broker then checks the **Restore directory for archived files**. If the file is present in the restore directory, the Session Recording Broker sends the file to the Session Recording Player for playback. Otherwise, if the file is not found, the Session Recording Broker sends a file not found error to the Session Recording Player.

Importing archived session recording files by using the ICLDB utility updates the Session Recording Database with session recording information from the session recording file, including a new storage path for the session recording file. Using the ICLDB utility to import an archived session recording file does not move the file back to the original storage location when the session was recorded.

**Note:** An imported session recording file has the archive time and archive note cleared in the Session Recording Database. Therefore, the next time the ICLDB archive command is run, the imported session recording file might become archived again.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

The ICLDB import command is useful to import a large number of archived session recording files, repair, or update incorrect and missing session recording data in the Session Recording Database, or move session recording files from one storage location to another storage location on the Session Recording Server. The ICLDB **import** command can also be used to repopulate the Session Recording Database with session recordings after executing the ICLDB **removeall** command.

The **import** command of the ICLDB utility has several parameters that are described as follows:

- **/LISTFILES** –Lists the full path and file name of session recording files while they are being imported. This is an optional parameter.
- **/RECURSIVE** –Searches all subdirectories for session recording files. This is an optional parameter.
- **/L** –Logs the results and errors to the Windows event log the number of session recording files imported. This is an optional parameter.
- **/F** –Forces the import command to run without prompts. This is an optional parameter.

**To restore session recording files by using the restore directory for archived files**

1. Log on to the server where the Session Recording Server is installed as a local administrator.
2. In Session Recording Player Properties, determine the File ID and Archive Time of the archived session recording file.
3. Locate the session recording file in your backups using the File ID specified in Session Recording Player Properties. Each session recording has a file name of **i_<FileID>.icl**, where FileID is the ID of the session recording file.
4. Copy the session recording file from your backup to the restore directory for archived files. To determine the restore directory for archived files:
    a) From the **Start** menu, choose **Start** > **All Programs** > **Citrix** > **Session Recording Server Properties**.
    b) In Session Recording Server Properties, select the **Storage** tab. The current restore directory appears in the **Restore directory for archived files** field.

**To restore session recording files by using the ICLDB import command**

1. Log on to the server where the Session Recording Server is installed as a local administrator.
2. Start a command prompt.
3. Change from the current working directory to the Bin directory of the Session Recording Server installation path (<Session Recording Server Installation Path>/Server/Bin).

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. Either:

    - Run the **ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>** command where **directory** is the name of one or more directories, separated by a space containing session recording files. Enter **Y** to confirm the import.
    - Run the **ICLDB IMPORT /LISTFILES /L <file>** command where **file** is the name of one or more session recording files, separated by a space. Wildcards might be used to specify session recording files. Enter **Y** to confirm the import.

## Configuration Logging

October 29, 2018

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 by 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 differnt 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 will be read in English, regardless of the locale of the reader.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

**Note:** Product editions that do not support Configuration Logging do not have a Logging node in Studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 the **Enable** radio button. 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 the **Disable** radio button. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.

To enable mandatory logging, select the **Prevent changes to the site configuration when the database is not available** radio button. No configuration change or administrative activity that would normally be logged will be allowed unless it can be written in the Configuration Logging database. You can enable mandatory logging only when Configuration Logging is enabled, that is, when the **Enable** radio button 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 the **Allow changes when to the site configuration when the database is not available** radio button. Configuration changes and administrative activities are allowed, even if the database used for Configuration Logging cannot be accessed. This is the default setting.

### Change the Configuration Logging database location

**Note:** 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. Valid formats are listed in the Databases article.
6. To allow Studio to create the database, click **OK**. When prompted, click **OK**, and the database will be 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 will indicate 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 displayed 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 middle pane, the lower middle 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 will create a surrogate high level operation.

To display configuration log content, select **Logging** in the Studio navigation pane. By default, the display in the center pane lists the log content chronologically (newest entries first), separated by date.

| To filter the display by | Complete this action |
| --- | --- |
| Search results | Enter text in the Search box at the top of the middle pane. The filtered display includes the number of search results. To return to the standard logging display, clear the text in the Search box. |
| Column heading | Click a column heading to sort the display by that field. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| To filter the display by | Complete this action |
| --- | --- |
| A date range | Select an interval from the drop down list box next to the Search box at the top of the middle pane. |

### 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) simply 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 built-in 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **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 should be 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

October 29, 2018

The following articles contain lists and descriptions of events that can be logged by XenApp and XenDesktop services.

This information is not comprehensive; readers should check individual feature articles for additional event information.

Citrix Broker Service events (HTML)

Citrix FMA Service SDK events (HTML)

Citrix Configuration Service events (HTML)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

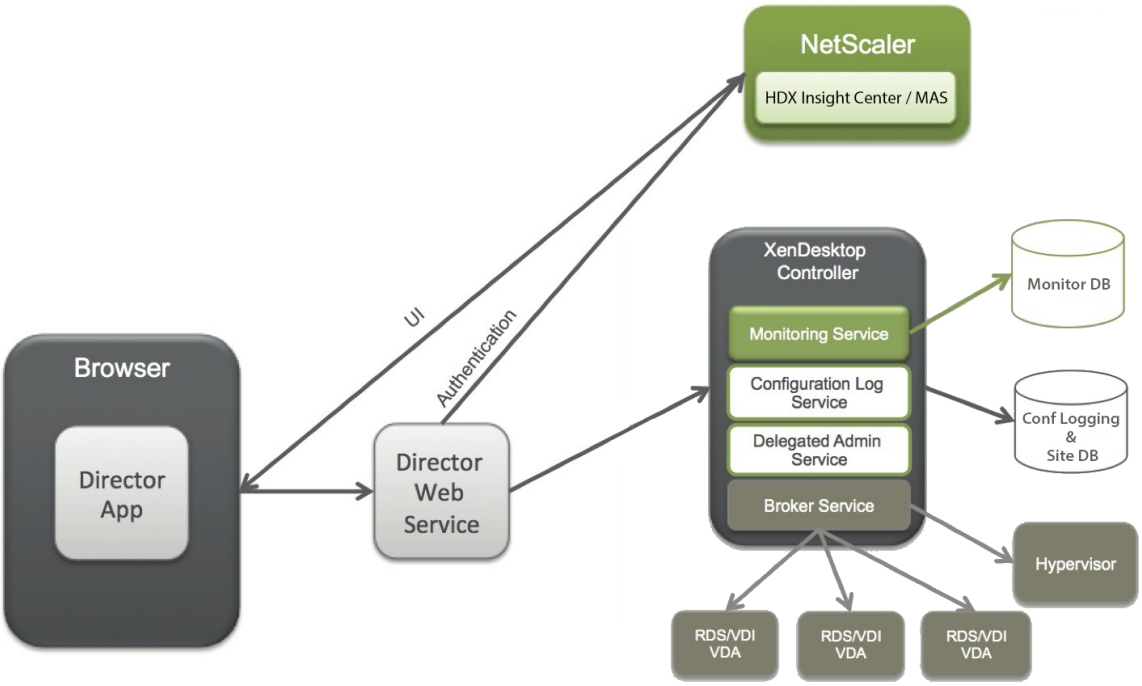
Citrix Delegated Administration Service events (HTML)

# Director

March 29, 2019

## About Director

Director is a monitoring and troubleshooting console for XenApp and XenDesktop.




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 NetScaler Insight Center or NetScaler MAS, to identify bottlenecks due to the network in your XenApp or XenDesktop environment.
- Historical data stored in the Monitor database to access the Configuration Logging database.
- ICA data from the NetScaler Gateway using NetScaler Insight Center or NetScaler MAS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - Gain visibility into end-user experience for virtual applications, desktops, and users for XenApp or XenDesktop.
  - Correlate network data with application data and real-time metrics for effective troubleshooting.
  - Integrate with XenDesktop 7 Director monitoring tool.

- Personal vDisk data that allows for runtime monitoring showing base allocation and gives help desk administrators the ability to reset the Personal vDisk (to be used only as a last resort).

  - The command line tool CtxPvdDiag.exe is used to gather the user log information into one file for troubleshooting.

Director uses a troubleshooting dashboard that provides real-time and historical health monitoring of the XenApp or XenDesktop 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.

#### 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.

### Deploy and configure Director

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.

This release of Director is not compatible with XenApp deployments earlier than 6.5 or XenDesktop deployments earlier than 7.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

**Tip**: If you intend to monitor XenApp 6.5 in addition to XenApp 7.5 or XenDesktop 7.x Sites, Citrix recommends installing Director on a separate server from the Director console that is used to monitor XenApp 6.5 Sites.

**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.

### To 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).
- Configure 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.
- For user devices with VDAs earlier than 7, additional configuration is required. See Configure permissions for VDAs earlier than XenDesktop 7.

### Install Director

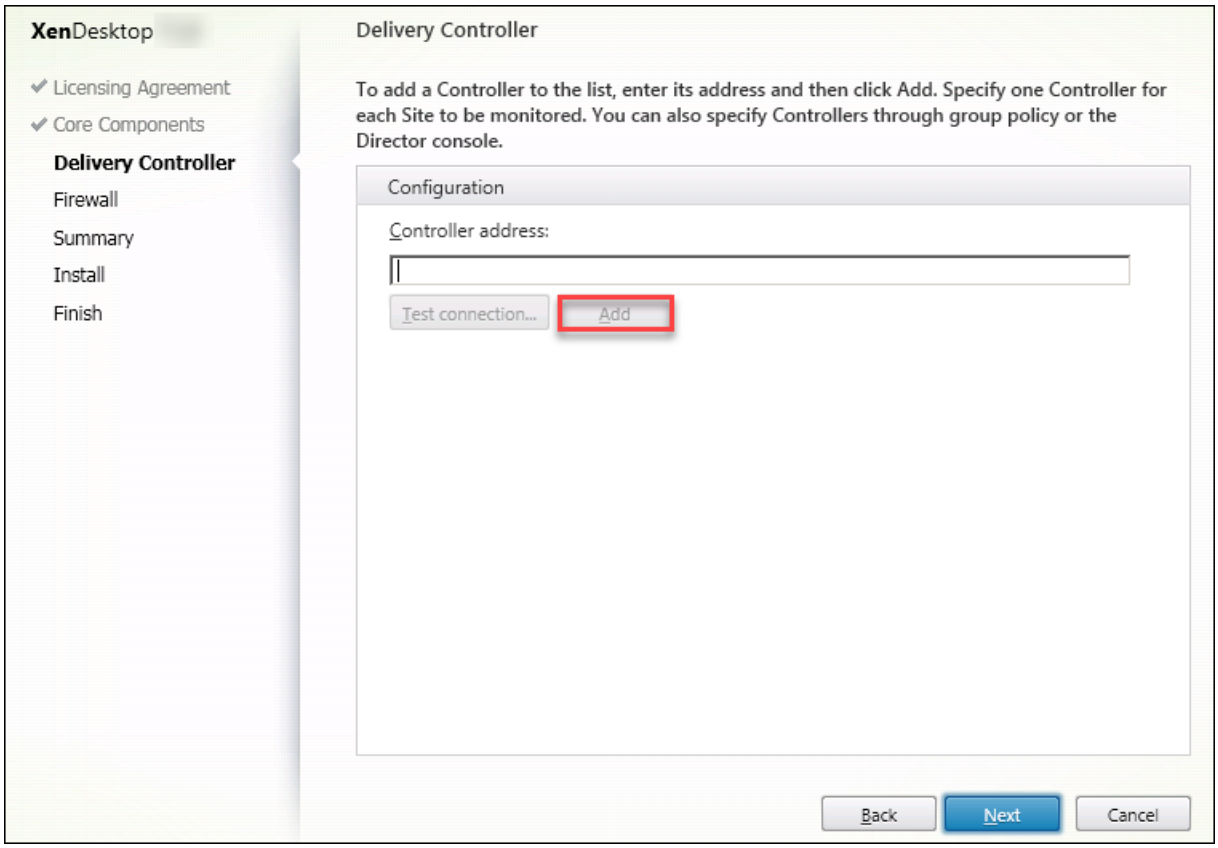
Install Director using the full product ISO Installer for XenApp and Desktop, which checks for prerequisites, installs any missing components, sets up the Director website, and performs basic configuration. The default configuration provided by the ISO installer handles typical deployments. If Director was

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Install Director for XenApp 6.5

To install Director for XenApp 6.5 follow these steps. Typically, Director is installed on a separate computer from the XenApp Controllers.

1. Install Director from the XenApp installation media. If Director is already installed for XenDesktop, skip this step and proceed to the next step.
2. Use the IIS Manager Console on each Director server to update the list of XenApp server addresses in the application settings as described in the **To add Sites to Director** section in Advanced configuration.
   Supply the server address of one Controller per XenApp Site: any of the other Controllers in a XenApp site are then used automatically for failover. Director does not load balance among Controllers.
   **Important**: For XenApp addresses, be sure to use the setting Service.AutoDiscoveryAddressesXA, not the default setting Service.AutoDiscoveryAddresses.
3. The Director WMI Provider installer is located at the **Support\DirectorWMIProvider** folder on the DVD. Install it on all appropriate XenApp servers (Controllers and workers where sessions are running).
   If **winrm** is not configured, run the **winrm qc** command.
4. Configure each XenApp worker server to accept WinRM queries as described in Configure permissions.
5. Configure a firewall exception for port 2513, used for communication between Director and XenApp.
6. 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. No Director configuration is required to enable TLS.

**Note:** To allow Director to find all the XenApp workers in the farm, you must add a reverse DNS zone for the subnets where the XenApp servers reside on the DNS servers used by the farm.

### Log on to Director

The Director website is located at https or `http://<ServerFQDN>/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.

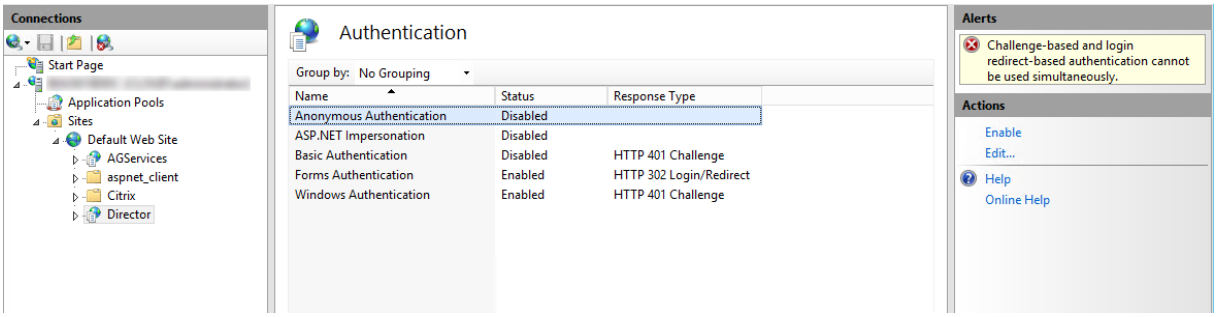
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Use Director with Integrated Windows Authentication

With Integrated Windows Authentication, domain-joined users gain direct access to Director without re-keying 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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**.

**Usage data collection by Google Analytics**

The Director Service uses Google Analytics to collect usage data anonymously after Director is installed. Statistics and information regarding the usage of the Trends page and its tabs are collected. Data collection is enabled by default when you install Director.

To opt out of the Google Analytics data collection, edit the registry key, HKEY_LOCAL_MACHINE\Software\Citrix\Met on the machine where Director is installed, as described in the Install and upgrade analytics section in Citrix Insight Services.

**Note**: The HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall registry key controls the collection of usage data by Citrix Insight Services as well as Google Analytics. Any change to the key value affects collection by both the services.

## Advanced configuration

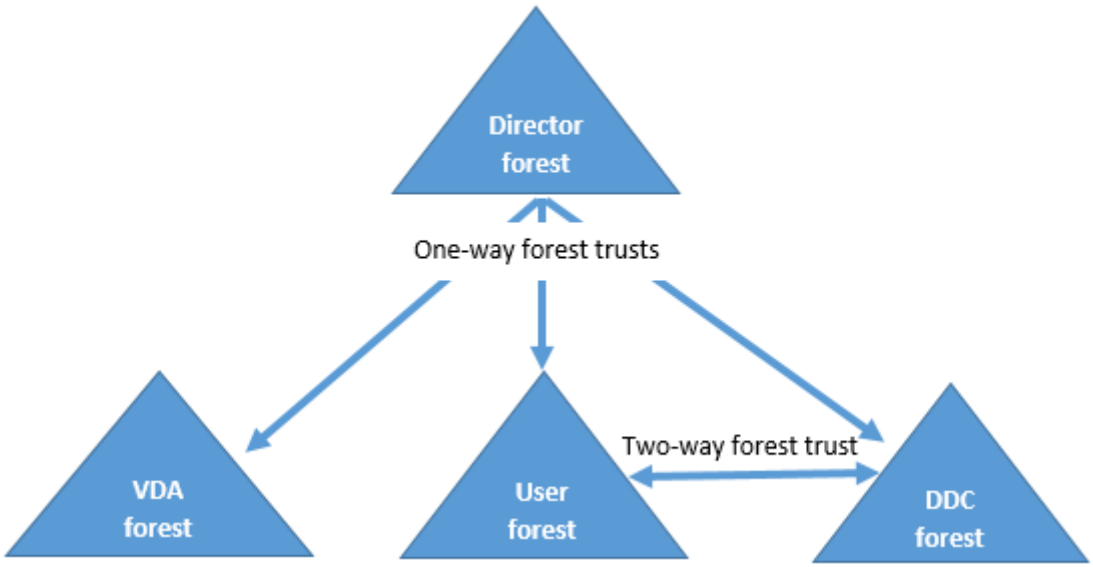
July 3, 2019

Director can support multi-forest environments spanning a forest configuration where users, Domain Delivery Controllers (DDC), VDAs, and Directors are located in different forests. This requires proper setup of trust relationships among the forests and configuration settings.

### Recommended configuration for Director to work in a multi-forest environment

The recommended configuration requires creation of outgoing and incoming forest trust relationships among the forests with domain-wide authentication.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




The trust relationship from the Director enables you to troubleshoot issues in user sessions, VDAs and Domain 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.

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 setting:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

> **Note:**
>
> In an environment with multiple forests, Director does not show the session details of users from other forests who have been assigned to the XenDesktop Delivery Group using the domain local group.

### 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
```

where *SiteAController* and *SiteBController* are the addresses of Delivery Controllers from two different Sites.

For XenApp 6.5 Sites, add an address of a Controller from each XenApp farm to the following setting:

```
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
```

where *FarmAController* and *FarmBController* are the addresses of XenApp Controllers from two different farms.

For XenApp 6.5 Sites, another way to add a Controller from a XenApp farm:

```
DirectorConfig.exe /xenapp FarmControllerName
```

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 is 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
   <!--NeedCopy-->
   ```

> **Important:**
>
> To disable the view of running applications, Citrix recommends making both changes to ensure that the data is not displayed in Activity Manager.

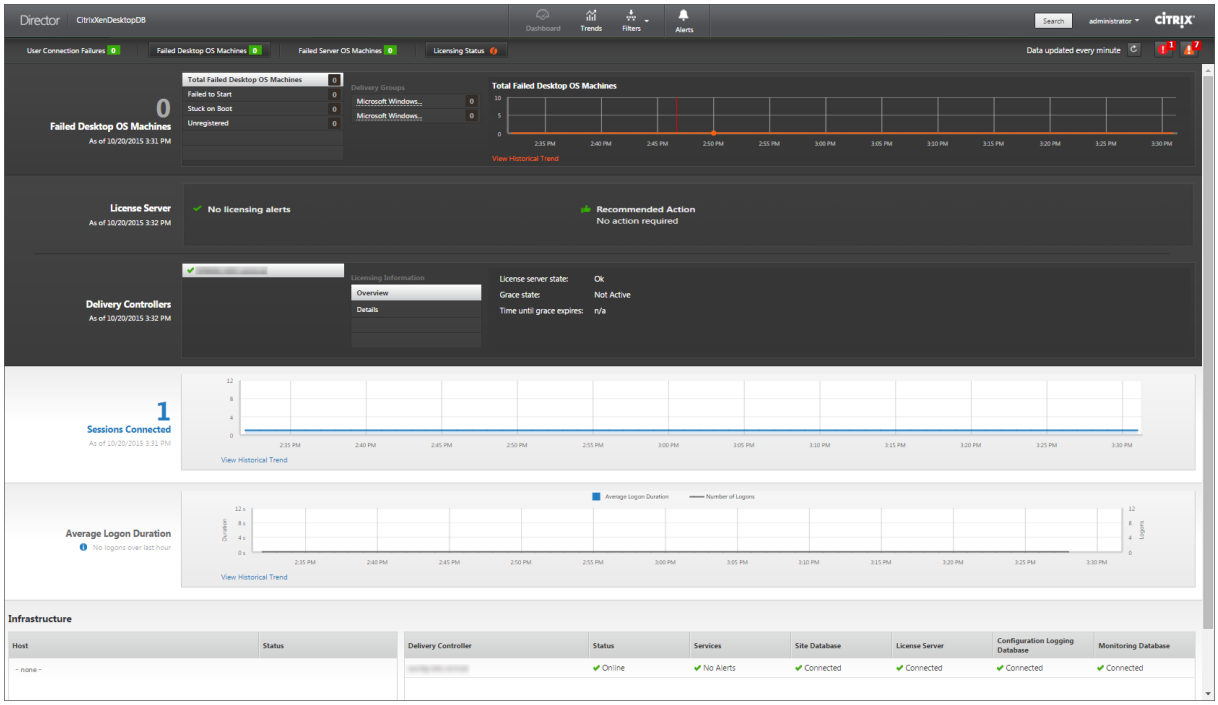
## Monitor deployments

January 31, 2020

### Monitor Sites

With full administrator permission, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a Site.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 Desktop OS Machines or Failed Server 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 Server OS machines, failures also include machines reaching maximum load. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |
| 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 XenServer 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, go to XenServer Current Release; see the XenCenter Performance Alerts section in the Citrix XenServer Administrator's Guide. |

**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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Monitor sessions

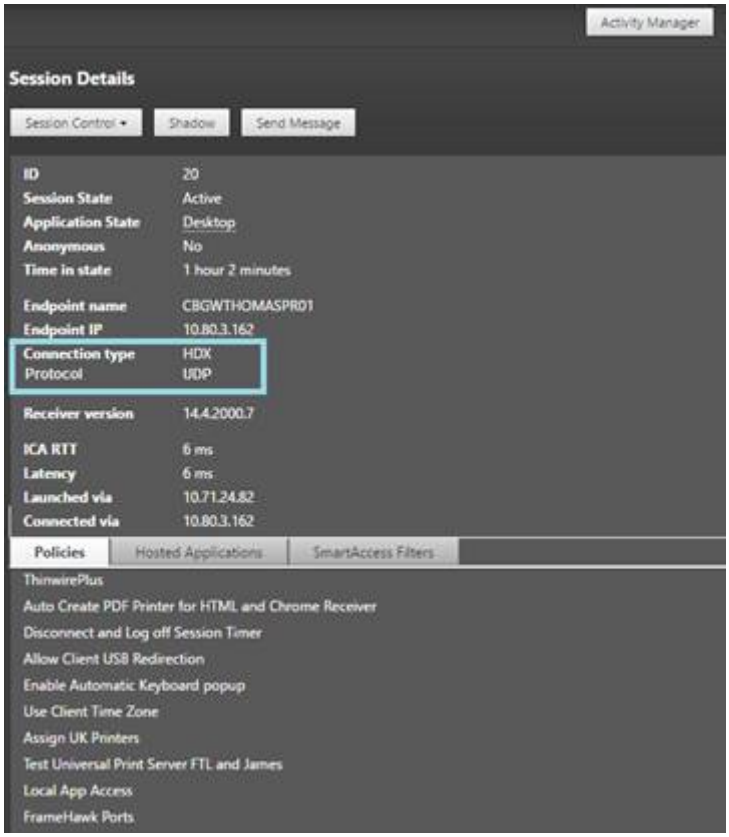
If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

| 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

### Filter data to troubleshoot failures

When you click numbers on the Dashboard or select a predefined filter from the Filters menu, the Filters view opens to display the 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Select a view:
    - **Machines**. Select Desktop OS Machines or Server OS Machines. These views show the number of configured machines. The Server 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 Desktop OS. The session idle time measurements are available for Application instances on VDAs of Server OS.
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. If needed, for **Machines** or **Connections** views, use power controls for all the machines you select in the filtered list. For the Sessions view, use the session controls or option to send messages.
9. In the **Machines** and **Connections** views, click the **Failure Reason** of a failed machine or connection to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended actions for Machine and Connection failures are available in the Citrix Director 7.12 Failure Reasons Troubleshooting Guide.
10. 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.
11. In the **Application Instances** view, sort or filter based on **Idle Time** greater than a threshold time period. Select the idle application instances to end. Log off or Disconnect of an application

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

instance ends all active application instances in the same session. For more information, see Troubleshoot applications.

**Note:** 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.

### Monitor historical trends across a Site

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 on 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 Platinum licensed Sites.
- Trend reports of up to Last month (31 days) are available in Enterprise licensed Sites.
- Trend reports of up to Last 7 days in non-Platinum and non-Enterprise 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.
- The default values of the trends data grooming retention by the Monitoring Service are available in the Data granularity and retention. Customers on Platinum licensed Sites can change the grooming retention to their desired number of retention days.

### 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.

**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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**View trends for machine failures:** From the Desktop OS Machine Failures tab or Server 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 Server OS machines. The filter options for this graph include the Delivery Group or Server OS machine in a Delivery Group, Server OS machine (available only if Server 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 desktop and server OS usage:** The Trends view shows the usage of Desktop 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 Server 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 Desktop OS Machines or Server OS Machines to obtain a real-time view of your VM usage, enabling you to quickly assess your Site's capacity needs.
Desktop OS availability - displays the current state of Desktop OS machines (VDIs) by availability for the entire Site or a specific Delivery Group.
Server OS availability - displays the current state of Server OS machines by availability for the entire Site or a specific Delivery Group.

**View resource utilization:** From the Resource Utilization tab, select Desktop OS Machines or Server 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

**Notes:**

- 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 NetScaler Insight Center or NetScaler MAS. 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. Desktop OS VDAs running Windows Vista and later, and Server OS VDAs running Windows Server 2008 and later are supported. For more information, see Historical application failure monitoring

By default, only application faults from Server OS VDAs are displayed. You can set the monitoring of application failures by using Monitoring policies. For more information, see Monitoring policy settings

**Create customized reports:** The Custom Reports tab provides a user interface for generating Custom Reports containing real-time and historical data from the Monitoring database in tabular format.

This feature requires Delivery Controller(s) **version 7.12** or later.

From the list of previously saved Custom Report queries, you can click **Execute** to export the report in CSV format, click **Copy OData** to copy and share the corresponding OData query, or click **Edit** to edit

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

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.

**Notes:**

- 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.

### 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 | 1000,000 |
| CSV | 100,000 (10,000,000 in Sessions tab) | UI.ExportCsvDrilldownLimit | 1000,000 |

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 the field or add a new field.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 2GB 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 Desktop OS machines, but might not be available for Server 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. |
| **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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.

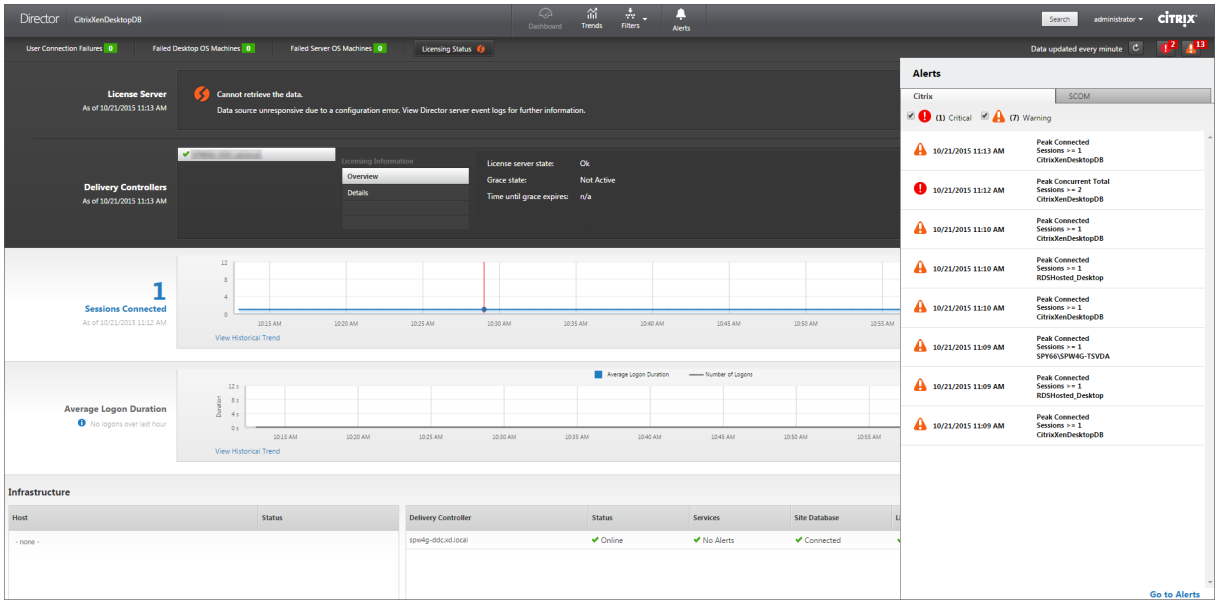
## Alerts and notifications

July 21, 2022

### Monitor alerts

Alerts are displayed in Director on the dashboard and other high level views with warning and critical alert symbols. Alerts are available for **Platinum** licensed Sites. Alerts update automatically every minute; you can also update alerts on demand.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

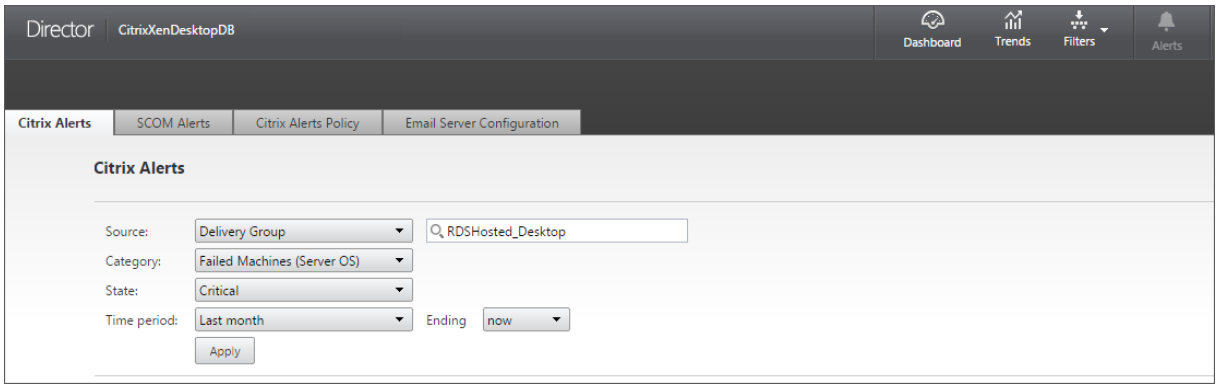



A warning alert (amber triangle) indicates that the warning threshold of a condition has been reached or exceeded.

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 Server OS machines for a specific Delivery Group over the last month, or all alerts for a specific user. For more information, see Export reports.



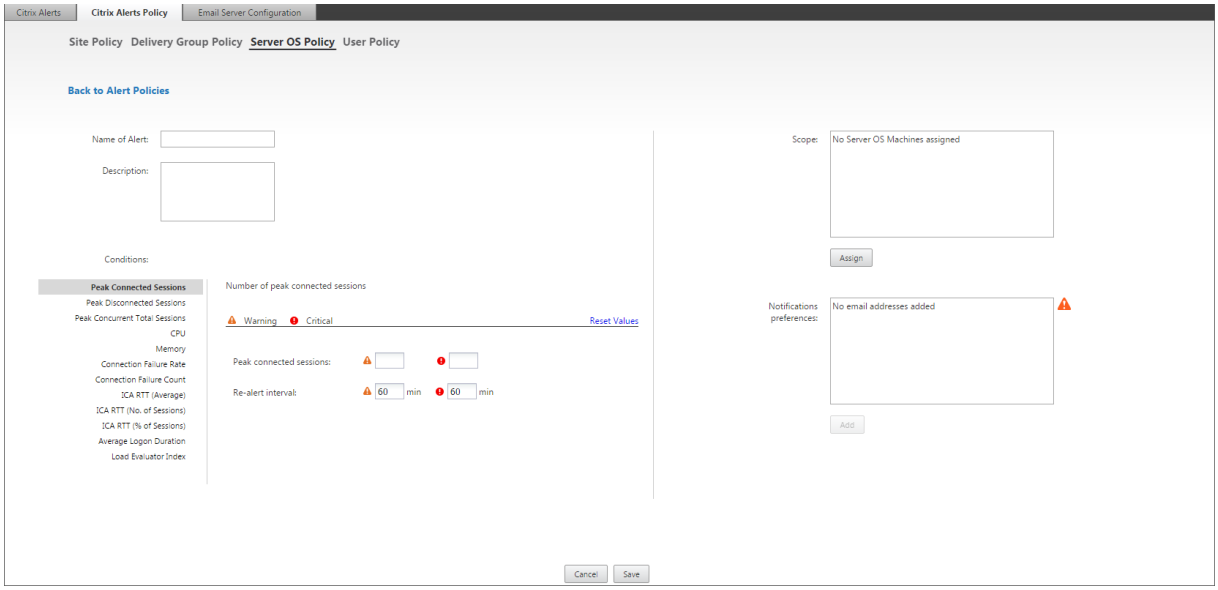

**Citrix alerts**. Citrix alerts are alerts monitored in Director that originate from Citrix components. You can configure Citrix alerts within Director in **Alerts** > **Citrix Alerts Policy**. As part of the configuration, you can set notifications to be sent by email to individuals and groups when alerts exceed the thresholds you have set up. You can configure the notification as Octoblu webhooks, or SNMP traps also. For more information on setting up Citrix Alerts, see Create alerts policies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

**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 SCOM alerts.

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 are met:

1. Go to **Alerts** > **Citrix Alerts Policy** and select, for example, Server 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

For information about Octoblu webhook configuration, see Configure alerts policies with Octoblu webhooks.

For information about SNMP trap configuration, see Configure alerts policies with SNMP traps.

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

| Alert policy condition | Description and recommended actions |
|---|---|
| Peak Connected Sessions | Number of peak connected sessions. Check Director Session Trends view for peak connected sessions. Check to ensure there is enough capacity to accommodate the session load. Add new machines if needed. |
| Peak Disconnected Sessions | Number of peak disconnected sessions. Check Director Session Trends view for peak disconnected sessions. Check to ensure there is enough capacity to accommodate session load. Add new machines if needed. Log off disconnected sessions if needed. |
| Peak Concurrent Total Sessions | Number of peak concurrent sessions. Check Director Session Trends view in Director for peak concurrent sessions. Check to ensure there is enough capacity to accommodate session load. Add new machines if needed. Log off disconnected sessions if needed. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Alert policy condition | Description and recommended actions |
| --- | --- |
| CPU | Percentage CPU usage. Identify the processes or resources consuming CPU. End the process if necessary. Ending the process will cause 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 will not be triggered. For more information, see Monitoring policy. |
| Memory | Percentage Memory usage. Identify the processes or resources consuming memory. End the process if necessary. Ending the process will cause 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 will not be triggered. For more information, see Monitoring policy settings. |
| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Alert policy condition | Description and recommended actions |
| --- | --- |
| ICA RTT (Average) | Average ICA round-trip time Check NetScaler HDX Insight for a breakdown of the ICA RTT to determine root cause. If NetScaler is not available, check the Director User Details view for the ICA RTT and Latency and determine if it is a network problem or XD/XA issue. For more information, see the NetScaler Insight Center documentation, Use Cases: HDX Insight. |
| ICA RTT (No. of Sessions) | Number of sessions which exceed the threshold ICA round-trip time. Check NetScaler HDX Insight for the number of sessions with high ICA RTT. For more information, see the NetScaler Insight Center documentation, HDX Insight Reports. If NetScaler is not available, work with the network team to determine root cause. |
| ICA RTT (% of Session) | Percentage of sessions which exceed the average ICA round-trip time. Check NetScaler HDX Insight for the number of sessions with high ICA RTT. For more information, see the NetScaler Insight Center documentation, HDX Insight Reports. If NetScaler is not available, work with the network team to determine root cause. |
| ICA RTT (User) | ICA round-trip time which is applied to sessions launched by the specified user. The alert is triggered if ICA RTT is higher than the threshold in at least one session. |
| Failed Machines (Desktop OS) | Number of failed Desktop OS machines. Failures can occur for various reasons as shown in the Director dashboard and Filters views. Run Citrix Scout diagnostics to determine root cause. For more information, see Troubleshoot user issues. |
| Failed Machines (Server OS) | Number of failed Server OS machines. Failures can occur for various reasons as shown in the Director dashboard and Filters views. Run Citrix Scout diagnostics to determine root cause. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Alert policy condition | Description and recommended actions |
| --- | --- |
| Average Logon Duration | Average logon duration for logons which 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 cause elongated logons. Check the baseline and break down of the logons to narrow down the cause. For more information, see Diagnose user logon issues. |
| Logon Duration (User) | Logon duration for logons for the specified user which occurred over the last hour. |
| Load Evaluator Index | Value of the Load Evaluator Index over the last 5 minutes. Check Director for Server OS Machines that may have a peak load (Max load).View both dashboard (failures) and Trends Load Evaluator Index report. |

### Configure alerts policies with Octoblu webhooks

Apart from email notifications, you can configure alerts policies with Octoblu webhooks to initiate IoT services.

**Note:** This feature requires Delivery Controller(s) version 7.11 or later.

Examples of IoT services that can utilize alerts include sending SMS notifications to support staff or integrating with custom incident resolution platforms to help in tracking notifications.

You can configure an alert policy with an HTTP callback or an HTTP POST using PowerShell cmdlets. They are extended to support webhooks.

For information on the creation of a new Octoblu workflow and obtaining the corresponding webhook URL, see the Octoblu Developer Hub.

To configure an Octoblu webhook URL for a new alert policy or an existing policy, use the following PowerShell cmdlets.

Create a new alerts policy with a webhook URL:

```
1 $policy = New-MonitorNotificationPolicy -Name <Policy name> -
    Description <Policy description> -Enabled $true -Webhook <Webhook
    URL>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Add a webhook URL to an existing alerts policy:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

For help on the PowerShell commands, use the PowerShell help, for example:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

Notifications generated from the alert policy trigger the webhook with a POST call to the webhook URL. The POST message contains the notification information in JSON format:

```
{
 "NotificationId" : \<Notification Id\>,

"Target" : \<Notification Target Id\>,

"Condition" : \<Condition that was violated\>,

"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
    dismissed\>,

"Site" : \<Site name\> }

<!--NeedCopy-->
```

### Configure alerts policies with SNMP traps

When an alert configured with an SNMP trap triggers, the corresponding SNMP trap message is forwarded to the configured network listener for further processing. Citrix alerts support traps of SNMP version 2 and later. Currently, the trap message can be forwarded to one listener.

**Note:** This feature requires Delivery Controller(s) version 7.12 or later.

To configure SNMP traps, use the following PowerShell cmdlets:

- Get the current SNMP server configuration:

  ```
  Get-MonitorNotificationSnmpServerConfiguration
  ```

- Set server configuration for SNMP version 2:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
    Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
    CommunityString public -Protocol V2
```

- Set server configuration for SNMP version 3:

```
$authpass = "<authentication password>" | ConvertTo-SecureString
    -AsPlainText -Force
$privpass = "<Privacy password>" | ConvertTo-SecureString -
    AsPlainText -Force
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
    Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
    EngineId <Engine Id> -AuthPassword $authpass -PrivPassword
    $privpass -PrivPasswordProtocol <Privacy password protocol> -
    AuthPasswordProtocol <Authentication password protocol> -
    Protocol V3
<!--NeedCopy-->
```

- Enable SNMP trap for an existing alert policy:

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy ID
    >
```

- Create a new alert policy with SNMP trap configuration:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    IsSnmpEnabled $true -Description <Policy description> -Enabled
     $true
```

The structure of the OIDs in the SNMP trap messages from Director is as follows:
**1.3.6.1.4.1.3845.100.1.*<UID>***
Here, ***<UID>*** is generated serially for every alert policy defined in Director. The OIDs are hence unique to each user environment.

- Use **1.3.6.1.4.1.3845.100.1** to filter all trap messages from Director.
- Use **1.3.6.1.4.1.3845.100.1.*<UID>*** to filter and handle traps messages for specific alerts.

Use the following cmdlet to get the UIDs for the alert policies defined in your environment:

```
Get-MonitorNotificationPolicy
```

You can forward the SNMP traps to SCOM. To do this, configure SCOM with the Delivery Controller to listen to the trap messages.

### Configure SCOM alerts integration

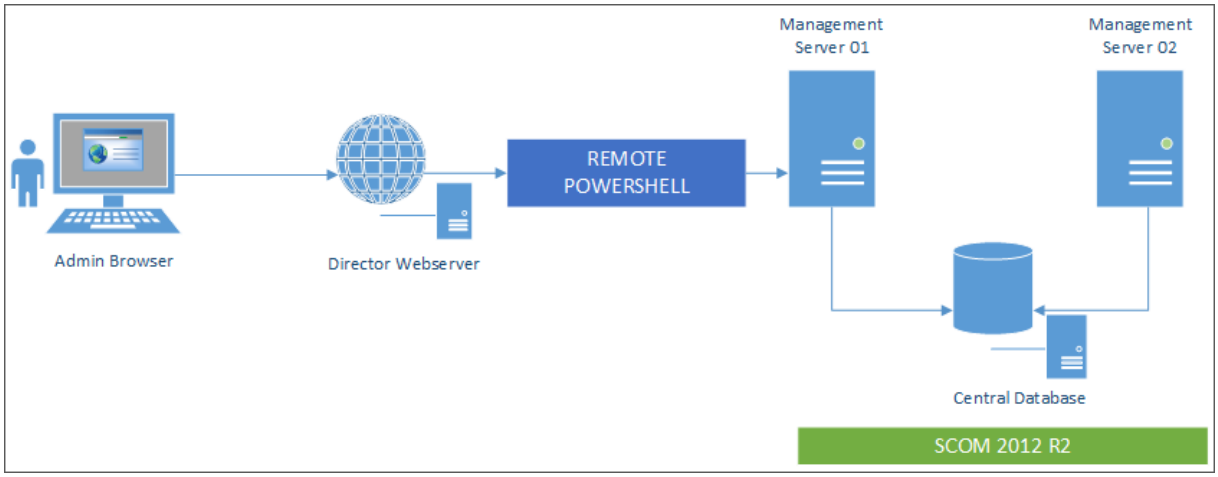
SCOM integration with Director lets you view alert information from SCOM on the Dashboard and in other high-level views in Director.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

**Note**:

- Citrix recommends that the Director administrator account is configured as a SCOM Operator role so that can 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 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):

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

a) Get the current list of TrustedHosts

```
        Get-Item WSMAN:\localhost\Client\TrustedHosts
<!--NeedCopy-->
```

```
1.  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>"
<!--NeedCopy-->
```

1. Configure SCOM using the DirectorConfig tool.

```
    C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
<!--NeedCopy-->
```

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.

   c) To modify any User Role, right-click on the role, then click **Properties**.

   d) 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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
   ```

   b) Modify MaxShellsPerUser:

   In CLI:

   ```
   winrm set winrm/config/winrs @{
    MaxShellsPerUser="20" }
   ```

   In PS:

   ```
   Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
   ```

   c) Modify MaxMemoryPerShellMB:

   In CLI:

   ```
   winrm set winrm/config/winrs @{
    MaxMemoryPerShellMB="1024" }
   ```

   In PS:

   ```
   Set -Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
   ```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## Delegated Administration and Director

March 20, 2024

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 document.

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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Administrator Role | Permissions in Director |
| --- | --- |
| Delivery Group Administrator | Full access to all views and can perform all commands, including shadowing a user's session, power management and session management, 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 Desktop OS Machines. Cannot access the Dashboard, Trends, Alerts, or Filters views. Cannot use power control options for Server OS machines. |
| Machine Catalog Administrator | No access. This administrator is not supported for Director and cannot view data. This user can access the Machine Details page (Machine-based search). |
| Host Administrator | No access. This administrator is not supported for Director and cannot view data. |

### To 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.

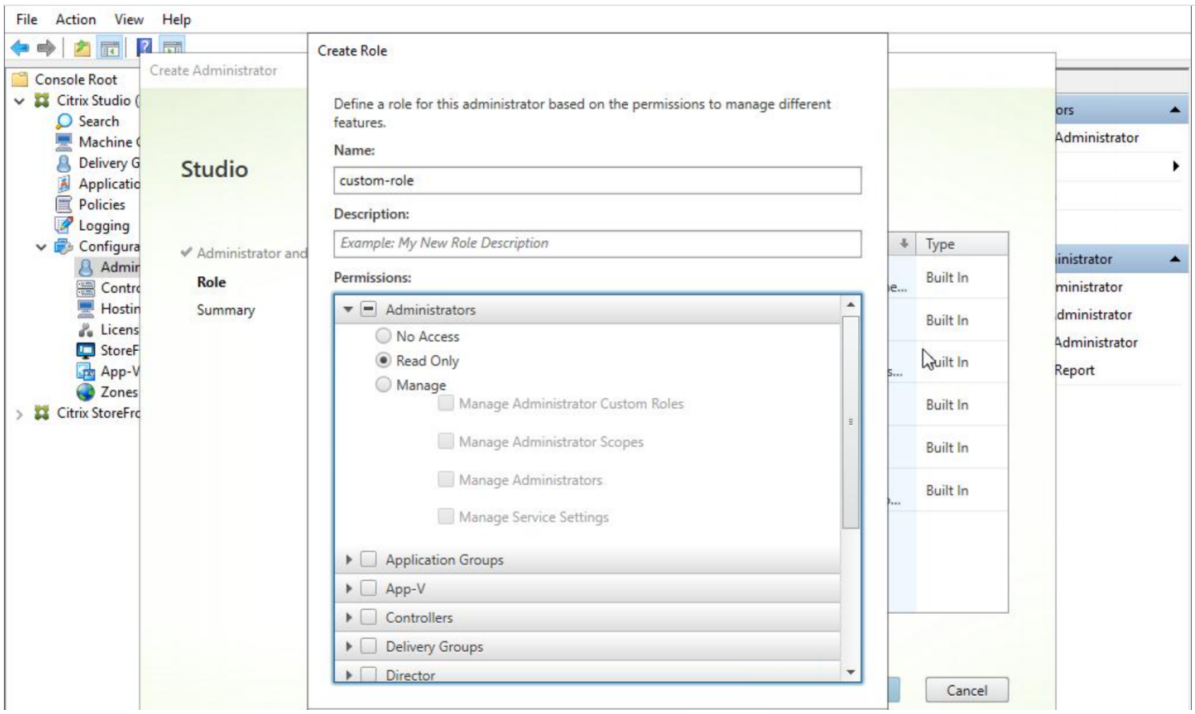
If you create a custom role with Director permissions, you must also give that role other generic permissions:

- Delivery Controller permission to log on to Director - at least read only access in Administrator

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

node

- Permissions to Delivery Groups to view the data related to those Delivery Groups in Director - at least read only access



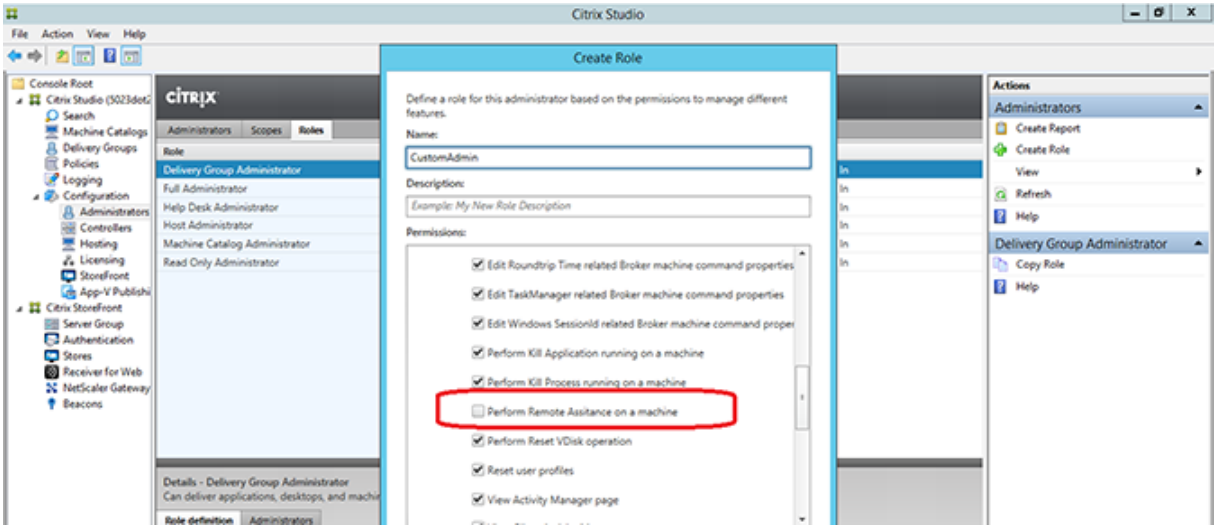

Alternatively, you can create a custom role by copying an existing role and include additional permissions for different views. For example, you can copy the Help Desk role and include permissions to view the Dashboard or Filters pages.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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

June 19, 2020

This article highlights areas that might have an impact on system security when deploying and configuring Director.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Configure Microsoft Internet Information Services (IIS)

You can configure Director with a restricted IIS configuration. Note that this is not the default IIS configuration.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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 NetScaler using TLS, not IPsec.

To secure communications between Director and XenApp and XenDesktop servers (for monitoring and reports), refer to Data Access Security.

To secure communications between Director and NetScaler (for NetScaler 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Configure permissions for VDAs earlier than XenDesktop 7

August 17, 2018

If users have VDAs earlier than XenDesktop 7, Director supplements information from the deployment with real-time status and metrics through Windows Remote Management (WinRM).

In addition, use this procedure to configure WinRM for use with Remote PC in XenDesktop 5.6 Feature Pack1.

By default, only local administrators of the desktop machine (typically domain administrators and other privileged users) have the necessary permissions to view the real-time data.

For information about installing and configuring WinRM, see CTX125243.

To enable other users to view the real-time data, you must grant them permissions. For example, suppose there are several Director users (HelpDeskUserA, HelpDeskUserB, and so on) who are members of an Active Directory security group called HelpDeskUsers. The group has been assigned the Help Desk administrator role in Studio, providing them with the required Delivery Controller permissions. However, the group also needs access to the information from the desktop machine.

To provide the necessary access, you can configure the required permissions in one of two ways:

- Grant permissions to the Director users (impersonation model)
- Grant permissions to the Director service (trusted subsystem model)

## To grant permissions to the Director users (impersonation model)

By default, Director uses an impersonation model: The WinRM connection to the desktop machine is made using the Director user's identity. It is therefore the user that must have the appropriate permissions on the desktop.

You can configure these permissions in one of two ways (described later in this document):

1. Add users to the local Administrators group on the desktop machine.
2. Grant users the specific permissions required by Director. This option avoids giving the Director users (for example, the HelpDeskUsers group) full administrative permissions on the machine.

## To grant permissions to the Director service (trusted subsystem model)

Instead of providing the Director users with permissions on the desktop machines, you can configure Director to make WinRM connections using a service identity and grant only that service identity the appropriate permissions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

With this model, the users of Director have no permissions to make WinRM calls themselves. They can only access the data using Director.

The Director application pool in IIS is configured to run as the service identity. By default, this is the APPPOOL\Director virtual account. When making remote connections, this account appears as the server's Active Directory computer account; for example, MyDomain\DirectorServer$. You must configure this account with the appropriate permissions.

If multiple Director websites are deployed, you must place each web server's computer account into an Active Directory security group that is configured with the appropriate permissions.

To set Director to use the service identity for WinRM instead of the user's identity, configure the following setting, as described in Advanced configuration:

```
Service.Connector.WinRM.Identity = Service
<!--NeedCopy-->
```

You can configure these permissions in one of two ways:

1. Add the service account to the local Administrators group on the desktop machine.
2. Grant the service account the specific permissions required by Director (described next). This option avoids giving the service account full administrative permissions on the machine .

### To assign permissions to a specific user or group

The following permissions are required for Director to access the information it requires from the desktop machine through WinRM:

- Read and execute permissions in the WinRM RootSDDL
- WMI namespace permissions:
  - root/cimv2 - remote access
  - root/citrix - remote access
  - root/RSOP - remote access and execute
- Membership of these local groups:
  - Performance Monitor Users
  - Event Log Readers

The ConfigRemoteMgmt.exe tool, used to automatically grant these permissions, is on the installation media in the x86\Virtual Desktop Agent and x64\Virtual Desktop Agent folders and on the installation media in the C:\inetpub\wwwroot\Director\tools folder. You must grant permissions to all Director users.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

To grant the permissions to an Active Directory security group, user, computer account, or for actions like End Application and End Process, run the tool with administrative privileges from a command prompt using the following arguments:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name
<!--NeedCopy-->
```

where name is a security group, user, or computer account.

To grant the required permissions to a user security group:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
<!--NeedCopy-->
```

To grant the permissions to a specific computer account:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
<!--NeedCopy-->
```

For End Process, End Application, and Shadow actions:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
<!--NeedCopy-->
```

To grant the permissions to a user group:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
<!--NeedCopy-->
```

To display help for the tool:

```
ConfigRemoteMgmt.exe
<!--NeedCopy-->
```

## Configure network analysis

October 29, 2018

**Note:** The availability of this feature depends on your organization's license and your administrator permissions.

Director integrates with NetScaler Insight Center or NetScaler MAS to provide network analysis and performance management:

- Network analysis leverages HDX Insight reports from NetScaler Insight Center or NetScaler MAS to provide an application and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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:**

- ICA session Round Trip Time (RTT) shows data correctly for Receiver for Windows 3.4 or later and the Receiver for Mac 11.8 or later. For earlier versions of these Receivers, the data does not display correctly.
- 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 NetScaler Insight Center or NetScaler MAS in Director. Director requires NetScaler MAS Version 11.1 Build 49.16 or later. Insight Center and MAS are virtual appliances 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 NetScaler MAS documentation.

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 NetScaler Insight Center or NetScaler MAS machine name (FQDN or IP address), the username, password, HTTP or HTTPS connection type, and choose NetScaler Insight or NetScaler MAS integration.
3. To verify the changes, log off and log back on.

## Troubleshoot user issues

June 15, 2020

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 |
| 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.

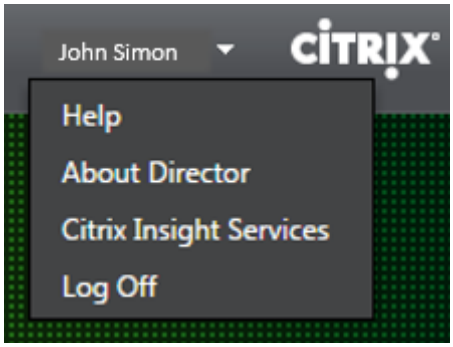
- Searches are not case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name (username, family name and first name, or display name), separated by a space, the results include matches for both strings. For example, if you type jo rob, the results might include strings such as "John Robertson"or Robert, Jones.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 XenApp or XenDesktop components. Depending on the version of Windows, Scout appears in the Windows Start Menu or Start Screen when you install or upgrade to XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7, or XenApp 7.7.

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.

## Send messages to users

July 2, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. In the Activity Manager view, select the user and click Details.
2. In the User Details view, locate the Session Details panel and click Send Message.
3. Type your message information in the Subject and Message fields, 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.

## Restore sessions

July 2, 2018

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 Server 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.

**Note**: If user devices are running VDAs earlier than XenDesktop 7, Director cannot display complete information about the session; instead, it displays a message that the information is not available.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

These messages might appear in the
User Details page and
Activity Manager.

## Reset a Personal vDisk

June 28, 2019

**Caution**: When you reset the disk, the settings revert to their factory default values and all data on it is deleted, including applications. The profile data is retained unless you modified the Personal vDisk default (of redirecting profiles from the C: drive), or you are not using a third-party profile solution.

To reset, the machine with the Personal vDisk must be running; however, the user does not have to be logged on to it.

This option is available only for Desktop OS machines; it is disabled for Server OS machines.

1. From the Help Desk view, choose the targeted Desktop OS machine.
2. From this view or in the Personalization panel of the User Details view, click Reset Personal vDisk.
3. Click Reset. A message appears warning that the user will be logged off. After the user is logged off (if the user was logged on), the machine restarts.

If the reset is successful, the Personal vDisk status field value in the Personalization panel of the User Details view is Running. If the reset is unsuccessful, a red X to the right of the Running value appears. When you point to this X, information about the failure appears.

## Run HDX channel system reports

July 2, 2018

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## Shadow users

October 29, 2018

From Director, use the shadow user feature to view and work directly on a user's virtual machine or session. 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.

1. In the User Details view, select the user session.
2. Activate shadowing for the selected user session:
    - For machine monitoring, in the Activity Manager view, click Shadow.
    - For session monitoring, in the User Details view, locate the Session Details panel and click Shadow.
3. After the connection initializes, a dialog box prompts you to open or save the .msrcincident file.
4. Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
5. Instruct the user to click Yes to start the machine or session sharing.

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.

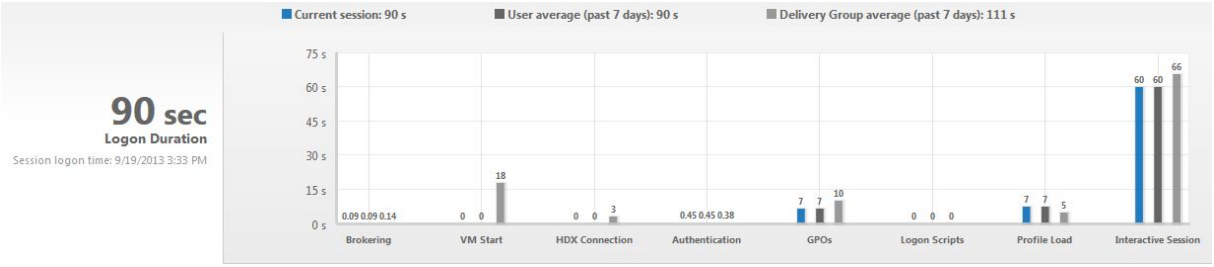
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

## Diagnose user logon issues

October 29, 2018

Use Logon Duration data to troubleshoot user logon issues. 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 XenApp and XenDesktop, the Monitor Service tracks the phases of the logon process from the time the user connects from Citrix Receiver 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) in the local time of the Administrator's web browser.

Use these general 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 phase | Description |
| --- | --- |
| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Logon process phase | Description |
| --- | --- |
| 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. |
| Login 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. |
| 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)**. |

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 might result in a longer logon duration than the sum.

**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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Escalate as needed. For example, if the VM startup is slow, the issue could 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 could 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.

## Record sessions

October 29, 2018

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 **Platinum** Sites.

To configure Session Recording on Director using the DirectorConfig tool, see the **Configure Director to use the Session Recording Server** section in Install, upgrade, and uninstall Session Recording.
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

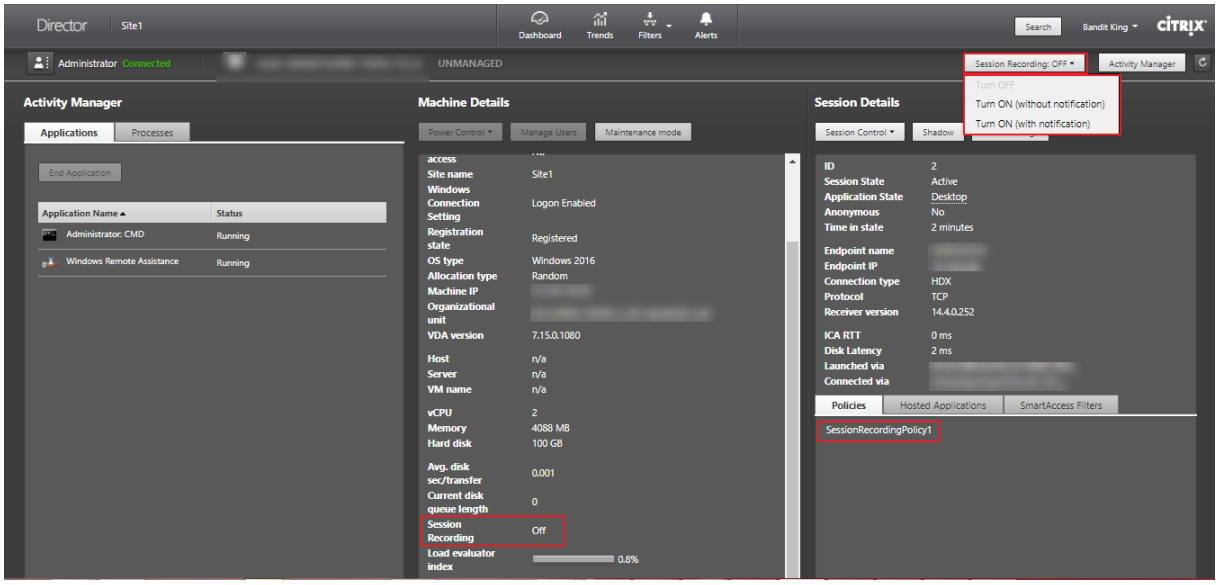
You can enable Session Recording for a specific user on the **Activity Manager** or the **User Details** screen. Subsequent sessions are recorded for the specific user on all supported servers.

You can:

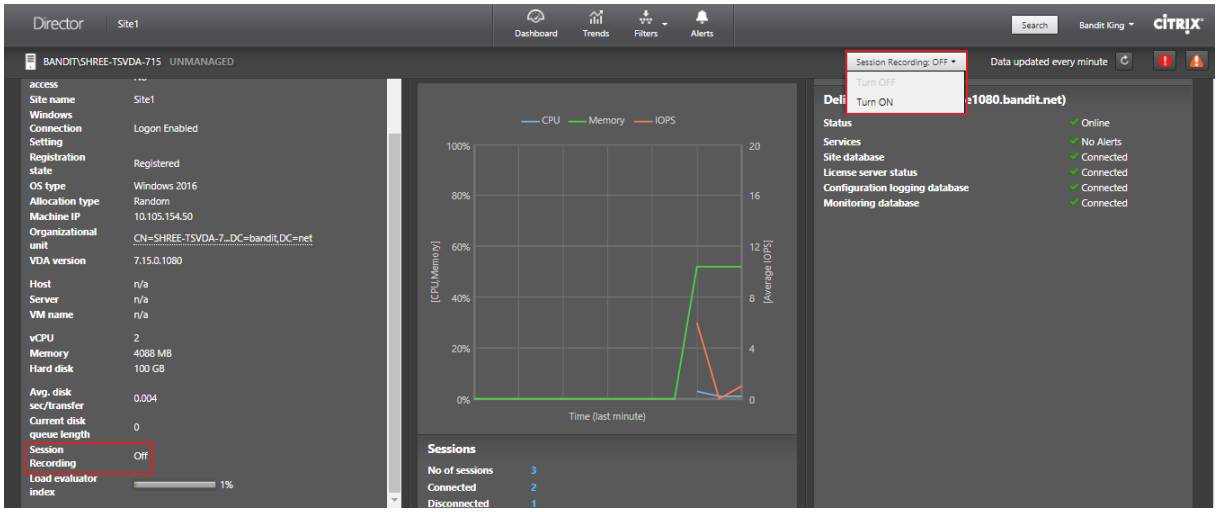
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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.




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

## Restore desktop connections

July 2, 2018

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. |

## Resolve application failures

February 22, 2019

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 greyed out, contact an administrator with the permission to enable the tab.

The list includes only those applications that were launched within the session.

For Server OS machines and Desktop 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Action | Description |
| --- | --- |
| 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 Desktop 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 Server 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. |

## Reset a user profile

July 2, 2018

**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),

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.

**Note**: The preceding steps assume you are using XenDesktop (Desktop VDA). If you are using XenApp (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

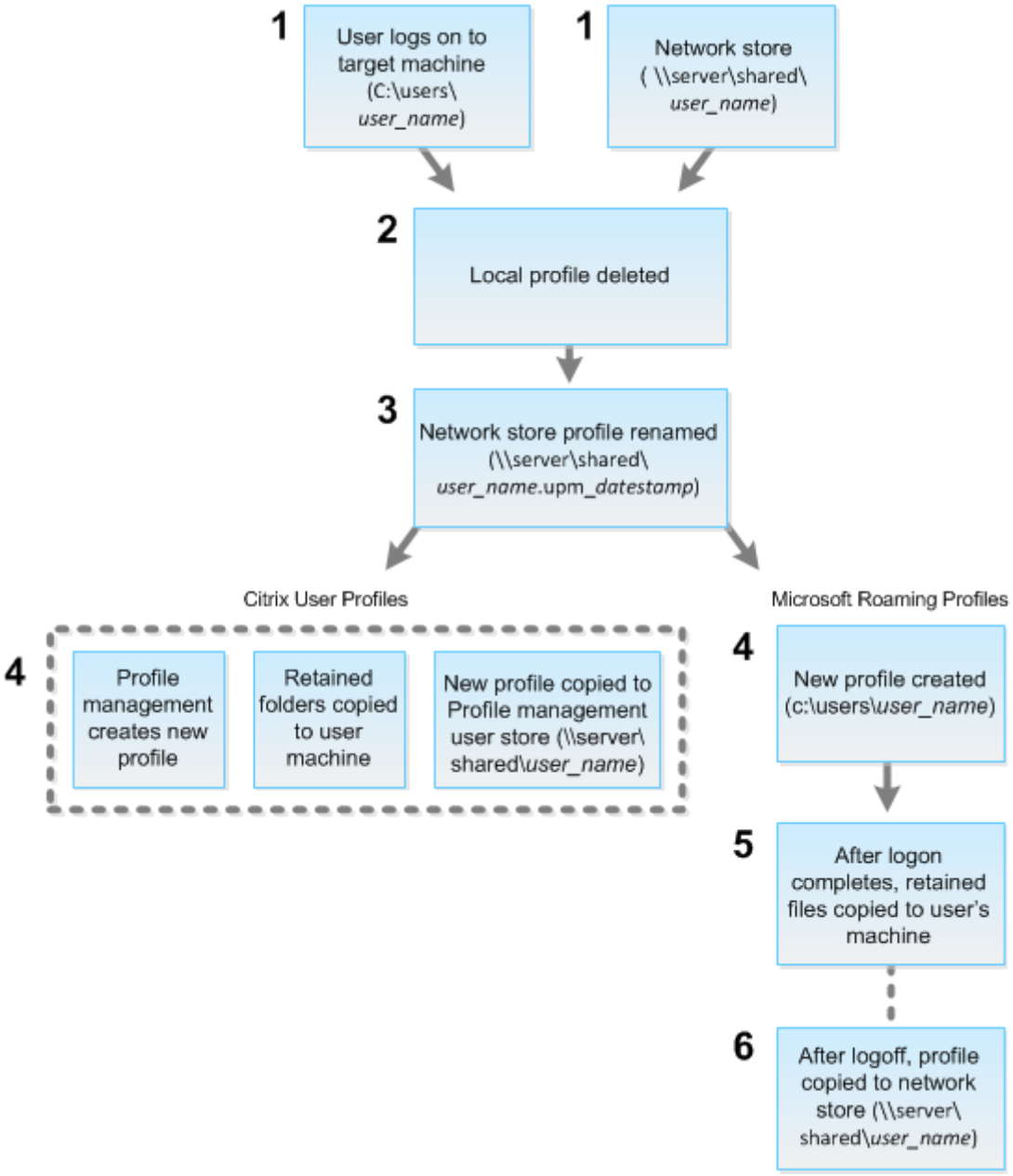
**Note**: In Windows 8 and later, cookies are not copied when profiles are reset.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




1. 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).
2. If a local profile is present, it is deleted.
3. The network profile is renamed.
4. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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.
Note: 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.

## Troubleshoot applications

October 29, 2018

### 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.

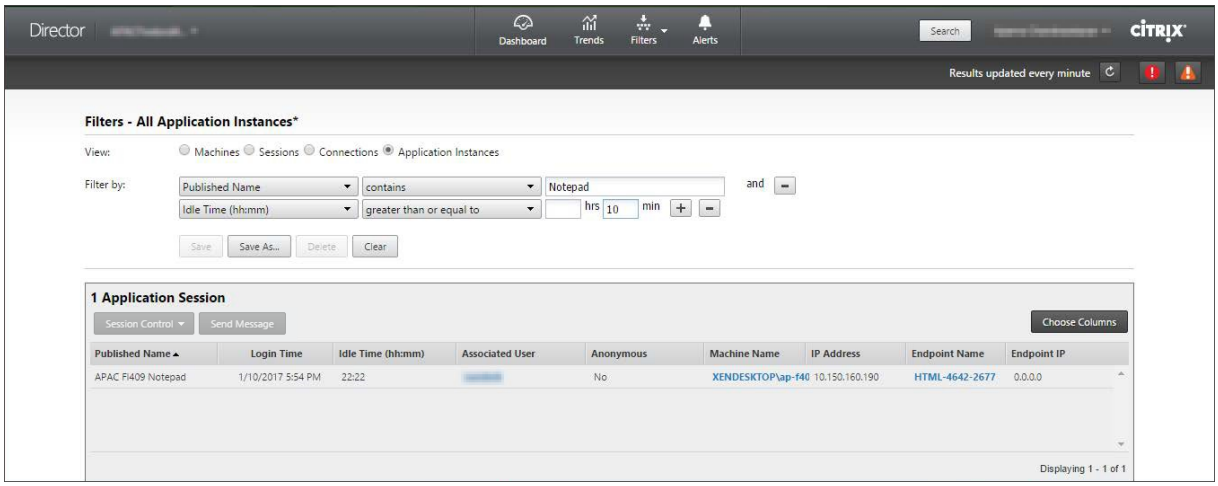
Typical use cases for application-based troubleshooting are in the healthcare sector, where employees share application licenses. There, you must end idle sessions and application instances to purge the XenApp and XenDesktop environment, to reconfigure poorly performing servers, or to maintain and upgrade applications.

The **Application Instances** filter page lists all application instances on VDAs of Server and Desktop OS. The associated idle time measurements are displayed for application instances on VDAs of Server OS that have been idle for at least 10 minutes.

**Note:** The Application Instances metrics are available on Sites of all license editions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

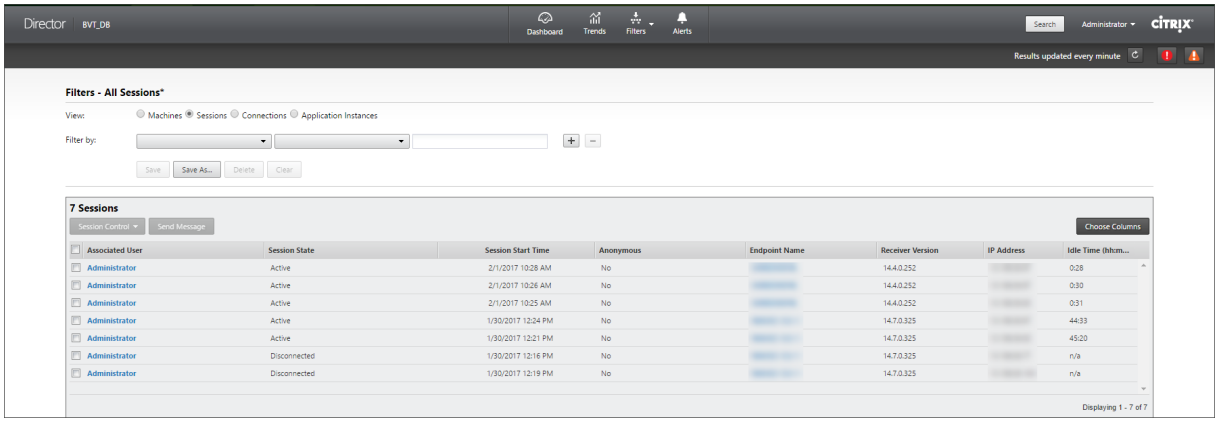
Use this information to identify the application instances that are idle beyond a specific time period and log off or disconnect them as appropriate. To do this, select **Filters > Application Instances** and select a pre-saved filter or choose **All Application Instances** and create your own filter.




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 Server 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 Desktop OS, or

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- is launched on a VDA running Version 7.12 or earlier.

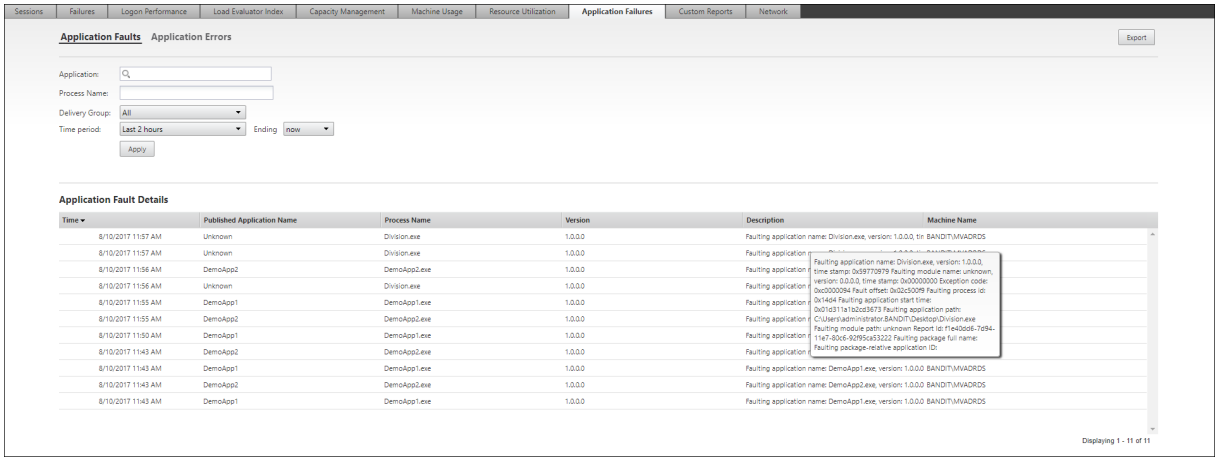
### Historical application failure monitoring

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 Platinum and Enterprise 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 Platinum and non-Platinum licensed Sites. You can change this setting using the PowerShell command:

```
*Set-MonitorConfiguration -\<setting name\> \<value\>*
```




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 Server OS VDAs are monitored. You can modify the monitoring settings through the Monitoring Group Policies: Enable monitoring of application failures,

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Enable monitoring of application failures on Desktop OS VDAs, and List of applications excluded from failure monitoring. For more information, see Policies for application failure monitoring in Monitoring policy settings.

## Troubleshoot machines

October 29, 2018

In the **Filters** > **Machines** view, select **Desktop OS Machines** or **Server OS Machines** to see the machines configured in the Site. The Server OS Machines tab 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.

Click the **Failure Reason** 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.

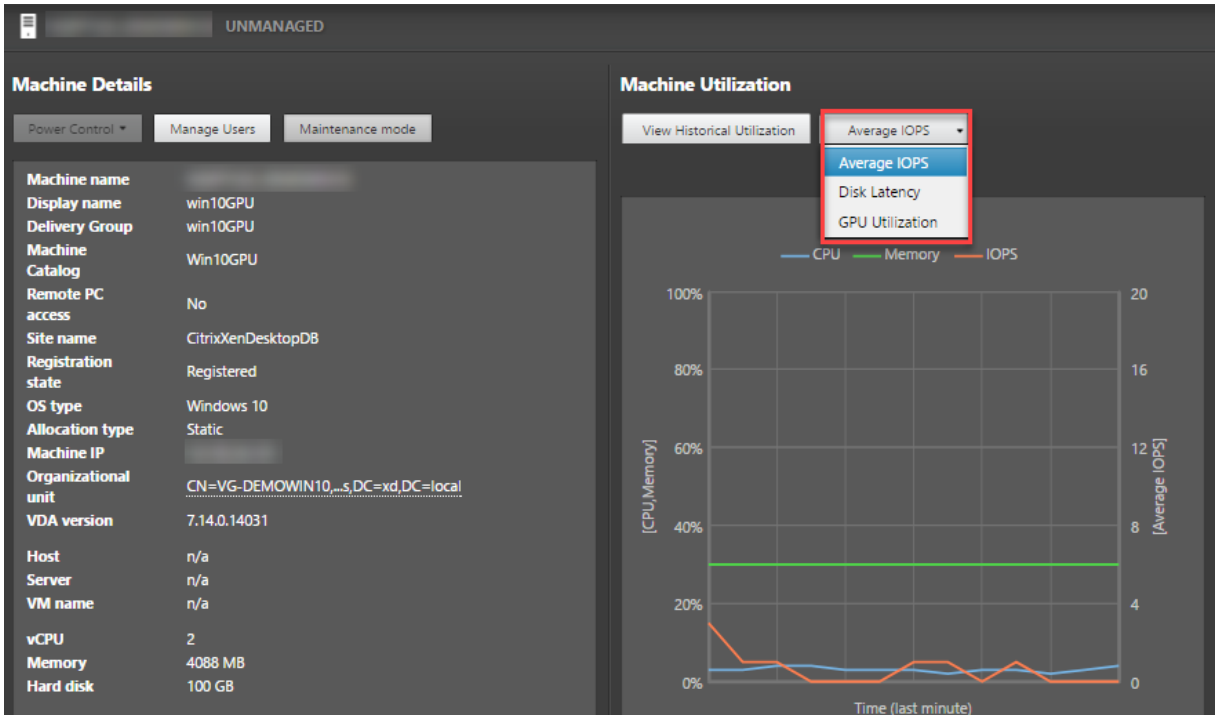
Click the machine name link to go to the **Machine Details** page. The Machine Details page lists the machine details, infrastructure details, and details of the hotfixes applied on the machine. The **Machine Utilization** panel displays the machine utilization graphs.

### 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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 Desktop 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 Desktop OS and GPU acceleration for Windows Server 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

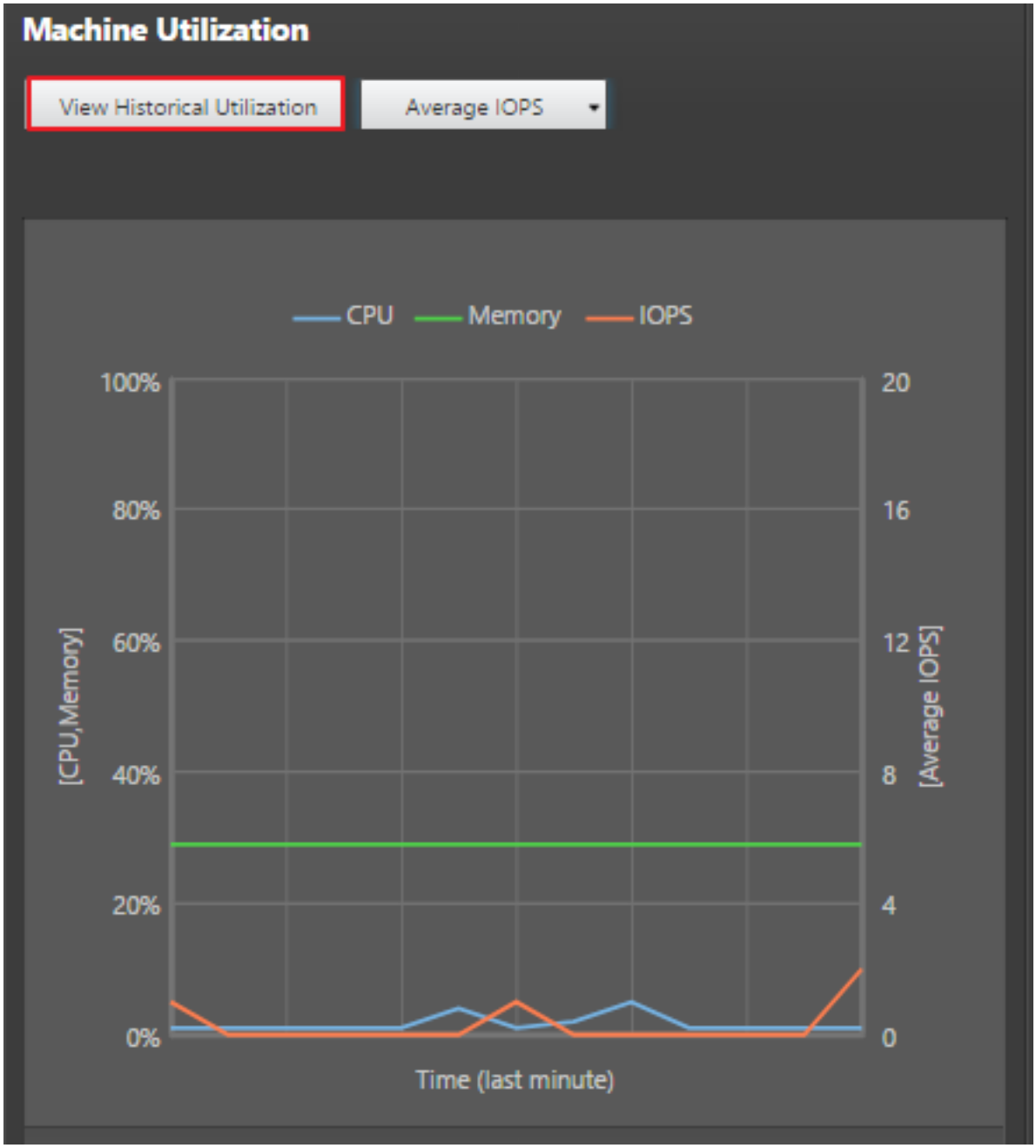
In the **Machine Utilization** panel, click **View Historical Utilization** to view the historical usage of resources on the selected machine.

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.

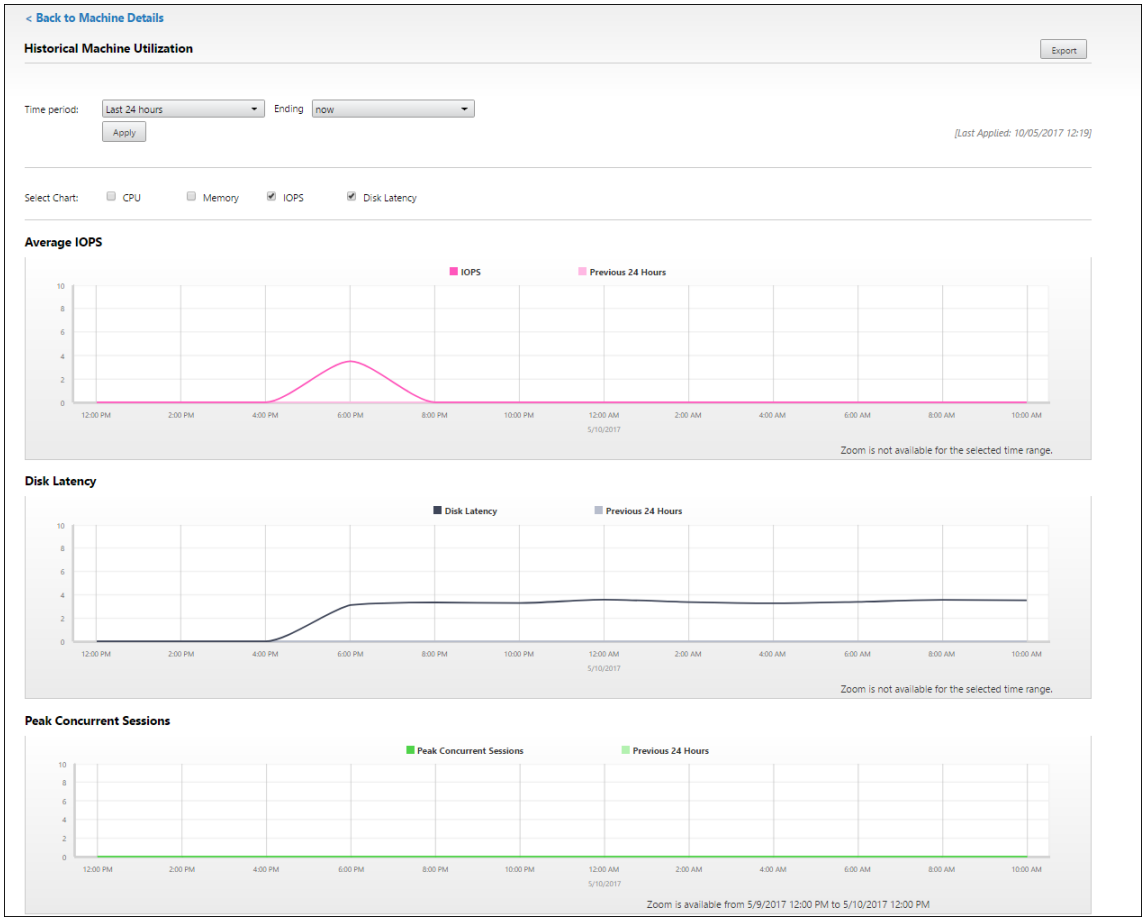
The CPU and memory utilization, average IOPS, and disk latency data is collected by default. You can disable the collection by using the **Enable Resource Monitoring** policy setting.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




1. From the **Machine Utilization** panel in the **Machine Details** view, select **View Historical Utilization**. This opens the **Historical Machine Utilization** page.
2. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




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.

5. Click **Export** to export the resource utilization data for the selected period. For more information, see Export reports section in Monitor Deployments.
6. 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".
7. To view the historical trend on the resource consumption of a particular process, drill into any of the Top 10 processes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Feature compatibility matrix

October 29, 2018

Within each Site, although you can use earlier versions of VDA or Delivery Controller, all the features in the latest version of Director might not be available. In addition, feature availability depends on the Site license edition. Citrix recommends having Director, Delivery Controller and VDA 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 table below lists Director features and the minimum version of Delivery Controller (DC), VDA and any other dependent components required along with License Edition.

| Director Version | Feature | Dependencies - min version required | Edition |
|---|---|---|---|
| 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 | Platinum |
| 7.12 | Automate Director notifications with SNMP traps | DC 7.12 and VDA 7.x | Platinum |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Director Version | Feature | Dependencies - min version required | Edition |
|---|---|---|---|
| 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 | Platinum |
| 7.11 | Export report improvements | DC 7.11 and VDA 7.x | All |
| 7.11 | Automate Director notifications with Citrix Octoblu | DC 7.11 and VDA 7.x | Platinum |
| 7.11 | Integration with NetScaler MAS | DC 7.11, VDA 7.x and MAS version 11.1 Build 49.16 | 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 | Platinum |
| 7.7 | SCOM integration | DC 7.7, VDA 7.x, SCOM 2012 R2, and PowerShell 3.0 | Platinum |
| 7.7 | Windows Authentication Integration | DC 7.x and VDA 7.x | All |
| 7.7 | Desktop and Server OS Usage | DC 7.7 and VDA 7.x | 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 | Platinum |
| 7 | HDX Insight integration | DC 7.6, VDA 7.x, and NetScaler Insight Center | Platinum |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Data granularity and retention

November 26, 2019

## 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 aggregated differently depending on its category. Understanding the aggregation of data values presented using the OData Method APIs is critical to interpreting the data. For example:

- Connected Sessions and Machine Failures occur over a period 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

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 Platinum licensed Sites can change the grooming retention to their desired number of retention days, otherwise the default is used.

To access the settings, run the following PowerShell commands on the Delivery Controller:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>

<!--NeedCopy-->
```

The following settings are used to control grooming:

| | Setting name | Affected grooming | Default value Platinum (days) | Default value non-Platinum (days) |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | Session and Connection records retention after Session termination | 90 | 7 |
| 2 | GroomFailuresRetentionDays | Machine-FailureLog and Connection-FailureLog records | 90 | 7 |
| 3 | GroomLoadIndexesRetentionDays | LoadIndex records | 90 | 7 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| | Setting name | Affected grooming | Default value Platinum (days) | Default value non-Platinum (days) |
|---|---|---|---|---|
| 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 |
| 5 | GroomSummariesRetentionDays | DesktopGroupSummary, FailureLogSummary, and LoadIndexSummary 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| | Setting name | Affected grooming | Default value Platinum (days) | Default value non-Platinum (days) |
|---|---|---|---|---|
| 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 |
| 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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| | Setting name | Affected grooming | Default value Platinum (days) | Default value non-Platinum (days) |
|---|---|---|---|---|
| 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 | GroomMachineMetricSummaryDataRetentionDays | Machine metrics summary data | 90 | 7 |
| 22 | GroomApplicationInstanceRetentionDays | Application error data | 1 | 1 |
| 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.

**Notes on grooming retention:**

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:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- 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 (100K 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

December 7, 2020

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 |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Category | Reason | Issue | Action |
| --- | --- | --- | --- |
| [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. |
| [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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Category | Reason | Issue | Action |
| --- | --- | --- | --- |
| [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. |
| [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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Category | Reason | Issue | Action |
| --- | --- | --- | --- |
| [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. |
| [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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Category | Reason | Issue | Action |
| --- | --- | --- | --- |
| [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. |
| [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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| Category | Reason | Issue | Action |
| --- | --- | --- | --- |
| [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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### 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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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. |

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

| 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

June 15, 2020

Several SDKs and APIs are available with this release. For details, see Developer Documentation. From there, you can access programming information for:

- Delivery Controller
- Monitor Service OData
- StoreFront

The Citrix Group Policy SDK allows you to display and configure Group Policy settings and filters. It 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 XenApp and XenDesktop SDK must be installed. See Group Policy SDK for more information.

### Delivery Controller SDK

The SDK comprises of a number of PowerShell snap-ins installed automatically by the installation wizard when you install the Delivery Controller or Studio component.

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 privileges to allow XenApp or XenDesktop to be installed, Citrix recommends that for normal

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

operation, you create Citrix administrators with the appropriate rights, rather than use the local administrators account. If you are running Windows Server 2008 R2, you must run the shell or script as a Citrix administrator, and not as a member of the local administrators group.

To 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 more information about PowerShell execution policy, see the Microsoft documentation.
3. Add the snap-ins you require into the PowerShell environment using the **Add -PSSnapin** cmdlet in the Windows PowerShell console.

V1 and V2 denote the version of the snap-in (XenDesktop 5 snap-ins are version 1; XenDesktop 7 snap-ins are version 2. For example, to install XenDesktop 7 snap-ins, type Add-PSSnapin Citrix.ADIdentity.Admin.V2). To import all the cmdlets, type: Add-PSSnapin Citrix.*.Admin.V*

After adding the snap-ins, you can access the cmdlets and their associated help.

**NOTE:** To see the current XenApp and XenDesktop PowerShell cmdlet help:

1. From the PowerShell console, add the Citrix snap-ins: Add –PSSnapin Citrix.*.Admin.V*.
2. Follow the instructions in PowerShell Integrated Scripting Environment (ISE).

### Group Policy SDK

To use the Group Policy SDK, either Studio or the XenApp and XenDesktop SDK must in installed.

To add the Group Policy SDK, 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.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).