XenApp and XenDesktop 7.9

Jun 15, 2016

What's new

System requirements

Technical overview

Install and configure

Remote PC Access

App-V

AppDisks

Local App Access and URL redirection

XenApp Secure Browser

Server VDI

Personal vDisk

Remove components

Upgrade and migrate

Upgrade a deployment

Migrate XenApp 6.x

Migrate XenDesktop 4

Secure

Security considerations and best practices

Delegated Administration

Smart cards

Transport Layer Security (TLS)

Federated Authentication Service

Print

Printing configuration example

Best practices, security considerations, and default operations

Printing policies and preferences

Provision printers

Maintain the printing environment

HDX

Thinwire Compatibility Mode

Framehawk virtual channel

HDX 3D Pro

Flash Redirection

Host to client redirection

GPU acceleration for Windows Desktop OS

Policies

Manage

Monitor

Director

Advanced configuration

Monitor deployments

Alerts and notifications

Delegated Administration and Director

Secure Director deployment

Configure permissions for VDAs earlier than XenDesktop 7

Configure HDX Insight

Troubleshoot user issues

SDKs and APIs

Monitor Service OData API

FIPS Sample Deployments

Citrix SCOM Management Pack for XenApp and XenDesktop

Citrix SCOM Management Pack for License Server

What's new

Jun 07, 2016

In this article:

About this release

The XenApp and XenDesktop 7.9 release comprises 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. This allows you to use all of the latest features, summarized below. For instructions, see the Prepare to install or Upgrade a deployment article.

- **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. This is often helpful when you want to test enhancements in a non-production environment. New and updated features in the VDAs are summarized below. For instructions, see the following articles:

  Install or upgrade VDAs using the graphical interface of the standalone VDA installer

  Install or upgrade VDAs from the command line interface of the standalone VDA installer

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

Provisioning Services

AppDNA

XenApp and XenDesktop 7.9

The product release includes the following new and enhanced features.

This section summarizes the changes in this release in the installation and configuration of XenApp and XenDesktop.

- Analytics are collected and stored locally when you install components.
- If you install a VDA and do not specify Controller addresses, you are reminded that the VDA cannot register until Controller addresses are provided.
- If you specify one or more Controller addresses when you install a VDA, the installer verifies whether a connection can be made between the VDA and the Controller, and reports the outcome.
- The installation wizards no longer offer Citrix Customer Experience Improvement Program enrollment; participation is assumed.
- The core component and VDA installation wizards now offer enrollment in Call Home.
- You can now install the Federated Authentication Service from the full product installer's graphical interface.

The following changes are implemented for possible use in future releases.

- Microsoft SQL Express LocalDB 2014 is installed automatically when you install a Delivery Controller. This software is not used for the Site, monitoring, or logging databases. There is no administrator interaction with this database. To prohibit its installation, install the Controller with the XenDesktopServerSetup.exe command with the /exclude "Microsoft SQL Server 2014 Express LocalDB" option.
- When you create a Site, if you choose to install the SQL Server Express database for use as the Site database (which is the default setting), a restart will occur after that database software is installed. That restart will not occur if you choose not to install the SQL Server Express software for use as the Site database.

During an upgrade, the installer no longer detects or upgrades the Citrix Receiver for Windows Enterprise, the Offline Plug-in for Windows, or the XenApp Plugin for Streamed Apps. For details, see the Upgrade a deployment article.

When you create a connection to a hypervisor or cloud service provider that will be used to host machines created with Machine Creation Services (MCS), you can now specify storage locations for different data types:

- Operating system data, which includes master images.
- Temporary data, which includes all non-persistent data written to MCS-provisioned machines, Windows page files, user profile data, and any data that is synchronized with ShareFile. This data is discarded each time a machine restarts.
- Personal data stored on personal vDisks.

Providing separate storage for each data type can reduce load and improve IOPS performance on each storage device, making best use of the host's available resources. It also enables appropriate storage to be used for the different data types - persistence and resilience is more important for some data than others.

When you choose storage shared by hypervisors, you can choose whether to use local storage for temporary machine data. When you create a Machine Catalog that uses that connection, you can enable and configure nondefault values for each VM's cache disk size and memory size.

When you choose storage local to the hypervisor, you can choose whether to use shared storage for personal vDisks (if you are using personal vDisks).

For more information, see the Connections and resources and Create Machine Catalogs articles.

If you will use Nutanix Acropolis to host provisioned VMs, install the Nutanix plugin on the Delivery Controllers to enable configuration of Nutanix connections in Studio.

When you use Studio to create a connection to Nutanix and a Machine Catalog that uses a Nutanix image, the wizards allow you to specify standard and Nutanix-specific configuration information.

For more information, see the Nutanix virtualization environments article.

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.

For more information, see the Create Application Groups and Manage Application Groups articles.

The introduction of Application Groups affects several other Studio areas. For example, when you edit an application's properties, its group membership can include Delivery Groups and/or Application Groups. Previously, an application had to be associated with at least one Delivery Group; now, it must be associated with at least one Delivery Group or Application Groups. For information about managing applications, see Applications.

The Citrix Federated Authentication Service is a privileged component designed to integrate with your Microsoft Certificate Authority. It dynamically issues certificates for users, allowing them to log on to a Citrix environment as if they had a smart card. This allows StoreFront to use a broader range of authentication options, such as SAML (Security Assertion Markup Language) assertions.

For more information, see the Federated Authentication Service article.

For more information about telemetry features, including how to participate, see the Citrix Insight Services article.

Installer analytics

When using the full product installer, analytic data is collected and stored locally when you install XenApp and XenDesktop components. If you encounter installation issues, Citrix may ask you to upload this data for analysis.

Call Home

Participation in Call Home (including always-on tracing) is offered in the full product installer. You can also change your enrollment, create custom upload schedules, and manually upload packages using PowerShell cmdlets.

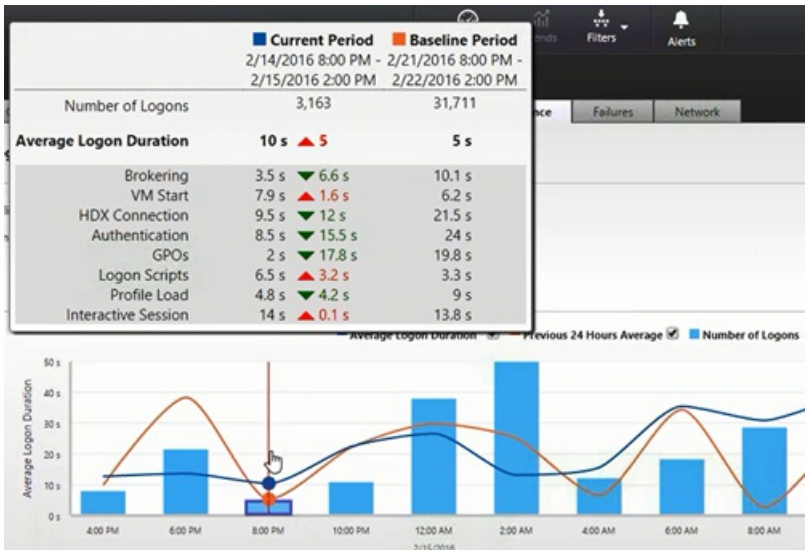
Citrix Customer Experience Improvement Program (CEIP)

Participation in the Citrix Customer Experience Improvement Program is now automatically enabled when you create a Site.

You do not need to enroll during the Site creation wizard. You can change your participation after you create the Site.

Director includes the following new and enhanced features:

- **Logon Duration improvements**. When you select a data point on the Logon Performance chart the "tooltip" data is more clearly laid out and easier to interpret. In addition, Number of Logons is represented by a bar chart (previously a line chart). The Number of Logons and the Previous baseline period can be toggled for display on the chart. There is a new table showing Logon Duration by User Session for the selected time period, displayed below the Logon Performance chart. The administrator can search for users and choose the columns and sort order to display. For more information, see Monitor deployments.



Virtual Delivery Agents (VDAs) 7.9

Version 7.9 of the VDA for Server OS and the VDA for Desktop OS include the following enhancements to printing, HDX technologies and platform support:

- **Load balancing for Citrix Universal Print Server (UPS)**. Administrators can add multiple load balanced print servers using two new policy settings, Universal Print Servers for load balancing and Universal Print Server out-of-service threshold. These allow XenApp and XenDesktop sessions on a VDA to seamlessly map session printers to different print servers at logon time. For more information, see Universal Print Server policy settings and Load balance the Universal Print Servers in the Maintain the printing environment article.
- **Stapling and paper source selection for Citrix XPS Universal print driver**. The Citrix XPS Universal print driver supports advanced printing features such as stapling and paper source selection. For more information, see Provision Printers.
- **Universal Print Server and CEIP**. Enrollment in CEIP is automatic when you install the Universal Print Server. No data is collected in the first seven days. During that time, or at any time in the future you can disable participation in CEIP for UPS with a registry setting. For more information, see Provision Printers and Citrix Insight Services.
- **LPT and COM port redirection policy settings in Studio**. LPT and COM port settings are now configurable in Studio. In VDA versions 7.0 through 7.8 these settings were only configurable using the registry. For more information,

see Port redirection policy settings and Bandwidth policy settings.

- **Extended HDX 3D Pro support for Intel CPUs with Intel Iris Pro graphics**. Use HDX 3D Pro graphics acceleration technologies with 5th and 6th Generation Intel CPUs with Intel Iris Pro graphics. This release includes support for multi-monitors (up to a maximum of three), console blanking, custom resolution and high frame rate. The VDA installers include a new file, GfxDisplayTool.exe, to support this feature. For more information, see GPU acceleration for Windows Desktop OS.
- **Support for Windows 10 in the HDX 3D Pro VDA**. This release adds support for Windows 10 in the HDX 3D Pro version of the VDA for Windows Desktop OS.
- **Support for Secure Boot for Remote PC access on Windows 10**. The Virtual Delivery Agent (VDA) for Desktop OS supports Secure Boot for XenDesktop Remote PC Access on Windows 10 and 8.1.
- **New default setting for Use video codec for compression**. Use video codec when preferred is the new default for the graphics policy setting, Use video codec for compression. This change is to support the use of Thinwire Compatibility mode by the VDA. For more information, see Graphics policy settings.
- **Linux VDA enhancements and improvements for Red Hat and SUSE.** Added support for VC CDM and CentOS (version 6.7, 7.2) with numerous improvements to address customer reported issues. For more information, see the Red Hat/CentOS and SUSE articles.
- **Generic USB redirection for mass storage devices on XenApp**. Generic USB redirection (USB plug-and-play) for mass storage devices is now supported in XenApp as well as XenDesktop. XenApp users can interact with mass storage devices in a XenApp session as if the storage device was physically attached. To use this feature in XenApp, you must first install the Microsoft security update KB3155784. In this release, this feature is disabled by default for XenApp and enabled with a registry key.

  To enable USB storage devices for Generic USB redirection in XenApp, create a value name **UsbStorageEnabled** under the key **HKLM\SOFTWARE\Citrix\Portica\GenericUSB** and set its value to **1**.

  Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

StoreFront 3.6

StoreFront includes the following new features:

- **Load balance non-identical farms.** In previous StoreFront versions when creating equivalent farm sets using a multisite configuration, all resources had to be published by every delivery controller for load balancing to succeed. The resource enumeration process where StoreFront obtained a list of available resources contacted only one of the delivery controllers in the equivalent farm set. In StoreFront 3.6, you can have some resources that are common to all delivery controllers in the equivalent farm set and some that are published only by specific delivery controllers. You can now set StoreFront to enumerate from all of them.
- **No Active Directory Domain requirement for single server deployments.** For various reasons, you might not want to add your servers to an Active Directory domain. This version eliminates that requirement for single server deployments and allows you to install StoreFront on a nondomain-joined server.
- **StoreFront REST API.** We have created a StoreFront REST API that NetScaler Gateway can query to determine the current gateway configuration of the StoreFront cluster. The NetScaler administration console creates a gateway configuration file combination of the StoreFront and NetScaler settings. You can import the configuration file into StoreFront using the StoreFront management console or PowerShell.

For more information, see the StoreFront 3.6 documentation.

Provisioning Services 7.9

Provisioning Services includes the following new features:

- **Citrix Customer Experience Improvement Program (CEIP)**. CEIP gathers anonymous configuration and usage data from Provisioning Services and automatically sends the data to Citrix. This data helps Citrix improve the quality, reliability, and performance of Provisioning Services.
- **BDM support for UEFI through the XenDesktop setup wizard**. UEFI BDM support now includes integration with XenDesktop setup wizard, which allows you to set the BDM boot option to target UEFI firmware. With this support, PVS supports booting from:
  - ISO
  - USB
  - boot partitions
- **Updating a BDM partition**. Provisioning Services 7.9 introduces functionality that allows you to upgrade the BDM partition based on the server IP address in the bootstrap of the PVS server to which you are connected. A BDM partition can be upgraded in one of three ways:
  - by collection
  - by a group of highlighted devices
  - by a single device

For more information, see the Provisioning Services 7.9 documentation.

AppDNA 7.9

AppDNA includes the following new features:

- **Import applications workflow enhancements**. Improvements to the import applications workflow provide feedback on the progress of server-side processing and the flexibility to add and cancel imports.
- **Compliance Manager module**. The Compliance Manager module helps you understand if applications that you are planning to deploy into your IT infrastructure could introduce security risks. This module contains an initial set of algorithms and reports, which will be extended in the future. This is a feature for evaluation in this release and should not be used to make decisions to deploy applications to the production environment.
- **Web client access to application attributes forms**. This release adds access to application attribute forms from the AppDNA web client. From the web client, select Applications, highlight an application and select Properties.

For more information, see the AppDNA 7.9 documentation.

Fixed issues

Jan 31, 2017

The following issues have been fixed since Version 7.8:

AppDNA	Provisioning Services
Citrix Director	StoreFront
Citrix Policy	Universal Print Server
Citrix Studio	VDA for Desktop OS
Controller	VDA for Server OS
HDX MediaStream Flash Redirection	Virtual Desktop Components - Other
Installer	

- When attempting to export a large amount of data in PDF format, the server's CPU and memory consumptions can approach 100% and the following error message appears:

  "Action failed. Data source unresponsive or reported an error. View server event logs for further information."

  This fix introduces a configurable limit for the PDF export and as a result, at least a portion of the report can be obtained.

  After installing this fix, you must configure the web.config file in the wwwroot\Director folder as follows:

  Add the following line to "appSettings" section:

  <add key="UI.ExportPdfDrilldownLimit" value="100"/>

  The limit depends on the capability of the server, such as the memory size where the value specifies the count of rows in the PDF report.

  [#LC4108]

- Attempts to export reports in any file format might fail with the following error message:

  "Action failed. Unexpected server error. View server event logs for further information."

[#LC4281]

- If a XenApp server has two IP addresses and the DNS server cannot resolve the first IP address, attempts to log on to Citrix Director by an administrator might fail with the following error message:

  "The system is currently unavailable. Please try again later or contact your administrator."

  [#LC4411]

- When attempting to export a large amount of data in CSV format, a timeout can occur and the export might fail with the following error message:

  "Action failed. Data source unresponsive or reported an error. View Director server event logs for further information."

  This fix lets you configure the timeout value for exporting data.

  After installing the fix, you must configure the web.config file in the wwwroot\Director folder as follows:

  Add the following line to "appSettings" section:
  <add key="Connector.DataServiceContext.Timeout" value="3600" /> where the value specifies the timeout in seconds.

  [#LC4467]

- Selecting a user to display that user's session details can result in the user name that appears in the top left corner to show as "NULL."

  [#LC4589]

- If the NetBios domain name contains an ampersand (&), shadowing from the Citrix Director console might fail. This issue occurs because the ampersand character is a reserved character in XML and can cause the parsing for the current logon to fail.

  [#LC4633]

- Citrix Director with Windows Integrated Authentication (WIA) might not work with a Kerberos Constrained Delegation setup.

  [#LC5196]

- Citrix Director administrators might not be able to view Citrix policies in session details.

  [#LC3941]

- Attempts to add multiple session printers to a group of user devices under the "Printer assignments" window fails to expand and display the scrollbar. As a result, attempts to add multiple session printers to a group of user devices can fail.

  [#LC4658]

- Citrix Director administrators might not be able to view Citrix policies in session details.

  [#LC4956]

- When using the Machine Creation Service to catalog VDAs for Server OS, unavailability of personal vDisk storage can incorrectly set the "CleanOnBoot" property of the catalog to "False." As a result, the catalog might fail to update.

  [#LC2959]

- Creating multiple applications in multiple folders under Delivery Groups in Citrix Studio might result in a large folder structure. The first time you open Citrix Studio and click folders or applications, the folders or applications might be dragged instead of being selected. This moves the selected object and causes the folder or application structure to change.

  [#LC3705]

- Attempts to open Citrix Studio by users that are not members of the Database administrators user group can result in permission errors on the SQL Server.

  [#LC4127]

- Attempts to provision additional resources to a multi-tenant offering in App Orchestration 2.6 can fail if the offering already contains two or more tenants.

  [#LC4170]

- When a Delivery Controller goes offline or becomes otherwise unavailable, Citrix Studio might operate slowly.

  [#LC4481]

- 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]

- Performing a scheduled restart of a VDA for Server OS that is connected to a VMware Vsphere Hypervisor can cause the server to shut down and remain in a powered off state.

  - To enable the fix, set the following registry key:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule
    Name: ShutdownTimeoutRecovery
    Type: DWORD
    Value: 1

  - To disable the fix, set the following registry key:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule
    Name: ShutdownTimeoutRecovery
    Type: DWORD
    Value: 0

  After setting the value, you must restart the Broker Service.

  [#LC3807]

- Attempts to open Citrix Studio by users that are not members of the Database administrators user group can result in permission errors on the SQL Server.

  [#LC4127]

- When the setting "SupportMultipleForest" is enabled on the Controller to allow NTLM authentication, the Linux VDA might fail to complete the registration process as its Service Principal Name (SPN) might not be set in the EndpointReference of the Windows Communication Foundation (WCF).

  [#LC4235]

- When a Delivery Controller goes offline or becomes otherwise unavailable, Citrix Studio might operate slowly.

  [#LC4481]

- The WaitForTask response causes the exception VimApi.MissingProperty which does not allow the update of Machine Catalogs.

  [#LC4573]

- When running the PowerShell command "Get-LogSummary" for a date range that encompasses a switch to or from daylight saving time, the following error message appears:

  "An item with the same key has already been added."

  The issue occurs when daylight saving time introduces ambiguous local dates or times. As a result, duplicate entries are created in the HashMap and an exception occurs.

  This fix introduces a message to inform users to split the time span to account separately for the point in time when daylight saving time begins or ends.

  [#LC4612]

- Attempts to update machine catalogs in Amazon Web Services (AWS) environments can fail intermittently. To enable the fix, you must run the command, "Set-ProvServiceConfigurationData –Name ImageManagementPrep_DoImagePreparation –Value $false" for the image preparation phase to be skipped during the machine catalog update.

  [#LC4709]

- Controllers occasionally lose connectivity with the database when there is a high number of apps and VDA processes running. When that happens, VDAs remain in the initialization state and applications are unavailable.

  [#LC4848]

- 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]

- This fix addresses an issue that prevents Machine Creation Services provisioning from working in Amazon Web Services when the Controller is isolated from Amazon's public API endpoints by way of a web proxy.

[#LC5109]

- With HDX Mediastream for Flash enabled, opening and closing multiple tabs in Internet Explorer with Flash content can cause Internet Explorer to exit unexpectedly.

  [#LA3065]

- With HDX Mediastream for Flash enabled, opening and closing multiple tabs in Internet Explorer can cause Internet Explorer to close unexpectedly.

  [#LC1141]

- With HDX MediaStream Flash Redirection enabled, Microsoft Internet Explorer might close unexpectedly when it runs pseudoserverinproc2.dll.

  To enable the fix, create the following registry key:

  - *On Windows 32-bit systems*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
    Name: AllowCOMObjectTrack
    Type: DWORD
    Value: 0

  - *On Windows 64-bit systems*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
    Name: AllowCOMObjectTrack
    Type: DWORD
    Value: 0

  [#LC1885]

- When browsing websites with HDX MediaStream Flash Redirection enabled, the Flash redirection feature fails if the registry value of HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs is set to just "mfaphook.dll" or "mfaphook64.dll" instead of the full path to "mfaphook.dll" or "mfaphook64.dll."

  [#LC4388]

- When installing a VDA, certain registry keys for performance might be installed even if you disable the "Optimize Performance" option during installation.

  [#LC4330]

Client

- The NextGen application occasionally fails when trying to print to the Universal Print Server.

  [#LC4246]

Server

- Batch printing using the Microsoft GDI Print API can fail to where the last page does not print, and the following error message appears:

  "Dispatch::CDriverTripSummary::PrintReport, Error Occured While Printing....Check Printer"

  [#LC3920]

- This fix introduces support for Citrix UPS Print Driver Certification Tool for Universal Print Server 7.6.300. For more information, see Knowledge Center article CTX142119.

  [#LC4265]

HDX MediaStream Windows Media Redirection

- If you play an .avi file with Windows Media Player within an ICA session (or published desktop session) and then start playing another .avi file without stopping the first one, the video frames might not be properly directed to the user device. As a result, the CPU usage of the mmvdhost.exe process can be higher than normal and the video might not render properly on the user device.

  [#LC4260]

- With HDX MediaStream Windows Media Redirection enabled, certain third party players might exit unexpectedly while rendering files on a VDA that is running on Windows 10.

  [#LC5110]

Printing

- The Citrix Print Spooler Service might exit unexpectedly.

  [#LC4180]

- The "Auto-create client printers" policy might fail to set default printers correctly in a published application and Microsoft XPS Document Writer is set as the default printer.

  [#LC4696]

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]

- When multiple webcams or video capturing devices are installed on an endpoint, only one of the devices is mapped into the client session. Additionally, the device is mapped as Citrix HDX Web Camera, leaving no obvious clue as to which of the devices is mapped.

  [#LC1919]

- Certain third-party published applications might fail to start on XenApp servers. As a result, the wfshell.exe process might close unexpectedly. When this error occurs, no indication that the session is starting or error messages appear on the user device.

  [#LC3766]

- After undocking the Thomson Reuters Eikon toolbar in a multiple monitor session, the space occupied by the toolbar is not reclaimed by the session.

  In monitor configurations where the primary monitor is not located in the top left corner of the array, you must also install Fix #LC1599, which is included in Receiver for Windows 4.4 and later.

  [#LC3773]

- When the App-V configuration setting "EnablePublishingRefreshUI" is enabled on the session host and "Session Lingering" is enabled as well, attempts to close an application on an iOS device can result in a black window that stays on the device screen.

  [#LC3800]

- If you power off or force a remote PC to restart while in an ICA session, all audio drivers might be disabled when the remote PC restart completes.

  [#LC4071]

- After installing Hotfix ICAWS760WX64032 and enabling SSL, attempts to reconnect to a VDA might fail intermittently. The issue occurs if the Citrix ICA Service exits unexpectedly or becomes unresponsive as a result of an SSL Listener failure.

  [#LC4438]

- After a network interruption between a VDA and Citrix Receiver, you cannot play back an .avi file on Windows Media Player.

  [#LC4670]

- Attempts to reconnect to a VDA session after a network interruption might fail. The issue occurs after upgrading VDA to Version 7.8.

  [#LC5040]

- This fix addresses an issue that breaks client-side fetching for DirectShow based applications, preventing videos from rendering.

  [#LC5098]

Smart Cards

- In Microsoft Internet Explorer, the user interface for smart card logons to certain websites can be intermittently unavailable.

  [#LC3988]

- The Sign-in option does not appear on Version 7.6.300 and later VDAs running on Windows 10 Build 10586 and later. As a result, smart card logons are not possible.

  [#LC4778]

System Exceptions

- The operating system experiences an error on ctxad.sys and a blue screen appears with bugcheck code 0xD1.

  [#LC4007]

- When you repeatedly play an .avi file on Windows Media Player, the memory consumption of the wfica32.exe process might continue to increase until the process exits unexpectedly.

  [#LC4335]

- If the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses is defined, attempts to restart the VDA and launch a published desktop can result in a blue screen.

  [#LC4597]

- A published application process might exit unexpectedly with an exception "c000041d" on MobileDesktopHook64.dll.

  [#LC4821]

User Experience

- When you switch from a touch-optimized published desktop to a regular published desktop, the Start button:
  - Does not highlight when you hover over it
  - Brings up the local desktop instead of the published desktop

[#LC3466]

User Interface

- After publishing seamless applications, the generic Citrix Receiver icon may appear instead of the published app icon in the taskbar.

  [#LC4757]

HDX MediaStream Windows Media Redirection	Smart Cards
Printing	System Exceptions
Server/Site Administration	User Experience
Session/Connection	User Interface

HDX MediaStream Windows Media Redirection

- If you play an .avi file with Windows Media Player within an ICA session (or published desktop session) and then start playing another .avi file without stopping the first one, the video frames might not be properly directed to the user device. As a result, the CPU usage of the mmvdhost.exe process can be higher than normal and the video might not render properly on the user device.

  [#LC4260]

- With HDX MediaStream Windows Media Redirection enabled, certain third party players might exit unexpectedly while rendering files on a VDA that is running on Windows 10.

  [#LC5110]

Printing

- The Citrix Print Spooler Service might exit unexpectedly.

  [#LC4180]

- With legacy printer names enabled, autocreated printers might not be available for use in a published application when multiple sessions are established on a single server for the same user.

  [#LC4517]

- Printer redirection can intermittently fail.

  [#LC4584]

- The "Auto-create client printers" policy might fail to set default printers correctly in a published application and Microsoft XPS Document Writer is set as the default printer.

[#LC4696]

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]

- Multiple, concurrent attempts to establish a Remote Desktop (RDP) connection to a VDA from separate user devices can cause the VDA to unregister.

  [#LC4014]

Session/Connection

- With the Client audio redirection or Windows Media Redirection policies disabled, the Volume control (Speaker) icon in the notification area of a published desktop session can display an incorrect audio state.

  [#LC2538]

- By default, Windows Quick Access shortcuts for "Desktop" and "Downloads" are recreated in %userprofile%\Links at logon even if you manually deleted them earlier. This behavior is not desirable in all scenarios. This fix introduces support for the following registry key that, when set to 0 (zero), prevents the automatic recreation of those two shortcuts:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell
  Name: CreateShortcutLinks
  Type: REG_DWORD
  Data: 0

  [#LC3274]

- This fix addresses an issue that results in the occasional corruption of files that are being written to mapped client drives.

  [#LC3684]

- Certain third-party published applications might fail to start on XenApp servers. As a result, the wfshell.exe process might close unexpectedly. When this error occurs, no indication that the session is starting or error messages appear on the user device.

  [#LC3766]

- After undocking the Thomson Reuters Eikon toolbar in a multiple monitor session, the space occupied by the toolbar is not reclaimed by the session.

  In monitor configurations where the primary monitor is not located in the top left corner of the array, you must also install Fix #LC1599, which is included in Receiver for Windows 4.4 and later.

  [#LC3773]

- With Excelhook enabled, if you have multiple Excel workbooks open and minimize them, you might not be able to bring any of the workbooks into focus.

[#LC3799]

- When the App-V configuration setting "EnablePublishingRefreshUI" is enabled on the session host and "Session Lingering" is enabled as well, attempts to close an application on an iOS device can result in a black window that stays on the device screen.

  [#LC3800]

- Even with the Client audio redirection policy enabled, audio (.wav) files can fail to play. The issue occurs in sessions where the session ID is reused and the Client audio redirection policy was disabled for the previous session.

  [#LC3882]

- 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]

- Using published instances of Microsoft Internet Explorer, attempts to download a file from a website and saving it to a mapped client drive ("Save as...") can fail.

  [#LC4300]

- The icaendpoint.dll file can cause the Windows Audio Service to exit unexpectedly.

  [#LC4356]

- If another process holds the same lock as picadm.sys, users cannot log off from the session and the session remains in a disconnected state.

  [#LC4415]

- On systems with Fix #LC0615 installed, session logoffs can take longer than expected.

  [#LC4674]

- 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\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*processname*> and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows 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]

- This fix addresses an issue that breaks client-side fetching for DirectShow based applications, preventing videos from rendering.

  [#LC5098]

Smart Cards

- In Microsoft Internet Explorer, the user interface for smart card logons to certain websites can be intermittently unavailable.

  [#LC3988]

- The Sign-in option does not appear on Version 7.6.300 and later VDAs running on Windows 10 Build 10586 and later. As a result, smart card logons are not possible.

  [#LC4778]

System Exceptions

- When you repeatedly play an .avi file on Windows Media Player, the memory consumption of the wfica32.exe process might continue to increase until the process exits unexpectedly.

  [#LC4335]

- If the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses is defined, attempts to restart the VDA and launch a published desktop can result in a blue screen.

  [#LC4597]

- A published application process might exit unexpectedly with an exception "c000041d" on MobileDesktopHook64.dll.

  [#LC4821]

User Experience

- When you switch from a touch-optimized published desktop to a regular published desktop, the Start button:
  - Does not highlight when you hover over it
  - Brings up the local desktop instead of the published desktop

  [#LC3466]

- When attempting to move a Microsoft Excel window within a seamless, dual-monitor session, the window might experience a delay while redrawing in the new location.

[#LC4441]

User Interface

- After publishing seamless applications, the generic Citrix Receiver icon may appear instead of the published app icon in the taskbar.

  [#LC4757]

Virtual Desktop Components - Other

- Applications that use App-V integration might fail to launch if the configured working directory does not exist.

  [#LC4839]

Known issues

Aug 03, 2016

The following caution applies to any workaround that suggests changing a registry entry.

> **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.

XenApp and XenDesktop

The XenApp and XenDesktop 7.9 release contains the following issues:

- When using a USB mass storage device on the endpoint, with the USB redirection policy enabled, a "Device in use" error message might appear when attempting to eject the device.
  - In a Remote PC Access environment, reinstall the VDA from the command line. This will prevent the error from occurring again.
  - In other environments, try one of the following workarounds:
    - Use optimized virtual channel redirection instead of generic. This allows the USB device to be ejected through the client machine. See CTX137939 and the USB device redirection article.
    - On the USB device, use Windows to disable write caching and optimize the device for quick removal. See the Microsoft documentation for details. [#628442]
- If the server where you installed the Delivery Controller already has SQL Server Express 2008 R2 (without any service packs) installed, Studio fails during Site creation. (This occurs even if you do not use that database for the Site, logging, or monitoring database.) To prevent this issue, complete one of these tasks before installing the Controller: install a SQL Server Express 2008 R2 service pack, or uninstall SQL Server Express 2008 R2 before installing the Controller. [#632483]
- If a machine used for AppDisk creation does not have a current ListOfDDCs (list of Delivery Controllers), a request from a Controller to create an AppDisk might not be acknowledged and will then fail. The normal auto-update feature will not work for these machines; you must manually update the ListOfDDCs through policy settings or the registry (see the Delivery Controllers article). [#633341]
- When you create a Site, if you choose to install the SQL Server Express database for use as the Site database (which is the default setting), a restart will occur after that database software is installed. That restart will not occur if you choose not to install the SQL Server Express software for use as the Site database. [#634316]
- VDA installation on a Windows Server OS may fail if the machine does not have the latest Windows updates. (Windows Server 2008R2 machine updates should include those in KB2685811; later supported OSs already have those updates.) [#635456]
- If you select Configuration > Licensing in the Studio navigation pane and then click **Log On** in the Actions pane, the Studio snap-in crashes if you do not have permission to use the Citrix License Server. To recover, relaunch Studio. (You can manage the License Server directly from the License Administration Console.) [#640925]
- When you have App-V servers configured in Studio, the Microsoft Management Console (MMC) may crash after you close Studio. [#652949]
- If you are using local storage for both your OS and writeback cache, make sure that the same storage is used for both. If the list of storage for writeback cache includes storage that is not available for OS storage, you may see the error "Unable to find file [Datastore]" during catalog creation. [#637430]
- When creating AppDisks using a Windows 10 machine, the sealing process may not end successfully. As a workaround, delete the AppDisk (using the PowerShell Remove-AppLibAppDisk cmdlet) and then create the AppDisk again. [#633998]
- Upgrading StoreFront using the XenApp and XenDesktop full-product installer may not complete successfully. To prevent this from recurring, restart the StoreFront server to remove any potential file locks, and then run the installer without opening any Citrix administration consoles or PowerShell sessions. [#641242]
- After upgrading from version 7.5 (or from 7.6 if that was an upgrade from 7.5), Studio or the High Level SDK may fail to start. Workaround: Complete a repair install of the Studio MSI ([XDInstallerRoot]\x64\DesktopStudio\DesktopStudio_x64.msi) or High Level SDK MSI ([XDInstallerRoot]\x64\Citrix Desktop Delivery Controller\XDPoshSnapin.msi). [#617897]
- In a large Site, some performance issues in Studio and Director can be caused by out-of-date SQL statistics and fragmented indexes. To avoid this, your database administrator should run a SQL Server maintenance plan during off-peak hours; that plan should include rebuilding indexes and statistics on the Site, Monitoring, and Configuration Logging databases. For details, see the maintenance plan documentation for your SQL Server version. [#641889]

- Logon duration values for a deleted Delivery Group show as n/a in the graph and the row is not shown in the table if the Delivery Group is deleted and that Delivery Group is selected. [#615106]

- Sorting by Usage Duration or Distinct Users in **Trends** > **Capacity Management** > **Hosted Applications Usage** causes an error. To work around this issue, restart Director. [#640508]
- Using the mouse wheel to click inside a Framehawk session may not produce the expected results. [#625408]
- After disconnecting an HDX 3D Pro VDA in a Remote PC Access deployment which uses Intel CPUs with Intel Iris Pro graphics, the console monitor brightness is reduced. This is a third-party issue. The workaround is to restart the Remote PC Access device to restore the monitor brightness. [#633101]
- In a Windows 10 (32-bit only) Remote PC Access deployment with an HDX 3D Pro VDA, the Remote PC Access device no longer starts after installing Intel driver version 20.19.15.9999. This is a third-party issue. The workaround is to use drivers from Windows Update. [#637294] **Note**: For Remote PC Access, the VDA is usually configured using the standard VDA option. For more information on configuring the VDA in standard or HDX 3D Pro mode, see the Prepare to install article.
- XenApp and XenDesktop does not continue to install after installing .NET 4.5.2. This issue has been observed on Windows Server 2008 R2. The workaround is to manually install .NET 4.5.2, then retry the install. [633721]
- When you unplug a USB Human Interface Device (HID) such as a touchpad during a Remote PC session which has more than one such device attached to it (excluding the mice and keyboards), and then plug it back in after disconnecting and reconnecting the session, the USB HID remains disabled. To work around this issue, manually enable the HID in Device Manager. [#638766]
- Some graphics corruption may occur when dragging a video across multiple monitors (observed in multi-monitor sessions with three or more monitors) in Thinwire compatibility mode. [#640437]
- If a user shuts down the Surface Pro, when it is powered back on, HDX connections using Remote PC Access may not work. The way to work around this is to reboot the machine. [#634830]
- When establishing a connection to a Surface Pro device with Windows 8.1, the session may appear to be slow for the first minute or so when Secure Boot is enabled. [#634382]
- If you enable Remote PC Access when you install a VDA using the graphical interface full-product installer, additional components (Machine Creation Services and Profile Management) get installed [#637741]. In this release, use the command line only for Remote PC Access deployments and do not change the order of syntax for /components and /remotepc. For example:

```
VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE
"AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet
```

If /remotepc is used before /components, the /remotepc option is ignored. For more information on command line options, see Install using the command line.

You can access a list of issues identified when using this XenApp and XenDesktop release with Windows Server 2016 Tech Preview in the Windows Server 2016 Tech Preview forum (Citrix account logon required).

Other components

Components available separately on the XenApp and XenDesktop download pages have the following known issues.

- 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 the **Local Users and Groups** > **Groups** > **Users** has

write permission for this folder. If not, manually add write permission. [#611487]

- Because Session Recording does not support Framehawk display mode, sessions in Framehawk display mode cannot be recorded and played back correctly. Sessions recorded in that mode might not contain the sessions activities. [#622085]
- You cannot record the Windows 7 desktop sessions correctly when **Legacy Graphics Mode** is enabled by XenDesktop site policy and **Disk-based Caching** is enabled by Citrix Receiver for Windows policy. Those recordings show a black screen. Workaround: **Disable Disk-based Caching** by deploying with GPO to the machines on which you installed Citrix Receiver for Windows. For more information about disabling **Disk-based Caching**, see http://support.citrix.com/article/CTX123169 and http://docs.citrix.com/en-us/receiver/windows/4-4/ica-overview-receiver-config/ica-import-icaclient-template-v2.html. [#618237]
- The rollover setting does not apply to VDI desktop sessions for XenDesktop 7.8, XenDesktop 7.9, and Session Recording Agent. In those cases, each recording file has a maximum size limit of 1GB and activities are not recorded after that limit is reached. [#584890]
- When Machine Creation Services (MCS) or Provisioning Services creates multiple VDAs with configured master image and Microsoft Message Queuing (MSMQ) installed, those VDAs have the same QMId. This might cause various issues, such as:
  - Sessions mighty not be recorded even if the recording agreement is accepted.
  - The session logoff signal might not be received by the Session Recording server, which leads to the session always in Live status. [#528678]

    The workaround to create a unique and persistent QMId for each VDA differs depending on the deploy methods.

    No extra actions are required if Desktop OS VDAs with the Session Recording agent installed will be created with PVS 7.7 or newer in static desktop mode; for example, configured to make all changes persistent with a separate Personal vDisk or local disk of the VDA.

    For Server OS VDAs created by MCS or PVS or dedicated Desktop OS VDAs created by MCS in static desktop mode, for example, configured to make all changes persistent with a separate Personal vDisk or local disk of VDA, use a script (GenQMID.ps1) to modify the QMId at system startup.

    For Desktop OS VDAs created by MCS or PVS and configured to discard all changes when user logs off, use another script (GenRandomQMID.ps1) to modify the QMId at system startup. Modify power management strategy to ensure that enough VDAs are running before users' login attempts.

    To use the script, do the following:

    1. Make sure the execution policy is set to RemoteSigned or Unrestricted, in PowerShell.

       Set-ExecutionPolicy RemoteSigned

    2. Create a scheduled task and set the trigger as At system startup and run with SYSTEM account on the Provisioning Services or MCS master image machine.

    3. Add the command as a startup task.

       powershell.exe -file C:\GenQMID.ps1
       OR
       powershell .exe -file C:\GenRandomQMID.ps1

Summary of the GenQMID.ps1:

1. Generate the QMId based on the hash value of the machine UUID.
2. Stop related services, including CitrixSmAudAgent and MSMQ.
3. Start services that stopped previously to apply QMId's change.

```
<p>function ConvertHexStringToByte($theString)</p>
<p>{<br>
    $bytes = New-Object Byte[] ($theString.Length / 2)</p>
<p>    for ($i = 0; $i -lt $theString.Length; $i += 2) {</p>
<p>        $bytes[$i / 2] = [System.Convert]::ToByte($theString.Substrin
    }</p>
<p>    return $bytes<br>
}<br>
<br>
Try {</p>
<p>    # Get UUID of machine</p>
<p>    $strUUID = (Get-WmiObject -Class Win32_ComputerSystemProduct | Select-Object -Prope
<br>
    # Remove &quot;-&quot;</p>
<p>    $strUUID = $strUUID.ToString().Replace(&quot;-&quot;, &quot;&quot;)<br>
<br>
    # Convert string to bytes</p>
<p>    $UUID = ConvertHexStringToByte($strUUID)<br>
<br>
    # Set UUID as QMId</p>
<p>    $new_QMID = $UUID</p>
<p>}<br>
Catch {</p>
<p>    # IF exception occurred, just use MD5 digest of FQDN as QMID<br>
<br>
    # Get FQDN</p>
<p>    $fqdn = [System.Net.Dns]::GetHostByName(($env:computerName)).HostName<br>
<br>
    # Calculate MD5 hash of FQDN</p>
<p>    $md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider
<br>
    # Set md5 digest as QMID</p>
<p>    $utf8 = new-object -TypeName System.Text.UTF8Encoding</p>
<p>    $new_QMID = $md5.ComputeHash($utf8.GetBytes($fqdn))<br>
}<br>
<br>
# Write new_QMID into registry</p>
<p>Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name &quot;QMId&quot; -Value $n
<br>
# Restart MSMQ to adopt new QMId<br>
<br>
# Get dependent services</p>
<p>$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name</p>
<p>Restart-Service -force MSMQ<br>
<br>
# Start dependent services</p>
<p>if ($depServices -ne $null) {</p>
<p>    foreach ($depService in $depServices) {</p>
```

```
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;$startMode = Get-WmiObject win32_service -filter &amp;quot;NAM
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;if ($startMode.StartMode -eq &amp;quot;Auto&amp;quot;) {</p>
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;Start-Service $depService.Name<
&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;}<br>
&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;}<br>
}</p>
```

Summary of the GenRandomQMID.ps1:

1. Remove current QMId from registry.
2. Add SysPrep = 1 in HKLM\Software\Microsoft\MSMQ\Parameters.
3. Stop related services, including CitrixSmAudAgent and MSMQ.
4. Start services that stopped previously to generate a random QMId.

```
<p># Remove old QMId from registry and set SysPrep flag for MSMQ</p>
<p>Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force</p>
<p>Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name &amp;quot;SysPrep&amp;quot; -Type DWord -Value
<p># Get dependent services</p>
<p>$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name</p>
<p># Restart MSMQ to get a new QMId</p>
<p>Restart-Service -force MSMQ</p>
<p># Start dependent services</p>
<p>if ($depServices -ne $null) {</p>
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp; foreach ($depService in $depServices) {</p>
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp; $startMode = Get-WmiObject win32_service -filter &amp;quot;NAME = '$(
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp; if ($startMode.StartMode -eq &amp;quot;Auto&amp;quot;) {</p>
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp; Start-Service $depService.Name</p>
<p>&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp; }<br>
}</p>
<p>}</p>
```

- When recording a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance. [#524973]
- When you change your XenApp or XenDesktop license type, the change does not take effect immediately for Session Recording. Workaround: Restart the VDA machine. [#532393]
- Limitation for Session Recording to support the Pre-Launched application sessions [#561109]
  - Problem:
    - If the active policy tries to match the application name, the application launched in the pre-launched session will not be matched, which results in the session not being recorded.
    - If the active policy records every application, when the user logs into the Windows Receiver (at the same time the pre-launched session is established) a notification for recording will appear and the empty session and any applications that will be launched in this session later will be recorded.
  - Workaround:
    - Publish the applications in separate Delivery Groups according to their recording policy. Do not use the application

name as the recording condition. This will ensure pre-launch sessions will be recorded. However, notifications will still appear.

Features not in this release

May 31, 2016

Tip: If your most recent experience is with XenApp 6.5 (or earlier XenApp releases), you should also review the architectural, terminology, and element differences described here.

The following features are not currently provided or are no longer supported.

- **Launch touch-optimized desktop** - This setting has been disabled for Windows 10 machines. For more information, see Mobile experience policy settings.
- **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, including legacy client printer name.
  - 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.
- **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.
- **Power and Capacity Management** - In releases earlier than 7.x, the Power and Capacity Management feature could be used to help reduce power consumption and manage server capacity. The Microsoft Configuration Manager is the replacement tool for this function.
- **Flash v1 Redirection** - Clients that do not support second generation Flash Redirection (including Citrix Receiver for Windows earlier than 3.0, Citrix Receiver for Linux earlier than 11.100, and Citrix Online Plug-in 12.1) will fall back to server-side rendering for legacy Flash Redirection features. VDAs included with 7.x releases support second generation Flash Redirection features.
- **Local Text Echo** - This feature was used with earlier Windows application technologies to accelerate the display of input text on user devices on high latency connections. It is not included in 7.x releases due to improvements to the graphics subsystem and HDX SuperCodec.
- **Smart Auditor** - In releases earlier than 7.x, Smart Auditor allowed you to record on-screen activity of a user's session. Beginning with 7.6 Feature Pack 1, this functionality is provided by Session Recording.
- **Single Sign-on** - This feature, which provides password security, is not supported for Windows 8 and Windows Server 2012 environments. 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: http://citrix.com/downloads.
- **Oracle database support** - 7.x releases require a SQL Server database.
- **Health Monitoring and Recovery (HMR)** - In releases earlier than 7.x, HMR could run tests on the servers in a server farm to monitor their state and discover any health risks. In 7.x releases, Director offers a centralized view of system health by presenting monitoring and alerting for the entire infrastructure from within the Director console.
- **Custom ICA files** - Custom ICA files were used to enable direct connection from user devices (with the ICA file) to a specific machine. In 7.x releases, this feature is disabled by default, but can be enabled for normal usage using a local

group or can be used in high-availability mode if the Controller becomes unavailable.

- **Management Pack for System Center Operations Manager (SCOM) 2007** - The management pack, which monitored the activity of farms using SCOM, does not support 7.x releases.
- **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, Delivery Controller auto-update is the replacement feature that 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 by creating a policy. 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 Studio releases earlier than 7.x, this 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 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.
- **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.
- **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.

- **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)

Third party notices

May 31, 2016

This release of XenApp and XenDesktop may include third party software licensed under the terms defined in the following documents:

- XenApp 7.9 and XenDesktop 7.9 Third Party Notices
- FLEXnet Publisher Documentation Supplement: Third Party and Open Source Software used in FlexNet Publisher 11.13.1
- Linux Virtual Desktop Version 1.2 Third Party Notices

System requirements

Aug 03, 2016

In this article:

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 Receivers and plug-ins, and Provisioning Services) are described in their respective documentation.

Important: Review Prepare to install before beginning an installation.

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

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

The disk space values are estimates only, and are in addition to space needed for the product image, operating system, and other software.

If you install all the core components (Controller with SQL Server Express, Studio, Director, StoreFront, and Licensing) on a single server, you need a minimum of 4 GB of RAM to evaluate the product; more is recommended when running an environment for users. Performance will vary depending on your exact configuration, including the number of users, applications, desktops, and other factors.

For globalization information, see CTX119253.

Delivery Controller

Supported operating systems:

- Windows Server 2016 current Technology Preview: Support for this operating system in this release is for evaluation only and not for production use
- 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 is also supported).
- Windows PowerShell 2.0 (included with Windows Server 2008 R2) or 3.0 (included with Windows Server 2016 TechnologyPreview, Windows Server 2012 R2 and Windows Server 2012).
- Visual C++ 2008 SP1 Redistributable package.
- Disk space: 100 MB.

  The use of optional features increases disk space requirements. For example, the amount of space 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 any instance, Citrix suggests providing several GBs of additional space.

Databases

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

- SQL Server 2016, Express, Standard, and Enterprise Editions.
- SQL Server 2014 through SP2, Express, Standard, and Enterprise Editions.
- SQL Server 2012 through SP3, Express, Standard, and Enterprise Editions. By default, SQL Server 2012 SP2 Express is installed when installing the Controller, if an existing supported SQL Server installation is not detected.
- SQL Server 2008 R2 SP2 and SP3, Express, Standard, Enterprise, and Datacenter Editions.

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

- SQL Server Clustered Instances
- SQL Server Mirroring
- SQL Server 2012 AlwaysOn Availability Groups

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

For more information, see the Databases article and CTX114501.

Citrix Studio

Supported operating systems:

- Windows 10, Professional, Enterprise, and Educational Editions
- Windows 8.1, Professional and Enterprise Editions
- Windows 8, Professional and Enterprise Editions

- Windows 7 Professional, Enterprise, and Ultimate Editions
- Windows Server 2016 current Technology Preview: Support for this operating system in this release is for evaluation only and not for production use
- 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:

- Disk space: 75 MB
- Microsoft .NET Framework 4.5.2 (4.6 is also supported)
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 and Windows 7 only)
- Microsoft Management Console 3.0 (included with all supported operating systems)
- Windows PowerShell 2.0 (included with Windows 7 and Windows Server 2008 R2) or 3.0 (included with Windows 10, Windows 8.1, Windows 8, Windows Server 2016 Technology Preview, Windows Server 2012 R2, and Windows Server 2012)

Citrix Director

Supported operating systems:

- Windows Server 2016 current Technology Preview: Support for this operating system in this release is for evaluation only and not for production use
- 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:

- Disk space: 140 MB.
- Microsoft .NET Framework 4.5.2 (4.6 is 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 theStatic Content role service installed. If these are not already installed, you are prompted for the WindowsServer installation media, then they are installed for you.

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, but Microsoft supports (and Citrix recommends using) version 11. 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.
- Microsoft Edge.

- Firefox ESR (Extended Support Release).
- Chrome.

The recommended screen resolution for viewing Director is 1366 × 1024.

Virtual Delivery Agent (VDA) for Desktop OS

Supported operating systems:

- Window 10, Professional, Enterprise, and Educational Editions. The following features are not supported on Windows 10: GPU acceleration for a VDA configured in standard mode, Desktop composition redirection, Legacy graphics mode, Secure boot (supported for Remote PC Access only), Publishing universal Windows apps using VM hosted apps.
- Windows 8.1, Professional and Enterprise Editions
- Windows 8, Professional and Enterprise Editions
- Windows 7 SP1, Professional, Enterprise, and Ultimate Editions

To use the Server VDI feature, you can use the command line interface to install a VDA for Windows Desktop OS on asupported server operating system; see the Server VDI article for guidance.

- Windows Server 2016 current Technology Preview: Support for this operating system in this release is for evaluation only and not for production use
- 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 is also supported)
- Microsoft .NET Framework 3.5.1 (Windows 7 only)
- Microsoft Visual C++ 2008 SP1, 2010 SP1, and 2013 Runtimes (32-bit and 64-bit)

Remote PC Access uses this VDA, which you install on physical office PCs.

This Virtual Delivery Agent (VDA) supports Secure Boot for XenDesktop Remote PC Access on Windows 10 and 8.1.

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.

During VDA installation, you can choose to install the HDX 3D Pro version of the VDA for Windows Desktop OS. That version 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.

You cannot install a current version of the VDA on a machine running Windows XP or Windows Vista; however, you can install an earlier Virtual Desktop Agent version on those operating systems if needed. See CTX140941 for details. The

Remote PC Access version in this release is not supported on Windows Vista operating systems.

Virtual Delivery Agent (VDA) for Server OS

Supported operating systems:

- Windows Server 2016 current Technology Preview: Support for this operating system in this release is for evaluation only and not for production use
- 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 is also supported)
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only)
- Microsoft Visual C++ 2008 SP1, 2010 SP1, and 2013 Runtimes (32-bit and 64-bit)

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

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that the Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features 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 2012 R2, Windows Server 2012, and Windows Server 2008 R2 editions, the Media Foundation feature is installed through the Server Manager (for Windows Server 2012 R2 and Windows Server 2012: 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.

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 and VMware hosts. See the feature documentation for details.

CTX131239 contains additional hypervisor version support information.

Supported host platforms:

XenServer

- XenServer 6.5 and SP1
- XenServer 6.2 SP1 plus hotfixes (you must apply SP1 to enable application of future hotfixes)
- XenServer 6.1

VMware vSphere. No support is provided for vSphere vCenter Linked Mode operation.

- VMware vSphere 6.0 and Updates 1 and 2
- VMware vSphere 5.5 and Updates 1 through 3
- VMware vSphere 5.1 Updates 2 and 3
- VMware vSphere 5.0 Updates 2 and 3
- VMware vCenter 5.5 / 6 appliance

System Center Virtual Machine Manager. Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.

- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5. Several XenApp and XenDesktop features are not available when using this platform; see CTX202032 for details. For more information on the use of the product with Acropolis, see https://portal.nutanix.com/#/page/docs.

Supported cloud environments:

Amazon Web Services (AWS)

- You can provision applications and desktops on supported Windows server operating systems.
- SQL Server 2012 Enterprise is not available on AWS.
- AWS does not offer desktop operating system instances.
- The Amazon Relational Database Service (RDS) is not supported.
- See Citrix XenDesktop on AWS for additional information.

Citrix 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

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

Active Directory functional levels

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

- 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 Receiver for Windows and Citrix Receiver for Linux 13.

Echo cancellation is supported on Citrix Receiver for Windows.

See the specific HDX feature support and requirements below.

The Windows user device or thin client must support or contain:

- DirectX 9
- Pixel Shader 2.0 (supported in hardware)
- 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.

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and realtime Windows Media multimedia transcoding: Citrix Receiver for Windows, Citrix Receiver for iOS, and Citrix Receiver 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 http://developer.nvidia.com/cuda/cuda-gpus.

The following clients and Adobe Flash Players are supported:

- Citrix Receiver 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 Receiver 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.
- 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.

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. GPU Passthrough is also available with VMware vSphere and VMware ESX, where it is referred to as virtual Direct Graphics Acceleration (vDGA).
- vGPU is available with Citrix XenServer and VMware vSphere; see www.citrix.com/go/vGPU (Citrix My Account credentials required).

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 optimized GPU frame buffer access 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.
- For optimized GPU frame buffer access using the Intel Media SDK, HDX 3D Pro can be used with supported Intel hardware platforms and Intel Iris Pro graphics. Supported Intel processors include 5th Generation Intel Core Processors and 6th Generation Intel Core i5 Processors.
- For vGPU using XenServer, HDX 3D Pro requirements include NVIDIA GRID K1 and K2 cards (see NVIDIA GRID).

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 Receiver must be installed.

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

Supported clients: Citrix Receiver for Windows, Citrix Receiver for Mac, and Citrix Receiver 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

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 encodingcapable reduces client-side CPU usage.
- Webcam drivers, obtained from the camera manufacturer if possible.

Session Recording

This section documents the system requirements for the:

Session Recording administration components

Session Recording Agent

Session Recording Player

The Session Recording administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) can be installed on a single server or on different servers.

Session Recording Database

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Supported Microsoft SQL Server versions:

- Microsoft SQL Server 2014 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2012 SP2 Enterprise and Express editions
- Microsoft SQL Server 2008 R2 SP3 Enterprise and Express editions

Requirement: .NET Framework Version 3.5 SP1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.

Session Recording Server

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

You must install prerequisites before installing the Session Recording Server. From the Server Manager, add the IIS role and select the following options:

- Application Development > ASP.NET 4.5 on Server 2012 and Server 2012 R2, ASP.NET on Server 2008 R2. Other components are automatically selected; click **Add** to accept the required roles.
- Security > Windows Authentication
- Management Tools > IIS 6 Management Compatibility: IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools, IIS 6 Management Console

Other requirements:

- .NET Framework Version 3.5 SP1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.
- 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.

Session Recording Policy Console

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Requirement: .NET Framework Version 3.5 SP 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

Requirements:

- XenApp 7.8 or XenDesktop 7.8 with Platinum license
- .NET Framework Version 4.5.2 or 4.6
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled

Supported operating systems:

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

Requirement: .NET Framework Version 3.5 SP1 (Windows 7 only), 4.5.2 or 4.6.

For optimal results, install Session Recording Player on a workstation with:

- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- 1GB 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 specification.

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 2012 R2 and 2012

- Windows Server 2008 R2 SP1
- Windows Server 2008 32-bit

Requirement: Microsoft Visual C++ 2013 Runtime

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 the Provision printers article.

Other

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.Citrix recommends installing or upgrading to the component software versions provided on the installation media for this release.

- StoreFront requires 2 GB of memory. See the StoreFront documentation for system requirements. StoreFront 2.6 is the minimum supported version with this release.
- When using Provisioning Services with this release, the minimum supported Provisioning Services version is 7.0.
- The Citrix License Server requires 40 MB of disk space. See the licensing documentation for system requirements. Only Citrix License Server for Windows is supported. The minimum supported version is 11.13.1.

The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the Site Configuration database. For more information, see the Microsoft documentation.

Multiple network interface cards are supported.

By default, the Citrix Receiver for Windows is installed when you install a VDA. For more information, see the Citrix Receiver for Windows documentation.

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

See the Local App Access article for supported browser information for Local App Access.

Client folder redirection - Supported operating systems:

- Server: Windows Server 2008 R2 SP1, Windows Server 2012, and Windows Server 2012 R2
- Client (with latest Citrix Receiver 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.

Technical overview

Jul 19, 2016

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 provide or restrict 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.

FMA key components

A typical XenApp or XenDesktop environment consists of a few key technology components, which interact when users connect to applications and desktops, and log data about Site activity.

Citrix Receiver: A software client that is installed on the user device, supplies the connection to the virtual machine via TCP port 80 or 443, and communicates with StoreFront using the StoreFront Service API.

Citrix StoreFront: The interface that authenticates users, manages applications and desktops, and hosts the application store. StoreFront communicates with the Delivery Controller using XML.

Delivery Controller: The central management component of a XenApp or XenDesktop Site that consists of services that manage resources, applications, and desktops; and optimize and balance the loads of user connections.

Virtual Delivery Agent (VDA): An agent that is installed on machines running Windows server or Windows desktop operating systems that allows these machines and the resources they host to be made available to users. The VDA-installed machines running Windows server OS allow the machine to host multiple connections for multiple users and are connected to users on one of the following ports:

- TCP port 80 or port 443 if TLS is enabled
- TCP port 2598, if Citrix Gateway Protocol (CGP) is enabled, which enables session reliability
- TCP port 1494 if CGP is disabled or if the user is connecting with a legacy client

Broker Service: A Delivery Controller service that tracks which users are logged in and where, what session resources the users have, and if users need to reconnect to existing applications. The Broker Service executes PowerShell and communicates with the Broker agent over TCP port 80. It does not have the option to use TCP port 443.

Broker agent: An agent that hosts multiple plugins and collects real-time data. The Broker agent is located on the VDA and is connected to the Controller by TCP port 80. It does not have the option to use TCP port 443.

Monitor Service: A Delivery Controller component that collects historical data and puts it in the Site database by default. The Monitor Service communicates on TCP port 80 or 443.

ICA File/Stack: Bundled user information that is required to connect to the VDA.

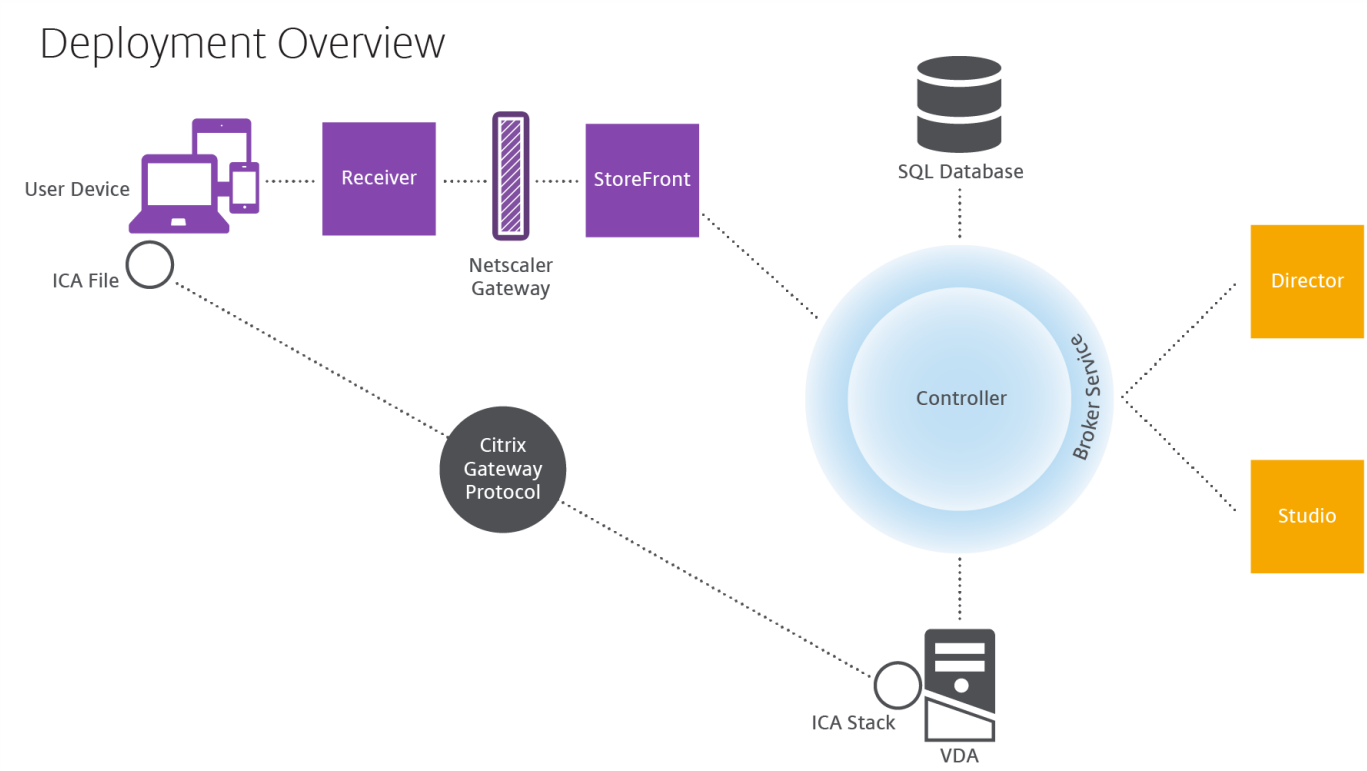
Site Database: A Microsoft SQL Server database that stores data for the Delivery Controller, such as Site policies, Machine Catalogs, and Delivery Groups.

NetScaler Gateway: A data-access solution that provides secure access inside or outside the LAN's firewall with additional credentials.

Citrix Director: A web-based tool that allows administrators and help desk personnel to access real-time data from the broker agent, historical data from the Site database, and HDX data from NetScaler for troubleshooting and support. Director communicates with the Controller on TCP port 80 or 443.

Citrix Studio: A management console that allows administrators to configure and manage Sites, and gives access to real-time data from the broker agent. Studio communicates with the Controller on TCP port 80.

XenApp and XenDesktop Sites are 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 XenApp or XenDesktop Site consists of VDA-installed servers and desktop machines, and the Delivery Controller, which manages access.



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

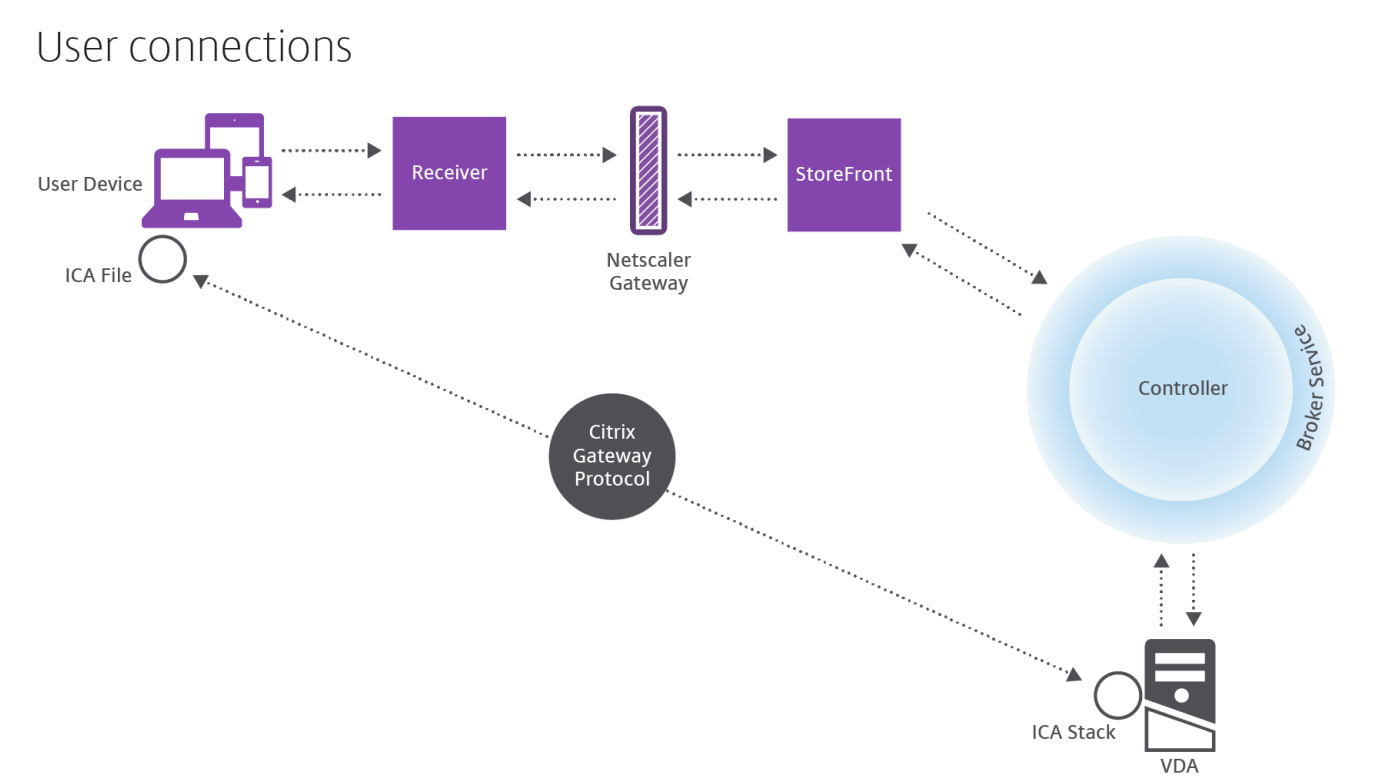
The Controller is made up of independent Windows services that manage resources, applications, and desktops, and optimize and balance user connections. Each Site has one or more Controllers, and because sessions are dependent on latency, bandwidth, and network reliability, all Controllers ideally should 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, which obtains their profiles and available resources based on the policies set for them.

To start a XenApp or XenDesktop session, the user connects either via Citrix Receiver, which is installed on the user's device, or via Citrix Receiver for Web (RFW).

Within Citrix Receiver, 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 what resources are needed by communicating with a Broker Service. It is recommended for administrators to put a SSL certificate on StoreFront to encrypt the credentials coming from Receiver.



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

Once the credentials are verified, the information about available apps 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, which 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 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 all the way to Citrix Receiver. Citrix Receiver bundles up all the information that has been generated in the session to create an Independent Computing Architecture (ICA) file on the user's device if Citrix Receiver is installed locally or on Citrix RFW if accessed through the web. As long as the Site was properly set up, the credentials remain encrypted throughout this process.

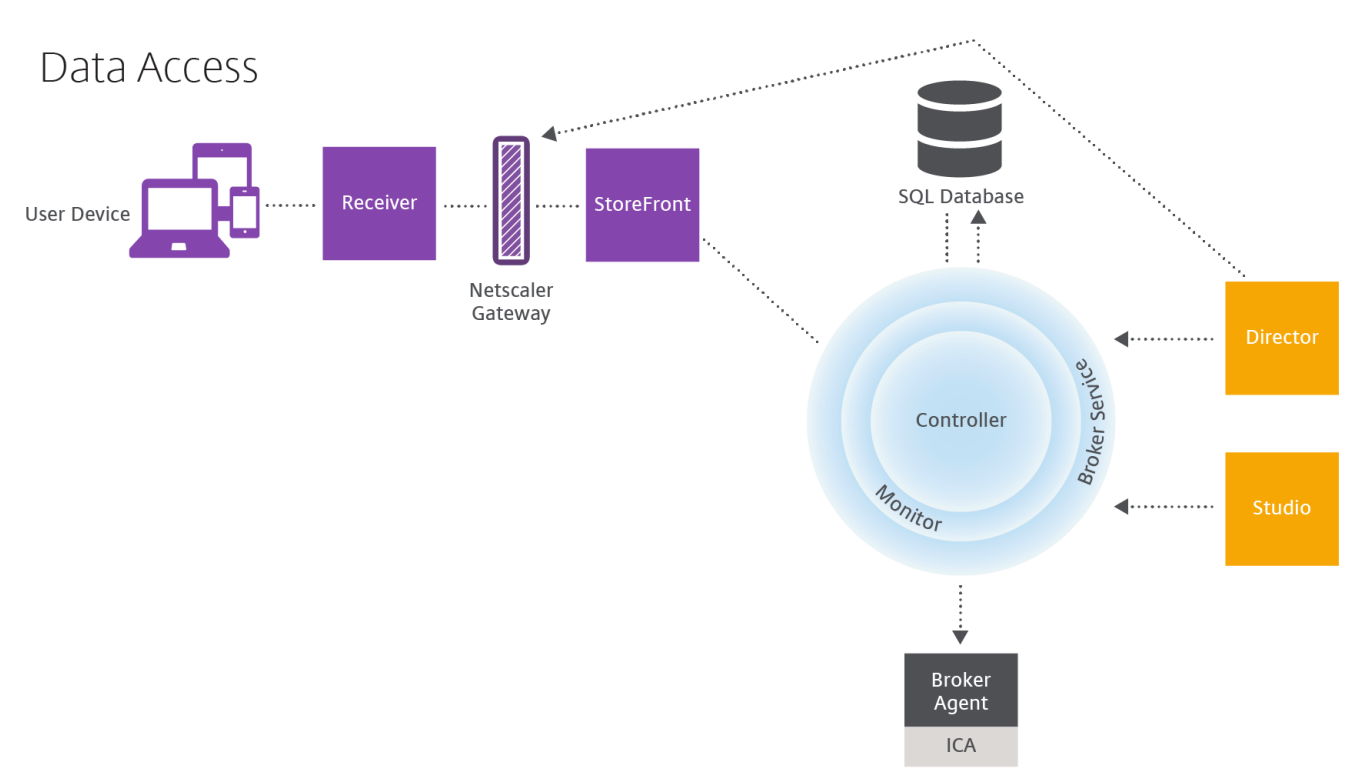
The ICA file is copied to the user's device and establishes a direct connection between the device and the ICA stack running on the VDA. This connection bypasses the management infrastructure: Citrix Receiver, StoreFront, and Controller.

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 Studio.

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

Every XenApp or XenDesktop session produces data that IT can access through Studio or Director. Studio allows administrators to access real-time data from the Broker Agent to better manage sites. Director has access to the same real-time data plus historical data stored in the Monitoring database as well as HDX data from NetScaler Gateway for help-desk support and troubleshooting purposes.



Within the Controller, the Broker Service reports session data for every session on the virtual 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 can communicate only with the Broker Service; therefore, it has access only to real-time data. Director communicates with the Broker Service (through a plugin in the Broker Agent) to access the Site database.

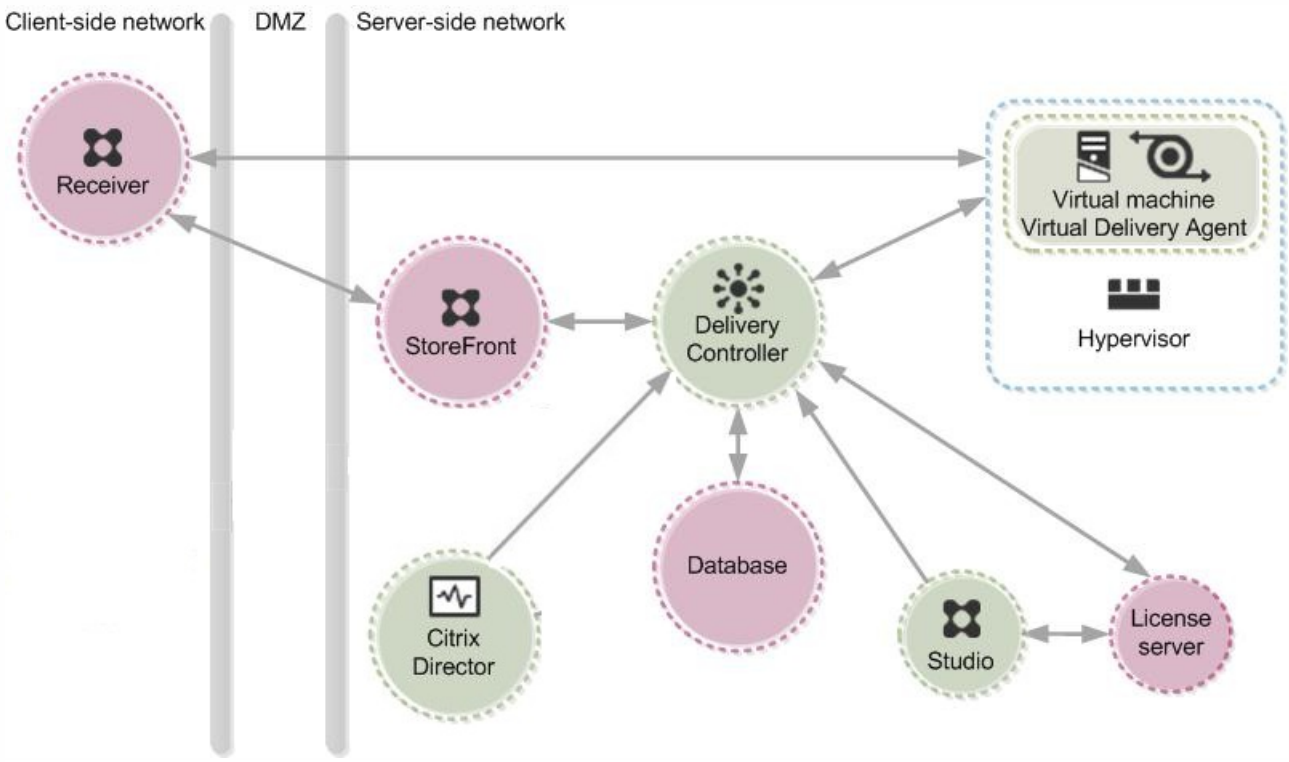
Director can also access NetScaler Gateway to get information on the HDX data.

- Concepts and components
- Delivery methods

Concepts and components

May 31, 2016

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



The components in this illustration are:

- **Delivery Controller:** The Delivery Controller is the central management component of any 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, install the Controller on more than one server.) If your deployment includes virtual machines hosted on a hypervisor or cloud service, the Controller services communicate with the hypervisor 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.
  Each service's data is stored in the Site database.

  The Controller manages the state of the 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 all 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.
- **Virtual Delivery Agent (VDA):** The VDA is installed on each physical or virtual machine in your Site that you want to make available to users. It enables the machine to register with the Controller, which in turn allows the machine and the resources it is hosting to be made available to users. VDAs establish and manage the connection between the machine

and the user device, 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 included in the VDA.
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.

- **Citrix StoreFront:** StoreFront authenticates users to Sites hosting resources and manages stores of desktops and applications that users access. It hosts your enterprise application store, which lets you give users self-service access to desktops and applications you make available to them. It also keeps track of users' application subscriptions, shortcut names, and other data to ensure they 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'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 deployment, eliminating the need for separate management consoles for managing delivery of applications and desktops. Studio provides various wizards to guide you through the process of setting up your environment, 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.

- **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 shows session and Site information from:

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

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

- **Citrix License Server:** The License Server manages your 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:** The hypervisor hosts the virtual machines in your Site. These can be the virtual machines you use to host applications and desktops as well as virtual machines 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. Citrix XenServer hypervisor is included with XenApp and XenDesktop; you can use other supported hypervisors, such as Microsoft Hyper-V or VMware vSphere.

  Although many implementations of XenApp and XenDesktop require a hypervisor, you don't need one to provide Remote

PC Access or when you are using Provisioning Services (included with some editions of XenApp and XenDesktop) instead of MCS to provision virtual machine.

These additional components, not shown in the illustration above, may also be included in typical XenApp or XenDesktop deployments:

- **Provisioning Services:** Provisioning Services is an optional component of XenApp and XenDesktop available with some editions. It provides an alternative to MCS for provisioning virtual machines. Whereas MCS creates copies of a master image, Provisioning Services streams the master image to user device. Provisioning Services doesn't require a hypervisor to do this, so you can use it to host physical machines. When Provisioning Services is included in a Site, it communicates with the Controller to provide users with resources.
- **NetScaler Gateway:** When users connect from outside the corporate firewall, this release can use Citrix NetScaler Gateway (formerly Access Gateway) technology to secure these connections with TLS. 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.
- **Citrix CloudBridge:** In deployments where virtual desktops are delivered to users at remote locations such as branch offices, Citrix CloudBridge (formerly Citrix Branch Repeater or WANScaler) technology can be employed to optimize performance. Repeaters accelerate performance across wide-area networks, so with Repeaters in the network, users in the branch office experience LAN-like performance over the WAN. CloudBridge can prioritize different parts of the user experience so that, for example, the user experience does not degrade in the branch location when a large file or print job is sent over the network. HDX WAN Optimization with CloudBridge provides tokenized compression and data deduplication, dramatically reducing bandwidth requirements and improving performance. For more information, see the Citrix CloudBridge documentation.

Setting up and assigning resources: Machine Catalogs and Delivery Groups

You set up the resources you want to provide to users with Machine Catalogs, but you designate which users have access to these resources with Delivery Groups.

Machine Catalogs

Machine Catalogs are collections of virtual or physical machines that you manage as a single entity. These machines, and the application or virtual desktops on them, are the resources you want to provide to your users. All the machines in a machine catalog have the same operating system and the same VDA installed. They also have the same applications or virtual desktops available on them. Typically, you create a master image and use it to create identical virtual machines in the catalog.When you create a machine catalog, you specify the type of machine and provisioning method for the machines in that catalog.

- **Server OS machines**: Virtual or physical machines based on a server operating system used for delivering XenApp published apps, also known as server-based hosted applications, and XenApp published desktops, also 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 (desktops running desktop operating systems that can be fully personalized, depending on the options you

choose), and VM-hosted apps (applications from desktop operating systems) and hosted physical desktops. Only one user at a time can connect each of these desktops.

- **Remote PC Access**: User devices that are included on a whitelist, enabling users to access resources on their office PCs remotely, from any device running Citrix Receiver. Remote PC Access enables you to manage access to office PCs through your XenDesktop deployment.

Provisioning methods

- **Machine Creation Services (MCS):** A collection of services that create virtual servers and desktops from a master image on demand, optimizing storage utilization and providing a virtual machine to users every time they log on. MCS is fully integrated and administered in Citrix Studio.
- **Provisioning Services:** Enables computers to be provisioned and reprovisioned in real-time from a single shared-disk image. Provisioning Services manages target devices as a device collection. The desktop and applications are delivered from a Provisioning Services vDisk that is imaged from a master target device, which enables you to leverage the processing power of physical hardware or virtual machines. Provisioning Services is managed through its own console.
- **Existing images:** Applies to desktops and applications that you have already migrated to virtual machines in the data center. You must manage target devices on an individual basis or collectively using third-party electronic software distribution (ESD) tools.

Delivery Groups

Delivery Groups are collections of users given access to a common group of resources. Delivery Groups contain machines from your Machine Catalogs, and Active Directory users who have access to your Site. Often it makes sense to assign users to your Delivery Groups by their Active Directory group because both Active Directory groups and Delivery Groups are ways of grouping together users with similar requirements.Each Delivery Group can contain machines from more than one Machine Catalog, and each catalog can contribute machines to more than one Delivery Group, but each individual machine can only belong to one Delivery Group at a time. You can set up a Delivery Group to deliver applications, desktops, or both.You define which resources users in the Delivery Group can access. For example, if you want to deliver different applications to different users, one way to do this is to install all the applications you want to deliver on the master image for one Machine Catalog and create enough machines in that catalog to distribute among several Delivery Groups. Then you configure each Delivery Group to deliver a different subset of the applications installed on the machines.

XenApp and XenDesktop 7.x differences from XenApp 6.5 and previous versions

If you are familiar with XenApp 6.5 and previous versions of XenApp, it may be helpful to think of 7.x versions of XenApp and XenDesktop in terms of how they differ from those earlier versions.

> **NOTE:** Throughout this section, 7.x refers to XenApp versions 7.5 or later, and XenDesktop versions 7 or later.

Although they are not exact equivalents, the following table helps map functional elements from XenApp 6.5 and previous versions to XenApp 7.x and XenDesktop 7.x:

Instead of this in XenApp 6.5 and before:	Think of this in XenApp and XenDesktop 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
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

XenApp 7.x and XenDesktop 7.x 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 and Delivery Groups to manage machines, load balancing, and hosted applications or desktops. You can also use application folders.

- **Virtual Delivery Agents (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.
- **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 functionality enable you to help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of a WAN.
- **Citrix Studio and Citrix 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. 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.
- **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 less 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 systemwide IT issues.

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 before:	Use this in XenApp and XenDesktop 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. See Configure session prelaunch and session linger.

Support for unauthenticated (anonymous) users provided by granting rights to anonymous user when setting the properties of published applications	Support for unauthenticated (anonymous) users provided by configuring this option when setting user properties of a Delivery Group. See Users.
Local host cache permits a worker servers to function even when a connection to the data store is not available	Connection leasing enables users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available. The connection leasing feature supplements the SQL Server high availability best practices. See Connection leasing.
Application streaming	App-V delivers streamed applications, managed using Studio.
Web Interface	Citrix recommends you transition to StoreFront.
SmartAuditor	Use Session Recording. You can also use configuration logging to log all session activities from an administrative perspective.

Active Directory

Feb 24, 2016

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 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 the Delivery Controllers article and CTX118976.

Tip: Do not change the computer name or the domain membership of a Controller after the Site is configured.

Note: 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. Refer to Microsoft documentation for more information 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. Be sure to 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.

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\VirtualDesktopAgent\ListOfSIDs
  - 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

Jul 07, 2016

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 will continue to function until a user either logs off or disconnects. New connections cannot be established if the database server is unavailable, except in certain cases when connection leasing is configured.

Citrix recommends that you back up the databases regularly so that you can restore from the backup if the database server fails. The backup strategy for each database may differ. For instructions, see CTX135207.

If your Site contains more than one zone, the Site database should always be 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** - 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 http://msdn.microsoft.com/en-us/library/hh510230.
- **SQL Server database mirroring** - Mirroring the database ensures that, should you lose the active database server, an automatic failover process happens in a matter of seconds, so that users are generally unaffected. This method is more expensive than other solutions because full SQL Server licenses are required on each database server; you cannot use SQL Server Express edition in a mirrored environment.
- **SQL clustering** - The Microsoft SQL clustering technology can be used to automatically allow one server to take over the tasks and responsibilities of another server that has failed. However, setting up this solution is more complicated, and the automatic failover process is typically slower than alternatives such as SQL mirroring.
- **Using the hypervisor's high availability features** - With this method, you deploy the database as a virtual machine and use your hypervisor's high availability features. This solution is less expensive than mirroring because it uses your existing hypervisor software and you can also use SQL Server Express edition. However, the automatic failover process is slower, as it can take time for a new machine to start for the database, which may interrupt the service to users.

Note: Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

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. For

more information, see the *Connection leasing* article.

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. This feature should be used 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.

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.

This installation uses the default Windows service accounts and permissions. Refer to 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. Refer to Microsoft documentation for details about hiding an instance of SQL Server Database Engine.

Most production deployments, and any deployment that uses Microsoft high availability features, should use supported non-Express editions of SQL Server installed on machines other than the server where the first Controller is installed. The System requirements article lists the supported SQL Server versions. The databases can reside on one or more machines.

Make sure 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* below. 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 a database later, after you create the Site; see *Change database locations* below.

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.

Tip: 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.

If you have the required database privileges, select the "Create and set up databases from Studio" option on the **Databases** page of the Site creation wizard, and then provide the names and addresses of the principal databases.

If a database exists at an address you specify, it must be empty. If databases don't exist at a specified address, you are informed that a database cannot be found, and then asked if you want the database to be created for you. When you confirm that action, Studio automatically creates the databases, if needed, and then applies the initialization scripts for the principal and replica databases.

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 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 should 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 will be 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, you'll see an error message.

Permissions required to set up databases

You must be a local administrator and a domain user to create and initialize the databases (or change the database location). You must also have certain SQL Server permissions. The following permissions can be explicitly configured or acquired by Active Directory group membership. If your Studio user credentials do not include these permissions, you are prompted for SQL Server user credentials.

Operation	Purpose	Server role	Database role
Create a database	Create a suitable empty database	dbcreator	
Create a schema	Create all service-specific schemas and add the first Controller to the Site	securityadmin *	db_owner
Add a Controller	Add a Controller (other than the first) to the Site	securityadmin *	db_owner
Add a Controller (mirror server)	Add a Controller login to the database server currently in the mirror role of a mirrored database	securityadmin *	
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 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:

- 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 databases. 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. Make sure 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 will create 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.

Delivery methods

Feb 24, 2016

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.

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

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.

This can extend the life of older machines, keep software up to date, and minimize downtime during upgrades.

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.

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

Many design firms and manufacturing companies rely heavily on professional 3-D 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 ad hoc methods.

XenDesktop's hosted physical desktop delivery method provides a single desktop image to workstations and blade servers without the need of hypervisors to run graphic-intensive 3-D 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 workstation to another.

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 XenApp 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 XenApp hosted desktops, users are restricted from installing applications, changing system settings, and restarting the server.

XenApp published apps and desktops

Sep 09, 2015

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

- 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 Machine 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.

VM hosted apps

Sep 09, 2015

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.

  Applications running on older operating systems such as Windows XP or Windows Vista, and older architectures, such as 32-bit or 16-bit. By isolating each application on its own virtual machine, if one machine fails, it does not impact other users.

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.
- 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 machine 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.

VDI desktops

Sep 09, 2015

Use Desktop OS machines to deliver VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system.

VDI desktops require more resources than XenApp published desktops, but do not require that applications installed on them support server-based operating systems. In additional, depending on the type of VDI desktop you choose, these desktop can be assigned to individual users and allow these users a high degree of personalization.

When you create a Machine Catalog for VDI desktops, you create one of these types of desktops:

- Random non-persistent desktops, also known as pooled VDI desktops. Each time users logs on to use one of these desktops, they connect to a dynamically selected desktop in a pool of desktops based on a single master image. All changes to the desktop are lost when the machine reboots.
- Static non-persistent desktop. The first time a user logs on the use one off these desktops, the user is assigned a desktop from a pool of desktops based on a single master image. After the first use, each time a user logs in to use one of these desktop, the user connects to the same desktop that user was assigned on first use. All changes to the desktop are lost when the machine reboots.
- Static persistent, also known as VDI with Personal vDisk. Unlike other types of VDI desktops, these desktops can be fully personalized by users. The first time a user logs on the use one off these desktops, the user is assigned a desktop from a pool of desktops based on a single master image. After the first use, each time a user logs in to use one of these desktop, the user connects to the same desktop that user was assigned on first use. Changes to the desktop are retained when the machine reboots because they are stored in a Personal vDisk.

To deliver VDI desktops:

1. Create 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. When defining the desktop experience for the machine catalog, decide whether you want users to connect to a new VM each time the log in or connect to the same machine each time they log in and specify how changes to the desktop are retained.
3. Create a Delivery Group to deliver the desktops to users.

See the installation and configuration articles for details.

Install and configure

Jul 08, 2016

Review the referenced articles before starting each deployment step, so that you will be familiar with what you see and specify during the deployment.

Use the following sequence to deploy XenApp or XenDesktop.

Prepare

Review the Prepare to install article, and complete any necessary tasks. That includes:

- Becoming familiar with XenApp and XenDesktop – the article tells you where to find information about concepts, features, differences from earlier releases, system requirements, and databases.
- Setting up your virtualization, hosting, or support environment, if you are using one.
- Setting up machines on which you'll install components.
- Setting up the Active Directory environment.

This article also explains what information you will need to select or specify when you install components and enable features.

If you will be installing Linux VDAs, be sure to review Red Hat Linux VDAs and SUSE Linux VDAs before beginning the installation.

Install core components

Install the Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server, and Citrix StoreFront. You can use a wizard-based graphical interface or a command line interface, which enables scripted installation. Both methods install most prerequisites automatically.

Create a Site

After you install the core components and launch Studio, you are automatically guided to create a Site using the Site creation wizard.

Install one or more Virtual Delivery Agents (VDAs)

Install a VDA on a machine running a Windows operating system, either on a master image you will use to create virtual machines or directly on each machine. You can use a graphical or command interface. Sample scripts are also provided if you want to install VDAs through Active Directory.

For machines with a Linux operating system, follow the instructions for installing a Red Hat Linux VDA or a SUSE Linux VDA.

For a Remote PC Access deployment, install a VDA for Desktop OS on each office PC; for efficiency, use the standalone VDA installer's command line interface and your existing Electronic Software Distribution (ESD) methods.

Install other optional components

If you plan to use the Citrix Universal Print Server, install its server component on your print servers. You can use a graphical or command interface. For more information, see Provision printers.

To allow StoreFront to use authentication options such as SAML assertions, install the Citrix Federated Authentication Service, preferably on a server that does not contain other Citrix components.

Optionally, integrate additional Citrix components into your XenApp or XenDesktop deployment. For example:

- Provisioning Services is an optional component of XenApp and XenDesktop that provisions machines by streaming a master image to target devices. See the Provisioning Services documentation.
- Citrix NetScaler Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data. See the Citrix NetScaler Gateway documentation.
- Citrix CloudBridge is a set of appliances that optimize WAN performance. See the Citrix CloudBridge documentation.

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. If you are using a supported hypervisor or cloud service to provide VMs, you must first create a master image on that host. Then, when you create the catalog, you specify that image, which will be 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 that specifies which users can access machines in a selected Machine 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

Jul 08, 2016

In this article:

General installation guidance

- If you are unfamiliar with the product and its components, review the Technical overview articles. If your current deployment is XenApp 6.x or earlier, the Concepts and components article explains the differences in the 7.x versions of XenApp and XenDesktop.
- When planning your deployment, review the security articles.
- Check the Known issues article for installation issues you might encounter.
- If you are using a supported hypervisor or cloud service to provide virtual machines for applications and desktops, you can configure the first connection to that host when you create a Site, after you install components. However, you can configure the virtualization environment at any time before then. See the information sources listed here.
- If you are using Microsoft System Center Configuration Manager to manage access to manage access to applications and desktops, see this article.
- If a component has a .NET prerequisite, the installer will deploy the required .NET version if it is not present. The .NET installation might require a restart of the machine.
- Review the Databases article to learn about the system databases and how to configure them. During Controller installation, you can choose whether to install Microsoft SQL Server 2012 Express on the same server. You configure most database information when you create a Site, after you install the core components.
- When you install the Citrix License Server, that user account is automatically made a full administrator on the license server. See the Delegated Administration article for details.
- When you create objects before, during, and after installation, it is best practice to specify unique names for each object - for example networks, groups, catalogs, and resources.
- If a component does not install successfully, the process stops with an error message. Components that installed successfully are retained; you do not need to reinstall them.
- Citrix Studio starts automatically after it is installed. When using the graphical interface, you can disable this action on the final page of the wizard.
- You can use the installer included in the product ISO to install core components and Virtual Delivery Agents (VDAs); this is referred to as the full-product installer. To install VDAs, you can use either the full-product installer or the standalone VDA installer, which is available on the product download site. Both installers offer graphical and command line interfaces.
- The product installation media contains sample scripts that install, upgrade, or remove VDAs for groups of machines in Active Directory. You can also apply the scripts to individual machines and use them to manage master images used by Machine Creation Services and Provisioning Services. For details, see the Install VDAs using scripts article.
- You can use the full-product installer to install the server component (UpsServer) of the Universal Print Server on your print servers, using either the graphical or command line interface. The product download site may also contain UpsServer download packages. For more information, see Provision printers.

- You can use the full-product installer to install the Federated Authentication Service.
- Analytics are collected automatically when you install components. Additionally, when you use the full-product installer graphical interface to install a Controller or a VDA, you can indicate whether or not you want to participate in the Citrix Call Home feature. For details on both features, see the Citrix Insight Services article.
- The product ISO no longer includes versions of the Citrix Receiver for Mac and the Citrix Receiver for Linux. You (or your users) can download and install the Citrix Receivers from the Citrix website. Alternatively, you can make those Citrix Receivers available from your StoreFront server (see the Make Citrix Receiver installation files available on the server section in the StoreFront 3.0.x documentation, or the equivalent content in the StoreFront version you are using).

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 either have elevated administrative privileges before starting the installation, or use **Run as administrator**.

Configure your Active Directory domain before beginning an installation.

- The System requirements article lists the supported Active Directory functional levels. The Active Directory article contains additional support information.
- You must have at least one domain controller running Active Directory Domain Services.
- Do not attempt to install any components on a domain controller.
- Do not use a forward slash (/) when you specify Organizational Unit names in Studio.
- See the Microsoft documentation for Active Directory configuration instructions.

Decide where you will install the components, and then prepare the machines and operating systems.

- Review the System requirements article for supported operating systems and versions for the Controller, Studio, Citrix Director, virtualization resources (hosts), and VDAs. Most component prerequisites are installed automatically; exceptions are noted in that article. See the Citrix StoreFront and the Citrix License Server documents for their supported platforms.
- You can install the core components on the same server or on different servers. For example, to manage a smaller deployment remotely, you can install Studio on a different machine than the server where you installed the Controller. To accommodate future expansion, consider installing components on separate servers; for example, install the License Server and Director on different servers.
- You can install both the Delivery Controller and the Virtual Delivery Agent for Windows Server OS on the same server. To do this, 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 Windows Server OS.
- Do not install any components on a 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.
- Be sure that each operating system has the latest updates.
- Be sure that all machines have synchronized system clocks. Synchronization is required by the Kerberos infrastructure that secures communication between the machines.

What to specify when installing core components

The following sections explain what you see and specify during installation. It follows the sequence of the graphical interface wizard; equivalent command line options are also provided. The installation articles provide details about how to launch the wizards and issue commands with options.

Components are installed in C:\Program Files\Citrix by default. You can specify a different location on the **Core Components** page, but it must have execute permissions for network service. (Command line option: /installdir to specify nondefault directory)

Choose or specify whether to install Microsoft SQL Server Express. If you're not familiar with the databases, review the Databases article. (Command line option: /nosql to prevent installation)

When you install Director, Windows Remote Assistance is installed automatically. You can choose whether to enable shadowing in Windows Remote Assistance for use with Director user shadowing, and open TCP port 3389. By default, this is enabled. (Command line option: /no_remote_assistance)

By default, the following ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable this default action and open the ports manually if you use a third-party firewall or no firewall, or if you prefer to do it yourself. For complete port information about this and other Citrix products, see CTX101810. (Command line option: /configure_firewall)

- Controller: TCP 80, 443
- Director: TCP 80, 443
- License Server: TCP 7279, 8082, 8083, 27000
- StoreFront: TCP 80, 443

VDA installation guidance

- The VDA installers offer graphical and command line interfaces.
- Review the System requirements article for supported operating systems and versions for VDAs. Most component prerequisites are installed automatically; exceptions are noted in that article. When you install a VDA for Windows Server OS, Remote Desktop Services role services are automatically installed and enabled, if they are not already installed and enabled.
- If you installing a VDA on a Windows 7 or Windows Server 2008 R2 machine, verify that .NET 3.5.1 is installed before you start the VDA installation. The Restarts section below has addition installation prerequisite considerations.
- 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 make sure that this service is enabled before installing a VDA.
- Profile management is installed automatically during VDA installation. Although you can exclude it if you are using the command line interface, that exclusion will affect monitoring and troubleshooting of VDAs with Director.
- When you install the VDA, a new local user group called Direct Access Users is created automatically. On a VDA for Windows Desktop OS, this group applies only to RDP connections; on a VDA for Windows Server OS, this group applies to ICA and RDP connections.
- For Remote PC Access configurations, install the VDA for Windows Desktop OS on each physical office PC that users will access remotely. Do not enable the optimize feature.
- If you are installing a VDA on a machine running a supported Linux operating system, see Red Hat Linux VDAs or SUSE

Linux VDAs for essential information.

- 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 it must be done! For more information, see the Delivery Controller addresses section below.
- After you install a VDA for Server OS on a Windows Server 2012 R2 system, use the Kerberos Enable Tool (XASsonKerb.exe) to ensure the correct operation of Citrix Kerberos authentication. The tool is located in the Support > Tools > XASsonKerb folder on the installation media; you must have local administrator privileges to use the tool. Run **xassonkerb.exe -install** from a command prompt on the server. If you later apply an update that changes the registry location HKLM\System\CurrentControlSet\Control\LSA\OSConfig, run the command again. To see all available tool options, run the command with the -help parameter.

You can install a VDA using the full-product installer or a standalone installation package. Both offer graphical and command line interfaces.

The full-product installer automatically detects your operating system and allows you to install only the Windows VDA supported on that system: VDA for Windows Server OS or VDA for Windows Desktop OS.

Standalone VDA installation package

The smaller standalone package more easily accommodates deployments using Electronic Software Distribution (ESD) packages that are staged or copied locally, have physical machines, or have remote offices. The standalone package is intended primarily for deployments that use command line (silent) installation; it supports the same command line parameters as the full-product installer. The package also offers a graphical interface that is equivalent to the full-product installer.

> How to use the graphical interface for the standalone VDA installer.
>
> How to use the command line interface for the standalone VDA installer.

There are two self-extracting standalone VDA installer packages: one for installation on supported server OS machines, and another for supported workstation (desktop) OS machines.

By default, files in the package 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. Files extracted to the Temp folder are not automatically deleted, but you can manually delete them (from C:\Windows\Temp\Ctx-*, where * is a random Globally Unique Identifier) after the installation completes. Alternatively, you can use the /extract command with an absolute path.

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 http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

A restart is required at the end of the VDA installation.

If you want to minimize the number of additional restarts needed during the installation sequence:

- 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.

Other prerequisites do not typically require machine restarts, so you can let the installer take care of those for you.

If you do not install prerequisites before beginning the VDA installation, and you specify the /noreboot option for a command line installation, you must manage the restarts. For example, when using automatic prerequisite deployment, the installer will suspend after installing RDS, waiting for a restart; be sure to run the command again after the restart, to continue with the VDA installation.

The latest VDAs are not supported on Windows XP or Windows Vista systems; additionally, some of the features in this and other recent releases cannot be used on those operating systems. Citrix recommends you replace those systems with currently-supported Windows desktop OS versions and then install a VDA from this release. If you must continue to accommodate machines running Windows XP or Windows Vista, you can install an earlier Virtual Desktop Agent version (5.6 FP1 with certain hotfixes). See CTX140941 for details. Keep in mind that:

- You cannot install core components (Controller, Studio, Director, StoreFront, License Server) on a Windows XP or Windows Vista system.
- If you use Windows XP or Windows Vista systems, when you create a Machine Catalog containing those machines, be sure to choose the 5.6 FP1 entry in the "Select the VDA version installed ..." listbox on the Master Image page.
- Remote PC Access is not supported on Windows Vista systems.
- Citrix support for Windows XP ended April 8, 2014 when Microsoft ended its extended support.
- Continuing to use older VDAs can affect feature availability and VDA registration with the Controller; see Mixed environment considerations.

What to specify when installing a VDA

The following sections explain what you specify during installation. It follows the sequence of the graphical interface wizard; equivalent command-line options are also provided. The installation articles provide details about how to launch the wizards or issue commands with options.

Check VDA installation guidance for tasks you may need to complete after VDA installation.

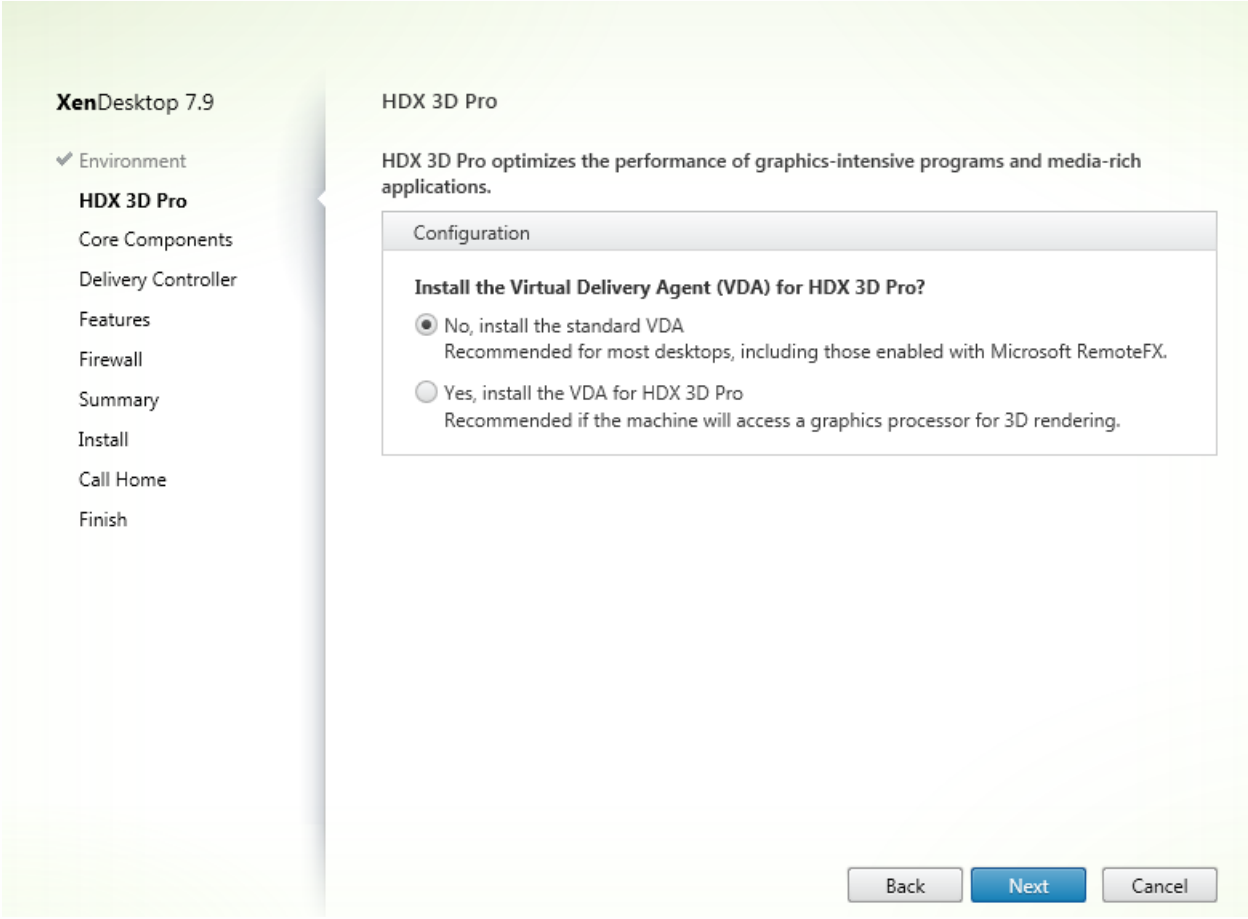
The VDA environment specifies how you will use the VDA:

- The default "master image" option indicates you will use Machine Creation Services (MCS) or Provisioning Services to create virtual machines based on a master image created in a hypervisor or cloud service. You install the VDA on the master image. (Command line option: /masterimage)
- The "Remote PC Access" option indicates you will install the VDA on a physical machine or on a VM that was provisioned without a VDA.

> **Important**
>
> In XenApp and XenDesktop 7.9, use the command line only for Remote PC Access deployments. For more information, see Install using the command line and Known issues [#637741].

When you install a VDA using the graphical interface, this page appears only when installing a VDA on a desktop OS machine (not on a server OS machine). Choose to configure the VDA for standard or HDX 3D Pro mode.

- The standard VDA mode is recommended for most desktops, including those enabled with Microsoft RemoteFX. This mode is configured by default.
- The VDA for HDX 3D Pro mode optimizes the performance of graphics-intensive programs and media-rich applications. It is recommended if the machine will access a graphics processor for 3D rendering. (Command line option valid only on desktop OS machines: /enable_hdx_3d_pro)



Standard VDA	VDA for HDX 3D Pro

• Generally best for virtual desktops without graphics hardware acceleration, and for Remote PC Access.
• Supports GPU acceleration with any GPU, with some application compatibility limitations:
  • On Windows 7, 8, and8.1, 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 limited to
	• Generally best for data center desktops with graphics hardware acceleration, unless more than four monitors are required.
	• Supports GPU acceleration with any GPU, however console blanking, non-standard screen resolutions and true multi-monitor support require NVIDIA GRID or Intel Iris Pro graphics
	• Leverages graphics vendor's driver for broadest application compatibility.

windowed (non full-screen) DirectX 10, 11, 12 applications; DirectX 9 and full-screen applications are software-rendered (WARP). • OpenGL application acceleration in remote sessions if supported by the GPU vendor (currently only NVIDIA). • Uses Citrix WDDM display driver, supporting arbitrary monitor resolutions (up to 4K) and up to 8 monitors. • Desktop Composition Redirection option for broadband access to Windows 7 and 8.x Aero desktops. • Windows desktop composition offloaded to user device (Windows or Mac).	• All 3D APIs (DirectX or OpenGL) that the GPU supports. • Full-screen 3D app support with Intel Iris Pro (Win10 only) and NVIDIA GRID. • Support for custom driver extensions and APIs. For example, CUDA or OpenCL. • Supports up to four monitors.

Remote PC Access and HDX 3D Pro mode

For Remote PC Access, the VDA is usually configured using the standard VDA option. 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), and NVIDIA Quadro and NVIDIA GRID GPUs.

VDAs are installed in C:\Program Files\Citrix by default. You can specify a different location during installation, but it must have execute permissions for network service. (Command line option: /installdir to specify nondefault directory)

By default, Citrix Receiver for Windows is installed with the VDA. You can disable this default action. (Command line option: use "/components vda" to prevent Citrix Receiver installation)

You can specify the addresses (FQDNs) of installed Controllers either when you install the VDA (recommended) or later. Although you are not required to specify Controller addresses when you install a VDA, keep in mind that that a VDA cannot register with a Controller without this information. If VDAs cannot register, users on machines containing those VDAs will be unable to access their applications and desktops. (Command line option: /controllers)

- If you specify Controller FQDNs when you install the VDA, the installer attempts to connect to the specified addresses. If the connection attempt fails, the installer provides informative messages.
- If you choose to specify Controller addresses later, the installer reminds you of that requirement. If you install a VDA without specifying a Controller address, you can either rerun the installer later or use Citrix Group Policy.

If you specify Controller addresses both during VDA installation and in Group Policy, the policy settings override settings provided during installation.

Remember that successful VDA registration also requires that the firewall ports used for communication with the Controller are open.

After you initially specify Controller locations (either when installing the VDA or later), you can use the auto-update feature to update VDAs when additional Controllers are installed.

For more information about how VDAs discover and register with Controllers, see the Delivery Controllers article.

You can enable or disable the following features that are used with VDAs:

- **Optimize performance:** (Default = enabled) When this feature is selected, the optimization tool is used for VDAs running in a VM on a hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. For more information, see CTX125874. Do not enable this option if you will be using Remote PC Access. (Command line option: /optimize)
- **Use Windows Remote Assistance:** (Default = enabled) When this feature is selected, Windows Remote Assistance is used with the user shadowing feature of Director, and Windows automatically opens TCP port 3389 in the firewall, even if you choose to open firewall ports manually. (Command line option: /enable_remote_assistance)
- **Use Real-Time Audio Transport for audio:** Default = enabled) When this feature is selected, UDP is used for audio packets, which can improve audio performance. (Command line option: /enable_real_time_transport)
- **Framehawk:** (Default = enabled) When selected, bidirectional UDP ports 3224-3324 are opened. (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 VDA to 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 more information, see the Framehawk article. (Command line option: /enable_framehawk_port)
- **Install Citrix App-V publishing components:** (Default: enabled) Select this feature if you will use applications from Microsoft App-V packages. For more information, see the App-V article. (Command line option: /no_appv to prevent component installation)
- **Personal vDisk:** (Default = disabled; available only when installing a VDA for Desktop OS on a VM.) When this feature is selected, Personal vDisks can be used with a master image. For more information, see the Personal vDisks articles. (Command line option: /baseimage)

By default, the following ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable this default action and open the ports manually if you use a third-party firewall or no firewall, or if you prefer to do it yourself. For complete port information, see CTX101810. (Command line option: /enable_hdx_ports)

- Controller Communications: TCP 80, 1494, 2598, 8008. For communication between user devices and virtual desktops, configure inbound TCP on ports 1494 and 2598 as port exceptions. For security, Citrix recommends that you do not use these registered ports for anything other than the ICA protocol and the Common Gateway Protocol. For communication between Controllers and virtual desktops, configure inbound port 80 as a port exception.
- Remote Assistance: TCP 3389. Windows opens this port automatically if the Windows Remote Assistance feature is enabled on the previous page, even if you choose to open the ports manually.
- Real Time Audio: UDP 16500-16509.
- Framehawk: UDP 3224-3324.

After you review the information presented and click **Install**, the display shows the progress of the installation. After the installation completes, a machine restart is required before the VDA can be used.

VMware virtualization environments

May 31, 2016

Follow this guidance if you use VMware to provide virtual machines.

Install and configure your hypervisor

Step 1. Install vCenter Server and the appropriate management tools. (No support is provided for vSphere vCenter Linked Mode operation.)

Step 2. Create a VMware user account with the following permissions, at the DataCenter level, at a minimum. This account has permissions to create new VMs and is used to communicate with vCenter.

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
System.Anonymous, System.Read, and System.View	Added automatically.
Task.Create	Tasks > Create task
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
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.CPUCount	Virtual machine > Configuration > Change CPU Count

VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.Resource	Virtual machine > Configuration > Change resource
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Inventory.Register	Virtual machine > Inventory > Register
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DiskRandomAccess	Virtual machine > Provisioning > Allow disk access
VirtualMachine.Provisioning.GetVmFiles	Virtual machine > Provisioning > Allow virtual machine download
VirtualMachine.Provisioning.PutVmFiles	Virtual machine > Provisioning > Allow virtual machine files upload
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
VirtualMachine.Provisioning.MarkAsVM	Virtual machine > Provisioning > Mark as virtual machine

VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Create snapshot vSphere 5.5: Virtual machine > Snapshot management > Create snapshot
VirtualMachine.State.RemoveSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Remove snapshot vSphere 5.5: Virtual machine > Snapshot management > Remove snapshot
VirtualMachine.State.RevertToSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Revert to snapshot vSphere 5.5: Virtual machine > Snapshot management > Revert to snapshot

Step 3. If you want the VMs you create to be tagged, add the following permissions for the user account:

SDK	User Interface
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

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.

Step 4. To create AppDisks, the user account must have the following additional permission:

- SDK: VirtualMachine.Config.EditDevice
- User Interface: Virtual machine > Configuration > Modify Device Settings

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. Follow this procedure:

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the hosts file on that server, located at %SystemRoot%/WINDOWS/system32/Drivers/etc/. This step is required only if the FQDN of the computer running vCenter Server is not already present in the domain name system.
2. Obtain the vCenter certificate using any of the following 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 where it shows the certificate error.
     4. View the certificate and click on 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:
     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 where it shows the certificate error.
     4. View the certificate.
   - 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.
     3. If you are using Windows Server 2008 R2:
        1. Select the Show physical stores check box.
        2. Expand Trusted People.
        3. Select Local Computer.
        4. Click Next, then click Finish.

        If you are using Windows Server 2012 or Windows Server 2012 R2:

        1. Select Trusted People, then click OK.
        2. Click Next, 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.

Use a master VM to provide user desktops and applications. 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.

If you are using Studio to create VMs, rather than selecting an existing Machine Catalog, specify the following information when setting up your hosting infrastructure to create virtual desktops.

1. Select the VMware vSphere host type.
2. Enter the address of the access point for the vCenter SDK.
3. Enter the credentials for the VMware user account you set up earlier that has permissions to create new VMs. Specify the username in the form domain/username.

VMware SSL thumbprint

The VMware SSL thumbprint feature addresses a frequently-reported error when creating a host connection to a VMware vSphere hypervisor. Previously, administrators had to manually create a trust relationship between the Delivery Controllers in the Site and the hypervisor's certificate before creating a connection. The VMware SSL thumbprint feature removes that manual requirement: the untrusted certificate's thumbprint is stored on the Site database so that the hypervisor can be continuously identified as trusted by 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.

Microsoft System Center Virtual Machine Manager virtualization environments

Jul 07, 2016

Follow this guidance if you use Hyper-V with Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

This release supports:

- VMM 2012 - Provides improved management capabilities, letting you manage the entire virtualized datacenter as well as virtual machines. This release now orchestrates cluster host patching as well as integrating with Windows Server Update Services, allowing you to define baselines of patches that each host needs.
- VMM 2012 SP1 - Provides performance improvements for Machine Creation Services (MCS) when using SMB 3.0 on file servers with clustered shared volumes and Storage Area Networks (SANs). These file shares provide low cost caching and reduced IO on the SAN storage improving the performance.
- VMM 2012 R2 - Enables at-scale management of major Windows Server 2012 R2 capabilities, including running VM snapshots, dynamic VHDX resize, and Storage Spaces.

This release supports only Generation 1 virtual machines with VMM 2012 R2. When creating VMs with MCS, Generation 2 VMs do not appear in the selection list for a master VM; they have Secure Boot enabled by default, which prevents the VDA from functioning properly.

- Upgrade from VMM 2012 to VMM 2012 SP1 or VMM 2012 R2
  For VMM and Hyper-V Hosts requirements, see http://technet.microsoft.com/en-us/library/gg610649.aspx. For VMM Console requirements, see http://technet.microsoft.com/en-us/library/gg610640.aspx.

  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)

1. Install and configure a hypervisor.
   1. Install Microsoft Hyper-V server and VMM on your servers. All Delivery Controllers must be in the same forest as the VMM servers.

2. Install the System Center Virtual Machine Manager console on all Controllers.
3. Verify the following account information:
   - The account you use to specify hosts in Studio is a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account only has the delegated administrator role in VMM, the storage data is not listed in Studio during the host creation process.
   - The user account used for Studio integration must also be a member of the administrators local security group on each Hyper-V server to support VM life cycle management (such as VM creation, update, and deletion).

   Note: Installing a Controller on a server running Hyper-V is not supported.
2. Create a master VM.
   1. Install a Virtual Delivery Agent on the master VM, and select the option to optimize the desktop. This improves performance.
   2. Take a snapshot of the master VM to use as a backup.
3. Create virtual desktops. If you are using MCS to create VMs, when creating a Site or a connection,
   1. Select the Microsoft virtualization host type.
   2. Enter the address as the fully qualified domain name of the host server.
   3. Enter the credentials for the administrator account you set up earlier that has permissions to create new VMs.
   4. In 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.

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.

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.
  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 Azure virtualization environments

Jun 16, 2016

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" />
```

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. 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 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://msdn.microsoft.com/en-us/library/azure/dn197896.aspx
- Virtual Machine Pricing: http://azure.microsoft.com/en-us/pricing/details/virtual-machines

Basic tier: VMs prefixed with "Basic" represent the basic disk. They are limited primarily by the Microsoft supported IOPS level of 300. These are not recommended for Desktop OS (VDI) or Server OS RDSH (Remote Desktop Session Host) workloads.

Standard tier: Standard tier VMs appear in four series: A, D, DS, and G.

Series	Appear in Studio as
A	Extra small, small, medium, large, extra large, A5, A6, A7, A8, A9, A10, A11. Medium and large are recommended to test using Desktop OS (VDI) or Server OS (RDSH) workloads, respectively.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. These VMs offer SSD for temporary storage.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. These VMs offer local SSD storage for all disks.
G	Standard_G1 – G5. These VMs are for high performance computing.

When provisioning machines in Azure premium storage, be sure to select a machine size that is supported in the premium storage account.

For US list pricing, the cost of each VM instance type per hour is available at http://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

When working with cloud environments, it is important to understand your actual computing requirements. For proof of concept or other testing activities, it can be tempting to leverage the high-performance VM instance types. It may also be tempting to use the lowest-performing VMs to save on costs. The better goal is to use a VM appropriate for the task. Starting with the best-performing may not get the results you need, and will become very expensive over time - in some cases, within a week. For lower-performing VM instance types with a lower cost, the performance and usability may not be appropriate for the task.

For Desktop OS (VDI) or Server OS (RDSH) workloads, testing results using LoginVSI against its medium workload found that instance types Medium (A2) and Large (A3) offered the best price/performance ratio.

Medium (A2) and Large (A3 or A5) represent the best cost/performance for evaluating workloads. Anything smaller is not recommended. More capable VM series may offer your applications or users the performance and usability they demand; however, it is best to baseline against one of these three instance types to determine if the higher cost of a more capable VM instance type provides true value.

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: http://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.

Microsoft System Center Configuration Manager environments

Jun 16, 2016

Sites that use System Center Configuration Manager (Configuration Manager) 2012 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** – Whether or not your environment includes Citrix Connector, the Remote PC Access Wake on LAN feature requires Configuration Manager. For more information, see below.
- **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 are available to Microsoft System Center Configuration Manager 2012 and 2012 R2 to manage virtual desktops.

Boolean properties displayed in Configuration Manager 2012 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 – 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.

Property	Description
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.
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. For information about the following tasks, see http://support.citrix.com/article/ctx140905.

- 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.

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 Configuration Manager 2012 within the organization, and then deploy the Configuration Manager client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run (or forcing one manually, if required). The access credentials you specify in Studio to configure the connection to Configuration Manager 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.
- For Configuration Manager Wake Proxy and/or magic packet support:
    - Configure Wake on LAN in each PC's BIOS settings.
    - For Configuration Manager Wake Proxy support, enable the option in Configuration Manager. 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 Configuration Manager 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 Configuration Manager Wake Proxy and magic packets, as well as change the packet transmission method.

See the Remote PC Access article for more information.

Nutanix virtualization environments

Jun 07, 2016

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.

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\RegisterPlugin.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.
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.

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.

Install using the graphical interface

Jun 01, 2016

Note: This article applies to installing components on machines with Windows operating systems. For information about VDAs for Linux operating systems, see Red Hat Linux VDAs and SUSE Linux VDAs.

In this article:

Introduction

Important: Before beginning any installation, review the Prepare to install article, which describes the installers and things you should be familiar with before installation. It also guides you through items you will see and specify in the graphical interface wizard. This article describes how to launch the graphical interface in a product installer.

You can use the graphical interface to:

- Install one or more core components: Delivery Controller, Citrix Studio, Citrix Director, License Server, and StoreFront.
- Install a Virtual Delivery Agent (VDA) on a master image or on a virtual or physical machine. You can also customize scripts provided on the media and then use them to install and remove VDAs in Active Directory.
- Customize a previously-installed VDA.
- Install a Universal Print Server server component. The Controller already has the Universal Print Server client functionality; you need only install the UpsServer component on the print servers in your environment. After you install the component, follow the configuration instructions in the Configure printers article.
- Upgrade components; see the Upgrade a deployment article.

Both the full-product installer and the standalone VDA installer have a graphical interface.

Use the full-product installer

You can use the full-product installer to install core components, VDAs, and the Universal Print Server server component.

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. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.
5. Choose whether to install XenApp or XenDesktop.
6. Select the component you want to install:

- If you are just getting started, select **Delivery Controller** in the left column. As the wizard continues, you can choose which components to install on the machine where you are running the installer (Delivery Controller, Studio, Director, License Server, StoreFront).

- If you have already installed some components and want to extend your deployment, click the component you want to install from the right column. This column offers core components and the Universal Print Server.
- To install a VDA, click the available VDA entry in the middle column; the installer knows which one is right for the operating system where you're running the installer.

Follow the wizard. Remember: the Prepare to install article provides guidance about information you see and specify in the wizard. If you are installing a VDA, an automatic restart is enabled by default when the installation completes; the restart is required before the VDA can be used in a Site.

Use the standalone VDA installer

Important: The Prepare to install article provides guidance about information you see and specify during installation, especially about handling restarts and extraction space when using the 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**. Disable User Account Control (UAC).

1. Download the appropriate package from Citrix: **VDAServerSetup.exe** (for server OS machines), or **VDAWorkstationSetup.exe** (for desktop OS machines). For single user, single server OS deployments (for example, delivering Windows Server 2012 to one user for web development), use the VDAWorkstationSetup.exe package. For more information, see the Server VDI article.
2. Right-click the package and choose **Run as administrator**.
3. Follow the wizard. An automatic restart is enabled by default when the installation completes; the restart is required before the VDA can be used in a Site.

Customize a VDA

If you want to customize a VDA that you've already installed:

1. From the Windows feature for removing or changing programs, select Citrix **Virtual Delivery Agent** <*version*>, then right-click and select **Change**.
2. Select **Customize Virtual Delivery Agent Settings**. When the installer launches, you can change the Controller addresses, TCP/IP port to register with the Controller (default = 80), or whether to automatically open Windows Firewall port exceptions.

Install using the command line

Sep 16, 2016

Note: This article applies to installing components on machines with Windows operating systems. For information about VDAs for Linux operating systems, see Red Hat Linux VDAs and SUSE Linux VDAs.

In this article:

Introduction

Important: Before beginning any installation, review the Prepare to install article, which describes the installers and things you should be familiar with before installation. It also guides you through options you can include with a command. This article describes how to launch the command line interface in a product installer.

You can use a command line interface to:

- Install one or more core components: Delivery Controller, Citrix Studio, Citrix Director, License Server, and StoreFront.
- Install a Virtual Delivery Agent (VDA) on a master image or on a virtual or physical machine. You can also customize scripts provided on the media and then use them to install and remove VDAs in Active Directory.
- Customize a previously-installed VDA.
- Install a Universal Print Server, which provisions network session printers. The Controller already has the Universal Print Server functionality; you need only install the Universal Print Server on the print servers in your environment.
- Upgrade components; see the Upgrade a deployment article.

You can also remove components from this version that you previously installed by using the /remove or /removeall options. For details, see the Remove components article.

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.

Both the full-product installer and the standalone VDA installer have a command line interface.

If you use the sample scripts provided to install, upgrade, or remove VDAs machines in Active Directory, you can specify VDA configuration options listed below in the Command line options for installing a VDA section. For information about the sample scripts, see the Install VDAs using scripts article.

Use the full-product installer

You can install core components and VDAs with the full-product installer.

- Download the product package from Citrix. Citrix account credentials are required to access the download site.

- Unzip the file. Optionally, burn a DVD of the ISO file.
- Log on to the server where you are installing the components, using a local administrator account.
- Insert the DVD in the drive or mount the ISO file.
- From the \x64\XenDesktop Setup directory on the media:

    To install core components, run the **XenDesktopServerSetup.exe** command. Use options listed in the Command line options for installing core components section below.

    To install a VDA, run the **XenDesktopVDASetup.exe** command. Use options listed in the Command line options for installing a VDA section below.

Example 1: The following command installs a XenDesktop Controller, Studio, Citrix Licensing, and SQL Server Express on the server. Ports required for component communications will be opened automatically.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver
/configure_firewall
```

Example 2: The following command installs a XenApp Controller, Studio, and SQL Server Express on the server. Ports required for component communication will be opened automatically.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components  controller,desktopstudio
/configure_firewall
```

Example 1: The following command installs a VDA for Windows 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,' and 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
```

Example 2: The following command installs a VDA for Windows Desktop OS and Citrix Receiver to the default location on an office PC that will be used with Remote PC Access. The machine will not be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named 'Contr-East' in the domain 'mydomain,' and will use UDP for audio packets. HDX ports will be opened if the Windows Firewall service is detected.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet  /components vda,plugins /controllers "Contr-
East.mydomain.local" /enable_hdx_ports  /enable_real_time_transport /noreboot
```

Use the standalone VDA installer

Important: The Prepare to install article provides guidance about information you see and specify during installation, especially about handling restarts and extraction space when using the standalone VDA installer.

Citrix account credentials are required to access the download site. You must either have elevated administrative privileges before starting the installation or use **Run as administrator**.

1. Download the appropriate package from Citrix: **VDAServerSetup.exe** (for server OS machines) or **VDAWorkstationSetup.exe** (for desktop OS machines). For single user, single server OS deployments (for example, delivering Windows Server 2012 to one user for web development), use the VDAWorkstationSetup.exe package. For more information, see the Server VDI article.
2. Either extract the files from the package 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 .\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia. Then in a separate command, run the **XenDesktopVdaSetup.exe** command from the directory containing the extracted content (in the example above, CitrixVDAInstallMedia). Use the options listed in the Command line options for installing a VDA section below.

    To just run the downloaded package, run its name: **VDAServerSetup.exe** or **VDAWorkstationSetup.exe**. Use the options listed in the Command line options for installing a VDA section below. (If you are familiar with the full product installer: you run the downloaded standalone package as if it was the XenDesktop VdaSetup.exe command in everything except its name.)

The following installation command is often used for Remote PC Access. It installs a VDA on a physical office PC, without installing Citrix Receiver or Citrix Profile Manager. The machine will not automatically be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named 'Contr-East'. Ports will be opened if the Windows Firewall Service is detected.

```
VDAWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

> **Note**
>
> Excluding Citrix Profile management from the installation (Using the /exclude "Citrix User Profile Manager" option) will affect monitoring and troubleshooting of VDAs with Citrix Director. On the User details and EndPoint pages, the Personalization panel and the Logon Duration panel will fail. On the Dashboard and Trends pages, the Average Logon Duration panel will display data only for machines that have Profile management installed.
>
> Even if you are using a third party user profile management solution, it is recommended that you install and run the Citrix Profile management Service to avoid loss of monitoring and troubleshooting in Citrix Director (enabling the Citrix Profile Management Service is not required).

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 the Command line options for installing a VDA section below.

- /reconfigure - this option is required when customizing a VDA
- /h or /help
- /quiet
- /noreboot

- /controllers
- /portnumber port
- /enable_hdx_ports

Command line options for installing core components

The following table lists the valid options for the **XenDesktopServerSetup.exe** command.

Option	Description
/components component [,component] ...	Comma-separated list of components to install or remove. Valid values are: • CONTROLLER – Controller • DESKTOPSTUDIO – Studio • DESKTOPDIRECTOR – Director • LICENSESERVER - Citrix License Server • STOREFRONT – StoreFront If this option is omitted, all components are installed (or removed, if the /remove option is also specified).
/configure_firewall	Opens all ports in the Windows firewall needed by 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.
/help or /h	Displays command help.
/installdir directory	Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.
/logpath path	Log file location. The specified folder must already 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 will be

	installed.
/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.
/tempdir directory	Directory that holds temporary files during installation. Default = c:\Windows\Temp.
/xenapp	Installs XenApp. If this option is omitted, XenDesktop is installed.

Command line options for installing a VDA

The following table lists the valid options for the **XenDesktopVDASetup.exe** command.

When installing a VDA for use with Remote PC Access, specify only options that are valid on physical machines (not VMs or master images) and for VDAs for Windows Desktop OS.

Unless otherwise noted, options apply to physical and virtual machines, and to VDAs for Windows Desktop OS and VDAs for Windows Server OS.

Important

In XenApp and XenDesktop 7.9, use the command line only for **Remote PC Access** deployments and do not change the order of syntax for /components and /remotepc. For example:

```
VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE "AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet
```

If /remotepc is used before /components, the /remotepc option is ignored.

Option	**Description**
/baseimage	(Valid only when installing a VDA for Windows Desktop OS on a VM.) Enables the use of Personal vDisks with a master image. For more information, see the Personal vDisks articles.
/components	Comma-separated list of components to install or remove. Valid values are:

component[,component]	• VDA - installs the VDA • PLUGINS - installs the 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.
/controllers "controller [controller] [...]"	Space-separated Fully Qualified Domain Names (FQDNs) of Controllers with which the VDA can communicate, enclosed in quotation marks. Do not specify both the /site_guid and /controllers options.
/enable_framehawk_port	Opens the UDP ports used by Framehawk. Default = false
/enable_hdx_3d_pro	Installs the VDA for HDX 3D Pro. For more information, see the HDX 3D Pro article.
/enable_hdx_ports	Opens ports in the Windows firewall required by the Controller and features you specified (Windows Remote Assistance, real-time transport, and optimize), 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.
/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 if 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 opens TCP port 3389 in the firewall, even if you omit the /enable_hdx_ports option.
/exclude "component"[,"component"]	Prevents installation of one or more comma-separated optional components, enclosed in quotation marks. For example, installing or upgrading a VDA on an image that is not managed by Machine Creation Services does not require the Personal vDisk or Machine Identity Service components. Valid values are: • Personal vDisk • Machine Identity Service • Citrix User Profile Manager Excluding Citrix Profile management from the VDA installation will affect monitoring and troubleshooting VDAs with Citrix Director. On the User details and EndPoint pages, the Personalization panel and the Logon Duration panel will fail. On the Dashboard and Trends pages, the Average Logon Duration panel will display data only for machines that have Profile management installed.
/h or /help	Displays command help.
/installdir directory	Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.
/logpath path	Log file location. The specified folder must already exist; the installer does not create it. (This option is not available in the graphical interface.) Default = "%TEMP%\Citrix\XenDesktop Installer"
/masterimage	(Valid only when installing a VDA on a VM.) Sets up the VDA as a master image.

/no_appv	Prevents installation of the Citrix App-V components. For more information, see the App-V article.
/nocitrixwddm	(Valid only on Windows 7 machines that do not include a WDDM driver.) Disables installation of the Citrix WDDM driver.
/nodesktopexperience	(Valid only when installing a VDA for Windows 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 will not be fully available for use until after a restart.
/optimize	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. For more information about the optimization tool, see CTX125874.
/portnumber port	(Valid only if 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.
/reconfig	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	Prevents installation of the following components on a desktop (workstation) OS: • App V Component - Citrix Personalization for App-V - VDA • UpmComponent - Citrix User Profile Manager • UpmVdaPlugin Component - Citrix User Profile Manager WMI Plugin • Mps Component - Machine Identity Service • VDisk Component - Personal vDisk During an upgrade, if any of these components are installed, the installer detects and upgrades them.
/remove	Removes the components specified with the /components option.
/removeall	Removes all installed VDA components.
/servervdi	Installs a VDA for Windows Desktop OS on a supported Windows Server. Omit this option when installing a VDA for Windows Server OS on a Windows Server. Before using this option, see the Server VDI article. (This option is not available in the graphical interface.)
/site_guid guid	Globally Unique Identifier of the site Active Directory Organizational Unit (OU). This associates a

	virtual desktop with a Site when you are using Active Directory for discovery (auto-update is the recommended and default discovery method). The site GUID is a site property displayed in Studio. Do not specify both the /site_guid and /controllers options.
/tempdir directory	Directory to hold temporary files during installation. (This option is not available in the graphical interface.) Default = c:\Windows\Temp.
/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.
/xa_server_location url	URL of the server for Windows server applications.

Install the Universal Print Server using the command line

Note: If you are installing the UpsServer component on a 32-bit Windows 2008 server, follow the steps in Before installing the Universal print Server on a 32-bit Windows 2008.

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 the Provision printers article.

Before deploying UpsServer_x86.msi on a 32-bit Windows 2008 machine, you must adjust the Minimum Version for Windows Installer for the cdf_x86.msi and UpsServer_x86.msi, using either Visual Basic scripts or a tool such as Orca.

1. Copy the 32-bit versions of the CDF and UPS MSI files (**cdf_x86.msi** and **UpsServer_x86.msi**) to a temp folder.
2. Install the WiSumInf.vbs script or the Orca tool, both available in the Windows SDK Components for Windows Installer Developers package. For information about the script, see the MSDN article Manage Summary Information.
3. Modify the Minimum Version for the Windows Installer using one of the following methods:

   Using the WiSumInf.vbs script: Copy WiSumInf.vbs to the same temp folder with the two Citrix msi's. Then, run the script for each package with the parameters **WiSumInf.vbs cdf_x86.msi Pages=405** and **WiSumInf.vbs UpsServer_x86.msi Pages=405**.

   Using Orca: Open each of the cdf_x86.msi and UpsServer_x86.msi packages, go to the View menu > Summary Information, and change the value of the **Schema** textbox to **405**.

After completing the above procedure, install the Universal Print Server on the print server.

Install VDAs using scripts

Sep 29, 2015

Note: This article applies to installing components on machines with Windows operating systems. For information about VDAs for Linux operating systems, see Red Hat Linux VDAs and SUSE Linux VDAs.

The installation media contains sample scripts that install, upgrade, or remove Virtual Delivery Agents (VDAs) for groups of machines in Active Directory. You can also apply the scripts to individual machines, and use them 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 from the full product ISO, or VDAWorkstationSetup.exe or VDAServerSetup.exe from the standalone installer.
- Logging details are stored on each local machine. If you also want 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 if the operation was successful with the prefix PASS or FAIL. You can use standard directory search tools to quickly find a failed installation or removal in the central log share, rather than searching locally on the target machines.

Important: Before beginning any installation, read and complete the tasks in the Prepare to install article.

To 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 location from which 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) will be 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 the Install using the command line article. 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 in Active Directory where your machines are located. This OU should contain only machines on which you want to install the VDA. When the machines in the OU are restarted, the script runs on all of them, installing a VDA on each machine that has a supported operating system.

To remove VDAs using the script

1. Obtain the sample script UninstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script.
   - Specify the version of the VDA to remove: SET CHECK_VDA_VERSION. For example, version 7 can be specified as 7.0; the full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018); however, a complete match is not required.
   - Optionally, specify a network share location for storing centralized logs.
3. Using Group Policy Startup Scripts, assign the script to the OU in Active Directory where your machines are located. 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, removing a VDA from each machine.

Troubleshooting

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 to the machine, so that you can verify that the overall process is working. If this log is not copied to the central log share as expected, you can troubleshoot further by inspecting the local machine: the script places two debugging log files in the %temp% folder on each machine, for early troubleshooting:

- Kickoff_VDA_Startup_Script_<DateTimeStamp>.log
- VDA_Install_ProcessLog_<DateTimeStamp>.log

Review the content of 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 Red Hat/CentOS Linux VDAs

Jun 13, 2016

You can create Linux virtual desktops based on a Red Hat/CentOS distribution. Prepare your Linux virtual machines, install the new software on them, configure your Delivery Controller, and then use Studio to make the desktops available to users.

For details, see the information contained in this article.

> **Note**
>
> The Linux shell commands used in this document have been verified to work with the GNU Bash shell.

The article includes the following sections:

System requirements

The following Linux distributions are supported by the Linux Virtual Desktop product:

- SUSE Linux Enterprise:
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2
- CentOS Linux
  - CentOS 6.7

- CentOS 7.2

> **Note**
>
> In all cases, the processor architecture supported is x86-64.

> **Tip**
>
> CentOS Linux is supported since version 1.3. The installation information contained in this article is also appropriate for CentOS.

The following versions of XenDesktop are supported by the Linux VDA:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

The configuration process for Linux VDAs differs slightly than for Windows VDAs. However, any Delivery Controller farm is capable of brokering both Windows and Linux desktops.

> **Note**
>
> The Linux VDA is incompatible with XenDesktop version 7.0 or earlier.

The following versions of Citrix Receiver are supported:

- Citrix Receiver for Windows version 4.4 or newer (this equates to v14.4 of wfica32.exe)
- Citrix Receiver for Linux version 13.3 or newer
- Citrix Receiver for Mac OSX version 12.1 or newer
- Citrix Receiver for Android version 3.8 or newer
- Citrix Receiver for iOS version 6.1.4 or newer
- Citrix Receiver for Chrome/HTML5 version 2.0 (only via Access Gateway)

The following hypervisors for hosting Linux VDA guest VMs are supported:

- XenServer
- VMware ESX and ESXi

- Microsoft Hyper-V

Bare metal hosting is also supported.

> **Tip**
>
> Refer to the hypervisor vendor's documentation for the list of supported platforms.

The following Active Directory integration packages or products are supported by the Linux VDA:

- Samba Winbind
- Quest Authentication Services v4.1 or newer
- Centrify DirectControl

> **Tip**
>
> Refer to the Active Directory Integration package vendor's documentation for the list of supported platforms.

The following hypervisors, Linux Distributions and NVIDIA GRID™ GPU are required to support HDX 3D Pro.

Hypervisors

The following hypervisors are supported:

- XenServer
- VMware ESX and ESXi

Linux distributions

The following Linux distribution supports HDX 3D Pro:

- Red Hat Enterprise Linux - Workstation 7.2

GPU

The following GPUs are supported:

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2

Configure delivery controllers

XenDesktop 7.7 or higher includes the necessary changes to support Linux Virtual Desktop, however, for previous versions a

hotfix or update script is required. The installation and verification of these are provided in this section.

For XenDesktop 7.6 SP2, apply the Hotfix Update 2 to update the Broker for Linux Virtual Desktops. Hotfixes Update 2 is available here:

- CTX142438: Hotfix Update 2 - For Delivery Controller 7.6 (32-bit) – English
- CTX142439: Hotfix Update 2 - For Delivery Controller 7.6 (64-bit) – English

For earlier versions of XenDesktop, a PowerShell script named **Update-BrokerServiceConfig.ps1** is provided which updates the broker service configuration. This is available in the following package:

- citrix-linuxvda-scripts-1.3.0.zip

Repeat the following steps on *every* Delivery Controller in the farm:

1. Copy the **Update-BrokerServiceConfig.ps1** script to the Delivery Controller machine.
2. Open a Windows PowerShell console in the context of the local administrator.
3. Browse to the folder containing the script.
4. Execute the script:

```
.\Update-BrokerServiceConfig.ps1
```

> **Note**
>
> By default, PowerShell is configured to prevent the execution of PowerShell scripts. If the script fails to run, you may need to change the PowerShell execution policy before trying again:
>
> ```
> Set-ExecutionPolicy Unrestricted
> ```

The **Update-BrokerServiceConfig.ps1** script updates the Broker service configuration file with new WCF endpoints required by the Linux VDA and restarts the broker service. The script determines the location of the broker service configuration file automatically. A backup of the original configuration file is created in the same directory with the extension **.prelinux**.

These changes will have no impact on the brokering of Windows VDA's configured to use the same Delivery Controller farm. This allows for a single Controller farm to manage and broker sessions to both Windows and Linux VDAs seamlessly.

To verify whether the required configuration changes have been applied to a Delivery Controller, confirm the string **EndpointLinux** appears five times in the file:

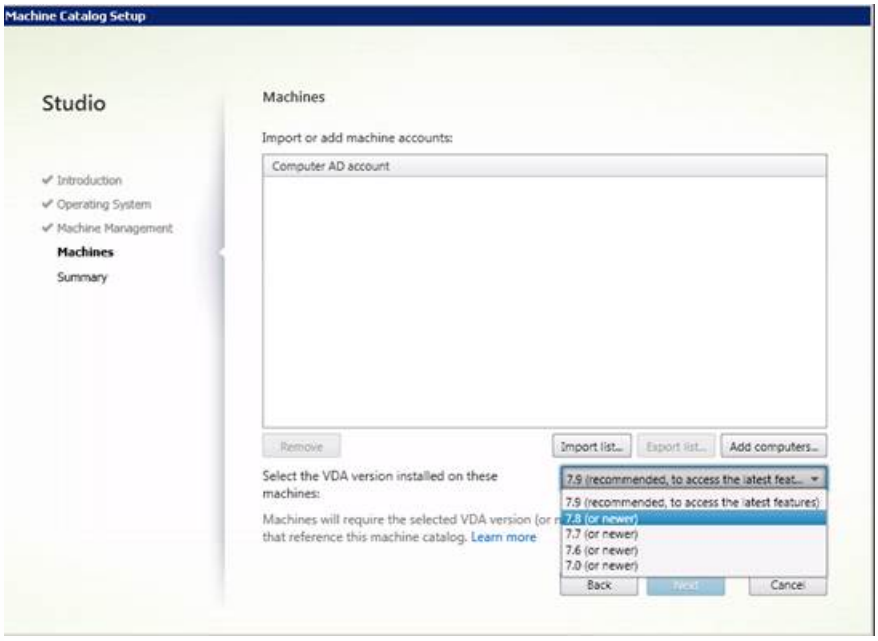
```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

From the Windows command prompt, logged on as a local administrator:

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config
```

Important

At version 1.3, the Linux VDA's broker agent is set to XenApp/XenDesktop 7.8. However, when adding a machine catalog using Studio's **Machine Catalog Setup** screen, the default value is automatically set to version 7.9. You must explicitly set the VDA version installed to **7.8 (or newer)**. Refer to the image below.



Prepare the Linux machine for VDA installation

Citrix recommends that the network is connected and properly configured correctly before proceeding.

RHEL 6 only: Set the hostname

To ensure that the hostname of the machine is reported correctly, change the **/etc/sysconfig/network** file to contain only the hostname of the machine.

HOSTNAME=**hostname**

RHEL 7 Only: Set the hostname

To ensure that the hostname of the machine is reported correctly, change the **/etc/hostname** file to contain only the hostname of the machine.

Assign a loopback address to the hostname

To ensure that the DNS domain name and FQDN of the machine are reported back correctly, change the following line of the **/etc/hosts** file to include the FQDN and hostname as the first two entries:

127.0.0.1 **hostname-fqdn hostname** localhost localhost.localdomain localhost4 localhost4.localdomain4

For example:

127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4

Remove any other references to **hostname-fqdn** or **hostname** from other entries in the file.

> **Note**
>
> The Linux VDA currently does not support NetBIOS name truncation, therefore the hostname must not exceed 15 characters.

> **Tip**
>
> Use a-z, 0-9 and hyphen (-) characters only. Avoid underscrore characters (_), spaces and other symbols. Do not start a hostname with a number and do not end with a hyphen.

Check the hostname

Verify that the hostname is set correctly:

hostname

This should return only the machine's host name and not its fully qualified domain name (FQDN).

Verify that the FQDN is set correctly:

hostname -f

This should return the machine's FQDN.

Check name resolution and service reachability

Verify that you can resolve the FQDN and ping the domain controller and XenDesktop Delivery Controller:

nslookup **domain-controller-fqdn**

ping **domain-controller-fqdn**

nslookup **delivery-controller-fqdn**

ping **delivery-controller-fqdn**

If you cannot resolve the FQDN or ping either of these machines, review the steps before proceeding.

Maintaining accurate clock synchronization between the VDAs, XenDesktop Controllers and domain controllers is crucial. Hosting the Linux VDA as a virtual machine can cause clock skew problems. For this reason, synchronizing time with a

remote time service is preferred.

RHEL 6.x and earlier releases use the NTP daemon (ntpd) for clock synchronization, whereas a default RHEL 7.x environment uses the newer Chrony daemon (chronyd) instead. The configuration and operational process between the two services is similar.

RHEL 6 only: Configure NTP service

As root, edit **/etc/ntp.conf** and add a server entry for each remote time server:

server **peer1-fqdn-or-ip-address** iburst

server **peer2-fqdn-or-ip-address** iburst

In a typical deployment, time should be synchronized from the local domain controllers and not directly from public NTP pool servers. Add a server entry for each Active Directory domain controller in the domain.

Remove any other **server** entries listed including loopback IP address, localhost, and public server ***.pool.ntp.org** entries.

Save changes and restart the NTP daemon:

sudo /sbin/service ntpd restart

RHEL 7 only: Chrony service

As root, edit **/etc/chrony.conf** and add a server entry for each remote time server:

server **peer1-fqdn-or-ip-address** iburst

server **peer2-fqdn-or-ip-address** iburst

In a typical deployment, time should be synchronized from the local domain controllers and not directly from public NTP pool servers. Add a server entry for each Active Directory domain controller in the domain.

Remove any other server entries listed including loopback IP address, localhost, and public server ***.pool.ntp.org** entries.

Save changes and restart the Chrony daemon:

sudo /sbin/service chronyd restart

There is a specific RHEL 6 issue that causes users to receive a popup asking for the root password after logging on.

To resolve this issue, as root, create the file **/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla** in a text editor and add the following content:

[No Show Proxy Dialog]

Identity=unix-user:*

Action=org.freedesktop.packagekit.system-network-proxy-configure

ResultAny=no

ResultInactive=no

ResultActive=no

> **Tip**
>
> For more information on this issue, refer to the RedHat solutions page here. The correct workaround is described in the comments section.

The Linux VDA is dependent on OpenJDK. The runtime environment should have been installed as part of the operating system installation.

RHEL 6 only: OpenJDK 1.7

Confirm the correct version with:

```
sudo yum info java-1.7.0-openjdk
```

The pre-packaged OpenJDK may be an earlier version. Update to the latest version as required:

```
sudo yum -y update java-1.7.0-openjdk
```

Set the **JAVA_HOME** environment variable by adding the following line to **~/.bashrc** file:

```
export JAVA_HOME=/usr/lib/jvm/java
```

Open a new shell and verify the version of Java:

```
java –version
```

RHEL 7.0 only: OpenJDK 1.8

Confirm the correct version with:

```
sudo yum info java-1.8.0-openjdk
```

The pre-packaged OpenJDK may be an earlier version. Update to the latest version as required:

```
sudo yum -y update java-1.8.0-openjdk
```

Set the **JAVA_HOME** environment variable by adding the following line to **~/.bashrc** file:

```
export JAVA_HOME=/usr/lib/jvm/java
```

Open a new shell and verify the version of Java:

```
java –version
```

> **Tip**
>
> To avoid problems, make sure you only installed either OpenJDK version 1.7.0 or 1.8.0. Remove all other versions of Java on your

system.

The Linux VDA requires either PostgreSQL 8.4 or newer on RHEL 6 or PostgreSQL version 9.2 or newer on RHEL 7.

Install the following packages:

```
sudo yum -y install postgresql-server
```

```
sudo yum -y install postgresql-jdbc
```

The following post-installation step is required to initialize the database and ensure service starts on boot. This will create database files under **/var/lib/pgsql/data**. This command differs between PostgreSQL 8 and 9.

RHEL 6 only: PostgreSQL 8

```
sudo /sbin/service postgresql initdb
```

RHEL 7 only: PostgreSQL 9

```
sudo postgresql-setup initdb
```

Start PostgreSQL

For either version PostgreSQL, configure the service to start on boot, and to start now:

```
sudo /sbin/chkconfig postgresql on
```

```
sudo /sbin/service postgresql start
```

Check the version of PostgreSQL using:

```
psql --version
```

Verify that the data directory is set using the **psql** command-line utility:

```
sudo -u postgres psql -c 'show data_directory'
```

The Linux VDA requires either the motif or openmotif package, depending on the distribution.

RHEL 6 only: Open Motif

```
sudo yum -y install openmotif
```

RHEL 7 only: Motif

```
sudo yum -y install motif
```

The Linux VDA requires both cups and foomatic filters.

RHEL 6 only: Printing support

sudo yum –y install cups

sudo yum -y install foomatic

RHEL 7 only: Printing support

sudo yum –y install cups

sudo yum -y install foomatic-filters

Install the other required packages:

sudo yum -y install redhat-lsb-core

sudo yum -y install ImageMagick

Some changes are required when running the Linux VDA as a virtual machine on a supported hypervisor. Make the following changes according to the hypervisor platform in use. No changes are required if you are running the Linux machine on bare metal hardware.

Fix time synchronization on Citrix XenServer

If the XenServer Time Sync feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and XenServer both trying to manage the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization. No changes are required in HVM mode.

On some Linux distributions, if you are running a paravirtualized Linux kernel with XenServer Tools installed, you can check whether the XenServer Time Sync feature is present and enabled from within the Linux VM:

su -

cat /proc/sys/xen/independent_wallclock

This will return either:

- 0 - The time sync feature is enabled, and needs to be disabled.
- 1 - The time sync feature is disabled, and no further action is required.

If the /proc/sys/xen/indepent_wallclock file is not present, the following steps are not required.

If enabled, disable the time sync feature by writing 1 to the file:

sudo echo 1 > /proc/sys/xen/independent_wallclock

To make this change permanent and persist after reboot, edit the /etc/sysctl.conf file and add the line:

xen.independent_wallclock = 1

To verify these changes, reboot the system:

```
reboot
```

After reboot, check that this has been set correctly:

```
su -

cat /proc/sys/xen/independent_wallclock
```

This should return the value 1.

Fix time synchronization on Microsoft Hyper-V

Linux VMs with Hyper-V Linux Integration Services installed can leverage the Hyper-V time synchronization feature to use the host operating system's time. To ensure the system clock remains accurate, this feature should be enabled alongside NTP services.

From the management operating system:

1. Open the Hyper-V Manager console.
2. For the settings of a Linux VM, select **Integration Services**.
3. Ensure **Time synchronization** is selected.

> ### Note
>
> This approach is different from VMware and XenServer, where host time synchronization is disabled to avoid conflicts with NTP. Hyper-V time synchronization can co-exist and supplement NTP time synchronization.

Fix time synchronization on ESX and ESXi

If the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and the hypervisor both trying to synchronize the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization.

If you are running a paravirtualized Linux kernel with VMware Tools installed:

1. Open the vSphere Client.
2. Edit settings for the Linux VM.
3. In the **Virtual Machine Properties** dialog, open the **Options** tab.
4. Select **VMware Tools**.
5. In the **Advanced** box, uncheck **Synchronize guest time with host**.

There are a number of methods for adding Linux machines to the Active Directory domain that are supported by XenDesktop for Linux:

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Follow the instructions below for your chosen method.

Samba Winbind

Install or Update Required Packages

Install or update the required packages:

```
sudo yum -y install samba-winbind \
    samba-winbind-clients \
    krb5-workstation \
    authconfig \
    oddjob-mkhomedir
```

Enable Winbind Daemon to Start on Boot

The Winbind daemon must be configured to start on boot:

```
sudo /sbin/chkconfig winbind on
```

Configure Winbind Authentication

Configure the machine for Kerberos authentication using Winbind:

```
sudo authconfig \
    --disablecache \
    --disablesssd \
    --disablesssdauth \
    --enablewinbind \
    --enablewinbindauth \
    --disablewinbindoffline \
    --smbsecurity=ads \
    --smbworkgroup=domain \
    --smbrealm=REALM \
    --krb5realm=REALM \
    --krb5kdc=fqdn-of-domain-controller \
```


--winbindtemplateshell=/bin/bash \

--enablemkhomedir --updateall

Where **REALM** is the Kerberos realm name in upper-case and **domain** is the short NetBIOS name of the Active Directory domain.

If DNS-based lookups of the KDC server and realm name is required, add the following two options to the above command:

--enablekrb5kdcdns --enablekrb5realmdns

Ignore any errors returned from the **authconfig** command about the winbind service failing to start. These are due to authconfig trying to start the winbind service without the machine yet being joined to the domain.

Open **/etc/samba/smb.conf** and add the following entries under the **[Global]** section, but after the section generated by the authconfig tool.

kerberos method = secrets and keytab

winbind refresh tickets = true

The system keytab file **/etc/krb5.keytab** is required by the Linux VDA to authenticate and register with the Delivery Controller. The **kerberos method** setting above will force Winbind to create the system keytab file when the machine is first joined to the domain.

Join Windows Domain

This requires that your domain controller is reachable and you have a Active Directory user account with permissions to add computers to the domain.

sudo net ads join REALM -U user

Where REALM is the Kerberos realm name in upper-case, and user is a domain user with permissions to add computers to the domain.

Configure PAM for Winbind

By default, the configuration for the Winbind PAM module **(pam_winbind)** does not enable Kerberos ticket caching and home directory creation. Open **/etc/security/pam_winbind.conf** and add or change the following entries under the **[Global]** section:

krb5_auth = yes

krb5_ccache_type = FILE

mkhomedir = yes

Ensure any leading semi-colons from each setting are removed. These changes require restarting the Winbind daemon:

sudo /sbin/service winbind restart

> **Tip**
>
> The winbind daemon will only stay running if the machine is joined to a domain.

Open **/etc/krb5.conf** and change the following setting under the [libdefaults] section from KEYRING to FILE type:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory.

Verify the machine is joined to a domain using Samba's **net ads** command:

```
sudo net ads testjoin
```

Additional domain and computer object information can be verified with:

```
sudo net ads info
```

Verify Kerberos Configuration

To verify Kerberos is configured correctly for use with the Linux VDA, check that the system keytab file has been created and contains valid keys:

```
sudo klist -ke
```

This should display the list of keys available for the various combinations of principal names and cipher suites. Run the Kerberos **kinit** command to authenticate the machine with the domain controller using these keys:

```
sudo kinit -k MACHINE\$@REALM
```

The machine and realm names must be specified in uppercase, and the dollar sign ($) must be escaped with a backslash (\) to prevent shell substitution. In some environments the DNS domain name is different from the Kerberos realm name; ensure the realm name is used. If this command is successful, no output is displayed.

Verify that the TGT ticket for the machine account has been cached using:

```
sudo klist
```

Examine the machine's account details using:

```
sudo net ads status
```

Verify User Authentication

Use the **wbinfo** tool to verify that domain users can authenticate with the domain:

```
wbinfo --krb5auth=domain\\username%password
```

The domain specified here is the AD domain name, not the Kerberos realm name. For the bash shell, the backslash (\) character must be escaped with another backslash. This command will return a message indicating success or failure.

To verify that the Winbind PAM module is configured correctly, logon locally with a domain user account that has not logged onto the machine previously.

ssh localhost -l **domain\\username**

id -u

Check that a corresponding Kerberos credential cache file was created for the uid returned by the **id -u** command:

ls /tmp/krb5cc_**uid**

Check that the tickets in the user's Kerberos credential cache are valid and not expired:

klist

Exit the session:

exit

A similar test can be performed by logging onto the Gnome or KDE console directly.

Quest authentication service

Configure Quest on Domain Controller

This assumes you have installed and configured the Quest software on the Active Directory domain controllers, and have been granted administrative privileges to create computer objects in Active Directory.

Enable Domain Users to Logon to Linux VDA Machines

For each domain user that needs to establish HDX sessions on a Linux VDA machine:

1. In the Active Directory Users and Computers management console, open Active Directory user properties for that user account.
2. Select **Unix Account** tab.
3. Check **Unix-enabled**.
4. Set the **Primary GID Number** to the group ID of an actual domain user group.

> **Note**
>
> These instructions are equivalent for setting up domain users for logon using the console, RDP, SSH or any other remoting protocol.

Configure Quest on Linux VDA

Workaround SELinux Policy Enforcement

The default RHEL environment has SELinux fully enforced. This interferes with the Unix domain socket IPC mechanisms used by Quest and prevents domain users from logging on.

> **Tip**
>
> There are a few ways to workaround outlined here.

The easiest is to disable SELinux. As root, edit /etc/selinux/config and change the SELinux setting:

```
SELINUX=disabled
```

This change requires a reboot:

```
reboot
```

> **Important**
>
> Use this setting carefully. Reenabling SELinux policy enforcement after disabling can cause a complete lockout, even for the root user and other local users.

Configure VAS daemon

Auto-renewal of Kerberos tickets needs to be enabled and disconnected; authentication (offline logon) needs to be disabled:

```
sudo /opt/quest/bin/vastool configure vas vasd \
                    auto-ticket-renew-interval 32400
sudo /opt/quest/bin/vastool configure vas vas_auth \
                    allow-disconnected-auth false
```

This sets the renewal interval to 9 hours (32400 seconds) which is an hour less than the default 10 hour ticket lifetime. Set this parameter to a lower value on systems with a shorter ticket lifetime.

Configure PAM and NSS

Quest requires that PAM and NSS be manually configured to enable domain user login via HDX and other services such as su, ssh, and RDP. To configure PAM and NSS:

```
sudo /opt/quest/bin/vastool configure pam
sudo /opt/quest/bin/vastool configure nss
```

Join Windows Domain

Join the Linux machine to the Active Directory domain using the Quest vastool command:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

The user is any domain user with permissions to join computers to the Active Directory domain. The domain-name is the DNS name of the domain; for example, example.com.

Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory. To verify that a Quest-joined Linux machine is on the domain:

sudo /opt/quest/bin/vastool info domain

If the machine is joined to a domain this will return the domain name. If not joined, you will see the following error:

ERROR: No domain could be found.

ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm

default_realm not configured in vas.conf. Computer may not be joined to domain

Verify User Authentication

To verify that Quest can authenticate domain users using PAM, logon with a domain user account that has not logged onto the machine previously:

ssh localhost -l **domain\\username**

id -u

Check that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

ls /tmp/krb5cc_uid

Check that the tickets in user's Kerberos credential cache are valid and not expired:

/opt/quest/bin/vastool klist

Exit the session:

exit

A similar test can be performed by logging onto the Gnome or KDE console directly.

Centrify DirectControl

Join Windows Domain

With the Centrify DirectControl Agent installed, join the Linux machine to the Active Directory domain using the Centrify **adjoin** command:

su –

adjoin -w -V -u **user domain-name**

The **user** parameter is any Active Directory domain user with permissions to join computers to the Active Directory domain. The domain-name parameter is the name of the domain to join the Linux machine to.

Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory. To verify that a Centrify-joined Linux machine is on the domain:

su –

adinfo

Check that the **Joined to domain** value is valid and the **CentrifyDC mode** returns **connected**. If the mode remains stuck in the starting state, then the Centrify client is experiencing server connection or authentication problems.

More comprehensive system and diagnostic information is available using:


```
adinfo --sysinfo all

adinfo –diag
```

To test connectivity to the various Active Directory and Kerberos services:

```
adinfo --test
```

Install NVIDIA GRID drivers

To enable HDX 3D Pro, additional installation steps are required to install the required graphics drivers on the hypervisor as well as to the VDA machines.

Configure the following:

1. Citrix XenServer
2. VMware ESX

Follow the instructions for your chosen hypervisor.

Citrix XenServer

This detailed section walks through the install and configuration of the NVIDIA GRID drivers on Citrix XenServer.

VMware ESX

Follow the information contained in this guide to install and configure the NVIDIA GRID drivers for VMware ESX.

VDA Machines

Follow these steps to to install and configure the drivers for each of the Linux VM guests:

1. Before starting ensure the Linux VM is shutdown.
2. In XenCenter, add a GPU in GPU Passthrough mode to the VM.
3. Start the RHEL VM.

To prepare the machine for the NVIDIA GRID drivers the following steps are required:

```
# yum install gcc

# yum install "kernel-devel-uname-r == $(uname -r)"

# systemctl set-default multi-user.target
```

Once complete, follow the steps in the Red Hat Enterprise Linux document to install the NVIDIA GRID Driver.

> **Note**
>
> During the GPU driver install, select the default ('no') for each question.

> **Important**
>
> Once GPU Passthrough has been enabled, the Linux VM is no longer accessable via XenCenter so you wil need to use SSH to

connect.

In order to verify if the NVIDIA GRID™ graphics driver is installed correctly, run “nvidia-smi”; the results should resemble:

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Set the correct configuration for the card:

```
etc/X11/ctx-nvidia.sh
```

To take advantage of large resolutions and multimonitor capabilities you will need a valid NVIDIA license. To apply the license follow the product documentation from “GRID Licensing Guide.pdf - DU-07757-001 September 2015”.

Configure Linux machine catalog and delivery group

The process for creating machine catalogs and adding Linux VDA machines is very similar to the traditional Windows VDA approach. Refer to the online Citrix Product documentation for a more complete description of how to complete these tasks.

For creating machine catalogs that contain Linux VDA machines, there are a few restrictions that differentiates the process from creating machine catalogs for Windows VDA machines:

- For operating system, select:
  - Window Server OS or Server OS option for a hosted shared desktops delivery model.
  - Windows Desktop OS or Desktop OS option for a VDI dedicated desktop delivery model.
- Ensure machines are set as not power managed.
- As PVS and MCS are not supported for Linux VDAs, choose the **Another service or technology** (existing images) deployment method.

- Do not mix Linux and Windows VDA machines in the same machine catalog.

> **Note**
>
> Early versions of Citrix Studio did not support the notion of a "Linux OS"; however, selecting the Windows Server OS or Server OS option implies an equivalent hosted shared desktops delivery model. Selecting the Windows Desktop OS or Desktop OS option implies a XenDesktop single user per machine delivery model.

The Citrix documentation for creating machine catalogs is referenced below:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Earlier versions of XenDesktop are not supported.

> **Tip**
>
> If a machine leaves and is rejoined to the Active Directory domain, the machine will need to be removed and re-added again to the machine catalog.

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical for Windows VDA machines. Refer to the online Citrix Product documentation for a more complete description of how to complete these tasks.

For creating delivery groups that contain Linux VDA machine catalogs, the following restrictions apply:

- For delivery type, select Desktops. Linux VDA machines do not support application delivery.
- Ensure the AD users and groups you select have been properly configured to logon to the Linux VDA machines.
- Do not allow logon of unauthenticated (anonymous) users.
- Do not mix the delivery group with machine catalogs that contain Windows machines.

The Citrix documentation for creating delivery groups is referenced below:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Earlier versions of XenDesktop are not supported.

Install the Linux VDA software

If you have previously installed a version of the Linux VDA older than v1.0, you should uninstall it before installing the new version.

Stop the Linux VDA services:

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

Uninstall the package:

```
sudo rpm -e XenDesktopVDA
```

> **Important**
>
> Upgrading from the Tech Preview to versions 1.0, 1.1, 1.2, or 1.3 is not supported.
>
> For RHEL 6.0, Citrix recommends that you retain Xorg-x11-server-Xorg version 1.15; do not upgrade this package.

> **Note**
>
> Starting with version 1.3, the installation path as changed. In previous releases, installation components were located in **/usr/local/**; the new location is **/opt/Citrix/VDA/**.
>
> To execute a command, the full path is needed; alternately, you can add **/opt/Citrix/VDA/sbin** and **/opt/Citrix/VDA/bin** to the system path.

Install the Linux VDA

Install the Linux VDA software using the RPM package manager:

For RHEL 6:

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.el6.x86_64.rpm
```

For RHEL 7.2:

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.el7.x86_64.rpm
```

If you have previously installed v1.1 or v1.2 of the Linux VDA, upgrade the Linux VDA software using the RPM package

manager:

For RHEL 6:

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.el6.x86_64.rpm
```

For RHEL 7.2:

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.el7.x86_64.rpm
```

> **Important**
>
> You must reboot the Linux VDA machine after upgrading.

After installing the package you will need to configure the Linux VDA by running the ctxsetup.sh script. If you have upgraded the package you will need to run the ctxsetup.sh script to finalise your upgrade. Before making any changes, this script will verify the environment and ensure all dependencies are installed. If required, this script can be re-run at any time to change settings.

The script can either be run manually with prompting or automatically with pre-configured responses. Review help about this script before proceeding:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

Prompted configuration

Run a manual configuration with prompted questions:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Automated configuration

For an automated install, the options required by the setup script can be provided with environment variables. If all of the required variables are present then the script will not prompt the user for any information, allowing the installation process to be scripted.

Supported environment variables include:

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - The Virtual Delivery Agent supports specifying a Delivery Controller name using a DNS CNAME record. This is typically set to N.
- CTX_XDL_DDC_LIST = list-ddc-fqdns – The Virtual Delivery Agent requires a space-separated list of Delivery Controller Fully Qualified Domain Names
- (FQDNs) to use for registering with a Delivery. At least one FQDN or CNAME alias must be specified.
- CTX_XDL_VDA_PORT = port-number – The Virtual Delivery Agent communicates with Delivery Controllers using a TCP/IP port. This is typically port 80.
- CTX_XDL_REGISTER_SERVICE = Y | N - The Linux Virtual Desktop services support starting during boot. This is typically set to Y.

- CTX_XDL_ADD_FIREWALL_RULES = Y | N – The Linux Virtual Desktop services require incoming network connections to be allowed through the system firewall. You can automatically open the required ports (by default ports 80 and 1494) in the system firewall for the Linux Virtual Desktop. This is typically set to Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 – The Virtual Delivery Agent requires Kerberos configuration settings to authenticate with the Delivery Controllers. The Kerberos configuration is determined from the installed and configured Active Directory integration tool on the system. Specify the supported Active Directory integration method to use:
  - 1 - Samba Winbind
  - 2 - Quest Authentication Service
  - 3 – Centrify DirectControl
- CTX_XDL_HDX_3D_PRO= Y | N – Linux Virtual Desktop supports HDX 3D Pro, a set of graphics acceleration technologies designed to optimize the virtualization of rich graphics applications. HDX 3D Pro requires a compatible NVIDIA Grid graphics card to be installed. If HDX 3D Pro is selected the Virtual Delivery Agent will be configured for VDI desktops (single-session) mode – (i.e. CTX_XDL_VDI_MODE=Y). This is not supported on SUSE. Ensure this value is set to N.
- CTX_XDL_VDI_MODE= Y | N - Whether to configure the machine as a dedicated desktop delivery model (VDI) or hosted shared desktop delivery model. For HDX 3D Pro environements this needs to be set to Y. This is typically set to N.
- CTX_XDL_SITE_NAME= dns-name – The Virtual Delivery Agent discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS search results to a local site, a DNS site name may be specified. This is typically empty [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers – The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with LDAP port (e.g. ad1.mycompany.com:389). This is typically empty [none].
- CTX_XDL_SEARCH_BASE= search-base – The Virtual Delivery Agent by default queries LDAP using a search base set to the root of the Active Directory Domain (e.g. DC=mycompany,DC=com), however to improve search performance, a search base may be specified (e.g. OU=VDI,DC=mycompany,DC=com). This is typically empty [none].
- CTX_XDL_START_SERVICE = Y | N - Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. This is typically set to Y.

Set the environment variable and run the configure script:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base
```



```
export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

You must provide the -E option with sudo to pass the existing environment variables to the new shell it creates. Citrix recommends that you create a shell script file from the commands above with #!/bin/bash on the first line.

Alternatively, all parameters can be specified with a single command:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Remove configuration changes

In some scenarios it may be necessary to remove the configuration changes made by the **ctxsetup.sh** script without uninstalling the Linux VDA package.

Review help about this script before proceeding:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

To remove configuration changes:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

> ### Important
>
> This script will delete all configuration data from the database and will make the Linux VDA inoperable.

Configuration logs

The **ctxsetup.sh** and **ctxcleanup.sh** scripts will display errors on the console, with additional information written to a configuration log file:

/tmp/xdl.configure.log

Restart the Linux VDA services to have the changes take effect.

Run the VDA software

Once you have configured the Linux VDA using the ctxsetup.sh script, you use the following commands to control the Linux VDA.

To start the Linux VDA services:

sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start

To stop the Linux VDA services:

sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop

To restart the Linux VDA services:

sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start

To check the running state of the Linux VDA services:

sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status

Uninstall the Linux VDA software

To check whether the Linux VDA is installed and to view the version of the package installed:

```
rpm -q XenDesktopVDA
```

To view more detailed information:

```
rpm –qi XenDesktopVDA
```

> **Note**
>
> Uninstalling the Linux VDA software will delete the associated PostgreSQL and other configuration data. However, the PostgreSQL package and other dependent packages that were setup prior to the installation of the Linux VDA will not be removed.

This article does not cover the removal of dependent packages including PostgreSQL.

Troubleshooting

Verify H.264 encoding is in use

Linux VDA v1.3 adds H264 and a HardwareEncoding value in the registry path HKLM\Software\Citrix\Ica\Session\<session id>\Graphics to help troubleshoot graphics issues encountered with the VDA.

Run the following command to advertise H.264 encoding in a Linux VDA before a session is launched:

```
/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"AdvertiseH264" -d "0x00000001" --force
```

Launch the session and check whether the key H264 is created in the registry path, if so, H.264 encoding is in use.

```
/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

Verify hardware encoding for 3D Pro is in use

3D Pro hardware encoding is disabled by default, use the command below to enable the function:

```
/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"HardwareEncoding" -d "0x00000001" --force
```

Launch the session and check the value of "HardwareEncoding" in the registry path; 0 means not in use, 1 means hardware encoding is being used.

/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"

Use the command below to query your session ID:

/opt/Citrix/VDA/bin/ctxqsession

Customize the desktop environment for each user

Currently, the Linux VDA does not allow the user to choose the desktop environment when logging in; to workaround this issue, the user can configure a file (for example, .xsession) for the Linux distribution to set the default desktop environment for each user. Refer to the documents accompanying the Linux distribution for more information.

To se the KDE as the default environment:

#! /usr/bin/env bash

exec startkde

To set GNOME as the default desktop envionment:

#! /usr/bin/env bash

exec gnome-session

Check the Linux machine has been prepared correctly

The most common issues are a direct result of Linux machine misconfiguration, mainly around networking, NTP time server configuration or Active Directory domain membership. Fixing the Linux machine's configuration will often resolve issues with the VDA software.

Configure logging and tracing

The broker agent and the HDX Service log to syslog. Citrix support have a set of tools that can enable addition trace during a support call.

HDX Service logging

The HDX Service is configured to log to syslog out-of-the-box and no further configuration is needed.

Broker Agent logging

The broker agent (also known as the ctxvda service) writes log da?ta to syslog via network sockets. This may not be configured out-of-the-box. To enable the broker agent logging to syslog logging, the following configuration is required.

Edit the /etc/rsyslog.conf file and add the following lines:

$ModLoad imudp

$UDPServerRun 514

Save and close the rsyslog.conf file. Restart the rsyslog service to have the change take affect:

sudo /sbin/service rsyslog restart

What to try if HDX sessions won't start

Ensure you have no orphaned processes which might be preventing new sessions from starting:

```
sudo pkill -9 ctxhdx

sudo pkill -9 ctxgfx

sudo pkill -9 ctxlogin

sudo pkill -9 ctxvfb
```

Restart the Linux VDA services and retry connection.

Verify ownership and permissions of key directories and files

Check the file ownership and permission of the following directories and files:

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

HDX 3D Pro multi-monitor redraw issues

If you are seeing redraw issues on screens other than the primary monitor check that the NVIDIA GRID license is available.

Audio is not being heard

Check that the volume control on the device running the Citrix Receiver as well as the Linux desktop are not muted or set to a low level.

Check that audio is enabled on the Linux VDA. Use the ctxreg tool to query the value of the configuration item fDisableCam:

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

A value of 0x1 means audio is disabled. To enable, set fDisableCam to 0x0:

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam  -d 0x00000000
```

If audio is still not being heard check that the Citrix audio sink is loaded by pulseaudio. This PulseAudio module is loaded into the pulseaudio daemon at session start. Use the pacmd tool to check the Citrix audio sink is loaded:

```
pacmd list-sinks
```

If the Citrix audio sink is loaded, the output should be:

```
name: <CitrixAudioSink>

driver: <module-ctx-sink.c>
```

If Citrix audio sink is not loaded, kill the ctxaudio process and restart it.

Audio is not being recorded

Check that audio is enabled on the Linux VDA and audio recording is enabled on the ICA client. If audio is still not being recorded check that the Citrix audio source is loaded by pulseaudio. If audio recording is enabled on the ICA client, this PulseAudio module will be loaded into the pluseaudio daemon at session start. Use the pacmd tool to check the Citrix audio source is loaded:

```
pacmd list-sources
```

If the Citrix audio source is loaded, the output should be:

```
name: <CitrixAudioSource>
```

```
driver: <module-ctx-source.c>
```

If the Citrix audio source is not loaded, kill the ctxaudio process and restart it.

Unable to Print

There are a number of items to check if printing is not working correctly. The print daemon is a per session process and should be running for the length of the session. Check that the printing daemon is running.

```
ps –ef | grep ctxlpmngt
```

If the ctxlpmngt process is not running manually start ctxlpmngt from a command line.

If printing is still not working the next item to check in the CUPS framework. The ctxcups service is for printer management and communicates with the Linux CUPS framework. This is a single process per machine and can be checked by:

```
service ctxcups status
```

If the service is not running, start it manually:

```
service ctxcups start
```

Extra log for print CUPS

As one of the components of the Linux VDA, the method of how to get the log of a printing component is similar to other components.

For Red Hat, some extra steps are necessary to configure the CUPS service file. Otherwise some logs cannot get logged in hdx.log

```
sudo service cups stop
```

```
sudo vi /etc/systemd/system/printer.target.wants/cups.service
```

```
PrivateTmp=false
```

```
sudo service cups start
```

```
sudo systemctl daemon-reload
```

This configuration is only for collecting the full printing log when an issue arises. Normally this configuration is not

recommended because this will break CUPS security.

Print output is garbled

Garbled output can be caused by an incompatible printer driver. A per user driver configuration is available and can be configured by editing the ~/.CtxlpProfile configuration file.

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
```

The printername is a field containing the name of the current client side default printer. This is a read-only value and shoud not be edited.

> **Important**
>
> The fields **ppdpath**, **model** and **drivertype** should not be set at the same time as only one takes effect for the mapped printer.

If the Universal Printer driver is not compatible with the client printer, the model of native printer driver can be configured with the model= option. The current model name of the printer can be found with the lpinfo command.

```
lpinfo –m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

...
```

The model can then be set to match the printer:

```
Model=xerox/ph3115.ppd.gz
```

If the Universal Printer driver is not compatible with client printer, the ppd file path of native printer driver can be configured. The value of ppdpath is the absolute path of native printer driver file.

For example, there is a ppd driver under /home/tester/NATIVE_PRINTER_DRIVER.ppd.

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

There are three types of Universal Printer Driver supplied by Citrix (postscript, pcl5 and pcl6). These can configured in the driver type if no native printer driver is available.

For example, if client default printer driver type is PCL5.

drivertype=pcl5

> **Note**
>
> Citrix Receiver for Mac and Citrix Receiver for Linux only support Postscript printers and so the PCL5 and PCL6 Universal Printer Drivers are not applicable. In this situation, ppdpath or the model of native printer driver has to be set to a non-Postscript printer.

CDM does not work

The CDM feature includes a daemon process (ctxcdmd); if the CDM feature fails, reboot the Linux VDA machine and verify whether the daemon launched correctly:

Ps -lef | grep ctxcdmd

The file naming in the mapped drive should follow the VDA and Receiver OS naming rules.

Known issues

Citrix Receiver for Android CAPS LOCK state can be reversed when session roaming

The CAPS LOCK state may be lost when roaming an existing connection to the Citrix Receiver for Android. The workaround is to use the shift key on the extended keyboard to switch between upper case and lower case.

Shortcut keys with ALT do not always work when connecting to a Linux VDA using the Citrix Receiver for Mac

The Citrix Receiver for Mac send AltGr for both left and right Options/Alt keys by default. It is possible to change this within the Citrix Receiver settings but the results vary with different applications.

Newer X client libraries can cause keyboard mapping issues on SuSE Linux Enterprise Desktop 11

Newer versions of the xorg-x11-libX11 packages on SuSE Linux Enterprise Desktop 11 may have problems handling keyboard mapping changes, which in turn may cause issues with keyboard functionality inside an HDX session. This can happen when the installed version of the packages is in the range 7.4-5.11.11.1 to 7.4-5.11.15.1.

The workaround is to rollback to the stock SP3 version of the xorg-x11-libX11 package, this will enable keyboard mapping changes to work as normal. For example:

rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm –i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1

This needs to be done before a user logs on to the machine – if this is done while a session is active, these settings will not

take affect until the user next logs in.

If upgrading from stock SP3, the above xorg-x11-libX11 packages can be locked to the current installed version so that they won't be changed during the upgrade. Before upgrading, run the following before proceeding with the upgrade as normal:

```
zypper al xorg-x11-libX11
```

```
zypper al xorg-x11-libX11-32bit
```

Long session launches may occur when using Linux VDA with a Delivery Controller from XenDesktop v7.1

The slow launch is caused by the presence of CGP settings in the ICA file generated by the v7.1 Delivery Controller. When these settings are present, Citrix Receiver attempts to establish a connection on TCP port 2598. The default firewall settings on some Linux distributions, such as SLED 12, is to drop the TCP SYN packets, resulting in a timeout and hence a long session launch. The workaround is to configure the firewall on the Linux VDA to reject the TCP SYN on port 2598. This issue has been addressed in newer versions of the Delivery Controller.

Registration fails when Linux VDA is rejoined to the domain

Under certain circumstances, when a Linux VDA is rejoined to the domain and a fresh set of Kerberos keys are generated, the Broker fails to establish a security context with the VDA. This is often caused by the Broker using a cached out-of-date VDA service ticket based on the previous set of Kerberos keys. This won't stop the VDA from connecting to the Broker, but the Broker will not be able to establish a return security context to the VDA. The usual symptom is that the VDA registration fails.

This problem will eventually resolve itself when the VDA service ticket eventually expires and is renewed, but service tickets are usually long-lived. This could potentially be hours.

The solution is to clear the Broker's ticket cache. You could simply reboot the broker or run the following on the Broker from a command prompt as Administrator:

```
klist -li 0x3e4 purge
```

This will purge all service tickets in the LSA cache held by the Network Service principal under which the Citrix Broker Service runs. This will remove service tickets for other VDAs and potentially other services. However, this is harmless – these service tickets will simply be reacquired from the KDC when needed again.

Lock screen icon missing when using HDX 3D Pro with GNOME

When the NVIDIA Grid drivers are active Gnome Desktop Manager (GDM) is not active and the GDM lock screen capability is not available.

Audio plug-n-play not supported

It is recommended that any audio capture device is connected to the client machine before starting to record audio in the ICA session. If a device is attached after the audio recording application has started the application may become unresponsive. If this issue occurs just restart the application. A similar issue may occur if a capture device is unplugged while recording.

Audio Distortion

Windows 10 Receiver may experience audio distortion during audio recording.

CTXPS driver isn't compatible with some PLC printers

If you see printing output corruptions set the printer driver to native printer driver provided by the manufacturer.

Slow printing performance for large documents

When you print a large document on a local client printer, the print file is transferred over the server connection. On slow connections, this may take a long time.

Printer and print job notifications seen from other sessions.

Linux does not have the same session concept as the Windows Operating system. Therefore all users get system wide notifications. The administrator can disable these notifications by modifying the CUPS configuration file, /etc/cups/cupsd.conf.

Find the current policy name configured in the file.

```
DefaultPolicy default
```

If the policy name is default, then add the following lines into default policy XML block.

```
<Policy default>
    # Job/subscription privacy...
    JobPrivateAccess default
    JobPrivateValues default
    SubscriptionPrivateAccess default
    SubscriptionPrivateValues default
    ... ...
    <Limit Create-Printer-Subscription>
        Require user @OWNER
        Order deny,allow
    </Limit>
    <Limit All>
        Order deny,allow
    </Limit>
</Policy>
```

Glossary

Broker - XenDesktop component responsible for brokering HDX sessions to the different VDAs within a XenDesktop

deployment. Also known as the DDC or XenDesktop Controller.

Broker Agent - Component on the Linux VDA machine providing the desktop to be delivered. The Broker Agent communicates with the Broker to enable the brokering of sessions. It is composed of two key components, the VDA Service and the HDX Service.

Citrix Director - Citrix helpdesk/support console for monitoring and controlling XenDesktop VDAs.

Citrix Studio - Citrix administration console used to configure XenDesktop.

DDC - XenDesktop Desktop Delivery Controller. Also known as the Broker or Delivery Controller.

FQDN – Fully Qualified Domain Name

HDX - High Definition Experience protocol. Formerly known as the Citrix ICA protocol.

HDX Service - The Linux service (ctxhdx) that remotes the virtual Linux desktop via the HDX protocol. It communicates with the VDA service to enable the brokering of sessions.

RHEL - Red Hat Enterprise Linux. A commercial Linux distribution provided by Red Hat.

SLED - SUSE Linux Enterprise Desktop. A commercial Linux distribution provided by Novell.

SLES - SUSE Linux Enterprise Server. A commercial Linux distribution provided by Novell.

VDA - Virtual Delivery Agent.

VDA Service - The Linux service (ctxvda) that communicates with the Broker to enable the brokering of sessions. It also communicates with the HDX Service for remote session delivery.

Install SUSE Linux VDAs

Jun 13, 2016

You can create Linux virtual desktops based on a SUSE distribution. Prepare your Linux virtual machines, install the new Linux VDA software on them, configure your Delivery Controller, and then use Studio to make the desktops available to users.

For details, see the information contained in this article.

> **Note**
>
> The Linux shell commands described in this article have been verified to work with the GNU Bash shell.

The article includes the following sections:

System requirements

The following Linux distributions are supported by the Linux Virtual Desktop product:

- SUSE Linux Enterprise:
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2
- CentOS Linux
  - CentOS 6.7
  - CentOS 7.2

> **Note**
>
> In all cases, the processor architecture supported is x86-64.

The following versions of XenDesktop are supported by the Linux VDA:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

The configuration process for Linux VDAs differs slightly than for Windows VDAs. However, any Delivery Controller farm is capable of brokering both Windows and Linux desktops.

> **Note**
>
> The Linux VDA is incompatible with XenDesktop version 7.0 or earlier.

The following versions of Citrix Receiver are supported:

- Citrix Receiver for Windows version 4.4 or newer (this equates to v14.4 of wfica32.exe)
- Citrix Receiver for Linux version 13.3 or newer
- Citrix Receiver for Mac OSX version 12.1 or newer
- Citrix Receiver for Android version 3.8 or newer
- Citrix Receiver for iOS version 6.1.4 or newer
- Citrix Receiver for Chrome/HTML5 version 2.0 (only via Access Gateway)

The following hypervisors for hosting Linux VDA guest VMs are supported:

- XenServer
- VMware ESX and ESXi
- Microsoft Hyper-V

Bare metal hosting is also supported.

> **Tip**
>
> Refer to the hypervisor vendor's documentation for the list of supported platforms.

The following Active Directory integration packages or products are supported by the Linux VDA:

- Samba Winbind
- Quest Authentication Services v4.1 or newer
- Centrify DirectControl

> **Tip**
>
> Refer to the Active Directory Integration package vendor's documentation for the list of supported platforms.

Configure delivery controllers

XenDesktop 7.7 or higher includes the necessary changes to support Linux Virtual Desktop, however, for previous versions a hotfix or update script is required. The installation and verification of these are provided in this section.

For XenDesktop 7.6 SP2, apply the Hotfix Update 2 to update the Broker for Linux Virtual Desktops. Hotfixes Update 2 is available here:

- CTX142438: Hotfix Update 2 - For Delivery Controller 7.6 (32-bit) – English
- CTX142439: Hotfix Update 2 - For Delivery Controller 7.6 (64-bit) – English

For earlier versions of XenDesktop, a PowerShell script named **Update-BrokerServiceConfig.ps1** is provided which updates the broker service configuration. This is available in the following package:

- citrix-linuxvda-scripts-1.3.0.zip

Repeat the following steps on *every* Delivery Controller in the farm:

1. Copy the **Update-BrokerServiceConfig.ps1** script to the Delivery Controller machine.
2. Open a Windows PowerShell console in the context of the local administrator.
3. Browse to the folder containing the script.
4. Execute the script:

```
.\Update-BrokerServiceConfig.ps1
```

> **Note**
>
> By default, PowerShell is configured to prevent the execution of PowerShell scripts. If the script fails to run, you may need to change the PowerShell execution policy before trying again:
>
> ```
> Set-ExecutionPolicy Unrestricted
> ```

The **Update-BrokerServiceConfig.ps1** script updates the Broker service configuration file with new WCF endpoints

required by the Linux VDA and restarts the broker service. The script determines the location of the broker service configuration file automatically. A backup of the original configuration file is created in the same directory with the extension **.prelinux**.

These changes will have no impact on the brokering of Windows VDA's configured to use the same Delivery Controller farm. This allows for a single Controller farm to manage and broker sessions to both Windows and Linux VDAs seamlessly.

To verify whether the required configuration changes have been applied to a Delivery Controller, confirm the string **EndpointLinux** appears five times in the file:

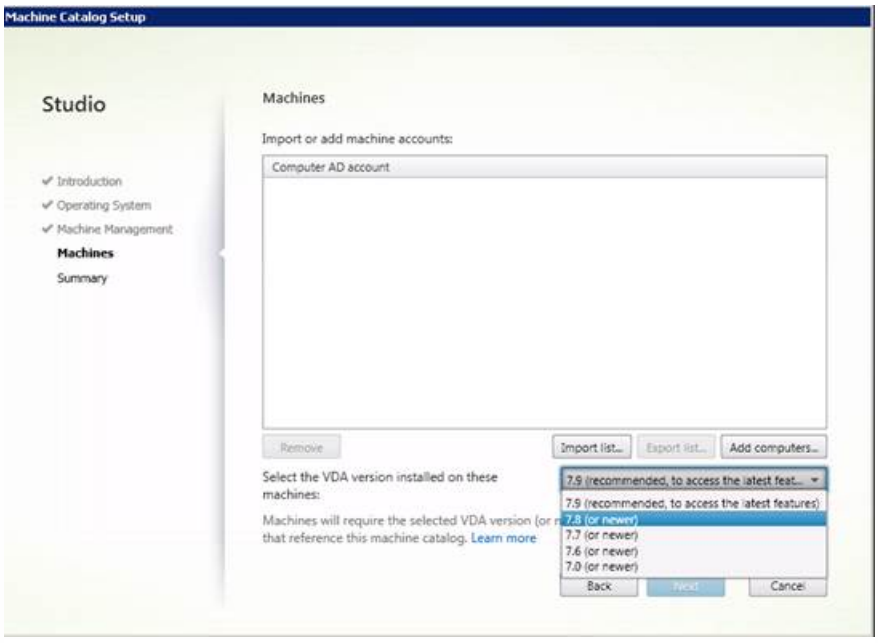
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config

From the Windows command prompt, logged on as a local administrator:

cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config

> ## Important
>
> At version 1.3, the Linux VDA's broker agent is set to XenApp/XenDesktop 7.8. However, when adding a machine catalog using Studio's **Machine Catalog Setup** screen, the default value is automatically set to version 7.9. You must explicitly set the VDA version installed to **7.8 (or newer)**. Refer to the image below.



Prepare Linux machine for VDA installation

The SUSE Linux Enterprise YaST tool is used for configuring all aspects of the operating system.

To launch the text-based YaST tool:

```
su -

yast
```

Alternatively, launch the UI-based YaST tool:

```
su -

yast2 &
```

The following sections provide information on configuring the various networking settings and services used by the Linux VDA. Configuring networking should be carried out via the YaST tool, not via other methods such as Network Manager. These instructions are based on using the UI-based YaST tool; the text-based YaST tool can be used but has a different method of navigation which is not documented here.

Configure hostname and DNS

1. Open YaST Network Settings.
2. SLED 12 Only: On the **Global Options** tab, change the **Network Setup Method** to **Wicked Service**.
3. Open the **Hostname/DNS** tab.
4. Uncheck **Change hostname via DHCP**.
5. Check **Assign Hostname to Loopback IP**.
6. Edit the following to reflect your networking setup:

- Hostname – Add the DNS hostname of the machine.
- Domain Name – Add the DNS domain name of the machine.
- Name Server – Add the IP address of the DNS server. This is typically the IP address of the AD Domain Controller.
- Domain Search list – Add the DNS domain name.

> ### Note
>
> The Linux VDA currently does not support NetBIOS name truncation, therefore the hostname must not exceed 15 characters.

> ### Tip
>
> Use a-z, 0-9 and hyphen (-) characters only. Avoid underscrore characters (_), spaces and other symbols. Do not start a hostname with a number and do not end with a hyphen.

Disable multicast DNS

On SLED only, the default settings have multicast DNS (mDNS) enabled, which can lead to inconsistent name resolution results. mDNS is not enabled on SLES by default, so no action is required.

To disable mDNS, edit /etc/nsswitch.conf and change the line containing:

hosts: files mdns_minimal [NOTFOUND=return] dns

To:

hosts: files dns

Check the hostname

Verify that the hostname is set correctly:

hostname

This should return only the machine's host name and not its fully qualified domain name (FQDN).

Verify that the FQDN is set correctly:

hostname -f

This should return the machine's FQDN.

Check name resolution and service reachability

Verify that you can resolve the FQDN and ping the domain controller and XenDesktop Delivery Controller:

nslookup **domain-controller-fqdn**

ping **domain-controller-fqdn**

nslookup **delivery-controller-fqdn**

ping **delivery-controller-fqdn**

If you cannot resolve the FQDN or ping either of these machines, review the steps before proceeding.

Maintaining accurate clock synchronization between the VDAs, XenDesktop Controllers and domain controllers is crucial. Hosting the Linux VDA as a virtual machine can cause clock skew problems. For this reason, maintaining time using a remote NTP service is preferred. Some changes might be required to the default NTP settings:

1. Open YaST NTP Configuration and select the **General Settings** tab.
2. In the Start NTP Daemon section, check **Now and on Boot**.
3. If present, select the **Undisciplined Local Clock (LOCAL)** item and click **Delete**.
4. Add an entry for an NTP server by clicking **Add**.
5. Select the **Server Type** and click **Next**.
6. Enter the DNS name of the NTP server in the Address field. This service is normally hosted on the Active Directory domain controller.
7. Leave the Options field unchanged.
8. Click **Test** to check that the NTP service is reachable.
9. Click **OK** through the set of windows to save the changes.

> **Note**
>
> For SLES 12 implementations, if the NTP daemon fails to start, this might be due to a known SUSE issue with AppArmor policies. Follow the resolution here for additional information.

The Linux VDA software for Suse Linux Enterprise is dependent on the following packages:

- PostgreSQL
  - SLED/SLES 11: Version 9.1 or newer
  - SLED/SLES 12: Version 9.3 or newer
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 or newer
- Cups
  - SLED/SLES 11: Version 1.3.7 or newer
  - SLED/SLES 12: Version 1.6.0 or newer
- Foomatic filters
  - SLED/SLES 11: Version 3.0.0 or newer
  - SLED/SLES 12: Version 1.0.0 or newer
- ImageMagick
  - SLED/SLES 11: Version 6.4.3.6 or newer
  - SLED/SLES 12: Version 6.8 or newer

Add respositories

Some required packages are not available in all Suse Linux Enterprise repositories:

- SLED 11: PostgreSQL is available for SLES 11 but not SLED 11.
- SLES 11: OpenJDK and OpenMotif are available for SLED 11 but not SLES 11.
- SLED 12: PostgreSQL is available for SLES 12 but not SLED 12. ImageMagick is available via the SLE 12 SDK ISO or online repository.
- SLES 12: There are no issues; all packages are available. ImageMagick is available via the SLE 12 SDK ISO or online repository.

To resolve this, the recommended approach is to obtain missing packages from the media for the alternate edition of SLE from which you are installing. That is, on SLED install missing packages from the SLES media, and on SLES install missing packages from the SLED media. The approach described below mounts both SLED and SLES ISO media files and adds repositories.

SLED 11	sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles

SLES 11	sudo mkdir -p /mnt/sled sudo mount -t iso9660 \ path-to-iso/SLED-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sled sudo zypper ar -f /mnt/sled sled
SLED 12	sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-12-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles
SLED/SLES 12	sudo mkdir -p /mnt/sdk sudo mount -t iso9660 \ path-to-iso/SLE-12-SDK-DVD-x86_64-GM-DVD1.iso /mnt/sdk sudo zypper ar -f /mnt/sdk sdk

Install Kerberos client

Install the Kerberos client for mutual authentication between the Linux VDA with the XenDesktop Controllers:

```
sudo zypper install krb5-client
```

The Kerberos client configuration is dependent on which Active Directory integration approach is used, which is described later.

Install OpenJDK

The Linux VDA dependent on OpenJDK 1.7.0.

> **Tip**
>
> To avoid problems, make sure you only installed the 1.7.0 version of OpenJDK. Remove all other versions of Java on your system.

SLED	On SLED, the Java runtime environment should have been installed with the operating system. Confirm this with: sudo zypper info java-1_7_0-openjdk Update to the latest version if status is reported as out-of-date: sudo zypper update java-1_7_0-openjdk

	Check the Java version: java -version
SLES	On SLES, the Java runtime environment needs to be installed: sudo zypper install java-1_7_0-openjdk Check the Java version: java -version

Install PostgreSQL

SLED/SLES 11	Install the packages: sudo zypper install libecpg6 sudo zypper install postgresql?init sudo zypper install postgresql91 sudo zypper install postgresql91?server sudo zypper install postgresql?jdbc Some post-installation steps are required to initialize the database service and ensure PostgreSQL starts on boot: sudo /sbin/insserv postgresql sudo /etc/init.d/postgresql restart
SLED/SLES 12	Install the packages: sudo zypper install postgresql-init sudo zypper install postgresql93-server sudo zypper install postgresql-jdbc Post-installation steps are required to initialize the database service and ensure PostgreSQL starts on boot: sudo systemctl enable postgresql sudo systemctl restart postgresql Database files will reside under /var/lib/pgsql/data.

Install the OpenMotif runtime environment

The Linux VDA requires either the motif or openmotif package, depending on the distribution.

SLED/SLES 11	Install the package: sudo zypper install openmotif-libs
SLED/SLES 12	Install the package: sudo zypper install motif

Install printing support

The Linux VDA requires both cups and foomatic filters.

SLED/SLES 11	Install the packages: sudo zypper install cups sudo zypper install foomatic-filters
SLED/SLES 12	Install the packages: sudo zypper install cups sudo zypper install cups-filters-foomatic-rip

Install ImageMagick

Install the ImageMagick package:

sudo zypper install ImageMagick

Remove repositories

With dependent packages installed, the alternative edition repositories setup earlier can now be removed and the media unmounted:

SLED 11	Remove the following packages: sudo zypper rr sles sudo umount /mnt/sles sudo rmdir /mnt/sles
	Remove the following packages:

SLES 11	sudo zypper rr sled sudo umount /mnt/sled sudo rmdir /mnt/sled
SLED 12	Remove the following packages: sudo zypper rr sles sudo umount /mnt/sles sudo rmdir /mnt/sles
SLED/SLES 12	Remove the following packages: sudo zypper rr sdk sudo umount /mnt/sdk sudo rmdir /mnt/sdk

Some changes are required when running the Linux VDA as a virtual machine on a supported hypervisor. Make the following changes according to the hypervisor platform in use. No changes are required if you are running the Linux machine on bare metal hardware.

Fix time synchronization on Citrix XenServer

If the XenServer Time Sync feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and XenServer both trying to manage the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization. No changes are required in HVM mode.

On some Linux distributions, if you are running a paravirtualized Linux kernel with XenServer Tools installed, you can check whether the XenServer Time Sync feature is present and enabled from within the Linux VM:

```
su -
cat /proc/sys/xen/independent_wallclock
```

This will return either:

- 0 - The time sync feature is enabled, and needs to be disabled.
- 1 - The time sync feature is disabled, and no further action is required.

If the /proc/sys/xen/indepent_wallclock file is not present, the following steps are not required.

If enabled, disable the time sync feature by writing 1 to the file:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

To make this change permanent and persist after reboot, edit the /etc/sysctl.conf file and add the line:

```
xen.independent_wallclock = 1
```

To verify these changes, reboot the system:

```
reboot
```

After reboot, check that this has been set correctly:

```
su -
cat /proc/sys/xen/independent_wallclock
```

This should return the value 1.

Fix time synchronization on Microsoft Hyper-V

Linux VMs with Hyper-V Linux Integration Services installed can leverage the Hyper-V time synchronization feature to use the host operating system's time. To ensure the system clock remains accurate, this feature should be enabled alongside NTP services.

From the management operating system:

1. Open the Hyper-V Manager console.
2. For the settings of a Linux VM, select **Integration Services**.
3. Ensure **Time synchronization** is selected.

> ### Note
>
> This approach is different from VMware and XenServer, where host time synchronization is disabled to avoid conflicts with NTP. Hyper-V time synchronization can co-exist and supplement NTP time synchronization.

Fix time synchronization on ESX and ESXi

If the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and the hypervisor both trying to synchronize the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization.

If you are running a paravirtualized Linux kernel with VMware Tools installed:

1. Open the vSphere Client.
2. Edit settings for the Linux VM.
3. In the **Virtual Machine Properties** dialog, open the **Options** tab.
4. Select VMware Tools.
5. In the **Advanced** box, uncheck **Synchronize guest time with host**.

There are a number of methods for adding Linux machines to the Active Directory domain that are supported by XenDesktop for Linux:

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Follow the instructions below for your chosen method.

Samba Winbind

Join Windows Domain

This requires that your domain controller is reachable and you have an Active Directory user account with permissions to add machines to the domain:

1. Open YaST Windows Domain Membership.
2. Make the following changes:

- Set the Domain or Workgroup to the name of your Active Directory domain or the IP address of the domain controller. Ensure the domain is entered in uppercase.
- Check Also Use SMB information for Linux Authentication.
- Check Create Home Directory on Login.
- Check Single Sign-on for SSH.
- Ensure Offline Authentiation is not checked. This option is not compatible with the Linux VDA.

3. Click OK. If prompted to install some packages, click Install.
4. If a domain controller is found, it will ask whether you want to join the domain. Click Yes.
5. When prompted, enter the credentials of a domain user with permission to add computers to the domain and click OK.
6. A message indicating success is displayed.
7. If prompted to install some samba and krb5 packages, click Install.

YaST may have indicated that these changes will require some services to be restarted or the machine needs to be rebooted. It is advisable to reboot:

```
su -

reboot
```

SLED/SLES 12 Only: Patch Kerberos credential cache name

SLED/SLES 12 has changed the default Kerberos credential cache name specification from the usual FILE:/tmp/krb5cc_%{uid} to DIR:/run/user/%{uid}/krb5cc. This new DIR caching method is not compatible with the Linux VDA and must be manually changed. As root, edit /etc/krb5.conf and add the following setting under the [libdefaults] section if not set:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

Verify domain membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory.

Verify that the machine is joined to a domain using Samba's net ads command:

```
sudo net ads testjoin
```

Verify additional domain and computer object information with:

```
sudo net ads info
```

Verify the Kerberos configuration

To verify Kerberos is configured correctly for use with the Linux VDA, check that the system keytab file has been created and contains valid keys:

```
sudo klist –ke
```

This should display the list of keys available for the various combinations of principal names and cipher suites. Run the Kerberos kinit command to authenticate the machine with the domain controller using these keys:

```
sudo kinit -k MACHINE\$@REALM
```

The machine and realm names must be specified in uppercase, and the dollar sign ($) must be escaped with a backslash (\) to prevent shell substitution. In some environments, the DNS domain name is different from the Kerberos realm name; ensure the realm name is used. If this command is successful, no output is displayed.

Verify that theTGT ticket for the machine account has been cached using:

```
sudo klist
```

Examine the machine account details using:

```
sudo net ads status
```

Verify user authentication

Use the wbinfo tool to verify that domain users can authenticate with the domain:

```
wbinfo --krb5auth=domain\\username%password
```

The domain specified here is the AD domain name, not the Kerberos realm name. For the bash shell, the backslash (\) character must be escaped with another backslash. This command will return a message indicating success or failure.

To verify that the Winbind PAM module is configured correctly, logon locally with a domain user account that has not logged onto the machine previously:

```
ssh localhost -l domain\\username
```

```
id -u
```

Check that a corresponding Kerberos credential cache file was created for the uid returned by the id -u command:

```
ls /tmp/krb5cc_uid
```

Check that the tickets in the user's Kerberos credential cache are valid and not expired:

```
klist
```

Exit the session:

```
exit
```

A similar test can be performed by logging onto the Gnome or KDE console directly.

Quest authentication service

Configure Quest on Domain Controller

This assumes you have installed and configured the Quest software on the Active Directory domain controllers, and have been granted administrative privileges to create computer objects in Active Directory.

Enable Domain Users to Logon to Linux VDA Machines

For each domain user that needs to establish HDX sessions on a Linux VDA machine:

1. In the Active Directory Users and Computers management console, open Active Directory user properties for that user account.
2. Select Unix Account tab.
3. Check Unix-enabled.
4. Set the Primary GID Number to the group ID of an actual domain user group.

> **Note**
>
> These instructions are equivalent for setting up domain users for logon using the console, RDP, SSH or any other remoting protocol.

Configure Quest on Linux VDA

Configure VAS daemon

Auto-renewal of Kerberos tickets needs to be enabled and disconnected; authentication (offline logon) needs to be disabled:

```
sudo /opt/quest/bin/vastool configure vas vasd \
                auto-ticket-renew-interval 32400
sudo /opt/quest/bin/vastool configure vas vas_auth \
                allow-disconnected-auth false
```

This sets the renewal interval to 9 hours (32400 seconds) which is an hour less than the default 10 hour ticket lifetime. Set this parameter to a lower value on systems with a shorter Kerberos ticket lifetime.

Configure PAM and NSS

Quest requires that PAM and NSS be manually configured to enable domain user login via HDX and other services such as su, ssh, and RDP. To configure PAM and NSS:

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
```

Join Windows Domain

Join the Linux machine to the Active Directory domain using the Quest vastool command:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

The user is any domain user with permissions to join computers to the Active Directory domain. The domain-name is the DNS name of the domain; for example, example.com.

Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory. To verify that a Quest-joined Linux machine is on the domain:

```
sudo /opt/quest/bin/vastool info domain
```

If the machine is joined to a domain, the domain name is returned. If not joined, you will see the following error:

```
ERROR: No domain could be found.

ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm

default_realm not configured in vas.conf. Computer may not be joined to domain
```

Verify User Authentication

To verify that Quest can authenticate domain users using PAM, logon with a domain user account that has not logged onto the machine previously:

```
ssh localhost -l domain\\username

id -u
```

Check that a corresponding Kerberos credential cache file was created for the uid returned by the id -u command:

```
ls /tmp/krb5cc_uid
```

Check that the tickets in user's Kerberos credential cache are valid and not expired:

```
/opt/quest/bin/vastool klist
```

Exit the session:

```
exit
```

A similar test can be performed by logging onto the Gnome or KDE console directly.

Centrify DirectControl

Join Windows Domain

With the Centrify DirectControl Agent installed, join the Linux machine to the Active Directory domain using the Centrify **adjoin** command:

```
su –

adjoin -w -V -u user domain-name
```

The **user** parameter is any Active Directory domain user with permissions to join computers to the Active Directory domain. The domain-name parameter is the name of the domain to join the Linux machine to.

Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory. To verify that a Centrify-joined Linux machine is on the domain:

```
su –

adinfo
```

Check that the **Joined to domain** value is valid and the **CentrifyDC mode** returns **connected**. If the mode remains stuck in the starting state, then the Centrify client is experiencing server connection or authentication problems.

More comprehensive system and diagnostic information is available using:

```
adinfo --sysinfo all

adinfo –diag
```

To test connectivity to the various Active Directory and Kerberos services:

```
adinfo --test
```

Configure Linux machine catalog and delivery group

The process for creating machine catalogs and adding Linux VDA machines is very similar to the traditional Windows VDA approach. Refer to the Citrix Product documentation for a more complete description of how to complete these tasks.

For creating machine catalogs that contain Linux VDA machines, there are a few restrictions that differentiates the process from creating machine catalogs for Windows VDA machines:

- For operating system, select:
  - Window Server OS or Server OS option for a hosted shared desktops delivery model.
  - Windows Desktop OS or Desktop OS option for a VDI dedicated desktop delivery model.
- Ensure machines are set as not power managed.
- As PVS and MCS are not supported for Linux VDAs, choose the **Another service or technology** (existing images) deployment method.
- Do not mix Linux and Windows VDA machines in the same machine catalog.

> **Note**
>
> Early versions of Citrix Studio did not support the notion of a "Linux OS"; however, selecting the Windows Server OS or Server OS option implies an equivalent hosted shared desktops delivery model. Selecting the Windows Desktop OS or Desktop OS option implies a XenDesktop single user per machine delivery model.

The Citrix documentation for creating machine catalogs is referenced below:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Earlier versions of XenDesktop are not supported.

> **Tip**
>
> If a machine leaves and is rejoined to the Active Directory domain, the machine will need to be removed and re-added again to the machine catalog.

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical for Windows VDA machines. Refer to the online Citrix Product documentation for a more complete description of how to complete these tasks.

For creating delivery groups that contain Linux VDA machine catalogs, the following restrictions apply:

- For delivery type, select Desktops. Linux VDA machines do not support application delivery.
- Ensure the AD users and groups you select have been properly configured to logon to the Linux VDA machines.
- Do not allow logon of unauthenticated (anonymous) users.
- Do not mix the delivery group with machine catalogs that contain Windows machines.

The Citrix documentation for creating delivery groups is referenced below:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Earlier versions of XenDesktop are not supported.

Install the Linux VDA software

If you have previously installed a version of the Linux VDA older than v1.0, you should uninstall it before installing the new version.

Stop the Linux VDA services:

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

Uninstall the package:

```
sudo rpm -e XenDesktopVDA
```

> ## Important
>
> Upgrading from the Tech Preview to versions 1.0, 1.1, 1.2, or 1.3 is not supported.

> ## Note
>
> Starting with version 1.3, the installation path as changed. In previous releases, installation components were located in **/usr/local/**; the new location is **/opt/Citrix/VDA/**.
>
> To execute a command, the full path is needed; alternately, you can add **/opt/Citrix/VDA/sbin** and /opt/Citrix/VDA/bin to the system path.

Install the Linux VDA software using the RPM package manager:

For SuSE 11:

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

For SuSE 12:

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

If you have previously installed v1.1 of the Linux VDA, upgrade the Linux VDA software using the RPM package manager:

For SuSE 11:

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

For SuSE 12:

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

> **Important**
>
> You must reboot the Linux VDA machine after upgrading.

After installing the package you will need to configure the Linux VDA by running the **ctxsetup.sh** script. If you have upgraded the package you will need to run the ctxsetup.sh script to finalize your upgrade. Before making any changes, this script will verify the environment and ensure all dependencies are installed. If required, this script can be re-run at any time to change settings.

The script can either be run manually with prompting or automatically with pre-configured responses. Review help about this script before proceeding:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

Prompted configuration

Run a manual configuration with prompted questions:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Automated configuration

For an automated install, the options required by the setup script can be provided with environment variables. If all of the required variables are present then the script will not prompt the user for any information, allowing the installation process to be scripted.

Supported environment variables include:

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - The Virtual Delivery Agent supports specifying a Delivery Controller name using a DNS CNAME record. This is typically set to N.
- CTX_XDL_DDC_LIST = list-ddc-fqdns – The Virtual Delivery Agent requires a space-separated list of Delivery Controller Fully Qualified Domain Names
- (FQDNs) to use for registering with a Delivery. At least one FQDN or CNAME alias must be specified.
- CTX_XDL_VDA_PORT = port-number – The Virtual Delivery Agent communicates with Delivery Controllers using a TCP/IP port. This is typically port 80.
- CTX_XDL_REGISTER_SERVICE = Y | N - The Linux Virtual Desktop services support starting during boot. This is typically set to Y.
- CTX_XDL_ADD_FIREWALL_RULES = Y | N – The Linux Virtual Desktop services require incoming network connections to be allowed through the system firewall. You can automatically open the required ports (by default ports 80 and 1494) in the system firewall for the Linux Virtual Desktop. This is typically set to Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 – The Virtual Delivery Agent requires Kerberos configuration settings to authenticate with the Delivery Controllers. The Kerberos configuration is determined from the installed and configured

Active Directory integration tool on the system. Specify the supported Active Directory integration method to use:
  - 1 - Samba Winbind
  - 2 - Quest Authentication Service
  - 3 – Centrify DirectControl
- CTX_XDL_HDX_3D_PRO= Y | N – Linux Virtual Desktop supports HDX 3D Pro, a set of graphics acceleration technologies designed to optimize the virtualization of rich graphics applications. HDX 3D Pro requires a compatible NVIDIA Grid graphics card to be installed. If HDX 3D Pro is selected the Virtual Delivery Agent will be configured for VDI desktops (single-session) mode – (i.e. CTX_XDL_VDI_MODE=Y). This is not supported on SUSE. Ensure this value is set to N.
- CTX_XDL_VDI_MODE= Y | N - Whether to configure the machine as a dedicated desktop delivery model (VDI) or hosted shared desktop delivery model. For HDX 3D Pro environements this needs to be set to Y. This is typically set to N.
- CTX_XDL_SITE_NAME= dns-name – The Virtual Delivery Agent discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS search results to a local site, a DNS site name may be specified. This is typically empty [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers – The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with LDAP port (e.g. ad1.mycompany.com:389). This is typically empty [none].
- CTX_XDL_SEARCH_BASE= search-base – The Virtual Delivery Agent by default queries LDAP using a search base set to the root of the Active Directory Domain (e.g. DC=mycompany,DC=com), however to improve search performance, a search base may be specified (e.g. OU=VDI,DC=mycompany,DC=com). This is typically empty [none].
- CTX_XDL_START_SERVICE = Y | N - Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. This is typically set to Y.

> **Note**
>
> HDX 3D Pro is not currently available on SUSE.

Set the environment variable and run the configure script:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers
```

```
export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

You must provide the **-E** option with **sudo** to pass the existing environment variables to the new shell it creates. Citrix recommends that you create a shell script file from the commands above with **#!/bin/bash** on the first line.

Alternatively, all parameters can be specified with a single command:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
    CTX_XDL_DDC_LIST=list-ddc-fqdns \
    CTX_XDL_VDA_PORT=port-number \
    CTX_XDL_REGISTER_SERVICE=Y|N \
    CTX_XDL_ADD_FIREWALL_RULES=Y|N \
    CTX_XDL_AD_INTEGRATION=1|2|3 \
    CTX_XDL_HDX_3D_PRO=Y|N \
    CTX_XDL_VDI_MODE=Y|N \
    CTX_XDL_SITE_NAME=dns-name \
    CTX_XDL_LDAP_LIST=list-ldap-servers \
    CTX_XDL_SEARCH_BASE=search-base \
    CTX_XDL_START_SERVICE=Y|N \
    /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Remove configuration changes

In some scenarios it may be necessary to remove the configuration changes made by the **ctxsetup.sh** script without uninstalling the Linux VDA package.

Review help about this script before proceeding:

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

To remove configuration changes:

```
sudo /usr/local/sbin/ctxcleanup.sh
```

> ### Important
>
> This script will delete all configuration data from the database and will make the Linux VDA inoperable.

Configuration logs

The **ctxsetup.sh** and **ctxcleanup.sh** scripts will display errors on the console, with additional information written to a configuration log file:

/tmp/xdl.configure.log

Restart the Linux VDA services to have the changes take effect.

Run the VDA software

Once you have configured the Linux VDA using the ctxsetup.sh script, you use the following commands to control the Linux VDA.

To start the Linux VDA services:

sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start

To stop the Linux VDA services:

sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop

To restart the Linux VDA services:

sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start

To check the running state of the Linux VDA services:

sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status

Uninstall the Linux VDA software

To check whether the Linux VDA is installed and to view the version of the package installed:

rpm -q XenDesktopVDA

To view more detailed information:

rpm –qi XenDesktopVDA

To uninstall the Linux VDA package:

sudo rpm -e XenDesktopVDA

> **Note**
>
> Uninstalling the Linux VDA software will delete the associated PostgreSQL and other configuration data. However, the PostgreSQL package and other dependent packages that were setup prior to the installation of the Linux VDA will not be removed.

This article does not cover the removal of dependent packages including PostgreSQL.

Troubleshooting

Linux VDA v1.3 adds H264 and a HardwareEncoding value in the registry path HKLM\Software\Citrix\Ica\Session\<session id>\Graphics to help troubleshoot graphics issues encountered with the VDA.

Run the following command to advertise H.264 encoding in a Linux VDA before a session is launched:

/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"AdvertiseH264" -d "0x00000001" --force

Launch the session and check whether the key H264 is created in the registry path, if so, H.264 encoding is in use.

/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"

3D Pro hardware encoding is disabled by default, use the command below to enable the function:

/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"HardwareEncoding" -d "0x00000001" --force

Launch the session and check the value of "HardwareEncoding" in the registry path; 0 means not in use, 1 means hardware encoding is being used.

```
/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

Use the command below to query your session ID:

```
/opt/Citrix/VDA/bin/ctxqsession
```

Currently, the Linux VDA does not allow the user to choose the desktop environment when logging in; to workaround this issue, the user can configure a file (for example, .xsession) for the Linux distribution to set the default desktop environment for each user. Refer to the documents accompanying the Linux distribution for more information.

To se the KDE as the default environment:

```
#! /usr/bin/env bash

exec startkde
```

To set GNOME as the default desktop envionment:

```
#! /usr/bin/env bash

exec gnome-session
```

The most common issues are a direct result of Linux machine misconfiguration, mainly around networking, NTP time server configuration or Active Directory domain membership. Fixing the Linux machine's configuration will often resolve issues with the VDA software.

The Broker Agent and the HDX Service log to syslog. Citrix Support provides a set of tools that can enable additional trace during a support call.

HDX Service Logging

The HDX Service is configured to log syslog out-of-the-box messages and no further configuration is needed.

Broker Agent logging

The Broker Agent (also known as the ctxvda service) writes log da?ta to syslog via network sockets. This may not be configured out-of-the-box. To enable the Broker Agent logging to syslog logging, the following configuration is required:

SLED/SLES 11

Edit the /etc/syslog-ng/syslog-ng.conf file and add the following line in the s_sys section:

```
udp(ip(127.0.0.1) port(514));
```

Save and close the syslog-ng.conf file. Restart the syslog-ng service apply the change:

sudo service syslog-ng restart

SLED/SLES 12

Edit the /etc/rsyslog.conf file and add the following lines:

$ModLoad imudp

$UDPServerRun 514

Save and close the rsyslog.conf file. Restart the rsyslog service apply the change:

sudo service rsyslog restart

Ensure you have no orphaned processes which might be preventing new sessions from starting:

sudo pkill -9 ctxhdx

sudo pkill -9 ctxgfx

sudo pkill -9 ctxlogin

sudo pkill -9 ctxvfb

Restart the Linux VDA services and retry connection.

Check the file ownership and permission of the following directories and files:

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

Check that the volume control on the device running the Citrix Receiver as well as the Linux desktop are not muted or set to a low level.

Check that audio is enabled on the Linux VDA. Use the ctxreg tool to query the value of the configuration item fDisableCam:

sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam

A value of 0x1 means audio is disabled. To enable, set fDisableCam to 0x0:

sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000

If audio is still not being heard check that the Citrix audio sink is loaded by pulseaudio. This PulseAudio module is loaded into the pulseaudio daemon at session start. Use the pacmd tool to check the Citrix audio sink is loaded:

pacmd list-sinks

If the Citrix audio sink is loaded, the output should be:

name: <CitrixAudioSink>

driver: <module-ctx-sink.c>

If Citrix audio sink is not loaded, kill the ctxaudio process and restart it.

Check that audio is enabled on the Linux VDA and audio recording is enabled on the ICA client. If audio is still not being recorded check that the Citrix audio source is loaded by pulseaudio. If audio recording is enabled on the ICA client, this PulseAudio module will be loaded into the pluseaudio daemon at session start. Use the pacmd tool to check the Citrix audio source is loaded:

pacmd list-sources

If the Citrix audio source is loaded, the output should be:

name: <CitrixAudioSource>

driver: <module-ctx-source.c>

If the Citrix audio source is not loaded, kill the ctxaudio process and restart it.

There are a number of items to check if printing is not working correctly. The print daemon is a per session process and should be running for the length of the session. Check that the printing daemon is running.

ps –ef | grep ctxlpmngt

If the ctxlpmngt process is not running manually start ctxlpmngt from a command line.

If printing is still not working the next item to check in the CUPS framework. The ctxcups service is for printer management and communicates with the Linux CUPS framework. This is a single process per machine and can be checked by:

service ctxcups status

If the service is not running, start it manually:

service ctxcups start

Garbled output can be caused by an incompatible printer driver. A per user driver configuration is available and can be configured by editing the ~/.CtxlpProfile configuration file.

[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=

The printername is a field containing the name of the current client side default printer. This is a read-only value and shoud not be edited.

> ## Important
>
> The fields **ppdpath**, **model** and **drivertype** should not be set at the same time as only one takes effect for the mapped printer.

If the Universal Printer driver is not compatible with the client printer, the model of native printer driver can be configured with the model= option. The current model name of the printer can be found with the lpinfo command.

lpinfo –m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

...

The model can then be set to match the printer:

Model=xerox/ph3115.ppd.gz

If the Universal Printer driver is not compatible with client printer, the ppd file path of native printer driver can be configured. The value of ppdpath is the absolute path of native printer driver file.

For example, there is a ppd driver under /home/tester/NATIVE_PRINTER_DRIVER.ppd.

ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd

There are three types of Universal Printer Driver supplied by Citrix (postscript, pcl5 and pcl6). These can configured in the driver type if no native printer driver is available.

For example, if client default printer driver type is PCL5.

drivertype=pcl5

> ## Note
>
> Citrix Receiver for Mac and Citrix Receiver for Linux only support Postscript printers and so the PCL5 and PCL6 Universal Printer Drivers are not applicable. In this situation, ppdpath or the model of native printer driver has to be set to a non-Postscript printer.

CDM does not work

The CDM feature includes a daemon process (ctxcdmd); if the CDM feature fails, reboot the Linux VDA machine and verify whether the daemon launched correctly:

```
Ps -lef | grep ctxcdmd
```

The file naming in the mapped drive should follow the VDA and Receiver OS naming rules.

Known issues

Citrix Receiver for Android CAPS LOCK state can be reversed when session roaming

The CAPS LOCK state may be lost when roaming an existing connection to the Citrix Receiver for Android. The workaround is to use the shift key on the extended keyboard to switch between upper case and lower case.

Shortcut keys with ALT do not always work when connecting to a Linux VDA using Citrix Receiver for Mac

Citrix Receiver for Mac sends AltGr for both left and right Options/Alt keys by default. It is possible to change this within the Citrix Receiver settings but the results vary with different applications.

Newer X client libraries can cause keyboard issues on SuSE Linux Enterprise Desktop 11

Newer versions of the xorg-x11-libX11 packages on SuSE Linux Enterprise Desktop 11 may have problems handling keyboard mapping changes, which in turn may cause issues with keyboard functionality inside an HDX session. This can happen when the installed version of the packages is in the range 7.4-5.11.11.1 to 7.4-5.11.15.1.

The workaround is to rollback to the stock SP3 version of the xorg-x11-libX11 package, this enables keyboard mapping changes to work as normal. For example:

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm –i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

This needs to be done before a user logs on to the machine – if this is done while a session is active, these settings will not take affect until the user next logs in.

If upgrading from stock SP3, the above xorg-x11-libX11 packages can be locked to the current installed version so that they won't be changed during the upgrade. Before upgrading, run the following before proceeding with the upgrade as normal:

```
zypper al xorg-x11-libX11

zypper al xorg-x11-libX11-32bit
```

Long session launches may occur when using Linux VDA with a Delivery Controller from XenDesktop v7.1

The slow launch is caused by the presence of CGP settings in the ICA file generated by the v7.1 Delivery Controller. When these settings are present, Citrix Receiver attempts to establish a connection on TCP port 2598. The default firewall

settings on some Linux distributions, such as SLED 12, is to drop the TCP SYN packets, resulting in a timeout and hence a long session launch. The workaround is to configure the firewall on the Linux VDA to reject the TCP SYN on port 2598. This issue has been addressed in newer versions of the Delivery Controller.

Registration fails when Linux VDA is rejoined to the domain

Under certain circumstances, when a Linux VDA is rejoined to the domain and a fresh set of Kerberos keys are generated, the Broker fails to establish a security context with the VDA. This is often caused by the Broker using a cached out-of-date VDA service ticket based on the previous set of Kerberos keys. This won't stop the VDA from connecting to the Broker, but the Broker will not be able to establish a return security context to the VDA. The usual symptom is that the VDA registration fails.

This problem will eventually resolve itself when the VDA service ticket eventually expires and is renewed, but service tickets are usually long-lived. This could potentially take an inordinate amount of time..

The solution is to clear the Broker's ticket cache. You could simply reboot the Broker or run the following on the Broker from a command prompt as Administrator:

```
klist -li 0x3e4 purge
```

This will purge all service tickets in the LSA cache held by the Network Service principal under which the Citrix Broker Service runs. This will remove service tickets for other VDAs and potentially other services. However, this is harmless – these service tickets will simply be reacquired from the KDC when needed again.

Audio plug-n-play not supported

It is recommended that any audio capture device is connected to the client machine before starting to record audio in the ICA session. If a device is attached after the audio recording application has started the application may become unresponsive. If this issue occurs just restart the application. A similar issue may occur if a capture device is unplugged while recording.

Audio Distortion

Windows 10 Receiver may experience audio distortion during audio recording.

CTXPS driver isn't compatible with some PLC printers

If you see printing output corruptions set the printer driver to native printer driver provided by the manufacturer.

Slow printing performance for large documents

When you print a large document on a local client printer, the print file is transferred over the server connection. On slow connections, this may take a long time.

Printer and print job notifications seen from other sessions

Linux does not have the same session concept as the Windows Operating system. Therefore all users get system wide notifications. The administrator can disable these notifications by modifying the CUPS configuration file, /etc/cups/cupsd.conf.

Find the current policy name configured in the file:

```
DefaultPolicy default
```


If the policy name is default, then add the following lines into default policy XML block.

```
<Policy default>
    # Job/subscription privacy...
    JobPrivateAccess default
    JobPrivateValues default
    SubscriptionPrivateAccess default
    SubscriptionPrivateValues default
    ... ...
    <Limit Create-Printer-Subscription>
        Require user @OWNER
        Order deny,allow
    </Limit>
     <Limit All>
        Order deny,allow
        </Limit>
    </Policy>
```

Glossary

Broker - XenDesktop component responsible for brokering HDX sessions to the different VDAs within a XenDesktop deployment. Also known as the DDC or XenDesktop Controller.

Broker Agent - Component on the Linux VDA machine providing the desktop to be delivered. The Broker Agent communicates with the Broker to enable the brokering of sessions. It is composed of two key components, the VDA Service and the HDX Service.

Citrix Director - Citrix helpdesk/support console for monitoring and controlling XenDesktop VDAs.

Citrix Studio - Citrix administration console used to configure XenDesktop.

DDC - XenDesktop Desktop Delivery Controller. Also known as the Broker or Delivery Controller.

FQDN – Fully Qualified Domain Name

HDX - High Definition Experience protocol. Formerly known as the Citrix ICA protocol.

HDX Service - The Linux service (ctxhdx) that remotes the virtual Linux desktop via the HDX protocol. It communicates with the VDA service to enable the brokering of sessions.

RHEL - Red Hat Enterprise Linux. A commercial Linux distribution provided by Red Hat.

SLED - SUSE Linux Enterprise Desktop. A commercial Linux distribution provided by Novell.

SLES - SUSE Linux Enterprise Server. A commercial Linux distribution provided by Novell.

VDA - Virtual Delivery Agent.

VDA Service - The Linux service (ctxvda) that communicates with the Broker to enable the brokering of sessions. It also communicates with the HDX Service for remote session delivery.

Create a Site

Jun 01, 2016

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 (if used), plus the Machine Catalogs and Delivery Groups you create and manage. 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 by selecting **Configuration** in the Studio navigation pane, then the Product Support tab, and following the guidance. For CEIP details, see http://more.citrix.com/XD-CEIP.

The user who creates a Site becomes a Full Administrator; for more information, see the Delegated Administration article.

Review this article before you start the Site creation wizard; it includes tasks to complete and decisions to consider before actually creating the Site.

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:

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*).

The **Databases** page contains selections for setting up the Site, Monitoring, and Configuration Logging databases. For details about database setup choices and requirements, see the Databases article.

When you create a Site, if you choose to install the SQL Server Express database for use as the Site database (which is the default setting), a restart will occur after that database software is installed. That restart will not occur if you choose not to install the SQL Server Express software for use as the Site database.

If you will not be using a default SQL Server Express Edition installation, make sure the SQL Server software is installed on

the machines before you create a Site; the System requirements article lists the supported versions.

If you want to add more Delivery Controllers to the Site, and have already installed the Controller software on other servers, you can add them to the Site from this page in the Site creation wizard. If you plan to generate scripts that will set up the databases, add the Controllers before you generate the scripts.

Consider whether you will use existing licenses or the 30-day free trial license that allows you to add license files later. You can also add or download license files from within the Site creation wizard. For more information, see the Licensing documentation.

Specify the License Server address in the form *name*:[*port*]. The name must be a Fully Qualified Domain Name (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.

See the Remote PC Access section below.

If you will be using VMs on a host (hypervisor or cloud service) to provide applications and desktops, you can optionally create (configure) the first connection to your host when you create a Site. You can also specify storage and network resources for that connection. You can modify this connection and resources later, and create additional connections.

Important: Use the Connections and resources article for guidance when configuring connection and resources information in the Site creation wizard:

- Connection type information sources indicates where to find information about each supported connection type.
- Host storage describes the storage types and storage management methods.
- Storage management and Storage selection describe how to configure storage information when creating a connection.

If you are not using VMs on a hypervisor or cloud service to provide applications and desktops (or if you will use Studio to manage user desktops hosted 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** host type.

On the **Connection** page, also specify whether you will use Citrix tools (such as Machine Creation Services) or other tools to create VMs on the host.

On the **Storage** and **Network** pages, configure the requested information, using guidance from the information sources linked above.

Reminder: The Connections and resources article contains detailed guidance.

You can select additional features to customize your Site. When you select the check box for an item that requires information, a configuration box appears.

AppDNA Integration

If you will be using AppDisks and have installed AppDNA, select this feature to allow analysis of applications in the AppDisks, review compatibility issues, and then take remedial actions to resolve those issues. For more information, see the AppDisks article.

App-V Publishing

Select this feature if you will use applications from Microsoft App-V packages that are located on App-V servers. When you select this check box, you are prommpted to provide the URL of the App-V management server, and the URL and port number of the App-V publishing server.

If you will 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 the App-V article.

For information about Remote PC Access deployments, see the Remote PC Access article.

If you are using the Wake on LAN feature, complete the configuration steps on the Microsoft System Center Configuration Manager before creating the Site. For details, see the Microsoft System Center Configuration Manager article.

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 of the wizard.

  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 machine accounts, and then click **Add machine accounts**. Click **Add OUs**. Select the domain and Organizational Units, and indicate if items in subfolders should be included. Click **Add OUs**.

Note: When you create a Remote PC Access Site, a Machine Catalog named Remote PC User Machine Accounts is created automatically, containing all the machine accounts you added in the Site creation wizard. A Delivery Group named Remote PC User Desktops is created automatically, containing all the users and user groups you added.

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've finished, click **Create** and the Site creation will begin.

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, and then click **Test site** in the center pane. You can view an HTML report of the Site test results.

Create Machine Catalogs

Jul 27, 2016

Collections of physical or virtual machines are managed as a single entity called a *Machine Catalog*. All of the machines in a Machine 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 Machine Catalog, Studio guides you to create your first Delivery Group. Later, you can change the catalog you created, and create more catalogs.

Overview

When you create a catalog that will contain VMs, you specify how those VMs will be provisioned: you can use tools supported by Studio, such as Machine Creations Services (MCS) or Provisioning Services, or you can use your own tools to provide machines. If your machines are already provided for you (so you do not need to use master images), you still create one or more Machine Catalogs for your machines.

- If you are using Provisioning Services to create machines, see the Provisioning Services documentation for instructions.
- If you choose MCS to provision VMs, you provide a master image (or snapshot) as a guide to create identical VMs in the catalog. Before you create the catalog, you first use tools on your hypervisor or cloud service to create and configure the master image - this includes installing a Virtual Delivery Agent (VDA) on the image. Then, when you create the Machine Catalog in Studio, you select that image (or a snapshot of it), specify the number of VMs to create in the catalog, and configure additional information.

When using MCS or PVS to create your first Machine Catalog, you use the host connection that you configured when you created the Site. Later (after you create your first Machine Catalog and Delivery Group), you can change information about that connection or create additional connections.

After you complete the Machine Catalog creation wizard, tests run automatically to ensure that it is configured correctly. When the tests complete, you can view a test report. Later, you can run the tests at any time from **Citrix Studio** *site-name* in the Studio navigation pane.

Tip: If you are creating 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.

If you have Windows XP or Windows Vista machines, they must use an earlier VDA version, and will not be able to use the latest product features. If you cannot upgrade those machines to a supported Windows operating system version, Citrix recommends you keep them in a separate Machine Catalog.

Here's a brief overview of MCS actions after you provide information in the Create Machine Catalog wizard.

- If you selected a master image (rather than a snapshot) in the wizard, MCS creates a snapshot.
- MCS creates a full copy of the snapshot and places this on each storage location defined in the host connection.
- MCS adds the desktops 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 VMs just created.
- 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 required. Each VM gets a difference disk. This is the disk that 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.

Prepare a master image on the hypervisor or cloud service

Tip: For information about creating connections to hypervisors and cloud providers, see the Connections and resources article.

The master image contains the operating system, non-virtualized applications, VDA, and other software.

Good to know:

- A master image might also be known as a clone image, golden image, base VM, or base image. Host vendors and cloud service providers may use different terms.
- When using Provisioning Services, you can use a master image or a physical computer as the master target device. Provisioning Services uses different terminology than MCS to refer to images; see its documentation for details.
- Make sure your host has sufficient processors, memory, and storage to accommodate the number of machines you will create.
- Configure the correct amount of hard disk space required for desktops and applications, because 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, your 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 will cause 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 because it significantly reduces costs by eliminating the need to update the master image after adding or reconfiguring an application. In addition, 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, and you will 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 Provisioning Services or MCS, do not run Sysprep on master images.

To prepare a master image:

1. Using your hypervisor's management tool, create a new master image and then install the operating system, plus all service packs and updates. Specify the number of vCPUs (you can also specify this value when you create the Machine Catalog, but only when using PowerShell; you cannot specify the number of vCPUs in the Studio user interface when creating a catalog). Be sure to configure the amount of hard disk space required for desktops and applications, because that value cannot be changed later or in the Machine Catalog.
2. Make sure that the hard disk is attached at device location 0. Most standard master image templates configure this location by default, but some custom templates may not.
3. Install and configure the software listed above on the master image:
4. When using Provisioning Services, 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. Join the master image to the domain where applications and desktops will be members, and make sure that the master image is available on the host where the machines will be created. Note that joining the master image to a domain is not required if you are using MCS: the provisioned machines are joined to the domain specified in the Create Machine Catalog 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 Machine Catalog, Studio creates a snapshot, but you cannot name it.

When using XenServer for your hosting infrastructure, GPU-capable machines require a dedicated master image. Those VMs require video card drivers that support GPUs, and must be configured 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 Passthough 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.

Create a Machine Catalog using Studio

Before you start the Machine Catalog creation wizard, review this section to learn about the choices you will make and information you will supply. When you start the wizard, some of the pages described below may not appear or they may have different titles, based on the selections you make.

Important: If you are using a master image, make sure you have installed a VDA on the image before creating the Machine Catalog.

From Studio:

- If you have created a Site but haven't yet created a Machine Catalog, Studio will guide you to the correct starting place to create a Machine Catalog.
- If you have already created a Machine Catalog and want to create another, select **Machine Catalogs** in the Studio navigation pane, and 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 selections you make.

Each catalog contains machines of only one type:

- **Server OS:** A Server OS catalog provides desktops and applications that can be shared by multiple users. The machines can be running supported versions of the Windows or Linux operating systems, but the catalog cannot contain both.
- **Desktop OS:** A Desktop OS catalog provides desktops and applications that are assigned to a variety of 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.

The **Machine Management** page indicates how machines are managed and which tool you will 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 have a connection to a hypervisor or cloud service already configured.
- Machines are not power managed through Studio, for example, physical machines.

If you indicated that machines are power managed through Studio or provisioned through a cloud environment, choose which tool you will use to deploy machines.

- **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.
- **Provisioning Services** – Manages target devices as a device collection. A Provisioning Services 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 you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.

The **Desktop Experience** page (which appears only when creating a catalog containing Desktop OS machines) determines the type of desktops that will be created. The types differ according to whether or not they are assigned to a user, and what happens to any changes the user made when the machine restarts.

There are three types:

- **Pooled, random:** Desktops are assigned randomly – users connect to a new (random) desktop each time they log on. When a user logs off, the desktop becomes available for another user. When the desktop is restarted, any changes that were made are discarded.
- **Pooled, static:** Desktops are permanently assigned – users connect to the same (static) desktop each time they log on. When that user logs off, the desktop remains available only for that user. When the desktop is restarted, any changes

that were made are discarded.
- **Dedicated:** Desktops are permanently assigned to a user. When that user logs off, the desktop remains available only for that user. When the desktop is restarted, any changes that were made are retained. You can save changes to a local VM disk or to a specified drive letter on a separate Personal vDisk.

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 Machine Catalog, the only available connection will be the one you configured when you created the Site.

Remember:

- If you are using Provisioning Services or MCS, 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 ensure you can use the latest product features, make sure the master image has the latest VDA version installed. Do not change the default **Select the VDA version installed** selection on the wizard page.

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.

Select one or more security groups for the VMs; these are shown only if the availability zone supports security groups.

Choose whether machines will use shared hardware or account-dedicated hardware.

The title of this page depends on the deployment method you chose on the **Machine Management** page.

- If you chose MCS, this page is titled **Virtual Machines**.
- If you chose Provisioning Services, this page is titled **Device Collection**.
- If you chose Other tools, this page is titled **VMs and users**.

On this page:

- Specify how many virtual machines to create.
- Choose the amount of memory (in MB) each machine will have.
- If you indicated on the **Desktop Experience** page that user changes to dedicated 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 using MCS to deploy machines and creating pooled random VMs that do not use personal vDisks, you can configure a cache to be used for temporary data on each machine. For details, see the following section.

Important: Each VM will have a hard disk. Its size is set in the master image; you cannot change the hard disk size in the catalog.

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.

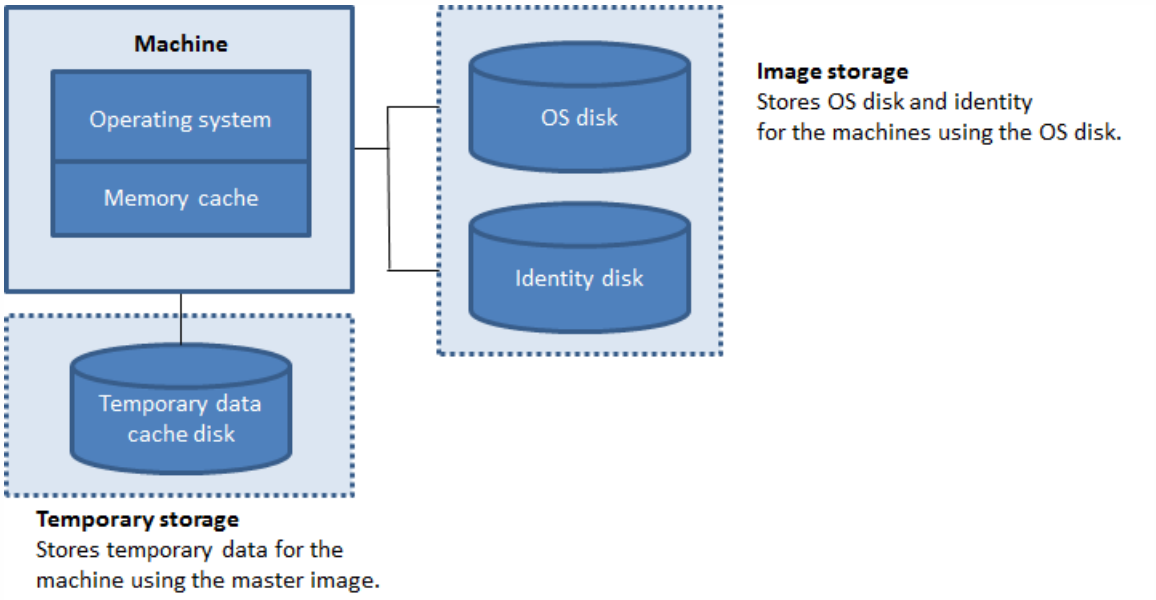
To enable the caching of temporary data, the VDA on each machine in the catalog must be minimum version 7.9.

You specify whether temporary data uses shared or local storage when you create the connection that the catalog uses; for details, see the Connections and resources article. 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.

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** checkbox, 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.

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.)

Caching should not be enabled if you intend to use this catalog to create AppDisks.

You cannot change the cache values in a Machine Catalog after it is created.

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.

(Valid only for 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.

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.

- 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

  ...

  Make sure 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 Provisioning Services, computer accounts for target devices are managed differently; see the Provisioning Services documentation.

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.

Manage Machine Catalogs

May 31, 2016

In this article:

Introduction

You can add or remove machines from a Machine Catalog, as well as 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, anti-virus software updates, operating system upgrades, or configuration changes.

- For Machine Catalogs containing pooled random machines created using Machine Creation Services (MCS), you can maintain machines by updating the master image used in the catalog and then updating the machines. This 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.
- For 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 the Connections and resources article.

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 will be created. Specify an account naming scheme, 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.
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, 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.

The machines are created as a background process, and can take a lot of time when creating a large number of 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 will stop 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.

Move a Machine Catalog to a different zone

If your Site has more than one zone, you can move a catalog from one zone to another.

Caution: 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 Machine 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 Machine 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 Machine Catalogs. Those accounts can then be used for other machines.
- Add accounts so that when more machines are added to the catalog, the computer accounts are already in place. Do not use a forward slash (/) in an OU name.

To manage Active Directory accounts:

1. Select **Machine Catalogs** in the Studio navigation pane.
2. Select a catalog and then select **Manage AD accounts** in the Actions pane.
3. Choose whether to add or delete computer accounts. If you add accounts, specify what to do with the account passwords: either reset them all or enter a password that applies to all accounts. You might reset passwords if you do not know the current account passwords; you must have permission to perform a password reset. If you enter a password, the password will be 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.

Note: 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 an 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, thereby minimizing user downtime. Do not delete, move, or rename master images; otherwise, you will not be able to 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.

Tip: For information about managing connections, see the Connections and resources article.

Before you update the Machine Catalog, either update an existing master image or create a new 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. Review these operating system optimization guides and apply the optimizations for your environment: Windows 7 Optimization Guide and Windows 8/8.1 Virtual Desktop Optimization Guide.
6. Power off the VM.
7. Take a snapshot of the VM, and give the snapshot a meaningful name that will be 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.

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.

Tip: 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 the next shutdown is provided when you are using the Citrix Connector for System Center Configuration Manager.

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.

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 Machine Catalog:

- If you're using Provisioning Services, upgrade the VDA version in the Provisioning Services console.
- Start the upgraded machines so that they register with the Controller. This lets Studio determine that the machines in the Machine Catalog need upgrading.

To upgrade a Machine 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 Machine 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 Machine 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.

Note: If you have Windows XP or Windows Vista machines, they must use an earlier VDA version, and will not be able to use the latest product features. If you cannot upgrade those machines to a currently supported Windows operating system, Citrix recommends you keep them in a separate catalog.

Create Delivery Groups

Jul 22, 2016

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.

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.
- 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.

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.

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.

For more information, see the AppDisks article.

Specify the users and user groups who can use the applications and desktops in the Delivery Group.

Where user lists are specified

Active Directory user lists are specified when you create or edit the following:

- A Site's user access list, which is not configured through Studio. By default, the application entitlement policy rule includes everyone; see the PowerShell SDK BrokerAppEntitlementPolicyRule cmdlets for details.
- Application Groups (if configured).
- Delivery Groups.
- Applications.

The list of users who can access an application through StoreFront is formed by the intersection of the above user lists. For example, to configure the use of application A to a particular department, without unduly restricing access to other groups:

- Use the default application entitlement policy rule that includes everyone.
- Configure the Delivery Group user list to allow all headquarters users to use any of the applications specified in the Delivery Group.
- (If Application Groups are configured) Configure the Application Group user list to allow members of the Administration and Finance business unit to access applications A through L.
- Configure application A's properties to restrict its visibility to only Accounts Receivable staff in Administration and Finance.

Authenticated and unauthenticated users

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types in a Delivery Group.

Authenticated

To access applications and desktops, the users and group members you specify by name must present credentials

such as smart card or user name and password to StoreFront or Citrix 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.

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 authenticated and unauthenticated users	Yes	Yes

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.

- **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.

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.
- Using the radio buttons, indicate who can launch a desktop (for groups with pooled machines) or who will be assigned a machine when they launch the desktop (for groups with assigned machines). The users can be either everyone who can access this Delivery Group, or specific users and user groups.
- If the group contains assigned machines, specify the maximum number of desktops per user. This must be a value of one or greater.
- Enable or disable the desktop (for pooled machines) or desktop assignment rule (for assigned machines). Disabling a desktop stops desktop delivery; disabling a desktop assignment rule stops desktop auto-assignment to users.
- When you are finished with the dialog box, click **OK**.

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

Jun 01, 2016

In this article:

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 the Applications article 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 the Delegated Administration article 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.

Setting	Description
Description	The text that StoreFront uses and that users see.
Enable Delivery Group	Whether or not the Delivery Group is enabled.
Desktops per user	(Assigned desktop OS machines only) The maximum number of shared desktops that a user can have active at the same time. In assign-on-first-use deployments, this value specifies how many desktops users can assign to themselves.
Time zone	
Enable Secure ICA	Secures communications to and from machines in the Delivery Group using SecureICA, which encrypts the ICA protocol (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.

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.
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.

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 Machine 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.

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 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 log on. 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 ten 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.

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 dropdown. 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 dropdown, 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.

Create a restart schedule for machines in a Delivery Group

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.
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** dropdown, 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** dropdown) 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.

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**.

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.

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 the Connections and resources article.

Restrict access to machines in a Delivery Group

Any changes you make to restrict access to machines in a Delivery Group supersede previous settings, regardless of the method you use. You can:

Restrict access for administrators using Delegated Administration scopes. You can create and assign a scope that permits administrators to access all applications, and another scope that provides access to only certain applications. 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.

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.

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, or send a message to Delivery Group users

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then select **View Machines** in the Actions pane.
3. To log a user off a session, select the session or desktop and select **Log off** in the Actions pane. The session closes and the machine becomes available to other users, unless it is allocated to a specific user.
4. To disconnect a session, select the session or desktop, and select **Disconnect** in the Actions pane. Applications continue to run and the machine remains allocated to that user. The user can reconnect to the same machine.
5. To send a message to users, select the session, machine, or user, and then select **Send message** in the Actions pane. Enter the message.

You can configure power state timers for Desktop OS machines to automatically handle unused sessions. See the Power manage machines section for details.

Configure session prelaunch and session linger in a Delivery Group

These features are supported on Server OS machines only.

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.

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 will cause 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.

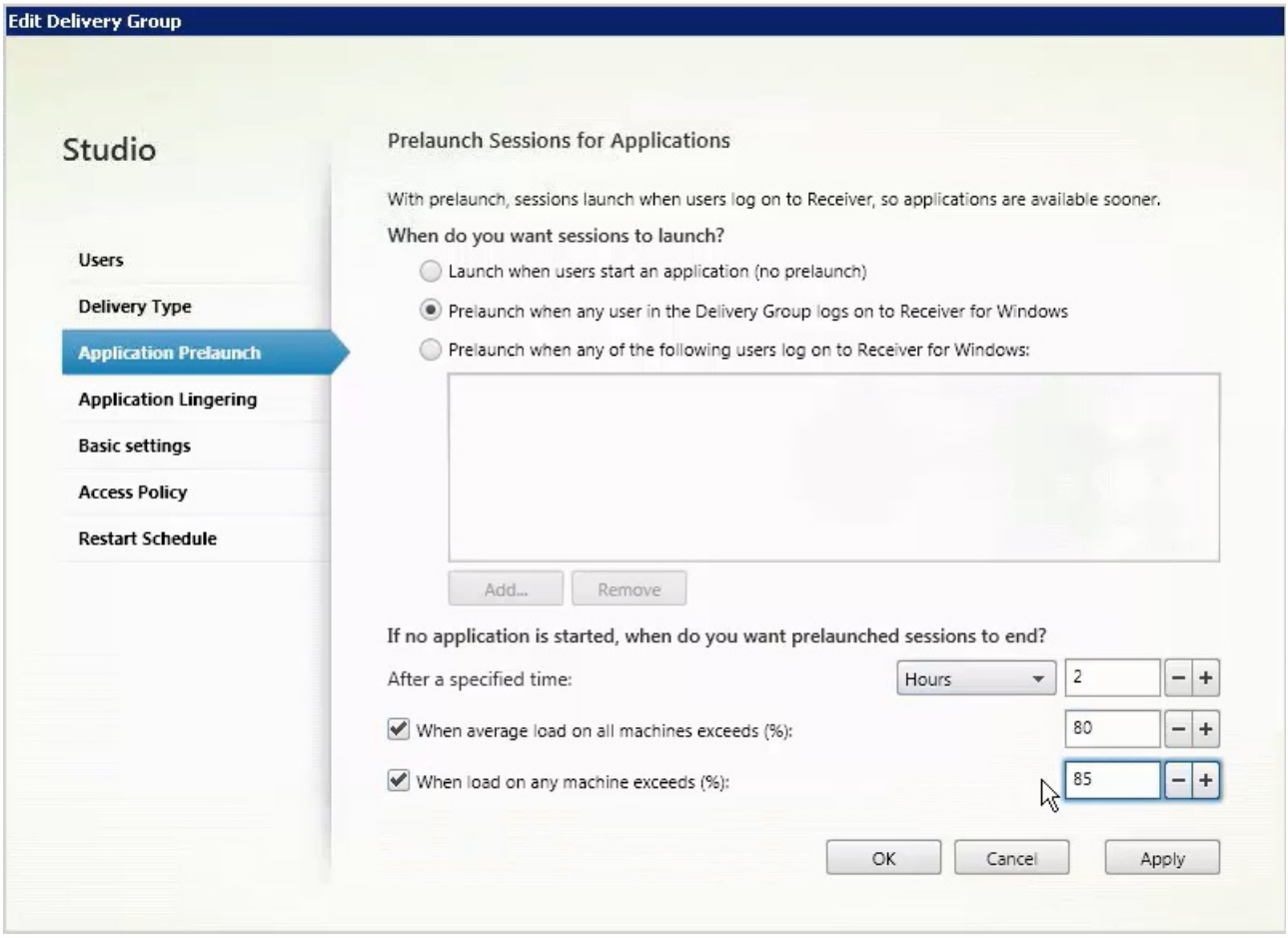
  You cannot disable this timeout from Studio, but you can in the SDK (New/Set-BrokerSessionPreLaunch cmdlet). If you disable the timeout, it will not appear in the Studio display for that Delivery Group or in the Edit Delivery Group wizard.

- **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 will cause prelaunch and lingering sessions to be ended automatically to free capacity.

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.

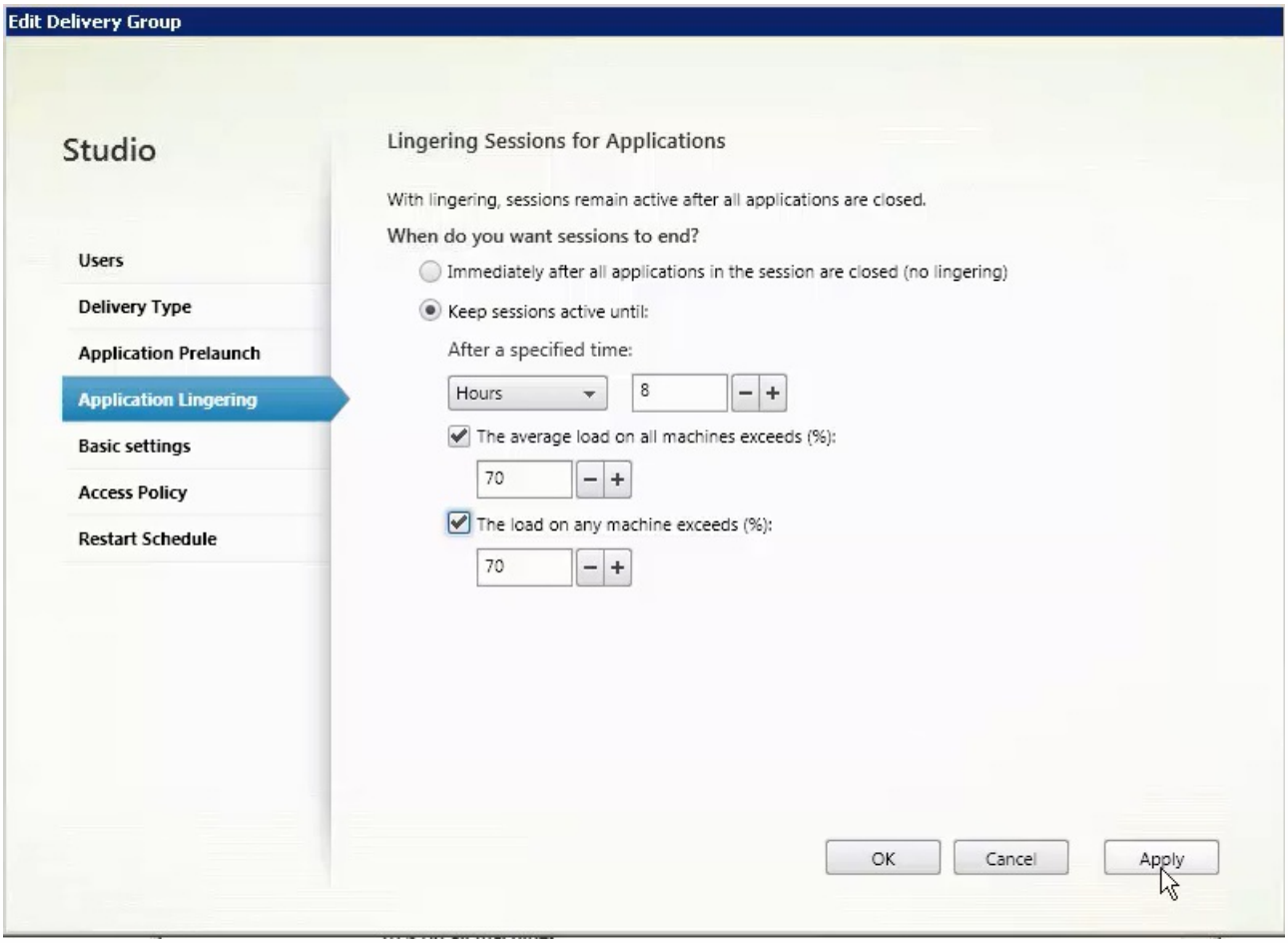


4. A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active.
   - When a specified time interval elapses. You can change 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.

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.



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.

Create Application Groups

Jun 03, 2016

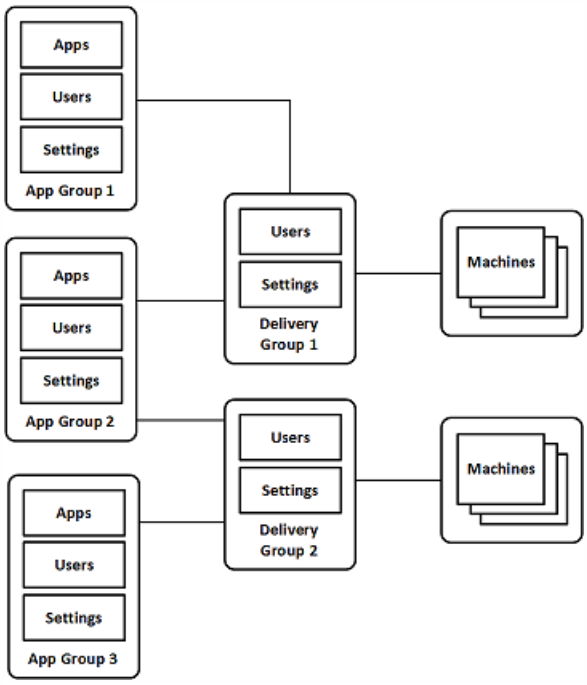
Introduction

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.

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.

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.

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 the Manage Application Groups article.

By default, application session sharing between Application Groups is enabled; see Session sharing between Application Groups below.

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 the Delegated Administration article for details.

This article refers to "associating" an application with more than one Application Group to differentiate that action from adding a new instance of that application from an available source. Similarly, Delivery Groups are associated with Application Groups (and vice versa), rather than being additions or components of one another.

Session sharing between Application Groups

When you use Application Groups, you can allow or prohibit application session sharing between Application Groups. (This extends the standard session sharing behavior available when using only Delivery Groups, as described in the first example below.) Application session sharing saves the costs associated with launching additional application sessions. It also enables the use of application features that involve the clipboard, such as copy-paste operations.

Example when enabling session sharing between Application Groups is helpful:

> A user in Application Group 1 starts an application session by launching Word, and then launches Excel, while Word is still running. If the Controller finds Excel on the same server, the session is shared. (This is the basic session sharing feature that is used in Delivery Groups, if you don't use Application Groups.) If Excel is not found on the same server, and session sharing is enabled for Application Group 1, the Controller then attempts to share the session if the

application is found on another server in the Delivery Groups associated with Application Group 1, or in Application Groups 2 and 3.

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.

IMPORTANT: 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, sharing is not allowed.

Application session sharing between Application Groups must be enabled if you want to use the session prelaunch and session linger features; however, those 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 the Manage Application Groups article.

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.

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.

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.

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:

- 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 Group user list.
- Delivery Group user list.
- 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.

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.

Source	Description
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 (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.

This page appears only if you have previously created a scope. By default, the **All** scope is selected. For more information, see the Delegated Administration article.

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

Jun 01, 2016

In this article:

Introduction

This article describes the procedures for managing Application Groups you created.

See the Applications article for information about managing applications in Application Groups or Delivery Groups, including how to:

- Add or remove applications in an Application Group
- Change an application's group associations

Managing Application Groups requires the Delegated Administration permissions of the Delivery Group Administrator built-in role. See the Delegated Administration article for details.

Enable or disable an Application Group

When an Application Group is enabled, it can deliver the applications that have been added to it. Disabling an Application Group disables each application in that group. However, if those applications are also associated with other enabled Application Groups, they can be delivered from those other groups. Similarly, if the application was explicitly added to Delivery Groups associated with the Application Group (in addition to being added to the Application Group), disabling the Application Group does not affect the applications in those Delivery Groups.

An Application Group is enabled when you create it; you cannot change this when you create the group.

1. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. On the **Settings** page, select or clear the **Enable Application Group** check box.
4. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

Enable or disable application session sharing between

Application Groups

Session sharing between Application Groups is enabled when you create an Application Group; you cannot change this when you create the group. For more information 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.

Rename an Application Group

1. Select **Applications** in the Studio navigation pane.
2. Select an Application Group in the middle pane and then select **Rename Application Group** in the Actions pane.
3. Specify the new unique name and then click **OK**.

Add, remove, or change 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 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.

Remote PC Access

Sep 28, 2016

Remote PC Access allows an end user to log on remotely from virtually anywhere to the physical Windows PC in the office.

> **Important**
>
> In XenApp and XenDesktop 7.9, use the command line only for Remote PC Access deployments. For more information, see Install using the command line and Known issues [#637741].

The Virtual Delivery Agent (VDA) is installed on the office PC; it registers with the Delivery Controller and manages the HDX connection between the PC and the end user client devices. Remote PC Access supports a self-service model; after you set up the whitelist of machines that users are permitted to access, those users can join their office PCs to a Site themselves, without administrator intervention. The Citrix Receiver running on their client device enables access to the applications and data on the office PC from the Remote PC Access desktop session.

A user can have multiple desktops, including more than one physical PC or a combination of physical PCs and virtual desktops.

Note: Sleep mode & Hibernation mode for Remote PC Access is not supported. Remote PC Access is valid only for XenDesktop licenses; sessions consume licenses in the same way as other XenDesktop sessions.

Active Directory considerations

Before configuring the Remote PC Access deployment Site, set up your Organizational Units (OUs) and security groups and then create user accounts. Use these accounts to specify users for the Delivery Groups you will use to provide Remote PC Access.

If you modify Active Directory after a machine has been added to a Machine Catalog, Remote PC Access does not reevaluate that assignment. You can manually reassign a machine to a different catalog, if needed.

If you move or delete OUs, those used for Remote PC Access can become out of date. VDAs might no longer be associated with the most appropriate (or any) Machine Catalog or Delivery Group.

Machine Catalog and Delivery Group considerations

A machine can be assigned to only one Machine Catalog and one Delivery Group at a time.

You can put machines in one or more Remote PC Access Machine Catalogs.

When choosing machine accounts for a Machine Catalog, select the lowest applicable OU to avoid potential conflicts with machines in another catalog. For example, in the case of bank/officers/tellers, select tellers.

You can allocate all machines from one Remote PC Access Machine Catalog through one or more Delivery Groups. For

example, if one group of users requires certain policy settings and another group requires different settings, assigning the users to different Delivery Groups enables you to filter the HDX policies according to each Delivery Group.

If your IT infrastructure assigns responsibility for servicing users based on geographic location, department, or some other category, you can group machines and users accordingly to allow for delegated administration. Ensure that each administrator has permissions for both the relevant Machine Catalogs and the corresponding Delivery Groups.

For users with office PCs running Windows XP, create a separate Machine Catalog and Delivery Group for those systems. When choosing machine accounts for that catalog in Studio, select the checkbox indicating that some machines are running Windows XP.

Deployment considerations

You can create a Remote PC Access deployment and then add traditional Virtual Desktop Infrastructure (VDI) desktops or applications later. You can also add Remote PC Access desktops to an existing VDI deployment.

Consider whether to enable the Windows Remote Assistance checkbox when you install the VDA on the office PC. This option allows help desk teams using Director to view and interact with a user sessions using Windows Remote Assistance.

Consider how you will deploy the VDA to each office PC. Citrix recommends using electronic software distribution such as Active Directory scripts and Microsoft System Center Configuration Manager. The installation media contains sample Active Directory scripts.

Review the security considerations for Remote PC Access deployments.

Secure Boot for Remote PC Access is currently supported on Windows 10 and 8.1. Disable Secure Boot if you intend to deploy the workstation VDA on any other operating system.

Each office PC must be domain-joined with a wired network connection.

Windows 7 Aero is supported on the office PC, but not required.

Connect the keyboard and mouse directly to the PC or laptop, not to the monitor or other components that can be turned off. If you must connect input devices to components such as monitors, they should not be turned off.

If you are using smart cards, see Smart cards.

Remote PC Access can be used on most laptop computers. To improve accessibility and deliver the best connection experience, configure the laptop power saving options to those of a desktop PC. For example:

- Disable the hibernate feature.
- Disable the sleep feature.
- Set the close lid action to Do Nothing.
- Set the press the power button action to Shut Down.
- Disable video card energy saving features.
- Disable network interface card energy saving features.
- Disable battery saving technologies.

The following are not supported for Remote PC Access devices:

- Docking and undocking the laptop.
- KVM switches or other components that can disconnect a session.
- Hybrid PCs, including All-in-One and NVIDIA Optimus laptops and PCs.

Citrix supports Remote PC Access on Surface Pro devices with Windows 10. To improve accessibility and deliver the best connection experience, configure the Surface device in a similar way to a desktop or laptop computer. For example:

- Disable the hibernate or sleep feature
- Use wired network connectivity
- Always have the keyboard attached when initiating or reconnecting a session
- Disable battery saving technologies

Install Citrix Receiver on each client device that remotely accesses the office PC.

Multiple users with remote access to the same office PC see the same icon in Citrix Receiver. When any user remotely logs on to the PC, that resource appears as unavailable to other users.

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.

> **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.
>
> HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001
>
> To further customize the behavior of this feature under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC
>
> RpcaMode (dword):
>
> 1 = The remote user will always win if he does not respond to the messaging UI in the specified timeout period.
>
> 2 = The local user will always win. If this setting is not specified, the remote user will always win by default.
>
> RpcaTimeout (dword):
>
> The number of seconds given to the user before the type of mode to enforce is determined. If this setting is not specified, the default value is 30 seconds. The minimum value here should be 30 seconds. The user must restart the machine for these changes to take place.
>
> When user wants to forcibly get the console access: The local user can press Ctr+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 asking whether or not to allow or deny the local user's connection. Allowing the connection will disconnect the remote user's session.

Remote PC Access and HDX 3D Pro mode

For Remote PC Access, the VDA is usually configured using the standard VDA option. 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), and NVIDIA Quadro and NVIDIA GRID GPUs.

For more information, see Prepare to install and GPU acceleration for Windows Desktop OS.

Wake on LAN

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use, saving energy costs. It also enables remote access when a machine has been turned off inadvertently, such as during weather events.

The Remote PC Access Wake on LAN feature is supported on both of the following:

- PCs that support Intel Active Management Technology (AMT)
- PCs that have the Wake on LAN option enabled in the BIOS

You must configure Microsoft System Center Configuration Manager (ConfigMgr) 2012 to use the Wake on LAN feature. ConfigMgr provides access to invoke AMT power commands for the PC, plus Wake-up proxy and magic-packet support. Then, when you use Studio to create a Remote PC Access deployment (or when you add another power management connection to be used for Remote PC Access), you enable power management and specify ConfigMgr access information.

Additionally:

- Using AMT power operations is preferred for security and reliability; however, support is also provided for two non-AMT methods: ConfigMgr Wake-up proxy and raw magic packets.
- On AMT-capable machines only, the Wake on LAN feature also supports the Force-Shutdown and Force-Restart actions in Studio and Director. Additionally, a Restart action is available in StoreFront and Receiver.

For more information, see Configuration Manager and Remote PC Access Wake on LAN.

For information about the Proof of Concept (POC) Wake on LAN SDK that enables you or a third party Wake on LAN solution to create a connector without the requirement of System Center 2012 R2, see CTX202272. Wake on LAN SDK in this release is for evaluation only and not for production use.

Configuration sequence and considerations

Before you create the Remote PC Access Site:

If you will use the Remote PC Access power management feature (also known as Remote PC Access Wake on LAN), complete the configuration tasks on the PCs and on Microsoft System Center Configuration Manager (ConfigMgr) before creating the Remote PC Access deployment in Studio. See Configuration Manager and Remote PC Access Wake on LAN for details.

In the Site creation wizard:

- Select the Remote PC Access Site type.
- On the Power Management page, you can enable or disable power management for the machines in the default Remote PC Access Machine Catalog. If you enable power management, specify ConfigMgr connection information.
- On the Users and Machine Accounts pages, specify users and machine accounts.

Creating a Remote PC Access Site creates a default Machine Catalog named Remote PC Access Machines and a default Delivery Group named Remote PC Access Desktops.

If you create another Machine Catalog for use with Remote PC Access:

- On the Operating System page, select Remote PC Access and choose a power management connection. You can also choose not to use power management. If there are no configured power management connections, you can add one after you finish the Machine Catalog creation wizard (connection type = Microsoft Configuration Manager Wake on LAN), and then edit the Machine Catalog, specifying that new connection.
- On the Machine Accounts page, you can select from the machine accounts or Organizational Units (OUs) displayed, or add machine accounts and OUs.

Install the VDA on the office PCs used for local and remote access. Typically, you deploy the VDA automatically using your package management software; however, for proof-of-concept or small deployments, you can install the VDA manually on each office PC.

When installing the VDA from the command line, include the **/remotepc** option. This prevents the installation of the following components on a desktop (workstation) OS:

- App V Component - Citrix Personalization for App-V - VDA
- UpmComponent - Citrix User Profile Manager
- UpmVdaPlugin Component - Citrix User Profile Manager WMI Plugin
- Mps Component - Machine Identity Service
- VDisk Component - Personal vDisk

During an upgrade, if any of the above components are installed, the installer detects and upgrades them.

After the VDA is installed, the next domain user that logs on to a console session (locally or through RDP) on the office PC is automatically assigned to the Remote PC Access desktop. If additional domain users log on to a console session, they are also added to the desktop user list, subject to any restrictions you have configured.

To use RDP connections outside of your XenApp or XenDesktop environment, you must add users or groups to the Direct Access Users group.

Instruct users to download and install Citrix Receiver onto each client device they will use to access the office PC remotely. Citrix Receiver is available from http://www.citrix.com or the application distribution systems for supported mobile devices.

Configure advanced connection settings

You can edit a power management connection to configure advanced settings. You can enable:

- Wake-up proxy delivered by ConfigMgr.
- 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.

Troubleshooting

The Delivery Controller writes the following diagnostic information about Remote PC Access 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

When power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are located on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method (ensure those settings are enabled in the advanced properties for the power management connection).

App-V

May 31, 2016

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 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

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 as well as 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
- 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.

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.

Setup

The following table summarizes the sequence of setup tasks for using App-V in XenApp and XenDesktop.

Management method		Task
Single admin	Dual admin	
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	X	Add App-V applications to Delivery Groups

For App-V deployment instructions, see http://technet.microsoft.com/en-us/virtualization/hh710199.

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 –UserRefreshonLogon 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.

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. Make sure that the Studio administrator who adds applications to Delivery Groups has at least read access to that location.
- For dual admin management, publish the packages on the App-V management server.

Regardless of whether packages are on the App-V server or on a network share, make sure the packages have appropriate security permissions to allow the Studio administrator to access them.

This procedure is valid only for the dual admin management method.

Specify App-V management and publishing server addresses for the dual admin management method either during or after Site creation. You can do this during or after creating the Site.

During Site creation:

On the **App-V** page of the wizard, enter the URL of the Microsoft App-V management server, and the URL and port number of the App-V publishing server. Test the connection before continuing with the wizard. If the test fails, see

the Troubleshoot section below.

After Site creation:

1. Select **Configuration > App-V Publishing** in the Studio navigation pane.
2. If you have not previously specified App-V server addresses, select **Add Microsoft Server** in the Actions pane.
3. To change App-V server addresses, select **Edit Microsoft Server** in the Actions pane.
4. Enter the URL of the Microsoft App-V management server, and the URL and port number of the App-V publishing server.
5. Test the connection to those servers before closing the dialog box. If the test fails, see the Troubleshoot section below.

Later, if you want to remove all links to the App-V management and publishing servers and stop Studio from discovering App-V packages from those servers, select **Remove Microsoft Server** in the Actions pane. This action is allowed only if no applications in packages on those servers are currently published in any Delivery Groups. If they are, you must remove those applications from the Delivery Groups before you can remove the App-V servers.

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.

Tip: After you install the App-V client, with Administrator permissions, run the PowerShell **Get-AppvClientConfiguration** cmdlet, and make sure 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; that process also creates an account with local administrator permissions for accessing the App-V publishing components.

You can control this default action during VDA installation. In the graphical interface, clear the **Install App-V publishing components** check box on the **Features** page. In the command line interface, include the **/no_appv** option.

If you expressly disable the Citrix App-V components feature 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.

This procedure is valid only for the single admin management method.

You must have at least read access to the network share containing the App-V packages.

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**.

The following procedure focuses on how to add App-V applications to Delivery Groups. For complete details about creating a Delivery Group, see the Create Delivery Groups article.

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** dropdown 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 checkboxes 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.
- 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."

Remove App-V packages 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.

Troubleshoot

Issues that can occur only when using the dual admin method are marked "(DUAL)".

(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 http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- Is the Studio administrator also an App-V server administrator?
- Is file sharing enabled on the App-V server? Enter **\\<*App-V server FQDN*>** in Windows Explorer or with the Run command.
- Does the App-V server have the same file sharing permissions as the App-V administrator? On the App-V server, add an entry for\\<*App-V Server FQDN*> in Stored User Names and Passwords, specifying the credentials of the user who has administrator privileges on the App-V server. For guidance, see http://support.microsoft.com/kb/306541.
- Is the App-V server in Active Directory?

  If the Studio machine and the App-V server are in different Active Directory domains that do not have a trust relationship, from the PowerShell console on the Studio machine, run **winrm s winrm/Config/client '@(TrustedHosts="<*App-V server FQDN*>")'**.

  If TrustedHosts is managed by GPO, the following error message 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" in order 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?
- 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 http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- 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, make sure 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, check whether UserRefreshonLogon is set to False. If not, the first App-V application launch typically fails.
- (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 machine containing 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. Make sure that the AppVServers key has the following value format: AppVManagementServer+metadata;PublishingServer (for example: http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082).
- On the machine containing the App-V client and VDA, make sure that CtxAppVCOMAdmin has administrator privileges. This is usually created during VDA installation and added to the Local Administrators Group on the VDA machine. However, depending on the Active Directory policy, this user might lose the administrative association. Run compmgmt.msc and browse to Local Users and Groups Users. If CtxAppVCOMAdmin is not an administrator, edit the group policy so that this user account retains its administrative association.
- 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.

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. Make sure to check in the local folder of the user for whom 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:\ProgramFiles\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:\ProgramFiles\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

Jul 25, 2016

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:

- 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 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.

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, Machine Creation Services (MCS) or Provisioning Services (PVS), and the Delivery Controller to distribute the selected AppDisks.

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) or the PVS version provided on the download page with your XenApp and XenDesktop version.
- Supported XenServer releases (see the System requirements article) or VMware minimum version 5.1. (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.

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).

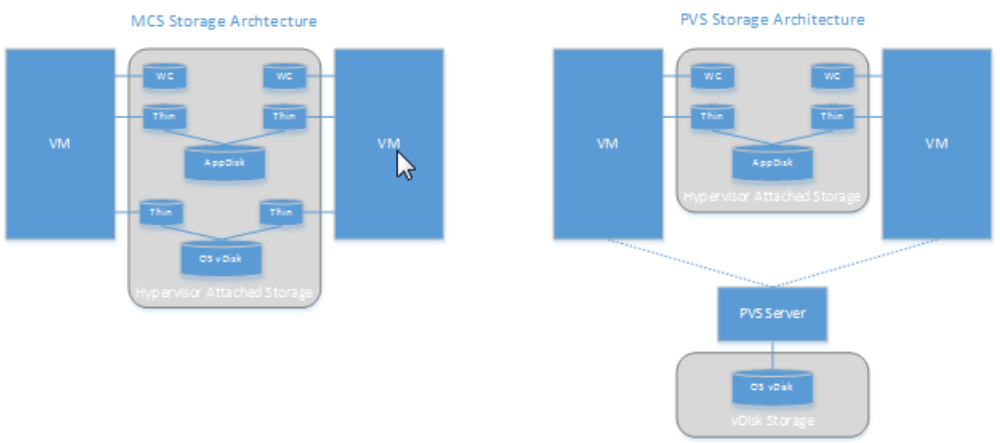
Machines on which Studio is installed must have .NET Framework 3.5 installed (in addition to any other installed .NET versions).

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.

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.



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.

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, its analysis automatically after the creation process completes. During this interval, the AppDisk's status in Studio is "Analyzing."

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.

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.

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.)

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.

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.

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.

Local App Access and URL redirection

May 31, 2016

In this article:

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. 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
- 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 File Type Association (FTA) redirection. FTA launches local applications when a file is encountered in the session. If the local app is launched, it 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.
  - 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.
- 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 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 Receiver:

- Install Citrix Receiver on the local client machine. You can enable both features during Citrix Receiver installation or you can enable Local App Access template using the Group Policy editor.
- Set the **Allow local app access** policy setting to **Enabled**. You can also configure URL whitelist and blacklist policy settings for URL redirection. For more information, see the Local App Access policy settings.

To enable Local App Access and URL redirection for all local applications:

1. Set the **Allow local app access** policy setting to **Enabled**. When this setting is enabled, the VDA allows the client to decide whether administrator-published applications and Local App Access shortcuts are enabled in the session. (When this setting is disabled, both administrator-published applications and Local App Access shortcuts do not work for the VDA.) This policy setting applies to the entire machine, as well as the URL redirection policy.
2. Enable Local App Access and URL redirection when you install Citrix Receiver for all users on a machine. This action also registers the browser add-ons required for URL redirection. From the command prompt, run the appropriate command to install the Receiver with the following option:

CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

1. Run **gpedit.msc**.
2. Select **Computer Configuration**. Right-click **Administrative Templates** and select **Add/Remote Templates > Add**.
3. Add the icaclient.adm template located in the Citrix Receiver Configuration folder (usually in c:\Program Files (x86)\Citrix\Online Plugin\Configuration). (After the icaclient.adm template is added to Computer Configuration, it is also available in User Configuration.)
4. Expand **Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Experience**.
5. Select **Local App Access settings**.
6. Select **Enabled** and then select **Allow URL Redirection**. For URL redirection, register browser add-ons using the command line, as described below.

To provide access to only published applications:

1. On the server where the Delivery Controller is installed, run **regedit.exe**.
   1. Navigate to HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
   2. Add the REG_DWORD entry ClientHostedAppsEnabled with a value of 1. (A 0 value disables Local App Access.)
2. Restart the Delivery Controller server and then restart Studio.
3. Publish Local App Access applications.
   1. Select **Delivery Groups** in the Studio navigation pane and then select the Applications tab.
   2. Select **Create Local Access Application** in the Actions pane.
   3. Select the desktop Delivery Group.
   4. Enter the full executable path of the application on the user's local machine.
   5. Indicate if the shortcut to the local application on the virtual desktop will be visible on the Start menu, the desktop, or both.
   6. Accept the default values on the Name page and then review the settings.
4. Enable Local App Access and URL redirection when you install Citrix Receiver for all users on a machine. This action also registers the browser add-ons required for URL redirection. From the command prompt, run the command to install Citrix Receiver with the following option:
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. Set the **Allow local app access** policy setting to **Enabled**. When this setting is enabled, the VDA allows the client to decide whether administrator-published applications and Local App Access shortcuts are enabled in the session. (When this setting is disabled, both administrator-published applications and Local App Access shortcuts do not work for the VDA.)

Note: The browser add-ons required for URL redirection are registered automatically when you install Citrix Receiver from the command line with 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 IE, FF, Chrome, or All.

For example, the following command registers Internet Explorer add-ons on a device running Citrix Receiver.

```
C:\Program Files\Citrix\ICA Client\redirector.exe/regIE
```

The following command registers all add-ons on a Windows Server OS VDA.

```
C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll
```

- By default, Internet Explorer redirects the URL entered. If the URL is not in the blacklist but is redirected to another URL by the browser or website, the final URL is not redirected, even if it is on the blacklist.

  For URL redirection to work correctly, enable the add-on when prompted by the browser. If the add-ons that are using Internet options or the add-ons in the prompt are disabled, URL redirection does not work correctly.

- The Firefox add-ons always redirect the URLs.

  When an add-on is installed, Firefox prompts to allow/prevent installing the add-on on a new tab page. You must 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. If 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.

1. On the hosted desktop, run **gpedit.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 with 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 local environment.
   - 3 - Local applications close when a user logs off or disconnects from the virtual desktop.

XenApp Secure Browser

Aug 29, 2016

As applications are ported to the web, users must rely on multiple browser vendors and versions in order to achieve compatibility with web-based apps. If the application is an internally hosted application, organizations are often required to install and configure complex VPN solutions in order to provide access to remote users. Typical VPN solutions require a client-side agent that must also be maintained across numerous operating systems.

With the XenApp Secure Browser, users can have a seamless web-based application experience where a hosted web-based application simply appears within the user's preferred local browser. For example, a user's preferred browser is Mozilla Firefox but the application is only compatible with Microsoft Internet Explorer. XenApp Secure Browser will display the Internet Explorer compatible application as a tab within the Firefox browser.

Deploying XenApp Secure Browser Edition

Citrix recommends that you leverage the Lifecycle Management Blueprint for the XenApp Secure Browser to simplify the deployment. As part of the XenApp Version 7.9 launch, all existing XenApp and XenDesktop customers with active Software Maintenance (SWM) or Subscription Advantage (SA) have access to the Deploy edition of Citrix Lifecycle Management.

The XenApp Secure Browser Blueprint includes scripts to automate the following tasks:

- Install XenApp, including the Citrix License Server and StoreFront
- Create a XenApp delivery site
- Join the provisioned machines to your existing domain

To use the Citrix Lifecyle Management Blueprint:

1. From the Workspace Cloud home page, navigate to Services; click Request Trial for Lifecycle Management. Once you request the trial, you'll receive an email notifying you when the trial service is available. This generally takes 5-10 minutes.
2. Click Manage in the email you received when you requested the trail to display the Lifecycle Management Overview page.
3. Download the Citrix XenApp Secure Browser Edition 7.9 ISO from the Citrix download site.

Consider the following after downloading the Secure Browser Edition 7.9 ISO:

- Start using the XenApp Secure Browser Blueprint by following the instructions specified in the following:
  - XenApp Secure Installation with a Citrix Lifecycle Management Blueprint
  - XenApp Secure Installation with a Citrix Lifecycle Management Blueprint with NetScaler on Azure
  - XenApp Secure Installation with a Citrix Lifecycle Management Blueprint with NetScaler on AWS
- After completing the installation, further optimize your environment for webapp delivery by using the configuration steps specified in the XenApp Secure Browser Deployment Guide.

To manually install XenApp Secure Browser version 7.9:

1. Download the Citrix XenApp Secure Browser Edition 7.9 ISO from the Citrix download site.
2. Follow the install instructions for various components of XenApp.
3. Configure the edition and license mode for the Secure Browser edition after installation, by perfoming the following additional steps:

    a. On the Delivery Controller, start a PowerShell session by clicking the blue icon on the taskbar, or by browsing to Start > All Programs > Accessories >Windows PowerShell > Windows PowerShell.

    Note: On 64-bit systems, this starts the 64-bit version. Both the 32-bit or 64-bit versions are supported.

    b. Type Asnp Citrix* and press Enter to load the Citrix-specific PowerShell modules.

    Note: “Asnp” represents Add-PSSnapin.

    c. Check the current site settings and license mode, by running the Get-ConfigSite cmdlet.

    d. Set the license mode to XenApp Secure Browser edition by running the Set-ConfigSite -ProductCode XDT -ProductEdition BAS.

    e. Confirm that the XenApp Secure Browser edition and license mode is set properly by running the Get-BrokerSite cmdlet.

> ## Note
>
> After completing the installation, further optimize your environment for webapp delivery by using the configuration steps specified in the XenApp Secure Browser Deployment Guide.

Server VDI

Oct 24, 2016

Use the Server VDI (Virtual Desktop Infrastructure) feature to deliver a desktop from a server operating system for a single user.

- Enterprise administrators can deliver server operating systems as VDI desktops, which can be valuable for users such as engineers and designers.
- Service Providers can offer desktops from the cloud; those desktops comply with the Microsoft Services Provider License Agreement (SPLA).

You can use the Enhanced Desktop Experience Citrix policy setting to make the server operating system look like a Windows 7 operating system.

The following features cannot be used with Server VDI:

- Personal vDisks
- Hosted applications
- Local App Access
- Direct (non-brokered) desktop connections
- Remote PC Access

For Server VDI to work with TWAIN devices such as scanners, the Windows Server Desktop Experience feature must be installed. In Windows Server 2012, this is an optional feature which you install from Administrative Tools > Server Manager > Features > Add features > Desktop Experience.

Server VDI is supported on the same server operating systems as the VDA for Windows Server OS.

1. Prepare the Windows server for installation: ensure that Remote Desktop Services role services are not installed and that users are restricted to a single session:
   - Use Windows Server Manager to ensure that the Remote Desktop Services role services are not installed. If they were previously installed, remove them.
   - Ensure that the 'Restrict each user to a single session' property is enabled.
     - On Windows Server 2008 R2, access this property through Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration. In the Edit settings > General section, the Restrict each user to a single session setting should indicate Yes.
     - On Windows Server 2012, edit the registry to set the Terminal Server setting. In registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer to set DWORD fSingleSessionPerUser to 1.
2. For Windows Server 2008 R2, install Microsoft .NET Framework 3.5 SP1 on the server before installing the VDA.
3. Use the command line interface to install a VDA on a supported server or server master image, specifying the /quiet and /servervdi options. (By default, the installer blocks the Windows Desktop OS VDA on a server operating system; using the command line overrides this behavior.)
   XenDesktopVdaSetup.exe /quiet /servervdi

   You can specify the Delivery Controller or Controllers while installing the VDA using the command line, using the **/controllers** option.

   Use the **/enable_hdx_ports** option to open porst in the firewall, unless the firewall is to be configured manually.

Add the **/masterimage** option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.

Add the **/enable_hdx_3d_pro** option to configure the VDA in HDX 3D Pro mode.

Do not include options for features that are not supported with Server VDI, such as /baseimage or /xa_server_location.

4. Create a Machine Catalog for Server VDI.
   1. On the Operating System page, select **Desktop OS**.
   2. On the Summary page, specify a machine catalog name and description for administrators that clearly identifies it as Server VDI; this will be the only indicator in Studio that the catalog supports Server VDI.

   When using Search in Studio, the Server VDI catalog you created is displayed on the Desktop OS Machines tab, even though the VDA was installed on a server.
5. Create a Delivery Group and assign the Server VDI catalog you created in the previous step.

If you did not specify the Delivery Controllers while installing the VDA, specify them afterward using Citrix policy setting, Active Directory, or by editing the VDA machine's registry values.

Personal vDisk

Feb 24, 2016

The personal vDisk feature retains the single image management of pooled and streamed desktops while allowing users to install applications and change their desktop settings. Unlike traditional Virtual Desktop Infrastructure (VDI) deployments involving pooled desktops, where users lose their customization and personal applications when the administrator changes the master image, deployments using personal vDisks retain those changes. This means administrators can easily and centrally manage their master images while providing users with a customized and personalized desktop experience.

Personal vDisks provide this separation by redirecting all changes made on the user's VM to a separate disk (the personal vDisk), which is attached to the user's VM. The content of the personal vDisk is blended at runtime with the content from the master image to provide a unified experience. In this way, users can still access applications provisioned by their administrator in the master image.

Personal vDisks have two parts, which use different drive letters and are by default equally sized:

- User profile - This contains user data, documents, and the user profile. By default this uses drive P: but you can choose a different drive letter when you create a catalog with machines using personal vDisks. The drive used also depends on the EnableUserProfileRedirection setting.
- Virtual Hard Disk (.vhd) file - This contains all other items, for example applications installed in C:\Program Files. This part is not displayed in Windows Explorer and, since Version 5.6.7, does not require a drive letter.

Personal vDisks support the provisioning of department-level applications, as well as applications downloaded and installed by users, including those that require drivers (except phase 1 drivers), databases, and machine management software. If a user's change conflicts with an administrator's change, the personal vDisk provides a simple and automatic way to reconcile the changes.

In addition, locally administered applications (such as those provisioned and managed by local IT departments) can also be provisioned into the user's environment. The user experiences no difference in usability; personal vDisks ensure all changes made and all applications installed are stored on the vDisk. Where an application on a personal vDisk exactly matches one on a master image, the copy on the personal vDisk is discarded to save space without the user losing access to the application.

Physically, you store personal vDisks on the hypervisor but they do not have to be in the same location as other disks attached to the virtual desktop. This can lower the cost of personal vDisk storage.

During Site creation, when you create a connection, you define storage locations for disks that are used by VMs. You can separate the Personal vDisks from the disks used by the operating system. Each VM must have access to a storage location for both disks. If you use local storage for both, they must be accessible from the same hypervisor. To ensure this requirement is met, Studio offers only compatible storage locations. Later, you can also add personal vDisks and storage for them to existing hosts (but not machine catalogs) from Configuration > Hosting in Studio.

Back up personal vDisks regularly using any preferred method. The vDisks are standard volumes in a hypervisor's storage tier, so you can back them up, just like any other volume.

What's new in personal vDisk 7.6.1

The following improvements are included in this release:

- This version of personal vDisk contains performance improvements that reduce the amount of time it takes to apply an

image update to a personal vDisk catalog.

The following known issues are fixed in this release:

- Attempting an in-place upgrade of a base virtual machine from Microsoft Office 2010 to Microsoft Office 2013 resulted in the user seeing a reconfiguration window followed by an error message; "Error 25004. The product key you entered cannot be used on this machine." In the past, it was recommended that Office 2010 be uninstalled in the base virtual machine before installing Office 2013. Now, it is no longer necessary to uninstall Office 2010 when performing an in-place upgrade to the base virtual machine (#391225).
- During the image update process, if a higher version of Microsoft .Net exists on the users personal vDisk, it was overwritten by a lower version from the base image. This caused issues for users running certain applications installed on their personal vDisk which required the higher version, such as Visual Studio (#439009).
- A Provisioning Services imaged disk with personal vDisk install and enabled, cannot be used to create a non-personal vdisk machine catalog. This restriction has been removed (#485189).

About Personal vDisk 7.6

New in version 7.6:

- Improved personal vDisk error handling and reporting. In Studio, when you display PvD-enabled machines in a catalog, a "PvD" tab provides monitoring status during image updates, plus estimated completion time and progress. Enhanced state displays are also provided.
- A personal vDisk Image Update Monitoring Tool for earlier releases is available from the ISO media (ISO\Support\Tools\Scripts\PvdTool). Monitoring capabilities are supported for previous releases, however the reporting capabilities will not be as robust compared to the current release.
- Provisioning Services test mode allows you to boot machines with an updated image in a test catalog. After you verify its stability, you can promote the test version of the personal vDisk to production.
- A new feature enables you to calculate the delta between two inventories during an inventory, instead of calculating it for each PvD desktop. New commands are provided to export and import a previous inventory for MCS catalogs. (Provisioning Services master vDisks already have the previous inventory.)

Known issues from 7.1.3 fixed in version 7.6:

- Interrupting a personal vDisk installation upgrade can result in corrupting an existing personal vDisk installation. [#424878]
- A virtual desktop may become unresponsive if the personal vDisk runs for an extended period of time and a non-page memory leak occurs. [#473170]

New known issues in version 7.6:

- The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the PROCESS exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. [#326735]
- Hard links between files inherited from the master image are not preserved in personal vDisk catalogs. [#368678]
- After upgrading from Office 2010 to 2013 on the Personal vDisk master image, Office might fail to launch on virtual machines because the Office KMS licensing product key was removed during the upgrade. As a workaround, uninstall Office 2010 and reinstall Office 2013 on the master image. [#391225]
- Personal vDisk catalogs do not support VMware Paravirtual SCSI (PVSCSI) controllers. To prevent this issue, use the default controller. [#394039]
- For virtual desktops that were created with Personal vDisk version 5.6.0 and are upgraded to 7, users who logged on to the master virtual machine (VM) previously might not find all their files in their pooled VM. This issue occurs because a new user profile is created when they log on to their pooled VM. There is no workaround for this issue. [#392459]

- Personal vDisks running Windows 7 cannot use the Backup and Restore feature when the Windows system protection feature is enabled. If system protection is disabled, the user profile is backed up, but the userdata.v2.vhd file is not. Citrix recommends disabling system protection and using Backup and Restore to back up the user profile. [#360582]
- When you create a VHD file on the base VM using the Disk Management tool, you might be unable to mount the VHD. As a workaround, copy the VHD to the PvD volume. [#355576]
- Office 2010 shortcuts remain on virtual desktops after this software is removed. To work around this issue, delete the shortcuts. [#402889]
- When using Microsoft Hyper-V, you cannot create a catalog of machines with personal vDisks when the machines are stored locally and the vDisks are stored on Cluster Shared Volumes (CSVs); catalog creation fails with an error. To work around this issue, use an alternative storage setup for the vDisks. [#423969]
- When you log on for the first time to a virtual desktop that is created from a Provisioning Services catalog, the desktop prompts for a restart if the personal vDisk has been reset (using the command ctxpvd.exe -s reset). To work around this issue, restart the desktop as prompted. This is a once-only reset that is not required when you log on again. [#340186]
- If you install .NET 4.5 on a personal vDisk and a later image update installs or modifies .NET 4.0, applications that are dependent on .NET 4.5 fail. To work around this issue, distribute .NET 4.5 from the base image as an image update."
- See also the
  — Known Issues
  documentation for the XenApp and XenDesktop 7.6 release.

About Personal vDisk 7.1.3

Known issues from 7.1.1 fixed in version 7.1.3:

- Direct upgrades from personal vDisk 5.6.0 to personal vDisk 7.x may cause the personal vDisk to fail. [#432992]
- Users might only be able to connect intermittently to virtual desktops with personal vDisks. [#437203]
- If a personal vDisk image update operation is interrupted while personal vDisk 5.6.5 or later is upgraded to personal vDisk 7.0 or later, subsequent update operations can fail. [#436145]

About Personal vDisk 7.1.1

Known issues from 7.1 fixed in version 7.1.1:

- Upgrading to Symantec Endpoint Protection 12.1.3 through an image update causes symhelp.exe to report corrupt antivirus definitions. [#423429]
- Personal vDisk can cause pooled desktops to restart if Service Control Manager (services.exe) crashes. [#0365351]

New known issues in version 7.1.1: none

About Personal vDisk 7.1

New in version 7.1:

- You can now use Personal vDisk with desktops running Windows 8.1, and event logging has been improved.
- Copy-on-Write (CoW) is no longer supported. When upgrading from Version 7.0 to 7.1 of Personal vDisk, all changes to data managed by CoW are lost. This was a feature for evaluation in XenDesktop 7 and was disabled by default, so if you did not enable it, you are not affected.

Known issues from 7.0.1 fixed in version 7.1:

- If the value of the Personal vDisk registry key EnableProfileRedirection is set to 1 or ON, and later, while updating the image, you change it to 0 or OFF, the entire Personal vDisk space might get allocated to user-installed applications, leaving no space for user profiles, which remain on the vDisk. If this profile redirection is disabled for a catalog and you enable it during an image update, users might not be able to log on to their virtual desktop. [#381921]
- The Desktop Service does not log the correct error in the Event Viewer when a Personal vDisk inventory update fails.

[#383331]

- When upgrading to Personal vDisk 7.x, modified rules are not preserved. This issue has been fixed for upgrades from Version 7.0 to Version 7.1. When upgrading from Version 5.6.5 to Version 7.1, you must first save the rule file and then apply the rules again after the upgrade. [#388664]
- Personal vDisks running Windows 8 cannot install applications from the Windows Store. An error message stating, "Your purchase couldn't be completed," appears. Enabling the Windows Update Service does not resolve this issue, which has now been fixed. However, user-installed applications must be reinstalled after the system restarts. [#361513]
- Some symbolic links are missing in Windows 7 pooled desktops with personal vDisks. As a result, applications that store icons in C:\Users\All Users do not display these icons in the Start menu. [#418710]
- A personal vDisk does not start if an Update Sequence Number (USN) journal overflow occurs due to a large number of changes made to the system after an inventory update. [#369846]
- A personal vDisk does not start with status code 0x20 and error code 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 displays the message "Proactive Threat Protection is malfunctioning" and this component's Live Update Status is not available. [#390204]

New known issues in version 7.1: See the
— Known Issues
documentation for the XenDesktop 7.1 release.

About Personal vDisk 7.0.1

New in version 7.0.1: Personal vDisk is now more robust to environment changes. Virtual desktops with personal vDisks now register with the Delivery Controller even if image updates fail, and unsafe system shutdowns no longer put the vDisks into a permanently disabled state. In addition, using rules files you can now exclude files and folders from the vDisks during a deployment.

Known issues from 5.6.13 fixed in version 7.0.1:

- Changes to a group's membership made by users on a pooled virtual desktop might be lost after an image update. [#286227]
- Image updates might fail with a low disk space error even if the personal vDisk has enough space. [#325125]
- Some applications fail to install on virtual desktops with a personal vDisk, and a message is displayed that a restart is required. This is due to a pending rename operation. [#351520]
- Symbolic links created inside the master image do not work on virtual desktops with personal vDisks. [#352585]
- In environments that use Citrix Profile management and personal vDisk, applications that examine user profiles on a system volume might not function properly if profile redirection is enabled. [#353661]
- The inventory update process fails on master images when the inventory is bigger than 2GB. [#359768]
- Image updates fail with error code 112 and personal vDisks are corrupted even if the vDisks have enough free space for the update. [#363003]
- The resizing script fails for catalogs with more than 250 desktops. [#363365]
- Changes made by users to an environment variable are lost when an image update is performed. [#372295]
- Local users created on a virtual desktop with a personal vDisk are lost when an image update is performed. [#377964]
- A personal vDisk may fail to start if an Update Sequence Number (USN) journal overflow occurred due to a large number of changes made to the system after an inventory update. To avoid this, increase the USN journal size to a minimum of 32 MB in the master image and perform an image update. [#369846]
- An issue has been identified with Personal vDisk that prevents the correct functioning of AppSense Environment Manager registry hiving actions when AppSense is used in Replace Mode. Citrix and AppSense are working together to resolve the issue, which is related to the behavior of the RegRestoreKey API when Personal vDisk is installed.[#0353936]

Release-independent known issues

- When an application installed on a personal vDisk (PvD) is related to another application of the same version that is installed on the master image, the application on the PvD could stop working after an image update. This occurs if you uninstall the application from the master image or upgrade it to a later version, because that action removes the files needed by the application on the PvD from the master image. To prevent this, keep the application containing the files needed by the application on the PvD on the master image.
  For example, the master image contains Office 2007, and a user installs Visio 2007 on the PvD; the Office applications and Visio work correctly. Later, the administrator replaces Office 2007 with Office 2010 on the master image, and then updates all affected machines with the updated image. Visio 2007 no longer works. To avoid this, keep Office 2007 in the master image. [#320915]

- When deploying McAfee Virus Scan Enterprise (VSE), use version 8.8 Patch 4 or later on a master image if you use personal vDisk. [#303472]
- If a shortcut created to a file in the master image stops working (because the shortcut target is renamed within PvD), recreate the shortcut. [#367602]
- Do not use absolute/hard links in a master image. [#368678]
- The Windows 7 backup and restore feature is not supported on the personal vDisk. [#360582]
- After an updated master image is applied, the local user and group console becomes inaccessible or shows inconsistent data. To resolve the issue, reset the user accounts on the VM, which requires resetting the security hive. This issue was fixed in the 7.1.2 release (and works for VMs created in later releases), but the fix does not work for VMs that were created with an earlier version and then upgraded. [#488044]
- When using a pooled VM in an ESX hypervisor environment, users see a restart prompt if the selected SCSI controller type is “VMware Paravirtual.” For a workaround, use an LSI SCSI controller type. [#394039]
- After a PvD reset on a desktop created through Provisioning Services, users may receive a restart prompt after logging on to the VM. As a workaround, restart the desktop. [#340186]
- Windows 8.1 desktop users might be unable to log on to their PvD. An administrator might see message "PvD was disabled due to unsafe shutdown" and the PvDActivation log might contain the message "Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]." This occurs when a user’s VM shuts down unsafely. As a workaround, reset the personal vDisk. [#474071]

Install and upgrade

Nov 05, 2014

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 Provisioning Services documentation.

Install and enable PvD

PvD is installed automatically when you install or upgrade a VDA for Desktop OS on a machine. 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.

VDA installation offers options to enable PvD (by selecting the “Personal vDisk” checkbox in the graphical interface or by specifying the /baseimage option in the command line interface). However, omitting this action during the VDA install (which is the default) still allows you to 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.

You can also upgrade just PvD using the PvD MSI from here.

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.

Configure and manage

Nov 12, 2014

This topic covers items you should consider when configuring and managing a personal vDisk (PvD) environment. It also covers best practice guidelines and task descriptions.

For procedures that include working in the Windows registry:
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Considerations: personal vDisk size

The following factors affect the size of the main personal vDisk volume:

- **Size of the applications that users will install on their PvDs**
  At restarts, PvD determines the free space remaining in the application area (UserData.v2.vhd). If this falls below 10%, the application area is expanded into any unused profile area space (by default, the space available on the P: drive). The space added to the application area is approximately 50% of the combined free space remaining in both the application area and the profile area.

  For example, if the application area on a 10 GB PvD (which by default is 5 GB) reaches 4.7 GB and the profile area has 3 GB free, the increased space that is added to the application area is calculated as follows:

  increased space = (5.0-4.7)/2 + 3.0/2 = 1.65 GB

  The space added to the application area is only approximate because a small allowance is made for storing logs and for overhead. The calculation and the possible resizing is performed on each restart.

- **Size of users' profiles (if a separate profile management solution is not used)**
  In addition to the space required for applications, ensure there is sufficient space available on personal vDisks to store users' profiles. Include any non-redirected special folders (such as My Documents and My Music) when calculating space requirements. Existing profile sizes are available from the Control Panel (sysdm.cpl).

  Some profile redirection solutions store stub files (sentinel files) instead of real profile data. These profile solutions might appear to store no data initially but actually consume one file directory entry in the file system per stub file; generally, approximately 4 KB per file. If you use such a solution, estimate the size based on the real profile data, not the stub files.

  Enterprise file sharing applications (such as ShareFile and Dropbox) might synchronize or download data to users' profile areas on the personal vDisks. If you use such applications, include enough space in your sizing estimates for this data.

- **Overhead consumed by the template VHD containing the PvD inventory**
  The template VHD contains the PvD inventory data (sentinel files corresponding to the master image content). The PvD application area is created from this VHD. Because each sentinel file or folder comprises a file directory entry in the file system, the template VHD content consumes PvD application space even before any applications are installed by the end user. You can determine the template VHD size by browsing the master image after an inventory is taken. Alternatively, use the following equation for an approximately calculation:

  template VHD size = (number of files on base image) x 4 KB

  Determine the number of files and folders by right-clicking the C: drive on the base VM image and selecting Properties.

For example, an image with 250,000 files results in a template VHD of approximately 1,024,000,000 bytes (just under 1 GB). This space will be unavailable for application installations in the PvD application area.

- **Overhead for PvD image update operations**
  During PvD image update operations, enough space must be available at the root of the PvD (by default, P:) to merge the changes from the two image versions and the changes the user has made to their PvD. Typically, PVD reserves a few hundred megabytes for this purpose, but extra data that was written to the P: drive might consume this reserved space, leaving insufficient 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 algorithm. In this case, you can increase the initial size of the application space to accommodate the user-installed applications.

Preferably, adjust the initial size of the VHD on a master image. Alternatively, you can adjust the size of the VHD on a virtual desktop when a user does not have sufficient space to install an application. However, you must repeat that operation on each affected virtual desktop; you cannot adjust the VHD initial size in a catalog that is already created.

Ensure the VHD is big enough to store antivirus definition files, which are typically large.

Locate and set the following registry keys in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (Do not modify other settings in this registry key.) All settings must be specified on the master image (except for MinimumVHDSizeInMB, which can be changed on an individual machine); settings specified on the master image are applied during the next image update.

- **MinimumVHDSizeMB**
  Specifies the minimum size (in megabytes) of the application part (C:) of the personal vDisk. The new size must be greater than the existing size but less than the size of the disk minus PvDReservedSpaceMB.

  Increasing this value allocates free space from the profile part on the vDisk to C:. This setting is ignored if a lower value than the current size of the C: drive is used, or if EnableDynamicResizeOfAppContainer is set to 0.

  Default = 2048

- **EnableDynamicResizeOfAppContainer**
  Enables or disables the dynamic resizing algorithm.
  - When set to 1, the application space (on C:) is resized automatically when the free space on C: falls below 10%. Allowed values are 1 and 0. A restart is required to effect the resize.

- When set to 0, the VHD size is determined according to the method used in XenDesktop versions earlier than 7.x

Default = 1

- **EnableUserProfileRedirection**

  Enables or disables redirecting the user's profile to the vDisk.
  - When set to 1, PvD redirects users' profiles to the personal vDisk drive (P: by default). Profiles are generally redirected to P:\Users, corresponding to a standard Windows profile. This redirection preserves the profiles in case the PvD desktop must be reset.
  - When set to 0, all of the space on the vDisk minus PvDReservedSpaceMB is allocated to C:, the application part of the vDisk, and the vDisk drive (P:) is hidden in Windows Explorer. Citrix recommends disabling redirection by setting the value to 0, when using Citrix Profile management or another roaming profile solution.
    This setting retains the profiles in C:\Users instead of redirecting them to the vDisk, and lets the roaming profile solution handle the profiles.

    This value ensures that all of the space on P: is allocated to applications.

    It is assumed that if this value is set to 0, a profile management solution is in place. Disabling profile redirection without a roaming profile solution in place is not recommended because subsequent PvD reset operations result in the profiles being deleted.

  Do not change this setting when the image is updated because it does not change the location of existing profiles, but it will allocate all the space on the Personal vDisk to C: and hide the PvD.

  Configure this value before deploying a catalog. You cannot change it after the catalog is deployed.

  Important: Beginning with XenDesktop 7.1, changes to this value are not honored when you perform an image update. Set the key's value when you first create the catalogs from which the profiles will originate. You cannot modify the redirection behavior later.
  Default = 1

- **PercentOfPvDForApps**

  Sets the split between the application part (C:) and the profile part of the vDisk. This value is used when creating new VMs, and during image updates when EnableDynamicResizeOfAppContainer is set to 0.

  Changing PercentOfPvDForApps makes a difference only when EnableDynamicResizeOfAppContainer is set to 0. By default, EnableDynamicResizeOfAppContainer is set to 1 (enabled), which means is that the AppContainer (which you see as the C drive) only expands when it is close to being full (that is, dynamic) - when less than 10% free space remains.

  Increasing PercentOfPvDForApps only increases the maximum space for which the Apps portion is allowed to expand. It does not provision that space for you immediately. You must also configure the split allocation in the master image, where it will be applied during the next image update.

  If you have already generated a catalog of machines with EnableDynamicResizeOfAppContainer set to 1, then change that setting to 0 in the master image for the next update, and configure an appropriate allocation split. The requested split size will be honored as long as it is larger than the current allocated size for the C drive.

  If you want to maintain complete control over the space split, set this value to 0. This allows full control over the C drive size, and does not rely on a user consuming space below the threshold to expand the drive.

  Default = 50% (allocates equal space to both parts)

- **PvDReservedSpaceMB**
  Specifies the size of the reserved space (in megabytes) on the vDisk for storing Personal vDisk logs and other data.

  If your deployment includes XenApp 6.5 (or an earlier version) and uses application streaming, increase this value by the size of the Rade Cache.

  Default = 512

- **PvDResetUserGroup**
  Valid only for XenDesktop 5.6 - Allows the specified group of users to reset a Personal vDisk. Later 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:
- 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.
- 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.

- 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.
3. In the Citrix Personal vDisk dialog box, click Update Inventory. This step may take several minutes to complete.
   Important: If you interrupt the following shutdown (even to make a minor update to the image), the Personal vDisk's inventory no longer matches the master image. This causes the Personal vDisk feature to stop working. If you interrupt the shutdown, you must restart the machine, shut it down, and when prompted click Update Inventory again.
4. When the inventory operation shuts down the machine, take a snapshot of the master image.

You can export an inventory to a network share and then import that inventory to a master image. For details, see Export and import a PvD inventory.

How-to: Configure connection throttling settings

The Citrix Broker Service controls the power state of the machines that provide desktops and applications. The Broker Service can control several hypervisors through a Delivery Controller. Broker power actions control the interaction between a Controller and the hypervisor. To avoid overloading the hypervisor, actions that change a machine's power state are assigned a priority and sent to the hypervisor using a throttling mechanism. The following settings affect the throttling. You

specify these values by editing a connection (Advanced page) in Studio.

To configure connection throttling values:

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Edit Connection in the Actions pane.
3. You can change the following values:
   - **Simultaneous actions (all types)** - The maximum number of simultaneous in-progress power actions allowed. This setting is specified as both an absolute value and as a percentage of the connection to the hypervisor. The lower of the two values is used.
     Default = 100 absolute, 20%
   - **Simultaneous Personal vDisk inventory updates** - The maximum number of simultaneous Personal vDisk power actions allowed. This setting is specified as both an absolute value and a percentage of the connection. The lower of the two values is used.
     Default = 50 absolute, 25%

     To calculate the absolute value: determine the total IOPS (TIOPS) supported by the end-user storage (this should be specified by the manufacturer or calculated). Using 350 IOPS per VM (IOPS/VM), determine the number of VMs that should be active at any given time on the storage. Calculate this value by dividing total IOPS by IOPS/VM.

     For example, if the end-user storage is 14000 IPS, the number of active VMs is 14000 IOPS / 350 IOPS/VM = 40.
   - **Maximum new actions per minute** - The maximum number of new power actions that can be sent to the hypervisor per minute. Specified as an absolute value.
     Default = 10

To help identify optimal values for these settings in your deployment:

1. Using the default values, measure the total response time for an image update of a test catalog. This is the difference between the start of an image update (T1) and when the VDA on the last machine in the catalog registers with the Controller (T2). Total response time = T2 - T1.
2. Measure the input/output operations per second (IOPS) of the hypervisor storage during the image update. This data can serve as a benchmark for optimization. (The default values may be the best setting; alternatively, the system might max out of IOPS, which will require lowering the setting values.)
3. Change the “Simultaneous Personal vDisk inventory updates” value as described below (keeping all other settings unchanged).
   1. 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.
   2. 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.
    1. Install the Configuration Manager client on the master image.
    2. Stop the ccmexec service (SMS Agent) and disable it.
    3. Delete SMS or client certificates from the local computer certificate store as follows:
        - Mixed mode: Certificates (Local Computer)\SMS\Certificates
        - Native mode
            - Certificates (Local Computer)\Personal\Certificates
            - Delete the client certificate that was issued by your certificate authority (usually, an internal Public Key Infrastructure)
    4. Delete or rename C:\Windows\smscfg.ini.
2. Remove information that uniquely identifies the client.
    1. (Optional) Delete or move log files from C:\Windows\System32\CCM\Logs.
    2. Install the Virtual Delivery Agent (if not installed previously), and take the PvD inventory.
    3. 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

Mar 02, 2017

You can use the following tools and utilities to tailor, expedite, and monitor PvD operations.

Custom rules files

The custom rule files provided with PvD let you modify the default behavior of PvD image updates in the following ways:

- The visibility of files on the PvD
- How changes made to the files are merged
- Whether the files are writable

For detailed instructions on the custom rules files and the CoW feature, refer to the comments in the files located in C:\ProgramData\Citrix\personal vDisk\Config on the machine where PvD is installed. The files named "custom_*" describe the rules and how to enable them.

Resize and poolstats scripts

Two scripts are provided to monitor and manage the size of PvDs; they are located in the Support\Tools\Scripts folder on the XenDesktop installation media. You can also use the PvD Image Update Monitoring Tool, which is located in the Support\Tools\Scripts\PvdTool folder; see http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/ for details.

Use resize-personalvdisk-pool.ps1 to increase the size of the PvDs in all of the desktops in a catalog. The following snap-ins or modules for your hypervisor must be installed on the machine running Studio:

- XenServer requires XenServerPSSnapin
- vCenter requires vSphere PowerCli
- System Center Virtual Machine Manager requires the VMM console

Use personal-vdisk-poolstats.ps1 to check the status of image updates and to check the space for applications and user profiles in a group of PvDs. Run this script before updating an image to check whether any desktop is running out of space, which helps prevent failures during the update. The script requires that Windows Management Instrumentation (WMI-In) firewall is enabled on the PvD desktops. You can enable it on the master image or through GPO.

If an image update fails, the entry in the Update column gives the reason.

Reset the application area

If a desktop becomes damaged or corrupted (by installing a broken application or some other cause), you can revert the application area of the PvD to a factory-default (empty) state. The reset operation leaves user profile data intact.

To reset the application area of the PvD, use one of the following methods:

- Log on to the user's desktop as Administrator. Launch a command prompt, and run the command C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset.
- Locate the user's desktop in Citrix Director. Click Reset Personal vDisk and then click OK.

Export and import a PvD inventory

The image update process is an integral part of rolling out new images to PvD desktops; it includes adjusting the existing Personal vDisk to work with the new base image. For deployments that use Machine Creations Services (MCS), you can

export an inventory from an active VM to a network share, and then import it into a master image. A differential is calculated using this inventory in the master image. Although using the export/import inventory feature is not mandatory, it can improve the performance of the overall image update process.

To use the export/import inventory feature, you must be an administrator. If required, authenticate to the file share used for the export/import with "net use." The user context must be able to access any file shares used for the export/import.

- To export an inventory, run the export command as an administrator on a machine containing a VDA with PvD enabled (minimum version 7.6):
  Ctxpvdsvc.exe exportinventory "<path-to-export-location>"

  The software detects the current inventory's location and exports the inventory to a folder named "ExportedPvdInventory" to the specified location. Here's an excerpt from the command output:
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory
  \\share location\ExportedInventory
  Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS
  ...
  Exporting current inventory to location \\ ....
  ...
  Deleting any pre-existing inventory folder at \\ ....
  .Successfully exported current inventory to location \\ .... Error code = OPS
- To import a previously-exported inventory, run the import command as an administrator on the master image:

To import

Run the import command as an administrator on the master image.

Ctxpvdsvc.exe importinventory "<path-to-exported-inventory>"

The <path to exported inventory> should be the full path to the inventory files, which is usually <network location\ExportedPvdInventory>.

The inventory is obtained from the import location (where it was previously exported using the exportinventory option) and imports the inventory to the inventory store on the master image. Here's an excerpt of the command output:
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory
\\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \\share location\ExportedInventory\ExportedPvdInventory
...
Successfully added inventory \\share location\ExportedInventory\ExportedPvdInventory to the store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
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

Dec 01, 2014

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 error 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 gold image.
- **There are syntax errors in the rule files. Review the logs for further details.**
  Error code 2. The rule file contains syntax errors. The Personal vDisk log file contains the name of the rule file and line number where the syntax error was found. Fix the syntax error in the rule file and retry the operation.
- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is corrupt or unreadable.**
  Error code 3. The last inventory is stored in “UserData.V2.vhd” in “\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST”. Restore the inventory corresponding to the last version of the master image by importing the ‘VER-LAST’ folder from a known working PvD machine associated with the previous version of the master image.
- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is higher version.**
  Error code 4. This is caused by personal vDisk version incompatibility between the last master image and the current master image. Retry updating the catalog after installing the latest version of personal vDisk in the master image.
- **Change journal overflow was detected.**
  Error code 5. A USN journal overflow was caused by a large number of changes made to the master image while creating the inventory. If this continues to occur after multiple attempts, use procmon to determine if third party software is creating/deleting a large number of files during inventory creation.
- **The Personal vDisk could not find a disk attached to the system for storing user data.**
  Error code 6. First, verify that the PvD disk is attached to the VM through the hypervisor console. This error typically happens due to “Data Leak Prevention” software preventing access to the PvD disk. If the PvD disk is attached to the

VM, try adding an exception for “attached disk” in the “Data Leak Prevention” software configuration.

- **The system has not been rebooted post-installation. Reboot to implement the changes.**
  Error code 7. Restart the desktop and retry the operation.

- **Corrupt installation. Try re-installing Personal vDisk.**
  Error code 8. Install personal vDisk and try again.

- **Personal vDisk inventory is not up to date. Update the inventory in the master image, and then try again.**
  Error code 9. The personal vDisk inventory was not updated in the master image before shutting down the desktop. Restart the master image and shut down the desktop through the “Update personal vDisk” option, and then create a new snapshot; use that snapshot to update the catalog.

- **An internal error occurred while starting the Personal vDisk. Review the Personal vDisk logs for further details.**
  Error code 10. This could be caused by the PvD driver failing to start a virtualization session due to an internal error or personal vDisk corruption. Try restarting the desktop through the Controller. if the problem persists, collect the logs and contact Citrix Support.

- **The Personal vDisk timed out while trying to find a storage disk for users' personalization settings.**
  Error code 11. This error occurs when the PvD driver fails to find the PvD disk within 30 seconds after restart. This is usually caused by an unsupported SCSI controller type or storage latency. If this occurs with all desktops in the catalog, change the SCSI controller type associated with the “Template VM” / “Master VM” to a type supported by personal vDisk technology. If this occurs with only some desktops in the catalog, it might be due to spikes in storage latency due to a large number of desktops starting at the same time. Try limiting the maximum active power actions setting associated with the host connection.

- **The Personal vDisk has been de-activated because an unsafe system shutdown was detected. Restart the machine.**
  Error code 12. This could be due to a desktop failing to complete the boot process with PvD enabled. Try restarting the desktop. If the problem persists, watch the desktop startup through the hypervisor console and check if the desktop is crashing. If a desktop crashes during startup, restore the PvD from backup (if you maintain one) or reset the PvD.

- **The drive letter specified for mounting the Personal vDisk is not available.**
  Error code 13. This could be caused by PvD failing to mount the PvD disk at the mount specified by the administrator. The PvD disk will fail to mount if the drive letter is already used by other hardware. Select a different letter as the mount point for the personal vDisk.

- **Personal vDisk kernel mode drivers failed to install.**
  Error code 14. Personal vDisk installs drivers during the first inventory update after installation. Some antivirus products prevent installation of the driver when attempted outside the context of an installer. Temporarily disable the antivirus real time scan or add exceptions in the antivirus for PvD drivers during the first time inventory creation.

- **Cannot create a snapshot of the system volume. Make sure that the Volume Shadow Copy service is enabled.**
  Error code 15. This could occur because the Volume Shadow Copy service is disabled. Enable the Volume Shadow Copy service and retry taking an inventory.

- **The change journal failed to activate. Try again after waiting for few minutes.**
  Error code 16. Personal vDisk uses change journal for tracking changes made to master image. During an inventory update, if PvD detects that the change journal is disabled, it attempts to enable it; this error occurs when that attempt fails. Wait for few minutes and retry.

- **There is not enough free space in the system volume.**
  Error code 17. There is not enough free space available on the C drive of the desktop for the image update operation. Expand the system volume or removed unused files to free space in the system volume. The image update should begin again after the next restart.

- **There is not enough free space in the Personal vDisk storage. Expand Personal vDisk storage to provide more space.**
  Error code 18. There is not enough free space available on the personal vDisk drive when performing an image update operation. Expand personal vDisk storage or remove unused files to free space in the personal vDisk storage. The image update should restart after next reboot.

- **Personal vDisk storage is over-committed. Expand Personal vDisk storage to provide more space.**
  Error code 19. There is not enough free space available on the personal vDisk drive to fully accommodate thick provisioned “UserData.V2.vhd”. Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

- **Corrupt system registry.**
  Error code 20. The system registry is corrupt, damaged, missing, or unreadable. Reset the personal vDisk or restore it from an earlier backup.

- **An internal error occurred while resetting the Personal vDisk. Check Personal vDisk logs for further details.**
  Error code 21. This is a catch-all for all the errors encountered during a personal vDisk reset. Collect the logs and contact Citrix Support.

- **Failed to reset the Personal vDisk because there is not enough free space in the personal vDisk storage.**
  Error code 22. There is not enough free space available on the Personal vDisk drive when performing a reset operation. Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

Error messages: earlier than 7.6

The following errors are valid for PvD 7.x versions earlier than 7.6:

- **Startup failed. Personal vDisk was unable to find a storage disk for user personalization settings.**
  The PvD software could not find the Personal vDisk (by default, the P: drive) or could not mount it as the mount point selected by the administrator when they created the catalog.
  - Check the PvD service log for following entry: "PvD 1 status --> 18:183".
  - If you are using a version of PvD earlier than Version 5.6.12, upgrading to the latest version resolves this issue.
  - If you are using Version 5.6.12 or later, use the disk management tool (diskmgmt.msc) to determine whether the P: drive is present as an unmounted volume. If present, run chkdsk on the volume to determine if it is corrupt, and try to recover it using chkdsk.
- **Startup failed. Citrix Personal vDisk failed to start. For further assistance .... Status code: 7, Error code: 0x70**
  Status code 7 implies that an error was encountered while trying to update the PvD. The error could be one of the following:

Error code	Description
0x20000001	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000004	Failed to acquire required privileges for updating the PvD.

Error code	Description
0x20000006	Failed to load hive from the PvD image or from PvD inventory, most likely due to corrupt PvD image or inventory.
0x20000007	Failed to load the file system inventory, most likely due to a corrupt PvD image or inventory.
0x20000009	Failed to open the file containing file system inventory, most likely due to a corrupt PvD image or inventory.
0x2000000B	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000010	Failed to load the diff package.
0x20000011	Missing rule files.
0x20000021	Corrupt PvD inventory.
0x20000027	The catalog "MojoControl.dat" is corrupt.
0x2000002B	Corrupt or missing PvD inventory.
0x2000002F	Failed to register user installed MOF on image update, upgrade to 5.6.12 to fix the issue.
0x20000032	Check the PvDactivation.log.txt for the last log entry with a Win32 error code.
0x20	Failed to mount application container for image update, upgrade to 5.6.12 to fix the issue.
0x70	There is not enough space on the disk.

- **Startup failed. Citrix Personal vDisk failed to start [or Personal vDisk encountered an internal error]. For further assistance ... Status code: 20, Error code 0x20000028**
  The personal vDisk was found but a PvD session could not be created.

  Collect the logs and check SysVol-IvmSupervisor.log for session creation failures:
  1. Check for the following log entry " IvmpNativeSessionCreate: failed to create native session, status XXXXX".
  2. If the status is 0xc00002cf, fix the problem by adding a new version of the master image to the catalog. This status code implies that the USN Journal overflowed due to a large number of changes after an inventory update.
  3. Restart the affected virtual desktop. If the problem persists, contact Citrix Technical Support.
- **Startup failed. Citrix Personal vDisk has been deactivated because an unsafe system shutdown was detected. To retry, select Try again. If the problem continues, contact your system administrator.**
  The pooled VM cannot complete its startup with the PvD enabled. First determine why startup cannot be completed. Possible reasons are that a blue screen appears because:
  - An incompatible antivirus product is present, for example old versions of Trend Micro, in the master image.

- The user has installed software that is incompatible with PvD. This is unlikely, but you can check it by adding a new machine to the catalog and seeing whether it restarts successfully.
- The PvD image is corrupt. This has been observed in Version 5.6.5.

To check if the pooled VM is displaying a blue screen, or is restarting prematurely:

- Log on to the machine through the hypervisor console.
- Click Try Again and wait for the machine to shut down.
- Start the machine through Studio.
- Use the hypervisor console to watch the machine console as it starts.

Other troubleshooting:

- Collect the memory dump from the machine displaying the blue screen, and send it for further analysis to Citrix Technical Support.
- Check for errors in the event logs associated with the PvD:
  1. Mount UserData.V2.vhd from the root of the P: drive using DiskMgmt.msc by clicking Action > Attach VHD.
  2. Launch Eventvwr.msc.
  3. Open the system event log (Windows\System32\winevt\logs\system.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.
  4. Open the application event log (Windows\System32\winevt\logs\application.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.

- **The Personal vDisk cannot start. The Personal vDisk could not start because the inventory has not been updated. Update the inventory in the master image, then try again. Status code: 15, Error code: 0x0**
  The administrator selected an incorrect snapshot while creating or updating the PvD catalog (that is, the master image was not shut down using Update Personal vDisk when creating the snapshot).

Events logged by Personal vDisk

If Personal vDisk is not enabled, you can view the following events in Windows Event Viewer. Select the Applications node in the left pane; the Source of the events in the right pane is Citrix Personal vDisk. If Personal vDisk is enabled, none of these events are displayed.

An Event ID of 1 signifies an information message, an ID of 2 signifies an error. Not all events may be used in every version of Personal vDisk.

Event ID	Description
1	Personal vDisk Status: Update Inventory Started.
1	Personal vDisk Status: Update Inventory completed. GUID: %s.
1	Personal vDisk Status: Image Update Started.
1	Personal vDisk Status: Image Update completed.
1	Reset in progress.
1	OK.

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.

Remove components

Sep 09, 2015

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.

To 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.

To 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
```

To 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 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.

Upgrade and migrate

May 31, 2016

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:

- From XenDesktop version 5 (or a later version) to the current XenDesktop release
- From XenApp version 7.5 to the current XenApp release

You can also upgrade a XenApp 6.5 worker server to a curent VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5.

To upgrade a XenDesktop 5 (or later) farm or a XenApp 7.5 Site:

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 more information, see Upgrade a deployment.

For information about installing Controller hotfixes, see Knowledge Center article CTX201988.

To upgrade a XenApp 6.5 worker server to a current VDA:

1. Run the product installer on the XenApp 6.5 worker server. The software removes the server from the XenApp 6.5 farm, removes the XenApp 6.5 software, and installs a current VDA for Windows Server OS.
2. After upgrading the server, add it to Machine Catalogs and Delivery Groups in the current Site.

For more information, see Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS.

Migrate

Migrating moves data from an earlier deployment to the newest version. You can migrate a XenApp 6.5 or a XenDesk 4 deployment. 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.

To migrate from XenApp 6.5:

1. Install core components and create a new XenApp Site.
2. From the XenApp 6.5 controller, use PowerShell cmdlets to export policy and/or farm data to XML files. You can edit the XML file content to tailor the information you will import.
3. From the new Site, use PowerShell cmdlets and the XML files to import policy and/or application data to the new Site.
4. Complete post-migration tasks on the new Site.

For more information, see Migrate XenApp 6.x.

To migrate from XenDesktop 4:

1. Install core components and create a new XenDesktop Site.
2. From the XenDesktop 4 farm, use the export command tool to export farm data to an XML file. You can edit the XML file content to tailor the information you will import.
3. From the new Site, use the import command tool and the XML file to import the farm data to the new Site.
4. Complete post-migration tasks on the new Site.

For more information, see Migrate XenDesktop 4.

Upgrade a deployment

Aug 15, 2016

In this article:

Introduction

You can upgrade certain deployments to newer versions without having to first set up new machines or Sites; this is called an in-place upgrade. You can upgrade:

- From XenDesktop version 5 (or a later version) to the latest released (current) XenDesktop version
- From XenApp version 7.5 (or a later version) to the latest released (current) XenApp version

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. The installer determines which components require upgrading and then starts the upgrade at your command. After upgrading the components, you use the newly upgraded Studio to upgrade the Site database and the Site.

In this content, the word product refers to XenApp 7.x or XenDesktop 7.x, unless otherwise noted.

Which product component versions can be upgraded

Using the product installer and Studio, you can upgrade:

- Delivery Controllers 5 or later
- VDA 5.0 SP1 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 5.0 SP1 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 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

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.
  - 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.
- Microsoft System Center Virtual Machine Manager SCVMM. The current product supports SCVMM 2012 and SCVMM 2012 SP1; XenDesktop 5.x supports earlier versions. Use the following upgrade sequence to avoid downtime:
  1. If you have Controllers running versions earlier than XenDesktop 5.6 FP1, upgrade them to XenDesktop 5.6 FP1 (see the XenDesktop documentation for that version).
  2. Upgrade the SCVMM server to SCVMM 2012; see the Microsoft documentation for instructions.
  3. Upgrade XenDesktop components to the current version.
  4. Optionally, upgrade the SCVMM server to SCVMM 2012 SP1.
- StoreFront.

Requirements, limits, and preparation

- You must use the product installer's graphical or command-line interface to upgrade core components and VDAs; you cannot import or migrate data from an earlier version.
- 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, if an upgrade includes new versions of the Controller and Studio, and you upgrade only 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.
- Before upgrading the Citrix License Server, be sure your 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 2016.0518.
- You cannot upgrade XenDesktop Express Edition. Obtain and install a license for a currently supported edition, then upgrade it.
- Before beginning any upgrade activity, back up the database, as described in CTX135207, so you can restore it if any issues are discovered after the database upgrade.
- Optionally, back up templates and upgrade hypervisors, if used.
- Make sure the Site is in a stable and functional state before starting an upgrade. If a Site has issues, upgrading will not fix them, and could leave the Site in a complex state that is difficult to recover from.
- Before starting an upgrade, close all programs that could 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.)
- If you must continue to run earlier version Sites and current version Sites, see Mixed environment considerations.
- If you have VDAs installed on Windows XP or Windows Vista machines, see VDAs on machines running Windows XP or Windows Vista.
- If you do not plan to upgrade all VDAs to the latest version, review Mixed VDA support.

- If your deployment includes Web Interface, Citrix recommends using StoreFront.
- In addition to being a domain user, you must be a local administrator on the machines where you are upgrading product components.
- Review the upgrade sequence below so you can plan for and mitigate potential outages.

You cannot upgrade:

- From an Early Release or Technology Preview version
- From a XenApp version earlier than 7.5 (except replacing XenApp 6.5 software on a server with a current VDA for Server OS; see Migrate XenApp 6.x)
- From a XenDesktop version earlier than 5.6; see Migrate XenDesktop 4

When you upgrade, you do not choose or specify the product (XenApp or XenDesktop), which was set during the initial installation.

Recommendation: Before and during the upgrade, check Site health. Run **Test Site** at the following checkpoints:

- Before making backups.
- After each Controller is upgraded.
- After VDAs and other components are upgraded.
- After the Site is upgraded from 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 7.1 Site and a XenDesktop 7.5 Site). For details, see the StoreFront documentation.

- In a mixed environment, continue using the Studio and Director versions for each release, but make sure 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. See Mixed VDA considerations below.

- 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.
- Configuring App-V applications from Studio.
- Configuring Receiver StoreFront addresses from Studio.
- Automatic support for Microsoft Windows KMS licensing when using Machine Creation Services. SeeCTX128580.
- 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

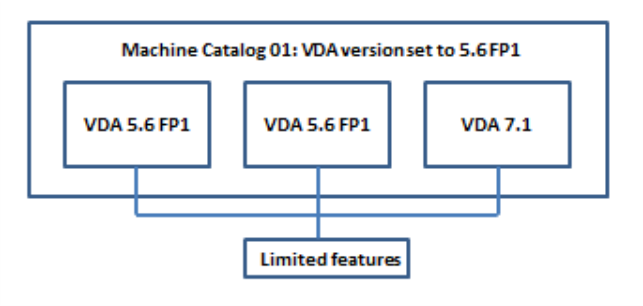
To upgrade VDAs installed on machines running Windows 8.x or Window 7 to Windows 10, Citrix recommends reimaging Windows 7 and Windows 8.x machines to Windows 10 and then installing the supported VDA for Windows 10. If reimaging is not an option, uninstall the VDA prior to upgrading the operating system, 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. For example, to use the session prelaunch, session linger, and unauthenticated users features in the 7.6 release, the VDAs must have a minimum version of 7.6 installed.

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 can have unintended effects

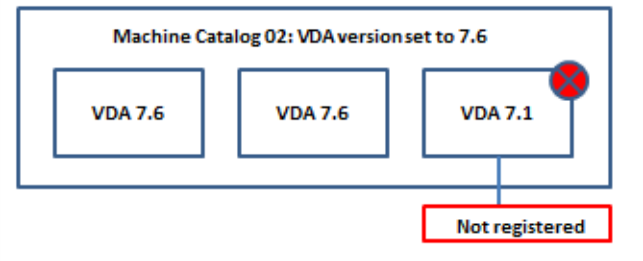
As noted above, if your deployment includes Windows XP and Windows Vista systems, you must use an earlier VDA version, and the machine catalog containing those machines must specify VDA version 5.6 FP1. The VDAs will register successfully with the Controller, but those machines will be unable to use many of the new features in the 7.x versions (including StoreFront). This also applies to any machines you add to that catalog that have 7.x version VDAs. The following graphic illustrates this.



In the above case, if you must continue to use older VDAs, place them in a machine catalog by themselves.

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.

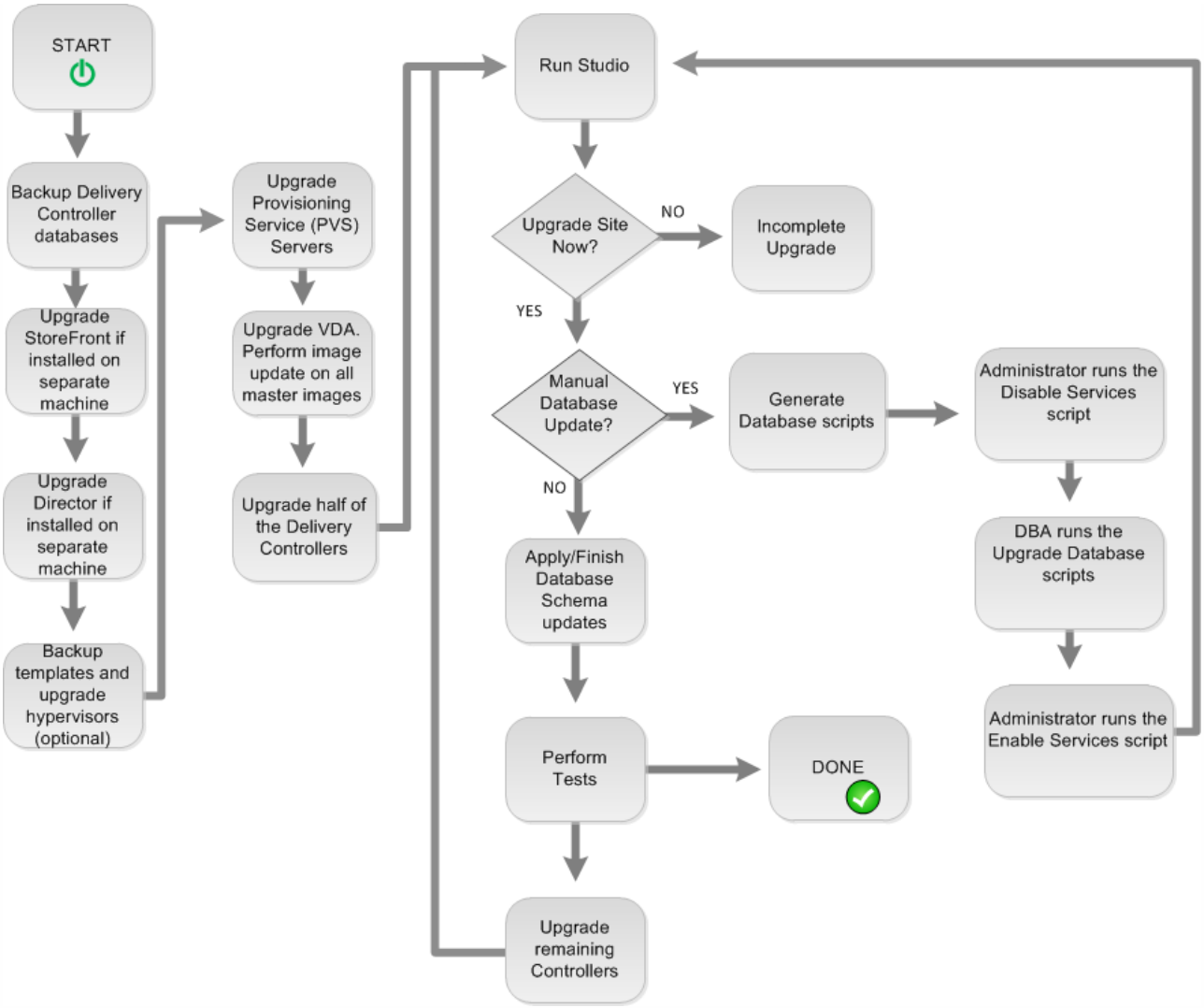
For example, assume the most recent VDA version is 7.6. You create a machine catalog with the default VDA setting: "7.6 (recommended, to access the latest features)." You add three machines to that catalog: two with VDA 7.6 and one with VDA 7.1.



In this example, the machine with VDA 7.1 will not register with the Controller. If you cannot upgrade that VDA, consider creating a separate machine catalog configured with a VDA setting of "version 7.0 or later" and adding that machine. Although that machine will not be able to take advantage of new 7.6 features, it will be able to register with the Controller.

Upgrade sequence

The upgrade sequence is illustrated below; descriptions follow. If components are installed on different machines, run the installer on each of those machines.



Upgrade components

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 (in the preferred order: License Server, StoreFront, and then Director).
2. Upgrade the Provisioning Services servers and clients, using the guidance in the Provisioning Services documentation.
3. Run the product installer on machines containing VDAs. Although you can upgrade VDAs before or after upgrading the Controllers, Citrix recommends you do so before, because it allows you to quickly enable new features after the upgrade. When upgrading VDAs from an earlier 7.x version that are installed on physical machines (including Remote PC Access), use the command-line interface with the parameter: /EXCLUDE "Personal vDisk","Machine Identity Service". For example:

   C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"

4. Run the product installer on half of the Controllers. (This will also upgrade 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 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 of the Controllers you upgraded in the previous step, 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 database and 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, close and then reopen Studio.
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 Customer Experience Improvement Program (CEIP), which collects anonymous information about your deployment. That information is then used to improve product quality, reliability, and performance.
11. After upgrading components, the database, and the Site, use Studio to:
    - 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.
    - Update all master images that use the upgraded VDA.
    - Upgrade Machine Catalogs and Delivery Groups.

Upgrade the Site database 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.

- 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. If the SQL scripts are run manually, they should be run using either the SQLCMD utility or using the SQL Management Studio in SQLCMD mode. Inaccurate errors may result otherwise.

Important: Citrix strongly recommends you back up the database before upgrading, as described in 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: This process includes generating and running scripts.

1. Launch the newly upgraded Studio. After you choose to manually upgrade the Site, 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:

Script	Description
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, using a tool such as SQL Server Management Studio.
UpgradeMonitorDatabase.sql	SQL script to be run by the database administrator on the server containing the Monitor database, using a tool such as SQL Server Management Studio.
UpgradeLoggingDatabase.sql	SQL script to be run by the database administrator on the server containing the Configuration Logging database, using a tool such as SQL Server Management Studio. 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 you complete the displayed checklist tasks, select **Finish upgrade**.

Upgrade a XenApp 6.5 worker to a new VDA

Aug 25, 2014

When you run the current product installer on a XenApp 6.5 worker server, it:

- Removes the server from the XenApp 6.5 farm (this task automatically invokes the XenApp 6.5 installer's command-line interface)
- Removes the XenApp 6.5 software
- Installs a new (XenApp 7.6 or later supported release) VDA for Windows Server OS

When you use the installer's graphical interface, you are guided through the same wizard that you used when installing VDAs for Windows Server OS in your new XenApp Site. Similarly, the command-line interface uses the same commands and parameters you use to install other VDAs.

NOTE: Although you can upgrade a XenApp 6.5 worker server, installing the current VDA software on a clean machine provides better security.

You are probably already familiar with using the installer from installing your XenApp core components and other VDAs. Launch the installer (Install using the graphical interface) or issue the command (Install using the command line) on the XenApp 6.5 worker server.

Good to know:

- This upgrade is valid on XenApp 6.5 servers that are configured in session-host only mode (also called session-only or worker servers).
- Uninstalling XenApp 6.5 requires several server restarts. When using the command-line interface, you can use the /NOREBOOT option to inhibit that automatic action; however, you must restart the server for the uninstallation and subsequent installation to proceed.
- If an error occurs during the XenApp uninstallation process, check the uninstall error log referenced in the error message. Uninstall log files reside in the folder "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\."
- After the upgrade, review IMA-specific settings and registry entries, plus HDX-related system settings and registries. Some settings may no longer apply or might not work in the same way.
- After you upgrade the XenApp 6.5 worker servers, from Studio in the new XenApp Site, create Machine Catalogs (or edit existing catalogs) for the upgraded workers.
- If you migrated policy and application settings from a XenApp 6.5 controller server (see Migrate XenApp 6.x), assign the Delivery Groups containing the migrated published applications to the machine catalog that hosted those applications in XenApp 6.5.

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 the following:
     1. Citrix XenApp 6.5
     2. Microsoft Visual C++ 2005 Redistributable (x64), version 8.0.56336
  4. Restart the server.
  5. Run the XenApp installer to install the VDA for Windows Server OS.

Migrate XenApp 6.x

Sep 01, 2015

Important: Review this entire article before beginning a migration.

The XenApp 6.x Migration Tool (the migration tool) is a collection of PowerShell scripts containing cmdlets that migrate XenApp 6.x (6.0 or 6.5) policy and farm data. On the XenApp 6.x controller server, you run export cmdlets that gather that data into XML files. Then, from the XenApp 7.6 Controller, you run import cmdlets that create objects using the data gathered during the export.

A video overview of the migration tool is available here.

The following sequence summarizes the migration process; details are provided later.

1. On a XenApp 6.0 or 6.5 controller:
   1. Import the PowerShell export modules.
   2. Run the export cmdlets to export policy and/or farm data to XML files.
2. Copy the XML files (and icons folder if you chose not to embed them in the XML files during the export) to the XenApp 7.6 Controller.
3. On the XenApp 7.6 Controller:
   1. Import the PowerShell import modules.
   2. Run the import cmdlets to import policy and/or farm data (applications), using the XML files as input.
4. Complete post-migration steps.

Before you run an actual migration, you can export your XenApp 6.x settings and then perform a preview import on the XenApp 7.6 site. The preview identifies possible failure points so you can resolve issues before running the actual import. For example, a preview might detect that an application with the same name already exists in the new XenApp 7.6 site. You can also use the log files generated from the preview as a migration guide.

Unless otherwise noted, the term 6.x refers to XenApp 6.0 or 6.5.

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 the support forum http://discussions.citrix.com/forum/1411-xenapp-7x/, so that Citrix can investigate them for potential improvements to the tool.
- 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
- 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.

Module or file	Description
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.
ImportXAFarm.psd1	PowerShell manifest file for script module ImportXAFarm.psm1.
PolicyData.xsd	XML schema for policy data.
XAFarmData.xsd	XML schema for XenApp farm data.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.
XmlUtilities.psm1	Shared PowerShell script module that contains XML functions.

Limitations

- Not all policies settings are imported; see Policy settings not imported. Settings that are not supported are ignored and noted in the log file.
- While all application details are collected in the output XML file during the export operation, only server-installed applications are imported into the XenApp 7.6 site. Published desktops, content, and most streamed applications are not supported (see the Import-XAFarm cmdlet parameters in Step-by-step: import data for exceptions).
- Application servers are not imported.
- Many application properties are not imported because of differences between the XenApp 6.x Independent Management Architecture (IMA) and the XenApp 7.6 FlexCast Management Architecture (FMA) technologies; see Application property mapping.
- A Delivery Group is created during the import. See Advanced use for details about using parameters to filter what is imported.
- Only Citrix policy settings created with the AppCenter management console are imported; Citrix policy settings created with Windows Group Policy Objects (GPOs) are not imported.
- The migration scripts are intended for migrations from XenApp 6.x to XenApp 7.6 only.
- Nested folders greater than five levels deep are not supported by Studio and will not be imported. If your application folder structure includes folders more than five levels deep, consider reducing the number of nested folder levels before importing.

Security considerations

The XML files created by the export scripts can contain sensitive information about your environment and organization, such as user names, server names, and other XenApp farm, application, and policy configuration data. Store and handle these files in secure environments.

Carefully review the XML files before using them as input when importing policies and applications, to ensure they contain no unauthorized modifications.

Policy object assignments (previously known as policy filters) control how policies are applied. After importing the policies, carefully review the object assignments for each policy to ensure that there are no security vulnerabilities resulting from the import. Different sets of users, IP addresses, or client names may be applied to the policy after the import. The allow/deny settings may have different meanings after the import.

Logging and error handling

The scripts provide extensive logging that tracks all cmdlet executions, informative messages, cmdlet execution results, warnings, and errors.

- Most Citrix PowerShell cmdlet use is logged. All PowerShell cmdlets in the import scripts that create new site objects are logged.
- Script execution progress is logged, including the objects being processed.
- Major actions that affect the state of the flow are logged, including flows directed from the command line.
- All messages printed to the console are logged, including warnings and errors.
- Each line is time-stamped to the millisecond.

Citrix recommends specifying a log file when you run each of the export and import cmdlets.

If you do not specify a log file name, the log file is stored in the current user's home folder (specified in the PowerShell $HOME variable) if that folder exists; otherwise, it is placed in the script's current execution folder. The default log name is "XFarmYYYYMMDDHHmmSS-xxxxxx" where the last six digits constitute a random number.

By default, all progress information is displayed. To suppress the display, specify the NoDetails parameter in the export and import cmdlet.

Generally, a script stops execution when an error is encountered, and you can run the cmdlet again after clearing the error conditions.

Conditions that are not considered errors are logged; many are reported as warnings, and script execution continues. For example, unsupported application types are reported as warnings and are not imported. Applications that already exist in the XenApp 7.6 site are not imported. Policy settings that are deprecated in XenApp 7.6 are not imported.

The migration scripts use many PowerShell cmdlets, and all possible errors might not be logged. For additional logging coverage, use the PowerShell logging features. For example, PowerShell transcripts log everything that is printed to the screen. For more information, see the help for the Start-Transcript and Stop-Transcript cmdlets.

Requirements, preparation, and best practices

Important: Remember to review this entire article before beginning a migration.
You should understand basic PowerShell concepts about execution policy, modules, cmdlets, and scripts. Although extensive scripting expertise is not required, you should understand the cmdlets you execute. Use the Get-Help cmdlet to review each migration cmdlet's help before executing it. For example:

```
Get-Help -full Import-XAFarm
```

Specify a log file on the command line and always review the log file after running a cmdlet. If a script fails, check and fix the error identified in the log file and then run the cmdlet again.

Good to know:

- To facilitate application delivery while two deployments are running (the XenApp 6.x farm and the new XenApp 7.6 site), you can aggregate both deployments in StoreFront or Web Interface. See the eDocs documentation for your StoreFront or Web Interface release (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 executed.
- In the step-by-step sections below, most <string> parameter values show surrounding quotation marks. These are optional for single-word strings.

For exporting from the XenApp 6.x server:

- The export must be run on a XenApp 6.x server configured with the controller and session-host (commonly known as controller) server mode.
- To run the export cmdlets, you must be a XenApp administrator with permission to read objects. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- Ensure the XenApp 6.x farm is in a healthy state before beginning an export. Back up the farm database. Verify the farm's integrity using the Citrix IMA Helper utility (CTX133983): from the IMA Datastore tab, run a Master Check (and then use the DSCheck option to resolve invalid entries). Repairing issues before the migration helps prevent export failures. For example, if a server was removed improperly from the farm, its data might remain in the database; that could cause cmdlets in the export script to fail (for example, Get-XAServer -ZoneName). If the cmdlets fail, the script fails.
- You can run the export cmdlets on a live farm that has active user connections; the export scripts read only the static farm configuration and policy data.

For importing to the XenApp 7.6 server:

- You can import data to XenApp 7.6 deployments (and later supported versions). You must install a XenApp 7.6 Controller and Studio, and create a site before importing the data you exported from the XenApp 6.x farm. Although VDAs are not required to import settings, they allow application file types to be made available.
- To run the import cmdlets, you must be a XenApp administrator with permission to read and create objects. A Full Administrator has these permissions. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- No other user connections should be active during an import. The import scripts create many new objects, and disruptions may occur if other users are changing the configuration at the same time.

Remember that you can export data and then use the -Preview parameter with the import cmdlets to see what would happen during an actual import, but without actually importing anything. The logs will indicate exactly what would happen during an actual import; if errors occur, you can resolve them before starting an actual import.

Step-by-step: export data

A video of an export walk-through is available here.

Complete the following steps to export data from a XenApp 6.x controller to XML files.

1. Download the XAMigration.zip migration tool package from the Citrix download site. For convenience, place it on a network file share that can be accessed by both the XenApp 6.x farm and the XenApp 7.6 site. Unzip XAMigration.zip on the network file share. There should be two zip files: ReadIMA.zip and ImportFMA.zip.
2. Log on to the XenApp 6.x controller as a XenApp administrator with at least read-only permission and Windows permission to run PowerShell scripts.
3. Copy ReadIMA.zip from the network file share to the XenApp 6.x controller. Unzip and extract ReadIMA.zip on the controller to a folder (for example: C:\XAMigration).
4. Open a PowerShell console and set the current directory to the script location. For example:
   ```
   cd C:\XAMigration
   ```
5. Check the script execution policy by running Get-ExecutionPolicy.

6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example:
   `Set-ExecutionPolicy RemoteSigned`
7. Import the module definition files ExportPolicy.psd1 and ExportXAFarm.psd1:
   `Import-Module .\ExportPolicy.psd1`

   `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 "<string>.xml"	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist. Default: None; this parameter is required.
-LogFile "<string>"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console

   Example: The following cmdlet exports policy information to the XML file named MyPolicies.xml. The operation is logged to the file named MyPolicies.log.
   `Export-Policy -XmlOutputFile ".\MyPolicies.XML"`
   `-LogFile ".\MyPolicies.Log"`
9. To export farm data, run the Export-XAFarm cmdlet, specifying a log file and an XML file.

Parameter	Description
-XmlOutputFile "<string>.xml"	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist. Default: None; this parameter is required.
-LogFile "<string>"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten

Parameter	Description
-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.
-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: The purpose of the -IgnoreOthers switch is to allow you to proceed with an export when an error exists that would not affect the actual data being used for the exporting or importing process.
-AppLimit <integer>	Number of applications to be exported. See 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 <integer>	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

A video of an import walk-through is available here.

Remember that you can run a preview import (by issuing the Import-Policy or Import-XAFarm cmdlet with the Preview parameter) and review the log files before performing an actual import.

Complete the following steps to import data to a XenApp 7.6 site, using the XML files generating from the export.

1. Log on to the XenApp 7.6 controller as an administrator with read-write permission and Windows permission to run PowerShell scripts.
2. If you have not unzipped the migration tool package XAMigration on the network file share, do so now. Copy ImportFMA.zip from the network file share to the XenApp 7.6 Controller. Unzip and extract ImportFMA.zip on the Controller to a folder (for example: C:\XAMigration).
3. Copy the XML files (the output files generated during the export) from the XenApp 6.x controller to the same location on the XenApp 7.6 Controller where you extracted the ImportFMA.zip files.
   If you chose not to embed the application icon data in the XML output file when you ran the Export-XAFarm cmdlet, be sure to copy the icon data folder and files to the same location on the XenApp 7.6 controller as the output XML file containing the application data and the extracted ImportFMA.zip files.

4. Open a PowerShell console and set the current directory to the script location.
   cd C:\XAMigration
5. Check the script execution policy by running Get-ExecutionPolicy.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example:
   Set-ExecutionPolicy RemoteSigned
7. Import the PowerShell module definition files ImportPolicy.psd1 and ImportXAFarm.psd1:
   Import-Module .\ImportPolicy.psd1

   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.

Parameter	Description
-XmlInputFile "<string>.xml"	XML input file name; this file contains data collected from running the Export-Policy cmdlet. Must have an .xml extension. Default: None; this parameter is required.
-XsdFile "<string>"	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 "<string>"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import. Default: False; a real import occurs

   Example: The folowing cmdlet imports policy data from the XML file named MyPolcies.xml. The operation is logged to the file named MyPolicies.log.
   Import-Policy -XmlInputFile ".\MyPolicies.XML"
   -LogFile ".\MyPolicies.Log"
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 "<string>.xml"	XML input file name; this file contains data collected from running the Export-XAFarm cmdlet. Must have an .xml extension. Default: None; this parameter is required.
-XsdFile "<string>"	XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use for how-to-use information. Default: XAFarmData.XSD

Parameter	Description
-LogFile "<string>"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import. Default: False; a real import occurs
-DeliveryGroupName "<string>"	Delivery Group name for all imported applications. See Advanced use for how-to-use information. Default: "<xenapp-farm-name> - Delivery Group"
-MatchFolder "<string>"	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 "<string>"	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 "<string>"	Import only those applications from servers whose names match the string. See Advanced use for how-to-use information.
-NotMatchServer "<string>"	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 "<string>"	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
-NotMatchWorkerGroup "<string>"	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 "<string>"	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 "<string>"	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

Parameter	Description
-IncludeStreamedApps	Import applications of type "StreamedToClientOrServerInstalled" . (No other streamed applications are imported.) Default: Streamed applications are not imported
-IncludeDisabledApps	Import applications that have been marked as disabled. Default: Disabled applications are not imported

Example: The following cmdlet imports applications from the XML file named MyFarm.xml. The operation is logged to the file named MyFarm.log.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

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.

- **Policies and policy settings**
  Importing policies is essentially a copy operation, with the exception of deprecated settings and policies, which are not imported. The post-migration check essentially involves comparing the two sides.

  1. The log file lists all the policies and settings imported and ignored. First, review the log file and identify which settings and policies were not imported.
  2. Compare the XenApp 6.x policies with the policies imported to XenApp 7.6. The values of the settings should remain the same (except for deprecated policy settings, as noted in the next step).
     - If you have a small number of policies, you can perform a side-by-side visual comparison of the policies displayed in the XenApp 6.x AppCenter and the policies displayed in the XenApp 7.6 Studio.
     - If you have a large number of policies, a visual comparison might not be feasible. In such cases, use the policy export cmdlet (Export-Policy) to export the XenApp 7.6 policies to a different XML file, and then use a text diff tool (such as windiff) to compare that file's data to the data in the XML file used during the policy export from XenApp 6.x.
  3. Use the information in the Policy settings not imported section to determine what might have changed during the import. If a XenApp 6.x policy contains only deprecated settings, as a whole policy, it is not imported. For example, if a XenApp 6.x policy contains only HMR test settings, that policy is completely ignored because there is no equivalent setting supported in XenApp 7.6.
     Some XenApp 6.x policy settings are no longer supported, but the equivalent functionality is implemented in XenApp 7.6. For example, in XenApp 7.6, you can configure a restart schedule for Server OS machines by editing a Delivery Group; this functionality was previously implemented through policy settings.
  4. Review and confirm how filters will apply to your XenApp 7.6 site versus their use in XenApp 6.x; significant differences between the XenApp 6.x farm and the XenApp 7.6 site could change the effect of filters.

- **Filters**
  Carefully examine the filters for each policy. Changes may be required to ensure they still work in XenApp 7.6 as originally intended in XenApp 6.x.

Filter	Considerations
Access Control	Access Control Should contain the same values as the original XenApp 6.x filters and should work without requiring changes.
Citrix CloudBridge	A simple Boolean; should work without requiring changes.
Client IP Address	Lists client IP address ranges; each range is either allowed or denied. The import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Client Name	Similar to the Client IP Address filter, the import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Organizational Unit	Values might be preserved, depending on whether or not the OUs can be resolved at the time they are imported. Review this filter closely, particularly if the XenApp 6.x and XenApp 7.6 machines reside in different domains. If you do not configure the filter values correctly, the policy may be applied to an incorrect set of OUs. The OUs are represented by names only, so there is a small chance that an OU name will be resolved to an OU containing different members from the OUs in the XenApp 6.x domain. Even if some of the values of the OU filter are preserved, you should carefully review the values.
User or Group	Values might be preserved, depending on whether or not the accounts can be resolved at the time they are imported. Similar to OUs, the accounts are resolved using names only, so if the XenApp 7.6 site has a domain with the same domain and user names, but are actually two different domains and users, the resolved accounts could be different from the XenApp 6.x domain users. If you do not properly review

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.

and modify the filter values, incorrect policy applications can occur.

To recap, filters that involve domain user changes require the most attention if the XenApp 6.x farm and the XenApp 7.6 site are in different domains. Because the import script uses only strings of domain and user names to resolve users in the new domain, some of the accounts might be resolved and others might not. While there is only a small chance that different domains and users have the same name, you should carefully review these filters to ensure they contain correct values.

- **Applications**
  The application importing scripts do not just import applications; they also create objects such as Delivery Groups. If the application import involves multiple iterations, the original application folder hierarchies can change significantly.
  1. First, read the migration log files that contain details about which applications were imported, which applications were ignored, and the cmdlets that were used to create the applications.
  2. For each application:
     - Visually check to ensure the basic properties were preserved during the import. Use the information in 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.
  3. Application servers are not imported. This means that none of the imported applications can be accessed yet. The Delivery Groups that contain these applications must be assigned machine catalogs that contain the machines that have the published applications' executable images. For each application:
     - Ensure that the executable name and the working directory point to an executable that exists in the machines assigned to the Delivery Group (through the machine catalogs).
     - Check a command line parameter (which may be anything, such as file name, environment variable, or executable name). Verify that the parameter is valid for all the machines in the machine catalogs assigned to the Delivery Group.
- **Log files**
  The log files are the most important reference resources for an import and export. This is why existing log files are not overwritten by default, and default log file names are unique.

  As noted in the "Logging and error handling" section, if you chose to use additional logging coverage with the PowerShell Start-Transcript and Stop-Transcript cmdlets (which record everything typed and printed to the console), that output, together with the log file, provides a complete reference of import and export activity.

  Using the time stamps in the log files, you can diagnose certain problems. For example, if an export or import ran for a very long time, you could determine if a faulty database connection or resolving user accounts took most of the time.

  The commands recorded in the log files also tell you how some objects are read or created. For example, to create a Delivery Group, several commands are executed to not only create the Delivery Group object itself, but also other objects such as access policy rules that allow application objects to be assigned to the Delivery Group.

  The log file can also be used to diagnose a failed export or import. Typically, the last lines of the log file indicate what caused the failure; the failure error message is also saved in the log file. Together with the XML file, the log file can be used to determine which object was involved in the failure.

After reviewing and testing the migration, you can:

1. Upgrade your XenApp 6.5 worker servers to current Virtual Delivery Agents (VDAs) by running the 7.6 installer on the server, which removes the XenApp 6.5 software and then automatically installs a current VDA. See Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS for instructions.
   For XenApp 6.0 worker servers, you must manually uninstall the XenApp 6.0 software from the server. You can then use the 7.6 installer to install the current VDA. You cannot use the 7.6 installer to automatically remove the XenApp 6.0 software.
2. From Studio in the new XenApp site, create machine catalogs (or edit existing catalogs) for the upgraded workers.
3. Add the upgraded machines from the machine catalog to the Delivery Groups that contain the applications installed on those VDAs for Windows Server OS.

Advanced use

By default, the Export-Policy cmdlet exports all policy data to an XML file. Similarly, Export-XAFarm exports all farm data to an XML file. You can use command line parameters to more finely control what is exported and imported.

- **Export applications partially** - If you have a large number of applications and want to control how many are exported to the XML file, use the following parameters:
  - AppLimit - Specifies the number of applications to export.
  - SkipApps - Specifies the number of applications to skip before exporting subsequent applications.

  You can use both of these parameters to export large quantities of applications in manageable chunks. For example, the first time you run Export-XAFarm, you want to export only the first 200 applications, so you specify that value in the AppLimit parameter.

```
Export-XAFarm -XmlOutputFile "Apps1-200.xml"
-AppLimit "200"
```

  The next time you run Export-XAFarm, you want to export the next 100 applications, so you use the SkipApps parameter to disregard the applications you've already exported (the first 200), and the AppLimit parameter to export the next 100 applications.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"
```

-AppLimit "100" -SkipApps "200"

- **Do not export certain objects** - Some objects can be ignored and thus do not need to be exported, particularly those objects that are not imported; see Policy settings not imported and Application property mapping. Use the following parameters to prevent exporting unneeded objects:
  - IgnoreAdmins - Do not export administrator objects
  - IgnoreServers - Do not export server objects
  - IgnoreZones - Do not export zone objects
  - IgnoreOthers - Do not export configuration logging, load evaluator, load balancing policy, printer driver, and worker group objects
  - IgnoreApps - Do not export applications; this allows you to export other data to an XML output file and then run the export again to export applications to a different XML output file.

  You can also use these parameters to work around issues that could cause the export to fail. For example, if you have a bad server in a zone, the zone export might fail; if you include the IgnoreZones parameter, the export continues with other objects.

- **Delivery Group names** - If you do not want to put all of your applications into one Delivery Group (for example, because they are accessed by different sets of users and published to different sets of servers), you can run Import-XAFarm multiple times, specifying different applications and a different Delivery Group each time. Although you can use PowerShell cmdlets to move applications from one Delivery Group to another after the migration, importing selectively to unique Delivery Groups can reduce or eliminate the effort of moving the applications later.
  1. Use the DeliveryGroupName parameter with the Import-XAFarm cmdlet. The script creates the specified Delivery Group if it doesn't exist.
  2. Use the following parameters with regular expressions to filter the applications to be imported into the Delivery Group, based on folder, worker group, user account, and/or server names. Enclosing the regular expression in single or double quotation marks is recommended. For information about regular expressions, see http://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx.
     - MatchWorkerGroup and NotMatchWorkerGroup - For example, for applications published to worker groups, the following cmdlet imports applications in the worker group named "Productivity Apps" to a XenApp 7.6 Delivery Group of the same name:
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
     - MatchFolder and NotMatchFolder - For example, for applications organized in application folders, the following cmdlet imports applications in the folder named "Productivity Apps" to a XenApp 7.6 Delivery Group of the same name.
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchFolder 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
       For example, the following cmdlet imports applications in any folder whose name contains "MS Office Apps" to the default Delivery Group.
       Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"
     - MatchAccount and NotMatchAccount - For example, for applications published to Active Directory users or user groups, the following cmdlet imports applications published to the user group named "Finance Group" to a XenApp 7.6 Delivery Group named "Finance."
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName 'Finance'
     - MatchServer and NotMatchServer - For example, for applications organized on servers, the following cmdlet imports applications associated with the server not named "Current" to a XenApp Delivery Group named "Legacy."
       Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
       -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
- **Customization** - PowerShell programmers can create their own tools. For example, you can use the export script as an inventory tool to keep track of changes in a XenApp 6.x farm. You can also modify the XSD files or (create your own XSD files) to store additional data or data in different formats in the XML files. You can specify a nondefault XSD file with each of the import cmdlets.
  Note: Although you can modify script files to meet specific or advanced migration requirements, support is limited to the scripts in their unmodified state. Citrix Technical Support will recommend reverting to the unmodified scripts to determine expected behavior and provide support, if necessary.

Troubleshooting

- If you are using PowerShell verison 2.0 and you added the Citrix Group Policy PowerShell Provider snap-in or the Citrix Common Commands snap-in using the Add-PSSnapIn cmdlet, you might see the error message "Object reference not set to an instance of an object" when you run the export or import cmdlets. This error does not affect script execution and can be safely ignored.
- Avoid adding or removing the Citrix Group Policy PowerShell Provider snap-in in the same console session where the export and import script modules are used, because those script modules automatically add the snap-in. If you add or remove the snap-in separately, you might see one of the following errors:
  - "A drive with the name 'LocalGpo' already exists." This error appears when the snap-in is added twice; the snap-in attempts to mount the drive LocalGpo when it's loaded, and then reports the error.
  - "A parameter cannot be found that matches parameter name 'Controller'." This error appears when the snap-in has not been added but the script attempts to mount the drive. The script is not aware that the snap-in was removed. Close the console and launch a new session. In the new session, import the script modules; do not add or remove the snap-in separately.
- When importing the modules, if you right-click a .psd1 file and select Open or Open with PowerShell, the PowerShell console window will rapidly open and close until you stop the process. To avoid this error, enter the complete PowerShell script module name directly in the PowerShell console window (for example, Import-Module .\ExportPolicy.psd1).
- If you receive a permission error when running an export or import, ensure you are a XenApp administrator with permission to read objects (for export) or read and create objects (for import). You must also have sufficient Windows permission to run PowerShell scripts.
- If an export fails, check that the XenApp 6.x farm is in a healthy state by running the DSMAINT and DSCHECK utilities on the XenApp 6.x controller server.
- If you run a preview import and then later run the import cmdlets again for an actual migration, but discover that nothing was imported, verify that you removed the Preview parameter from the import cmdlets.

Policy settings not imported

The following computer and user policy settings are not imported because they are no longer supported. Please note, unfiltered policies are never imported. The features and

components that support these settings have either been replaced by new technologies/components or the settings do not apply because of architectural and platform changes.

Computer policy settings not imported

- Connection access control
- CPU management server level
- DNS address resolution
- Farm name
- Full icon caching
- Health monitoring, Health monitoring tests
- License server host name, License server port
- Limit user sessions, Limits on administrator sessions
- Load evaluator name
- Logging of logon limit events
- Maximum percent of servers with logon control
- Memory optimization, Memory optimization application exclusion list, Memory optimization interval, Memory optimization schedule: day of month, Memory optimization schedule: day of week, Memory optimization schedule: time
- Offline app client trust, Offline app event logging, Offline app license period, Offline app users
- Prompt for password
- Reboot custom warning, Reboot custom warning text, Reboot logon disable time, Reboot schedule frequency, Reboot schedule randomization interval, Reboot schedule start date, Reboot schedule time, Reboot warning interval, Reboot warning start time, Reboot warning to users, Scheduled reboots
- Shadowing *
- Trust XML requests (configured in StoreFront)
- Virtual IP adapter address filtering, Virtual IP compatibility programs list, Virtual IP enhanced compatibility, Virtual IP filter adapter addresses programs list
- Workload name
- XenApp product edition, XenApp product model
- XML service port

* Replaced with Windows Remote Assistance

User policy settings not imported

- Auto connect client COM ports, Auto connect client LPT ports
- Client COM port redirection, Client LPT port redirection
- Client printer names
- Concurrent logon limit
- Input from shadow connections *
- Linger disconnect timer interval, Linger terminate timer interval
- Log shadow attempts *
- Notify user of pending shadow connections *
- Pre-launch disconnect timer interval, Pre-launch terminate timer interval
- Session importance
- Single Sign-On, Single Sign-On central store
- Users who can shadow other users, Users who cannot shadow other users *

* Replaced with Windows Remote Assistance

Application types not imported

The following application types are not imported.

- Server desktops
- Content
- Streamed applications (App-V is the new method used for streaming applications)

Application property mapping

The farm data import script imports only applications. The following application properties are imported without change.

IMA Property	FMA Property
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel

IMA Property Description	FMA Property Description
DisplayName	PublishedName
Enabled	Enabled
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Note: IMA and FMA have different restrictions on folder name length. In IMA, the folder name limit is 256 characters; the FMA limit is 64 characters. When importing, applications with a folder path containing a folder name of more than 64 characters are skipped. The limit applies only to the folder name in the folder path; the entire folder path can be longer than the limits noted. To avoid applications from being skipped during the import, Citrix recommends checking the application folder name length and shortening it, if needed, before exporting.

The following application properties are initialized or uninitialized by default, or set to values provided in the XenApp 6.x data:

FMA Property	Value
Name	Initialized to the full path name, which contains the IMA properties FolderPath and DisplayName, but stripped of the leading string "Applications\"
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialized using the XenApp 6.x command line arguments
IconFromClient	Uninitialized; defaults to false
IconUid	Initialized to an icon object created using XenApp 6.x icon data
SecureCmdLineArgumentsEnabled	Uninitialized; defaults to true
UserFilterEnabled	Uninitialized; defaults to false
UUID	Read-only, assigned by the Controller
Visible	Uninitialized; defaults to true

The following application properties are partially migrated:

IMA Property	Comments
FileTypes	Only the file types that exist on the new XenApp site are migrated. File types that do not exist on the new site are ignored. File types are imported only after the file types on the new site are updated.
IconData	New icon objects are created if the icon data has been provided for the exported applications.
Accounts	The user accounts of an application are split between the user list for the Delivery Group and the application. Explicit users are used to initialize the user list for the application. In addition, the "Domain Users" account for the domain of the user accounts is added to the user list for the Delivery Group.

The following XenApp 6.x properties are not imported:

IMA Property	Comments
ApplicationType	Ignored.

IMA Property	Comments
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.
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.

IMA Property	Comments
WorkerGroupNames	FMA does not support worker groups.

Migrate XenDesktop 4

Jul 07, 2014

You can transfer data and settings from a XenDesktop 4 farm to a XenDesktop 7.x Site using the Migration Tool, which is available in the Support > Tools > MigrationTool folder on the XenDesktop installation media. The tool includes:

- The export tool, XdExport, which exports XenDesktop 4 farm data to an XML file (default name: XdSettings.xml). The XML file schema resides in the file XdFarm.xsd.
- The import tool, XdImport, which imports the data by running the PowerShell script Import-XdSettings.ps1.

To successfully use the Migration Tool, both deployments must have the same hypervisor version (for example, XenServer 6.2), and Active Directory environment.

You cannot use this tool to migrate XenApp, and you cannot migrate XenDesktop 4 to XenApp.

Tip: You can upgrade XenDesktop 5 (or later XenDesktop versions) to the current XenDesktop version; see Upgrade a deployment.

Limitations

Not all data and settings are exported. The following configuration items are not migrated because they are exported but not imported:

- Administrators
- Delegated administration settings
- Desktop group folders
- Licensing configuration
- Registry keys

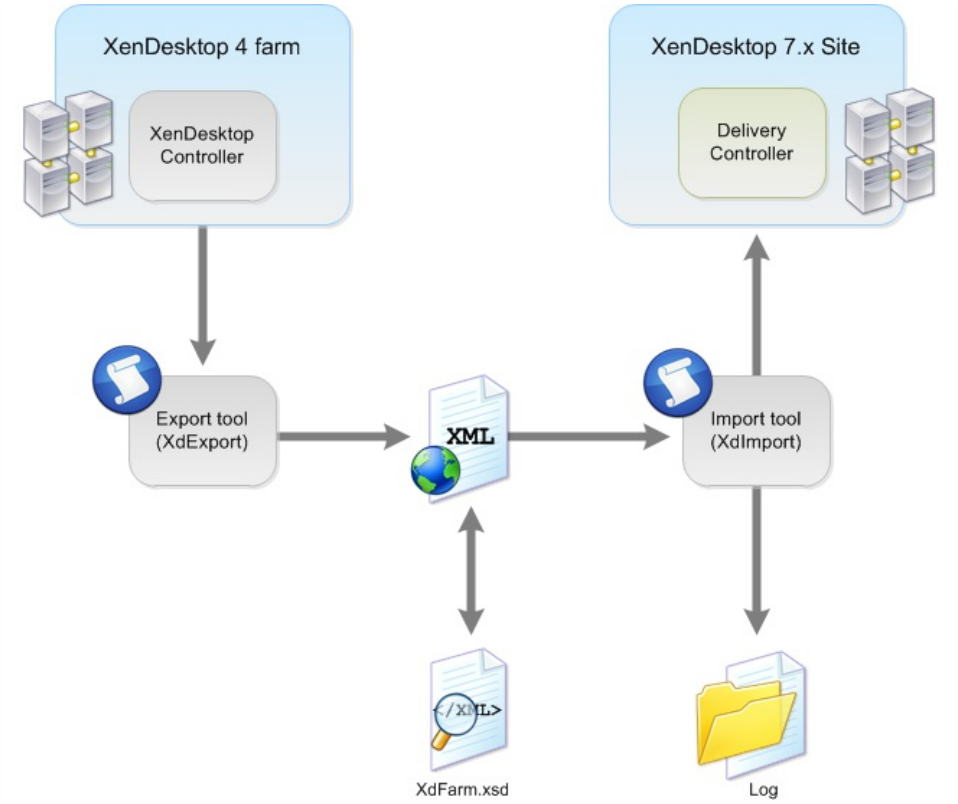
These use cases are not directly supported in migration:

- Merging settings of policies or desktop group or hosting settings.
- Merging private desktops into random Delivery Groups.
- Adjusting existing component settings through the migration tools.

For more information, see What is and is not migrated.

Migration steps

The following figure summarizes the migration process.



The migration process follows this sequence:

1. In the Studio console on the XenDesktop 4 Controller, turn on maintenance mode for all machines to be exported.
2. Export data and settings from your XenDesktop 4 farm to an XML file using XdExport; see Export from a XenDesktop 4 farm.
3. Edit the XML file so that it contains only the data and settings you want to import into your new XenDesktop Site; see Edit the Migration Tool XML file.
4. Import the data and settings from the XML file to your new XenDesktop Site using XdImport; see Import XenDesktop 4 data.
5. To make additional changes, repeat steps 3 and 4. After making changes, you might want to import additional desktops into existing Delivery Groups. To do so, use the Mergedesktops parameter when you import.
6. Complete the post-migration tasks; see Post-migration tasks.

Before migrating

Complete the following before beginning a migration:

- Make sure you understand which data can be exported and imported, and how this applies to your own deployment. See What is and is not migrated.
- Citrix strongly recommends that you manually back up the Site database so that you can restore it if any issues are discovered.
- Install the XenDesktop 7.x components and create a Site, including the database.
- To migrate from XenDesktop 4 , all VDAs must be at a XenDesktop 5.x level so that they are compatible with both XenDesktop 4 and XenDesktop 7.x controllers. After the Controller infrastructure is fully running XenDesktop 7.x, Windows 7 VDAs can be upgraded to XenDesktop 7.x. For details, see Migration examples.

Export from a XenDesktop 4 farm

Jul 07, 2014

The export tool, XdExport, extracts data from a single XenDesktop 4 farm and produces an XML file from representations of the data values.

The schema of the XML file resides in the file XdFarm.xsd, which is included in the migration tool download XdExport.zip and XdImport.zip.

Run XdExport on a XenDesktop 4 Controller in the farm from which you want to export data. This machine must have the XenDesktop 4 PowerShell SDK installed. You must have the following permissions to export the data:

- The user identity of at least read-only Citrix administrator of the farm.
- Permission to read the registry.

Although not recommended, you can run the tool while the XenDesktop Controller is in active use (for example, users are logged in to VDAs).

Citrix strongly recommends:

- The XenDesktop 4 Controller on which you run the tool be up-to-date with public hotfixes.
- Not making configuration changes to the Site while the export is running (for example, removing Desktop Groups).

1. Download XdExport.zip and extract the files to the XenDesktop 4 Controller.
2. At a command line prompt, run XdExport.exe with the following optional parameters:

Parameter	Description
-Verbose	Generates messages providing detailed progress information.
-FilePath <path>	Indicates the location of the XML file to which the farm data is exported. Default = .\XdSettings.xml
-Overwrite	Overwrites any file existing in the location specified in -FilePath. If you do not supply this parameter and an output file already exists, the tool fails with the message "Error: File already exists. Specify -Overwrite to allow the file to be overwritten. "
-? or -help	Displays text describing the parameters and exits without exporting any data.

3. If the tool runs successfully, the message Done appears. The XdSettings.xml file resides in the location specified in the FilePath parameter. If the tool fails, an error message appears.

Edit the Migration Tool XML file

Jul 07, 2014

Before importing data to a XenDesktop 7.x Site, check and edit the contents of the XML file generated by the export tool (XdExport), particularly if you migrate in multiple stages and import some users, Delivery Groups, and policies before importing others.

Use any text editor to view or change the file contents; you can use a specialized XML editor such as Microsoft XML Notepad.

Some elements within the XML content must be present for the XML file to be accepted by the import tool (XdImport).

The required XML schema is defined in the XdFarm.xsd file that is supplied as part of the Migration Tool download. When working with this file:

- A minOccurs attribute with a value of 1 or more indicates that particular elements must be present if the parent element is present.
- If the XML file supplied to the Import tool is not valid, the tool halts and an error message appears that should enable you to locate where the problem lies in the XML file.

Import a subset of desktops or Delivery Groups

To import only a subset of Delivery Groups and desktops, edit the contents of the DesktopGroups element. The DesktopGroups element can hold many DesktopGroup elements, and within each DesktopGroup element there is a Desktops element that can contain many Desktop elements.

Do not delete the DesktopGroups element, although you can delete all the DesktopGroup elements and leave it empty. Similarly, within each DesktopGroup element, the Desktops element must be present but can be empty of Desktop elements.

Delete Desktop or DesktopGroup elements to avoid importing particular single machines or entire Delivery Groups. For example, the XML file contains:

```
<DesktopGroups>
 <DesktopGroup name="Group1">
...
  <Desktops>
   <Desktop sameName="DOMAIN\MACHINE1$">
...
   </Desktop>
  </Desktops>
...
 </DesktopGroup>
 <DesktopGroup name="Group2">
...
  <Desktops>
   <Desktop samName="DOMAIN\MACHINE2$">
...
   </Desktop>
   <Desktop samName="DOMAIN\MACHINE3$">
...
```

```
  </Desktop>
 </Desktops>
...
</DesktopGroup>
</DesktopGroups>
```

In this example, the edits prevent Group1 group from being imported. Only Machine3 from the Group2 group will be imported:

```
<DesktopGroups>
 <DesktopGroup name="Group2">
...
 <Desktops>
  <Desktop samName="DOMAIN\MACHINE3$">
...
  </Desktop>
 </Desktops>
...
 </DesktopGroup>
</DesktopGroups>
```

Manage Delivery Groups with duplicate names

In XenDesktop 4, Desktop Groups can be organized in folders, Desktop Groups with the same name can appear in different folders, and the internal desktop group name is the name that appears to users. In this release, Delivery Groups cannot be placed in folders, and each Delivery Group must have a unique internal name, and the name that appears to users can be different from the internal name. To accommodate these differences, you might have to rename Desktop Groups.

For example, in your XenDesktop 4 farm, you could have two different Desktop Groups that appear with the name "My Desktop" to two different users, and you could use Desktop Groups folders to achieve this. If these Delivery Groups are to remain separate in the XenDesktop 7.x Site, you must edit the Desktop Group names in the XML file to make them unique.

If a Delivery Group in the XenDesktop 7.x Site has the same name as a Desktop Group to be imported, and the Delivery Groups are to remain separate in the XenDesktop 7.x Site, you must edit the XenDesktop 4 Desktop Group name in the XML file to keep the name unique in the Site. If the Desktop Group to be imported is really the same as the XenDesktop 7.x Delivery Group, and the machines in the XML file are to be merged into the existing Desktop Group, you do not need to rename the Desktop Group; instead, specify the -MergeDesktops parameter to the Import tool. For example, if the XML file contains:

```
<DesktopGroups>
 <DesktopGroup name="My Desktop">
...
  <Folder>\Sales</Folder>
 </DesktopGroup>
 <DesktopGroup name="My Desktop">
...
  <Folder>\Finance</Folder>
 </DesktopGroup>
</DesktopGroups>
```

Remove the duplicate names as follows:

```
<DesktopGroups>
 <DesktopGroup name="Sales Desktops">
...
```

```
  <Folder>\Sales</Folder>
 </DesktopGroup>
 <DesktopGroup name="Finance Desktops">
...
  <Folder>\Finance</Folder>
 </DesktopGroup>
</DesktopGroups>
```

Manage policy imports

You can delete policies from the XML file, and you can specify unique names to avoid policy name duplication. There is no support for merging policies.

- When you import policy data, either all polices are imported successfully or, if there is any failure, no policy data is imported.
- Importing large numbers of policies with many settings can take several hours.
- If you import policies in batches, their original prioritization may be affected. When you import policies, the relative priorities of the imported polices are maintained, but they are given higher priority than policies already in the Site. For example, if you have four polices to import with priority numbers 1 to 4, and you decide to import them in two batches, you should import policies with priorities 3 and 4 first, because the second batch of policies automatically gets higher priority.

To import only a subset of policies into the XenDesktop 7.x Site, edit the contents of the Policies element. The Policies element can hold many Policy elements. You must not delete the Policies element, although you can delete all the Policy elements and leave it empty. Delete entire Policy elements to avoid importing particular XenDesktop 4 farm policies. For example, if the XML file contains:

```
<Policies>
 <Policy name="Sales Policy">
...
 </Policy>
...
</Policies>
```

To avoid importing any XenDesktop 4 policies, and avoid clashes with policies already configured in the XenDesktop 7.x Site, edit the file to remove the individual Policy elements as follows:

```
<Policies>
</Policies>
```

Alternatively, edit the file so that the policy is imported with a different name as follows:

```
<Policies>
 <Policy name="XD4 Sales Policy">
...
 </Policy>
...
</Policies>
```

Import XenDesktop 4 data

Jul 07, 2014

The import tool, XdImport, reads settings from XenDesktop 4 that are contained in the XML file produced by the export tool, XdExport, and applies those settings to an existing XenDesktop 7.x Site. The Import tool uses the PowerShell script Import-XdSettings.ps1.

To apply only a subset of the exported data, edit the XML file before running the Import tool. For example, you might want to remove desktop groups and policies that are not needed in your XenDesktop 7.x deployment. The import tool runs successfully if you leave entire elements empty. For example, you can delete all the desktop groups without causing any issues. The tool always validates the XML file before attempting to import any data.

Run XdImport on any machine on which all the XenDesktop 7.x SDKs are installed. You must be a Full XenDesktop administrator identity to run the tool.

Before you import, make sure that you have set up a XenDesktop 7.x Site, including its database. Citrix recommends that you complete the import to XenDesktop 7.x before any user testing or general Site configuration occurs. Merge configurations only when the Site is not in use.

1. Create a XenDesktop 7.x Site.
2. Download XdImport.zip and extract the files to the machine where you will run the tool.
3. In a PowerShell session, run Import-XdSettings.ps1 with the following parameters:

Parameter	Description

-HypervisorConnectionCredentials	(Required.) A PowerShell hash table that maps Hypervisor addresses to PSCredential instances as required for the creation of Hypervisor connections. Default = @{}
	
	Enter credentials for the Hypervisor to which the XenDesktop 4 farm connects.
	
	For a single Hypervisor, create the argument as follows:
	
	`$credential = Get-Credential`
	`$mappings = @{"http://<HypervisorIP>"`
	`=$credential}`
	`.\Import-XdSettings.ps1`
	`-FilePath. \XdSettings.xml`
	`-HypervisorConnectionCredentials $mappings`
	The address specified in the hash table must exactly match the address in the XML file.
	
	For example, with both a XenServer and a VMware hypervisor, create the following argument:
	
	`$Xencredential = Get-Credential`
	`$VMWcredential = Get-Credential`
	`$mappings = @{"http://<XenHypervisorIP>"`
	`= $Xencredential;"http://<VmWHypervisorIP>/SDK"`

Parameter	Description
	= $VMWcredential} .\Import-XdSettings.ps1 -FilePath. \XdSettings.xml -HypervisorConnectionCredentials $mappings
-FilePath <path>	(The value for <path> is required.) The location of the XML file from which the farm data is to be imported.
-AdminAddress	The name of a Controller in the XenDesktop 7.x Site. Default = localhost
-MergeDesktops	Adds desktops defined in the XML file to Delivery Groups in the XenDesktop 7.x Site that have the same name as the groups described in the XML file. The associated machines and users are also added. If this parameter is not supplied, no content is added to existing Delivery Groups in the XenDesktop 7.x Site.
-SkipMachinePolicy	The script does not create a machine policy that contains site-level settings. If you do not supply this parameter and the machine policy for the Site exists, the script fails.
-WhatIf	Completes a trial run to determine what would be changed in or added to the XenDesktop 7.x Site. Including this parameter sends the information to the log file, but does not change the Site.
-LogFilePath <path>	Indicates the full path of the log file. The log file contains text describing all writes performed against the XenDesktop 7.x Site. Default = .\Import-XdSettings.log
-? or -help	Displays information about parameters and exits without importing any data.

If the XML file contains policy data, either all polices are imported successfully or if there is any failure, no policy data is imported. Importing large numbers of policies with many settings can take several hours.

When the script completes, the message Done appears. After successfully importing the data from the XML file, you can either run further export and import iterations, or if you have imported all the relevant data, complete the post-migration tasks.

Post-migration tasks

Jul 07, 2014

After successfully importing data from a XenDesktop 4 farm to a XenDesktop 7.x Site, complete the following tasks before using the new Site for production work:

- Upgrade the Virtual Delivery Agents (VDAs). Although it is not required, Citrix recommends that you upgrade VDAs before upgrading Controllers, Studio, or Director.
  - For Windows Vista and Windows XP, upgrade to XenDesktop 5. 6 Feature Pack 1 Virtual Desktop Agent.
  - For Windows 7, upgrade to the XenDesktop 7.x Virtual Delivery Agent.
- Create administrators you need for the XenDesktop 7.x Site.
- Update user devices — Citrix recommends that you update user devices with the latest version of Citrix Receiver to benefit from hotfixes and to receive support for the latest features.
- Modify the imported desktops to use registry-based Controller discovery, and point them to the XenDesktop 7.x Controllers using one of the following methods:
  - Manually edit the registry to remove the unnecessary Organizational Unit (OU) GUID registry entry, and add a ListOfDDCs registry entry.
  - Set up a machine policy to distribute the list of Controllers to the desktops, using the Active Directory policy GPMC.msc. You cannot use Studio to configure this setting.

  Registry-based Controller discovery is the default for XenDesktop 7.x, but Active Directory-based discovery is still available.

- Optionally, implement the following registry key settings described in the best practices for XenDesktop registry-based registration in CTX133384:
  - HeartbeatPeriodMS
  - PrepareSessionConnectionTimeoutSec
  - MaxWorkers
  - DisableActiveSessionReconnect
  - ControllersGroupGuid

  If you do not perform this action, the default XenDesktop 7.x settings for these keys are used.

- Turn off maintenance mode for the imported machines if they were in maintenance mode in XenDesktop 4 before the XML file was generated.
- Check the XenDesktop 7.x settings to make sure that they are correct, particularly if you had changed the PortICAConfig XML file on XenDesktop 4.
- Review all migrated components to make sure that the migration was successful.

Migration examples

Nov 18, 2014

Example 1: Single large-scale XenDesktop 4 farm to a XenDesktop 7 Site

In this example, a XenDesktop 4 farm is in use. The XenDesktop 4 farm has 50 desktop groups, where each group contains an average 100 desktops. The XenDesktop 4 desktops are provided through Provisioning Services (PVS), and the machines are running on VMware ESX hypervisors. The VDA installed on all the VMs is the XenDesktop version 4.

Migration steps

1. Upgrade all XenDesktop 4 VDAs to XenDesktop 5.6 Feature Pack 1 VDA software. This allows the VDAs to register with both the XenDesktop 4 controller and the XenDesktop 7 Delivery Controller.
2. Make sure that all users log off the XenDesktop 4 farm.
3. Make sure that all these machines are in maintenance mode.
4. Run the export tool (XdExport) on the XenDesktop 4 farm.
5. Install XenDesktop 7 components.
    1. Use Studio to create a full production mode Site.
    2. If Provisioning Services is part of the deployment, upgrade the Provisioning Services server and agents.
    3. Upgrade the License Server and associated licenses.
6. Unzip the Import Tool (XdImport) to a local directory on the XenDesktop 7 Controller.
7. Copy the XML file (XdSettings.xml) generated in Step 4 by the export tool to the local directory.
8. From the PowerShell console of the Studio root node on the XenDesktop 7 Site, start a PowerShell session.
9. Run the import tool (XdImport), passing the credentials of the associated hypervisors and the path of the XML file.
10. Manually recreate administrator settings from the Administrator node in the Studio navigation pane; see Delegated Administration for details.
11. Modify the imported desktops to use registry-based Controller discovery; and point them to the new XenDesktop 7 Controller.
12. For VDAs running on Windows 7, Citrix recommends you upgrade those VDAs to use the XenDesktop 7 VDA for Windows Desktop OS, which provides access to all new features.
    After upgrading the VDAs to XenDesktop 7 for machines in a catalog or Delivery Group, upgrade the catalog and Delivery Groups.
13. Turn off maintenance mode for the Delivery Groups.
14. Configure StoreFront to provide the desktops formerly provided through Web Interface. See the StoreFront documentation.

Example 2: XenDesktop 4 farm export with a partial import to XenDesktop 7.1 Site

In this example, the migration occurs in a number of steps, each step migrating a subset of the remaining desktops. A XenDesktop 4 farm is in use, and a XenDesktop 7.1 Site has already been created and is in use. The XenDesktop 4 farm has 50 desktop groups, and each group contains an average 100 desktops. The XenDesktop 4 desktops are provided through Provisioning Services, and the machines are running on Citrix XenServer hypervisors. The VDA installed on all the VMs is the XenDesktop version 4.

Migration steps

1. Run the export tool on the XenDesktop 4 farm.
    1. Unzip the Export Tool (XdExport) on one of the Desktop Delivery Controllers in the farm.

2. As a Citrix Administrator, run the export tool with no parameters.
2. Copy and edit the resulting XML file so that it contains only the groups and desktops that you want to migrate.
3. In the XenDesktop 4 farm, make sure that all users on desktops to be migrated have logged off and turn on maintenance mode for all desktops that are to be migrated.
4. Unzip the Import Tool (XdImport) to a local directory on the XenDesktop 7.1 Delivery Controller.
5. Copy the edited XML to the local directory.
6. From the PowerShell console of the Studio root node on the XenDesktop 7.1 Site, start a PowerShell session.
7. Run the Import Tool (XdImport), passing the credentials of the associated hypervisors and the path of the XML file.
8. Manually recreate Administrator settingsf rom the Administrator node in the Studio navigation pane; see Delegated Administration for details.
9. Modify the imported desktops to use registry-based Controller discovery; and point them to the new XenDesktop 7.1 Controller.
10. Upgrade all VDAs to the appropriate VDA software.
11. After upgrading all VDA software to XenDesktop 7 for machines in a catalog or Delivery Group, upgrade the catalog and Delivery Groups.
12. Turn off maintenance mode for the Delivery Groups.
13. Configure StoreFront to provide the desktops formerly provided through Web Interface. See the StoreFront documentation.

What is and is not migrated

Apr 27, 2015

What is migrated

Although not all inclusive, the following table describes what happens to the most significant data during migration to this release. Unless noted, the data type is imported.

Data type	Notes
Desktop Groups	Desktop Groups become Delivery Groups in this release. Desktop Group icons are not exported. SecureIcaRequired is set to True if the DefaultEncryptionLevel in XenDesktop 4 is not Basic. If a Desktop Group in the XenDesktop 4 farm has the same name as a Delivery Group in the XenDesktop 7.x Site, you can add desktops belonging to the XenDesktop 4 group to a Delivery group of the same name in the target Site. To do this, specify the MergeDesktops parameter when you run the import tool. The settings of the XenDesktop 7.x Delivery Group are not overwritten with the settings of the XenDesktop 4 group. If this parameter is not specified and there is a group with the same name as one defined in the XML file, the tool displays an error and stops before any data is imported.
Desktops	You cannot add private desktops to a random Delivery Group. Random desktops cannot be added to a static Delivery Group.
Machines	Machines are imported into four machine catalogs. The following machine catalogs are automatically created in the XenDesktop 7.x Site by the import tool: • Imported existing random (for pooled VMs) • Imported existing static (for assigned VMs) • Imported physical random (for pooled PCs or blades) • Imported physical static (for private PCs or blades). Any subsequent import of machines uses the same four machine catalogs.
Pool management pools	Includes multi-pool pools, and idle pool settings including schedule. • PeakBuffersizePercent is set to 10% by default. • OffPeakBufferSizePercent is set to 10% by default. • Any unselected days in the Business days setting on XenDesktop 4 are imported as part of the Weekend power time scheme in this release. • HostingXD4 action times are rounded up to the nearest minute. • Start times are rounded down to the nearest hour. • End times are rounded up to the nearest hour.
Farm settings	The following farm settings are imported as a Machine policy: • IcaKeepAlive

Data type	Notes
	• AutoClientReconnect • SessionReliability The setting to enable Flash player is not imported.
Policies	Some policy data is imported. Filters, settings, and printers are imported as User policies. For further details of user policy export and import, see the other table in this document. • New access policy rules are created from XenDesktop 4 group settings. • When policies are imported, their relative priority order is preserved. However, they are always added with a higher priority than any existing policies on the XenDesktop 7.x Site. • Policy merging is not supported. There is no option to import policies into Active Directory. They are always stored in the Site.
User assignments	
Hypervisor settings	This parameter is required with the XdImport tool. Hypervisor addresses are exported, but not the credentials required to access those hypervisors. To create hypervisor connections in the XenDesktop 7.x Site, extract the addresses from the XML file and create a PowerShell hash table that maps them to the relevant credential instances. Then specify this hash table in the import tool HypervisorConnectionCredentials parameter. For further details, see Import XenDesktop 4 data. Merging or updating hypervisor settings for existing Desktop Groups and hypervisor connections is not supported.
Administrators	(Not imported.) No administrator data is imported, including data about delegated administrators. You create new administrators for your XenDesktop 7.x Site.
Licensing configuration	(Not imported.) Includes information such as the License Server name and edition. License files are not exported.
Desktop Group folders	(Not imported.) This release does not support Desktop Group folders. If there are duplicate Desktop Group names (because different folders in the XenDesktop 4 farm contained groups with the same names) and you do not edit names in the XML file, the Import Tool halts.
Registry keys	(Not imported.) For information on implementing registry keys, see Post-migration tasks.

User policy data

The following table describes how User policy data is exported and imported.

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Bandwidth\Visual Effects\Session Limits OEM Virtual Channels	ClientOEMVCBandwidth	Not imported
Client Devices\Resources\Other Turn off OEM virtual channels	DisableOEMVirtualChannels	Not imported
User Workspace\Time Zones Do not use client's local time	DoNotUseClientLocalTime	Not imported
Security\Encryption SecureICA encryption	ClientSecurityRequirement	Not imported
Bandwidth\SpeedScreen Image acceleration using lossy compression	LossyCompression settings	ICA\Visual Display\Still Images Lossy compression level Lossy compression threshold value Heavyweight compression ICA\Visual Display\Moving Images Progressive compression level Progressive compression threshold value
Bandwidth\Visual Effects Turn off desktop wallpaper	TurnOffWallpaper	ICA\Desktop UI Desktop wallpaper
Bandwidth\Visual Effects Menu animation	TurnOffMenuWindowAnimation	ICA\Desktop UI Menu animation

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Bandwidth\Visual Effects Turn off window contents while dragging	DoNotShowWindowContentsWhileDragging	ICA\Desktop UI View window contents while dragging
Bandwidth\Visual Effects\Session Limits Audio	ClientAudioBandwidth__AllowedBandWidth	ICA\Bandwidth Audio redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits Clipboard	ClientClipboardBandwidth__AllowedBandWidth	ICA\Bandwidth Clipboard redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits COM Ports	ClientComBandwidth__AllowedBandWidth	ICA\Bandwidth COM port redirection bandwidth limit Not imported in XenDesktop 7.0 through 7.8
Bandwidth\Visual Effects\Session Limits Drives	ClientDriveBandwidth__AllowedBandWidth	ICA\Bandwidth File redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits LPT Ports	ClientLptBandwidth__AllowedBandWidth	ICA\Bandwidth LPT port redirection bandwidth limit Not imported in XenDesktop 7.0 through 7.8
Bandwidth\Visual Effects\Session Limits Overall Session	OverallBandwidth__AllowedBandWidth	ICA\Bandwidth Overall session bandwidth limit
Bandwidth\Visual Effects\Session Limits Printer	LimitPrinterBandWidth__AllowedBandWidth	ICA\Bandwidth Printer redirection bandwidth limit

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Client Devices\Resources\Audio Microphones	ClientAudioMicrophone__TurnOn	ICA\Audio Client microphone redirection
Client Devices\Resources\Audio Sound Quality	ClientAudioQuality__Quality	ICA\Audio Audio quality
Client Devices\Resources\Audio Turn off speakers	DisableClientAudioMapping	ICA\Audio Client audio redirection
Client Devices\Resources\Drives Connection	ConnectClientDriveAtLogon__TurnOn	ICA\File Redirection Auto connect drives
Client Devices\Resources\Drives Turn off Floppy disk drives	DisableClientDriveMapping__DisableFloppyDrive	ICA\File Redirection Client floppy drives
Client Devices\Resources\Drives Turn off Hard drives	DisableClientDriveMapping__DisableHardDrive	ICA\File Redirection Client fixed drives
Client Devices\Resources\Drives Turn off CD-ROM drives	DisableClientDriveMapping__DisableCdrom	ICA\File Redirection Client optical drives
Client Devices\Resources\Drives Turn off Remote drives	DisableClientDriveMapping__DisableRemote	ICA\File Redirection Client network drives
Client Devices\Resources\Drives Turn off USB disk drives	DisableClientDriveMapping__DisableUSB	ICA\File Redirection Client removable drives
Client Devices\Resources\Drives\Optimize Asynchronous writes	CDMAsyncWrites	ICA\File Redirection User asynchronous writes
Client Devices\Resources\Other Turn off clipboard mapping	DisableClientClipboardMapping	ICA Client clipboard redirection

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Client Devices\Resources\Ports Turn off COM ports	DisableClientCOMPortMapping	ICA\Port Redirection Client COM port redirection Not imported in XenDesktop 7.0 through 7.8
Client Devices\Resources\Ports Turn off LPT ports	DisableClientLPTPortMapping	ICA\Port Redirection Client LPT port redirection Not imported in XenDesktop 7.0 through 7.8
Client Devices\Resources\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\USB Devices Client USB device redirection
Printing\Client Printers Auto-creation	ConnectClientPrinterAtLogon__Flag	ICA\Printing\Client Printers Auto-create client printers
Printing\Client Printers Legacy client printers	LegacyClientPrinters__TurnOn	ICA\Printing\Client Printers Client printer names
Printing\Client Printers Printer properties retention	ModifiedPrinterProperties__WriteMethod	ICA\Printing\Client Printers Printer properties retention
Printing\Client Printers Print job routing	ClientPrintingForNetworkPrinter__TurnOn	ICA\Printing\Client Printers Direct connections to print servers
Printing\Client Printers Turn off client printer mapping	DisableClientPrinterMapping	ICA\Printing Client printer redirection
Printing\Drivers Native printer driver auto-install	PrintDriverAutoInstall__TurnOn	ICA\Printing\Drivers Automatic installation of inbox printer drivers
Printing\Drivers	ClientPrintDriverToUse	ICA\Printing\Drivers

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Universal driver Printing\Session printers	NetworkPrinters	Universal print driver use ICA\Printing
Session printers		Session printers
Printing\Session printers Choose client's default printer	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\Printing Default printer

What is not migrated

Not all XenDesktop 4 components are supported in this release. The following items are not migrated:

- **Virtual Delivery Agent** - Before a XenDesktop 7.x Delivery Controller can manage virtual desktops from XenDesktop 4, you must upgrade the VDAs to a minimum release of XenDesktop 5.x.
- **Controllers** - You must deploy new Controller servers. You cannot upgrade a XenDesktop 4 Controller to a XenDesktop 7.x Site. XenDesktop 7.x Sites cannot join a XenDesktop 4 farm, and XenDesktop 4 Controllers cannot join a XenDesktop 7.x Site. In addition, each version has different server requirements; XenDesktop 4 requires Windows Server 2003 and XenDesktop 7.x requires later Windows Server versions.
- **Web Interface** - Citrix recommends using StoreFront with XenDesktop 7.x. See the StoreFront documentation for installation and setup details. When the XenDesktop installer detects Web Interface, it installs StoreFront, but does not remove Web Interface.
- **Active Directory Organizational Unit (OU) configuration** - Sharing an Organizational Unit (OU) between two farms or two Sites, or a farm and a Site is not supported. If you plan to configure the new Site to use Active Directory-based Controller discovery rather than the default registry-based Controller discovery, you must create a new OU to support it.
- **PortICAConfig XML file** - If you have changed the default settings for this file you may need to configure these settings for the new Site through Group Policy Objects.
- **Configuration logging settings provided through XenDesktop 4 Service Pack 1**.
- **Provisioning Services-related data**.
- **Applications**.
- **List of Controllers**.
- **NetScaler Gateway**.
- **Event log throttling settings**.

Secure

Sep 09, 2015

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 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 through to antivirus software. A list of supported products can be found at http://www.citrix.com/ready.

Select releases of XenApp and XenDesktop are certified for Common Criteria standard. For a list of those standards, go to http://www.commoncriteriaportal.org/cc/.

Security considerations and best practices

Aug 23, 2016

This document describes:

- General security best practices when using this release, and any security-related differences between this release and a conventional computer environment
- Manage user accounts
- Manage user privileges
- Manage logon rights
- Configure user rights
- Configure service settings
- Deployment scenarios and their security implications
- Remote PC Access security considerations

Your organization may need to meet specific security standards to satisfy regulatory requirements. This document does not cover this subject, because such security standards change over time. For up-to-date information on security standards and Citrix products, consult http://www.citrix.com/security/.

Security best practices

Keep all machines in your environment up to date with security patches. One advantage is that you can use thin clients as terminals, which simplifies this task.

Protect all machines in your environment with antivirus software.

Consider using platform-specific anti-malware software 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.

Note: TCP ports 1494 and 2598 are used for ICA and CGP and are therefore likely to be open at firewalls so that users outside the data center can access them. Citrix recommends that you do not use these ports for anything else, to avoid the possibility of inadvertently leaving administrative interfaces open to attack. Ports 1494 and 2598 are officially registered with the Internet Assigned Number Authority (http://www.iana.org/).

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.

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.

Manage user accounts

If the option to install App-V publishing components is selected when installing a Virtual Delivery Agent (VDA), or if this feature is added later, the local administrative account CtxAppVCOMAdmin is added to the VDA. If you use the App-V publishing feature, do not modify this account. If you do not need to use the App-V publishing feature, do not select it at installation time. If you later decide not to use the App-V publishing feature, you can disable or delete this account.

Manage user privileges

Grant users only the capabilities they require. Microsoft Windows privileges continue to be applied to desktops in the usual way: configure privileges through User Rights Assignment and group memberships through Group Policy. One advantage of this release is that it is possible to grant a user administrative rights to a desktop without also granting physical control over the computer on which the desktop is stored.

Note the following when planning for desktop privileges:

- By default, when non-privileged users connect to a desktop, they see the time zone of the system running the desktop instead of the time zone of their own user device. For information on how to allow users to see their local time when using desktops, see the Manage Delivery Groups article.
- A user who is an administrator on a desktop has full control over that desktop. If a desktop is a pooled desktop rather than a dedicated desktop, the user must be trusted in respect of all other users of that desktop, including future users. All users of the desktop need to be aware of the potential permanent risk to their data security posed by this situation. This consideration does not apply to dedicated desktops, which have only a single user; that user should not be an administrator on any other desktop.
- A user who is an administrator on a desktop can generally install software on that desktop, including potentially malicious software. The user can also potentially monitor or control traffic on any network connected to the desktop.

Manage logon rights

Logon rights are required for both user accounts and computer accounts. As with Microsoft Windows privileges, logon rights continue to be applied to desktops in the usual way: configure logon rights through User Rights Assignment and group memberships through Group Policy.

The Windows logon rights are: log on locally, log on through Remote Desktop Services, log on over the network (access this computer from the network), log on as a batch job, and log on as a service.

For computer accounts, grant computers only the logon rights they require. The logon right "Access this computer from the network" is required:

- At VDAs, for the computer accounts of Delivery Controllers
- At Delivery Controllers, for the computer accounts of VDAs. See Active Directory OU-based Controller discovery.
- At StoreFront servers, for the computer accounts of other servers in the same StoreFront server group

For user accounts, grant users only the logon rights they require.

According to Microsoft, by default the group Remote Desktop Users is granted the logon right "Allow log on through Remote Desktop Services" (except on domain controllers).

Your organization's security policy may state explicitly that this group should be removed from that logon right. Consider the following approach:

- The Virtual Delivery Agent (VDA) for 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:

- 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.)

Delivery Controller installation also creates the following Windows services. These are also created when installed with other Citrix components:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Supports the collection of diagnostic information for use by Citrix Support.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Collects diagnostic information for analysis by Citrix, such that the analysis results and recommendations can be viewed by administrators to help diagnose issues with the site.

Delivery Controller installation also creates the following Windows services. These are not currently used, and are disabled. Do not enable them:

- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)

Except for the Citrix Storefront Privileged Administration Service, these services are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. You do not need to change these user rights. These privileges are not used by the Delivery Controller and are automatically disabled.

Configure service settings

Except for the Citrix Storefront Privileged Administration service and the Citrix Telemetry Service, the Delivery Controller Windows services listed above in the Configure user rights section are configured to log on as the NETWORK SERVICE identity. Do not alter these service settings.

The Citrix Storefront Privileged Administration service is configured to log on Local System (NT AUTHORITY\SYSTEM). This is required for Delivery Controller StoreFront operations that are not normally available to services (including creating Microsoft IIS sites). Do not alter its service settings.

The Citrix Telemetry Service is configured to log on as its own service-specific identity.

You can disable the Citrix Telemetry Service. Apart from this service, and services that are already disabled, do not disable any other of these Delivery Controller Windows services.

Configure registry settings

It is no longer necessary to enable creation of 8.3 file names and folders on the VDA file system. The registry key **NtfsDisable8dot3NameCreation** can be configured to disable creation of 8.3 file names and folders. You can also configure this using the **fsutil.exe behavior set disable8dot3** command.

Deployment scenario security implications

Your user environment can contain either user devices that are unmanaged by your organization and completely under the control of the user, or user devices that are managed and administered by your organization. The security considerations for these two environments are generally different.

Managed user devices

Managed user devices are under administrative control; they are either under your own control, or the control of another organization that you trust. You may configure and supply user devices directly to users; alternatively, you may provide terminals on which a single desktop runs in full-screen-only mode. Follow the general security best practices described above for all managed user devices. This release has the advantage that minimal software is required on a user device.

A managed user device can be configured to be used in full-screen-only mode or in window mode:

- Full-screen-only mode: Users log on to it with the usual Log On To Windows screen. The same user credentials are then used to log on automatically to this release.
- Users see their desktop in a window: Users first log on to the user device, then log on to this release through a web site supplied with the release.

Unmanaged user devices

User devices that are not managed and administered by a trusted organization cannot be assumed to be under administrative control. For example, you might permit users to obtain and configure their own devices, but users might not follow the general security best practices described above. This release has the advantage that it is possible to deliver desktops securely to unmanaged user devices. These devices should still have basic antivirus protection that will defeat keylogger and similar input attacks.

Data storage considerations

When using this release, you can prevent users from storing data on user devices that are under their physical control. However, you must still consider the implications of users storing data on desktops. It is not good practice for users to store data on desktops; data should be held on file servers, database servers, or other repositories where it can be appropriately protected.

Your desktop environment may consist of various types of desktops, such as pooled and dedicated desktops. Users should never store data on desktops that are shared amongst users, such as pooled desktops. If users store data on dedicated desktops, that data should be removed if the desktop is later made available to other users.

Mixed-version environments

Mixed-version environments are inevitable during some upgrades. Follow best-practice and minimize the time that Citrix components of different versions co-exist. In mixed-version environments, security policy, for example, may not be uniformly enforced.

Note: This is typical of other software products; the use of an earlier version of Active Directory only partially enforces Group Policy with later versions of Windows.

The following scenario describes a security issue that can occur in a specific mixed-version Citrix environment. When Citrix Receiver 1.7 is used to connect to a virtual desktop running the VDA in XenApp and XenDesktop 7.6 Feature Pack 2, the policy setting **Allow file transfer between desktop and client** is enabled in the Site but cannot be disabled by a Delivery Controller running XenApp and XenDesktop 7.1. It does not recognize the policy setting, which was released in the later version of the product. This policy setting allows users to upload and download files to their virtual desktop, which is the security issue. To work around this, upgrade the Delivery Controller (or a standalone instance of Studio) to version 7.6 Feature Pack 2 and then use Group Policy to disable the policy setting. Alternatively, use local policy on all affected virtual desktops.

Remote PC Access security considerations

Remote PC Access implements the following security features:

- Smart card use is supported.
- When a remote session connects, the office PC's monitor appears as blank.
- Remote PC Access redirects all keyboard and mouse input to the remote session, except CTRL+ALT+DEL and USB-enabled smart cards and biometric devices.
- SmoothRoaming is supported for a single user only.
- When a user has a remote session connected to an office PC, only that user can resume local access of the office PC. To resume local access, the user presses Ctrl-Alt-Del on the local PC and then logs on with the same credentials used by the remote session. The user can also resume local access by inserting a smart card or leveraging biometrics, if your system has appropriate third-party Credential Provider integration. This default behavior can be overridden by enabling Fast User Switching via Group Policy Objects (GPOs) or by editing the registry.

Note: Citrix recommends that you do not assign VDA administrator privileges to general session users.

Automatic assignments

By default, Remote PC Access supports automatic assignment of multiple users to a VDA. In XenDesktop 5.6 Feature Pack 1, administrators could override this behavior using the RemotePCAccess.ps1 PowerShell script. This release uses a registry entry to allow or prohibit multiple automatic remote PC assignments; this setting applies to the entire Site.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To restrict automatic assignments to a single user:

On each Controller in the Site, set the following registry entry:

HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple user assignment.

If there are any existing user assignments, remove them using SDK commands for the VDA to subsequently be eligible for a single automatic assignment.

- Remove all assigned users from the VDA: $machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
- Remove the VDA from the Delivery Group: $machine | Remove-BrokerMachine -DesktopGroup $desktopGroup

Restart the physical office PC.

Delegated Administration

Feb 24, 2016

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:

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.

  In certain product editions, you can create custom roles to match the requirements of your organization, and delegate permissions with more detail. You can use custom roles to allocate permissions at the granularity of an action or task in a console.

- **Scopes** — A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your

organization (for example, the set of Delivery Groups used by the Sales team). Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: 'All,' which contains all objects. The Full Administrator role is always paired with the All scope.

Example

Company XYZ decided to manage applications and desktops based on their department (Accounts, Sales, and Warehouse) and their desktop operating system (Windows 7 or Windows 8). The administrator created five scopes, then labeled each Delivery Group with two scopes: one for the department where they are used and one for the operating system they use.

The following administrators were created:

Administrator	Roles	Scopes
domain/fred	Full Administrator	All (the Full Administrator role always has the All scope)
domain/rob	Read Only Administrator	All
domain/heidi	Read Only Administrator Help Desk Administrator	All Sales
domain/warehouseadmin	Help Desk Administrator	Warehouse
domain/peter	Delivery Group Administrator Machine Catalog Administrator	Win7

- Fred is a Full Administrator and can view, edit, and delete all objects in the system.
- Rob can view all objects in the Site but cannot edit or delete them.
- Heidi can view all objects and can perform help desk tasks on Delivery Groups in the Sales scope. This allows her to manage the sessions and machines associated with those groups; she cannot make changes to the Delivery Group, such as adding or removing machines.
- Anyone who is a member of the warehouseadmin Active Directory security group can view and perform help desk tasks on machines in the Warehouse scope.
- Peter is a Windows 7 specialist and can manage all Windows 7 Machine Catalogs and can deliver Windows 7 applications, desktops, and machines, regardless of which department scope they are in. The administrator considered making Peter a Full Administrator for the Win7 scope; however, she decided against this, because a Full Administrator also has full rights over all objects that are not scoped, such as 'Site' and 'Administrator.'

How to use Delegated Administration

Generally, the number of administrators and the granularity of their permissions depends on the size and complexity of the deployment.

- In small or proof-of-concept deployments, one or a few administrators do everything; there is no delegation. In this case, create each administrator with the built-in Full Administrator role, which has the All scope.
- In larger deployments with more machines, applications, and desktops, more delegation is needed. Several administrators

might have more specific functional responsibilities (roles). For example, two are Full Administrators, and others are Help Desk Administrators. 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 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.
- 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.
- 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 <string>	Where to write the output. Default = stdout
-AdminAddress <string>	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.
<CommonParameters>	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For details, see the Microsoft documentation.

The following example writes an HTML table to a file named Roles.html and opens the table in a web browser.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html –Show
```

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
```

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"
```

Smart cards

Aug 29, 2016

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.

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 http://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 be used. For more information about Citrix-compatible smart cards and middleware, see http://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 more information about PIV usage with XenDesktop, see Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV Smart Card Authentication.

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 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.

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 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 http://support.microsoft.com/kb/949538.

You can reset PINs using a card management system or vendor utility.

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 http://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

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

Sep 14, 2015

The following types of smart card deployments are supported by this product version and by mixed environments containing this version. Other configurations might work but are not supported.

Type	StoreFront connectivity
Local domain-joined computers	Directly connected
Remote access from domain-joined computers	Connected through 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 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.

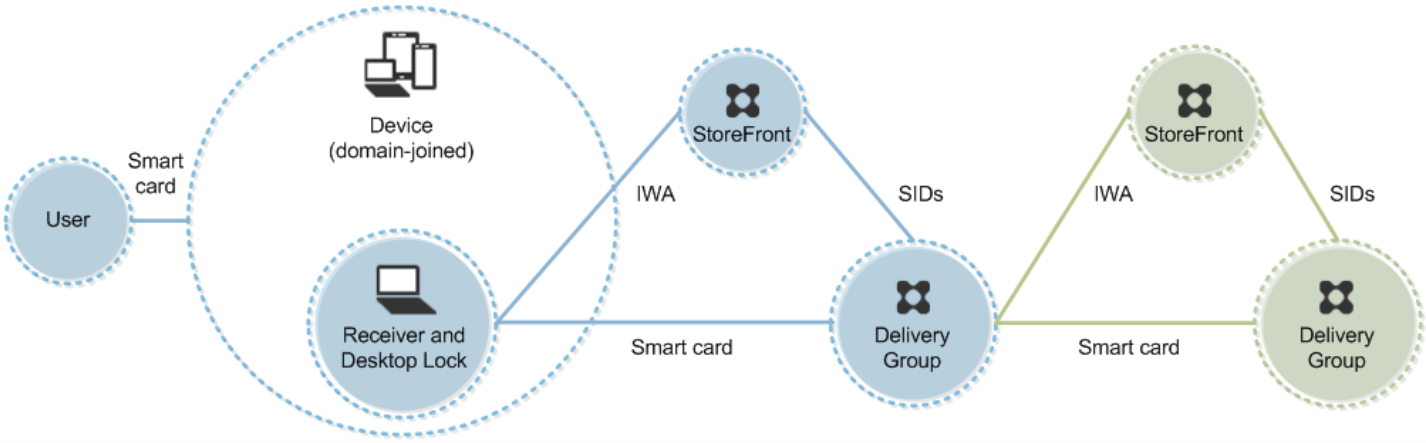
Policy setting	Desktop behavior
No action	No action.
Lock workstation	The desktop session is disconnected and the virtual desktop is locked.
Force logoff	The user is forced to log off. If the network connection is lost and this setting is enabled, the session may be logged off and the user may lose data.
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.

Deployment example: domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.

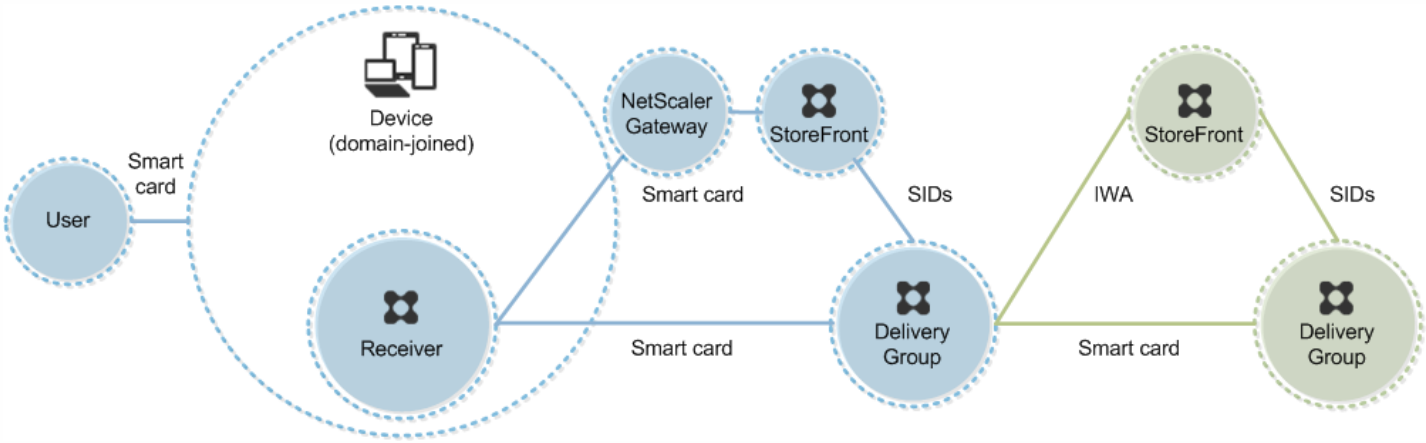


A user logs on to a device using a smart card and PIN. Receiver authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user 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.

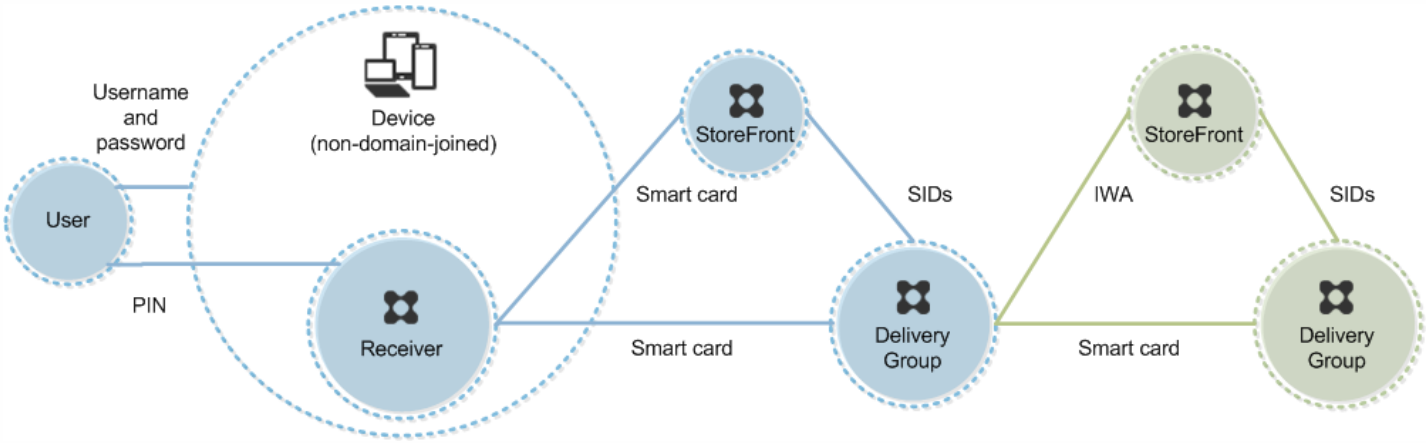
The user is automatically logged on to StoreFront, which passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is not prompted again for a PIN because the single sign-on feature is configured on Receiver.

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 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

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



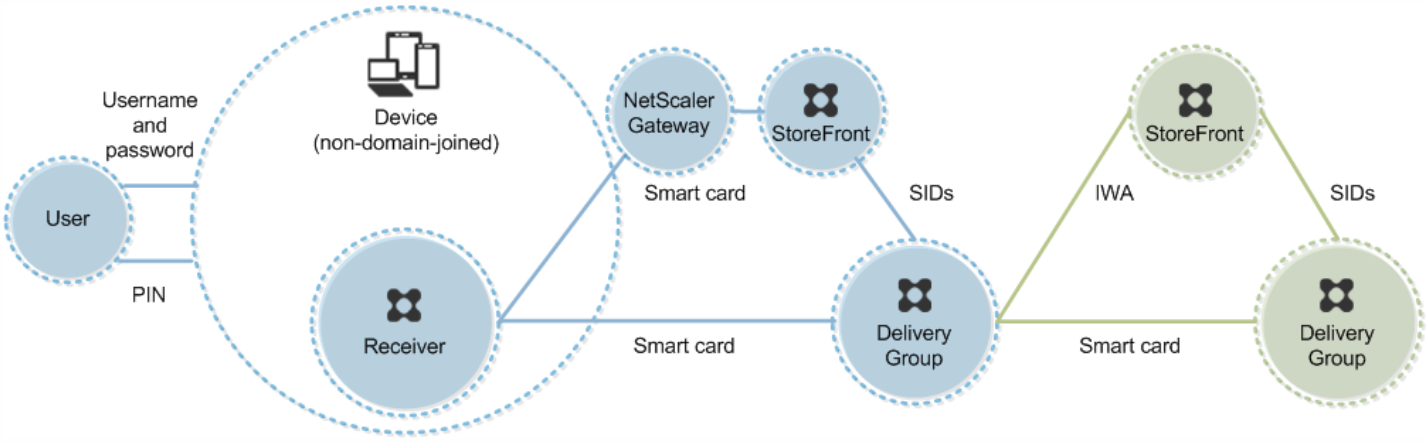
A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user 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 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 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.

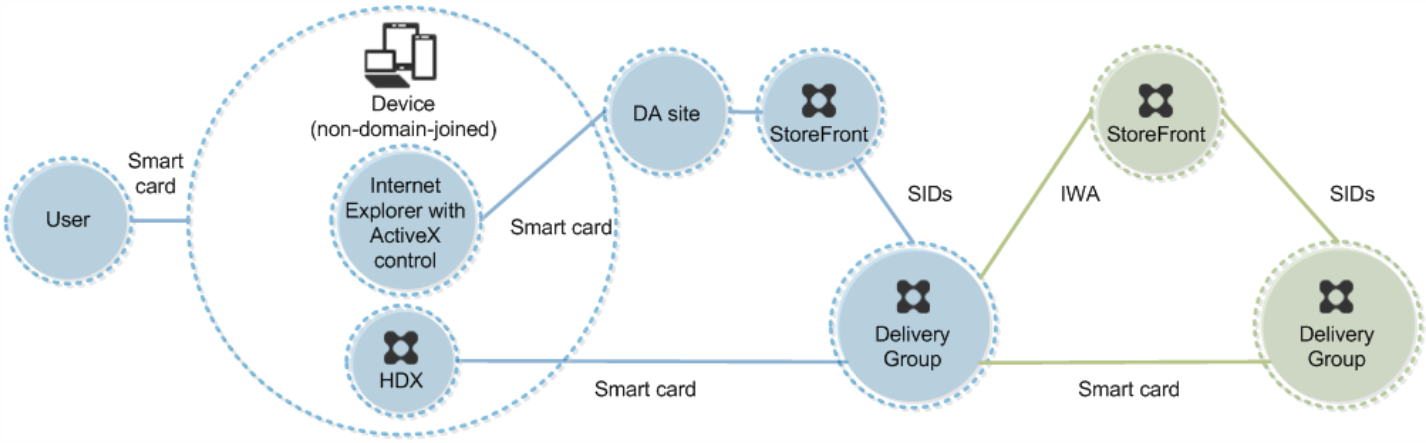
StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

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 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.



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.

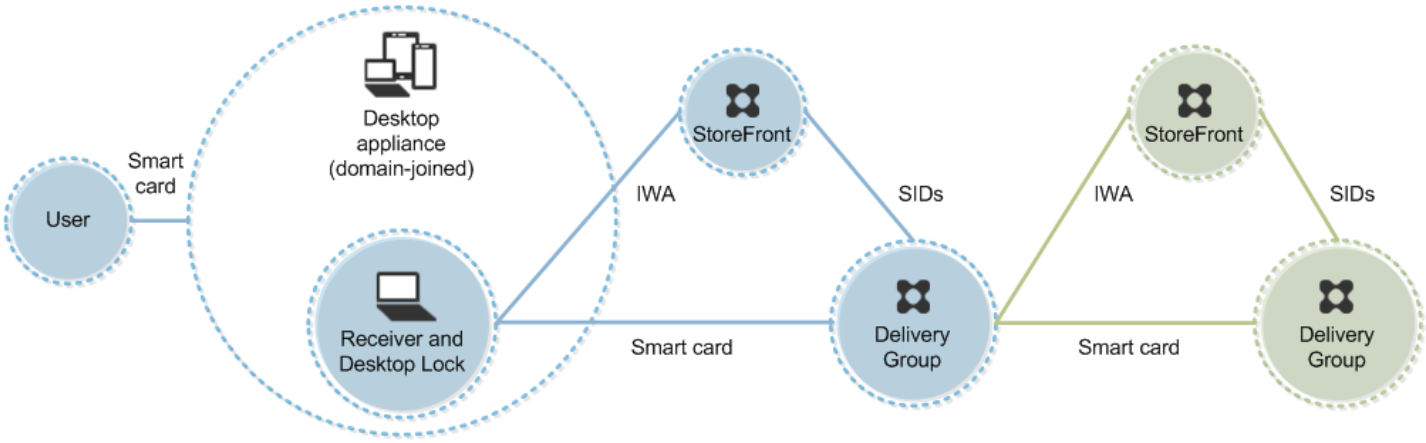
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown 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.



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

Jul 01, 2014

Pass-through authentication

Pass-through authentication with smart cards to virtual desktops is supported on user devices running Windows 10, and 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 2008 and Windows Server 2012.

To use pass-through authentication with smart cards hosted applications, ensure you enable the use of Kerberos when you configure Pass-through with smartcard as the authentication method for the site.

Note: The availability of pass-through authentication with smart cards depends on many factors including, but not limited to:

- Your organization's security policies regarding pass-through authentication.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Pass-through authentication with smart cards is configured on Citrix StoreFront. See *— Configure the authentication service* in 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)

Aug 12, 2016

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 SSL 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 SSL 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.

For tasks that include working in the Windows registry:
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
For information about enabling TLS to the Site database, see CTX137556.

Install TLS server certificates on Controllers

For HTTPS, the XML Service supports TLS features through the use of server certificates, not client certificates. To obtain, install, and register a certificate on a Controller, and to configure a port with the SSL certificate:

- If the Controller has IIS installed, follow the guidance in https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.
- If the Controller does not have IIS installed, one method of configuring the certificate is:
  1. Obtain an SSL server certificate and install it on the Controller using the guidance in http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx. For information on the certreq tool, see http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.
     If you intend to use the PowerShell script to configure TLS on VDAs, and unless you intend on specifying the SSL certificate's thumbprint, make sure the certificate is located in the Local Computer > Personal > Certificates area of

the certificate store. If more than one certificate resides in that location, the first one found will be used.

2. Configure a port with the certificate; see http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use non-default ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.
To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio:
BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>

where <http-port> is the port number for HTTP traffic and <https-port> is the port number for HTTPS traffic.

Note: After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
XML_HTTPS | Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
```

Enforce HTTPS traffic only

If you want the XML Service to ignore HTTP traffic, set the following registry value in HKLM\Software\Citrix\DesktopServer\ on the Controller and then restart the Broker Service.

To ignore HTTP traffic, set XmlServicesEnableNonSsl to 0.

There is a corresponding registry value to ignore HTTPS traffic: XmlServicesEnableSsl. Ensure that this is not set to 0.

About TLS settings on VDAs

When you configure TLS on VDAs, it changes permissions on the installed SSL certificate, 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 it is 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 customers review their usage of SSLv3 and take steps to reconfigure their 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 ciphers to allow**.
  A cipher suite is a list of common TLS ciphers. When a client connects and sends a list of supported TLS ciphers, the VDA matches one of the client's ciphers with one of the ciphers in its configured cipher suite and accepts the connection. If the client sends a cipher that is not in the VDA's cipher suite, the VDA rejects the connection.

  Three cipher suites are supported: GOV(ernment), COM(mercial), and ALL. The ciphers in those cipher suites depend on the Windows FIPS mode; see http://support.microsoft.com/kb/811833 for information about Windows FIPS mode. The following table lists the ciphers in each supported cipher suite.

TLS cipher suite	GOV	COM	ALL	GOV	COM	ALL
FIPS Mode	Off	Off	Off	On	On	On
RSA_KEYX	x	x	x	x	x	x
RSA_SIGN	x	x	x	x	x	x
3DES	x		x	x		x
RC4		x	x			
MD5	x	x	x			
SHA	x	x	x	x	x	x
SHA_256	x	x	x	x	x	x
SHA_384	x	x	x	x	x	x
SHA_512	x	x	x	x	x	x
AES	x	x	x	x	x	x

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.

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 result is that users can connect only over TLS; they cannot use raw ICA, CGP, or WebSocket to connect.

The script contains the following syntax descriptions, plus additional examples; you can use a tool such as Notepad++ to review this information.

You must specify either the –Enable or –Disable parameter; all other parameters are optional.

Syntax

Enable-VdaSSL {-Enable | -Disable} [–SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"<suite>"] [-CertificateThumbPrint "<thumbprint>"]

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.
–SSLPort <port>	TLS port. Default: 443
-SSLMinVersion "<min-ssl-version>"	Minimum TLS protocol version, enclosed in quotation marks. Valid values: "SSL_3.0", "TLS_1.0", "TLS_1.1", and "TLS_1.2". Default: "TLS_1.0" **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 "<suite>"	TLS cipher suite, enclosed in quotation marks. Valid values: "GOV", "COM", and "ALL". Default: "ALL"
-CertificateThumbPrint "<thumbprint>"	Thumbprint of the SSL certificate in the certificate store, enclosed in quotation marks. This parameter is generally used when the certificate store has multiple certificates; the script uses the thumbprint to select the certificate you want to use. Default: the first available certificate found in the Local Computer > Personal > Certificates area of the certificate store.

Examples

The following script installs and enables the TLS 1.2 protocol version value.

```
Enable-VdaSSL –Enable
```

The following script installs and enables the TLS listener, and specifies TLS port 400, the GOV cipher suite, and a minimum

TLS 1.2 SSL protocol value.

```
Enable-VdaSSL – Enable –SSLPort 400 'SSLMinVersion "TLS_1.2"
–SSLCipherSuite "GOV"
```

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:
    1. Select File > Add/Remove Snap-in.
    2. Select Certificates and then click Add.
    3. When prompted with "This snap-in will always manage certificates for:" choose "Computer account" and then click Next.
    4. When prompted with "Select the computer you want this snap-in to manage" choose "Local computer" and then click Finish.
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 SSL 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"
5. Double-click the installed SSL 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.
    1. Edit the SSL Thumbprint key and copy the value of the SSL certificate's thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as '0000' and special characters).
    2. Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
    3. If you want to change the default settings (optional), use the following in the same registry path:
        - SSLPort DWORD – SSL port number. Default: 443.
        - SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Default: 2 (TLS 1.0).
        - SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).
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.
   where <delivery-group-name> is the name of the Delivery Group containing VDAs.

4. Run Set-BrokerSite -DnsResolutionEnabled $true.

Troubleshooting

If a connection error occurs, check the VDA's system event log.

When using 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.

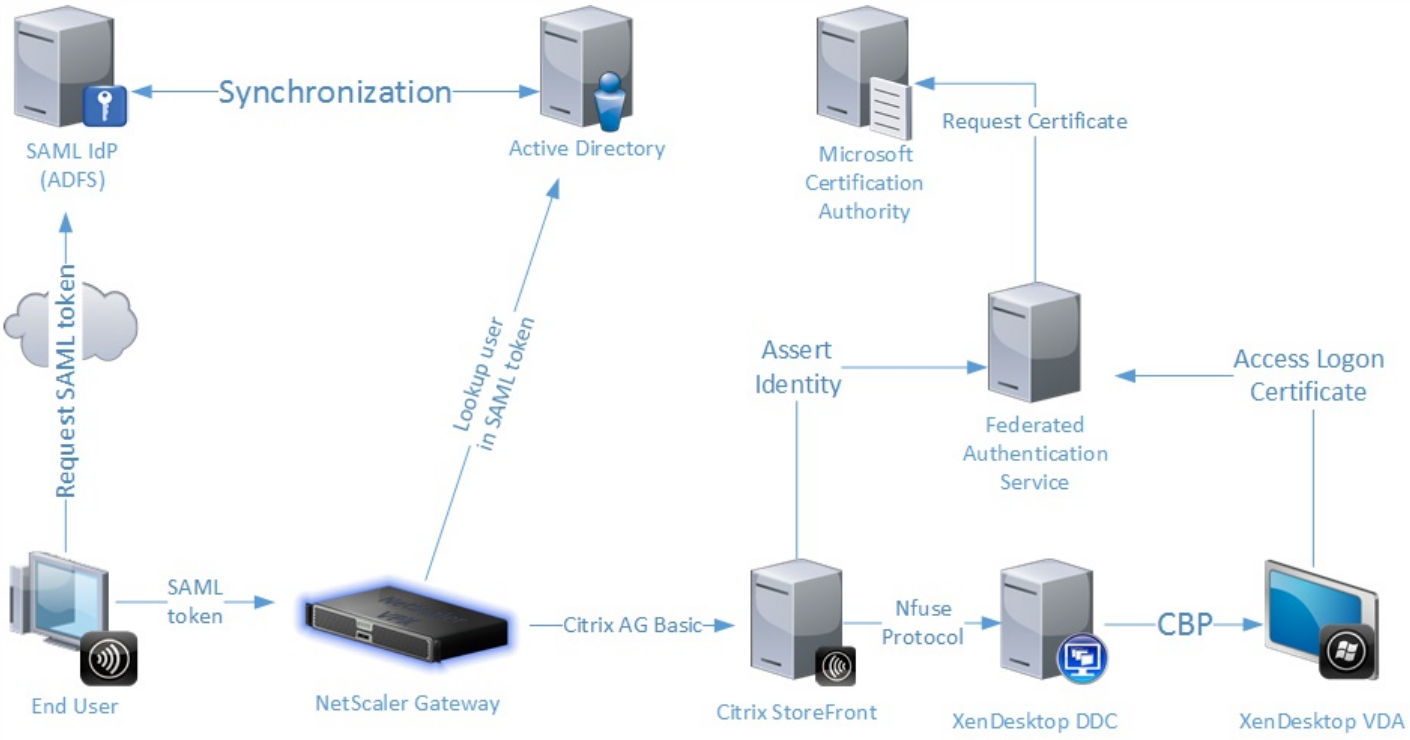
Communication between the Controller and VDA uses the basic256 algorithm suite, whose algorithms are as stated above.

Federated Authentication Service

Jun 22, 2016

The Citrix Federated Authentication Service 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. This 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.

The following diagram shows the Federated Authentication Service integrating with a Microsoft Certification Authority and providing support 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 the FAS and redeems the ticket. Only the FAS has access to the user certificate's private key; the VDA must send each signing and decryption operation that it needs to perform with the certificate to the FAS.

Requirements

The Federated Authentication Service is supported on Windows servers (Windows Server 2008 R2 or later).

- Citrix recommends installing the FAS on a server that does not contain other Citrix components.
- The Windows Server should be secured. It will have access to a registration authority certificate and private key that allows it to automatically issue certificates for domain users, and it will have access to those user certificates and private

keys.

In the XenApp or XenDesktop Site:

- The Delivery Controllers must be minimum version 7.9.
- The VDAs must be minimum version 7.9. Check that the Federated Authentication Service Group Policy configuration has been applied correctly to the VDAs before creating the Machine Catalog in the usual way; see the Configure Group Policy section for details.
- The StoreFront server must be minimum version 3.6 (this is the version provided with the XenApp and XenDesktop 7.9 ISO).

When planning your deployment of this service, review the Security considerations section.

References:

- Active Directory Certificate Services

  https://technet.microsoft.com/en-us/library/hh831740.aspx

- Configuring Windows for Certificate Logon

  http://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 that the FAS be installed on a dedicated server that is secured in a similar way to a domain controller or certificate authority. The FAS can be installed from the **Federated Authentication Service** button on the autorun splash screen when the ISO is inserted.

This will install the following components:

- 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 path text below may differ.

command COPY

```
<p>Get-Module &amp;quot;Citrix.StoreFront.*&amp;quot; -ListAvailable | Import-Module<br>
$StoreVirtualPath = &amp;quot;/Citrix/Store&amp;quot;<br>
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath<br>
$auth = Get-STFAuthenticationService -StoreService $store<br>
Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName &amp;quot;FASClaimsFactory&amp;quot;<br>
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider &amp;quot;FASLogonDataProvider&amp;quot;</p>
```

To stop using the FAS, use the following PowerShell script:

command COPY

```
<p>Get-Module &amp;quot;Citrix.StoreFront.*&amp;quot; -ListAvailable | Import-Module<br>
$StoreVirtualPath = &amp;quot;/Citrix/Store&amp;quot;<br>
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath<br>
$auth = Get-STFAuthenticationService -StoreService $store<br>
Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName &amp;quot;standardClaimsFactory&amp;quot;<br>
Set-STFStoreLaunchOptions -StoreService $store&amp;nbsp;-VdaLogonDataProvider &amp;quot;&amp;quot;</p>
```

Configure the Delivery Controller

To use the Federated Authentication Service, 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.

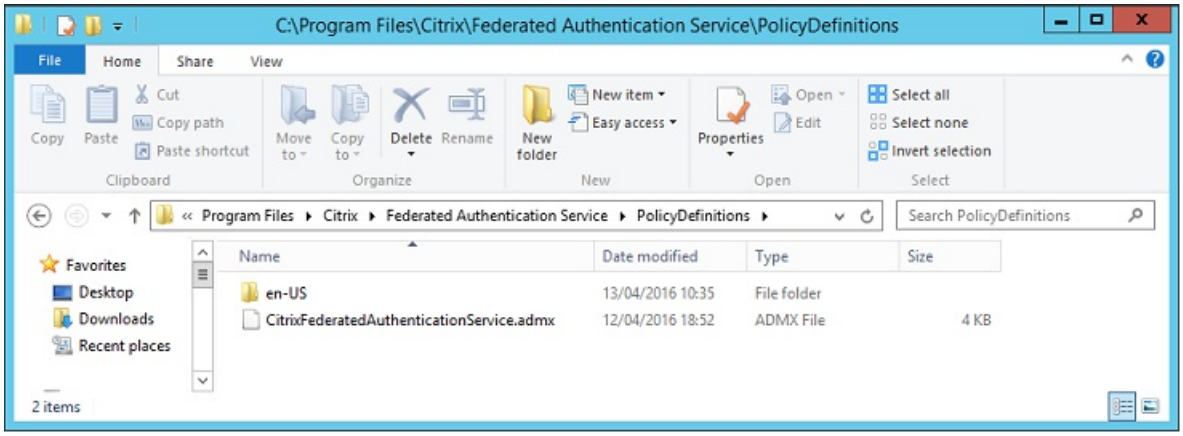
Configure Group Policy

After you install the Federated Authentication Service, you must specify the full DNS addresses of the FAS servers in Group Policy using the Group Policy templates provided in 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.

For simplicity, the following examples configure a single policy at the domain level that applies to all machines; however, that is not required. The FAS will function as long as the StoreFront servers, VDAs, and the machine running the FAS administration console see the same list of DNS addresses. Note that the Group Policy object adds an index number to each entry, which must also match if multiple objects are used.

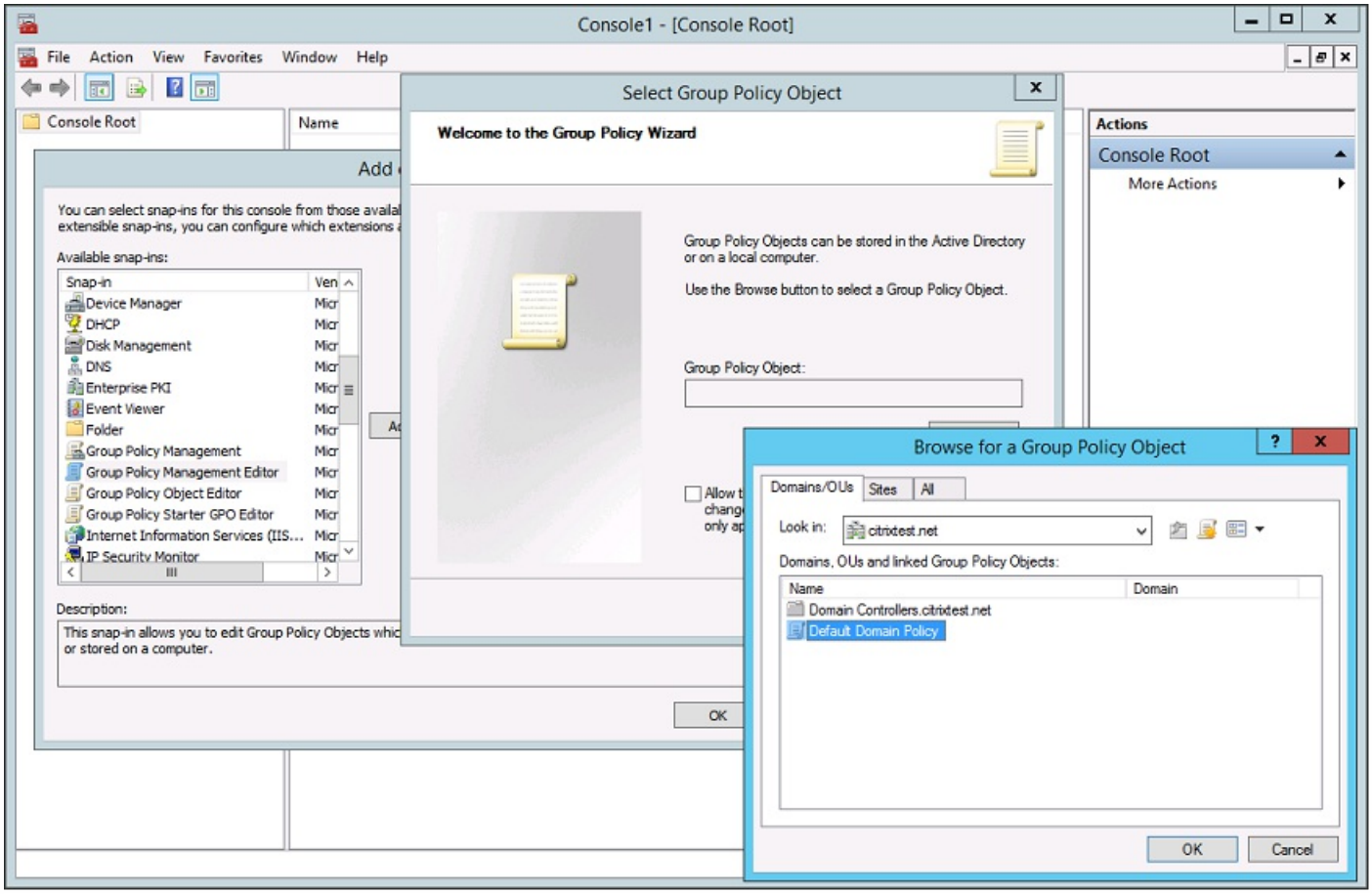
Step 1. On the server where you installed the FAS, locate the C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx file and the en-US folder.



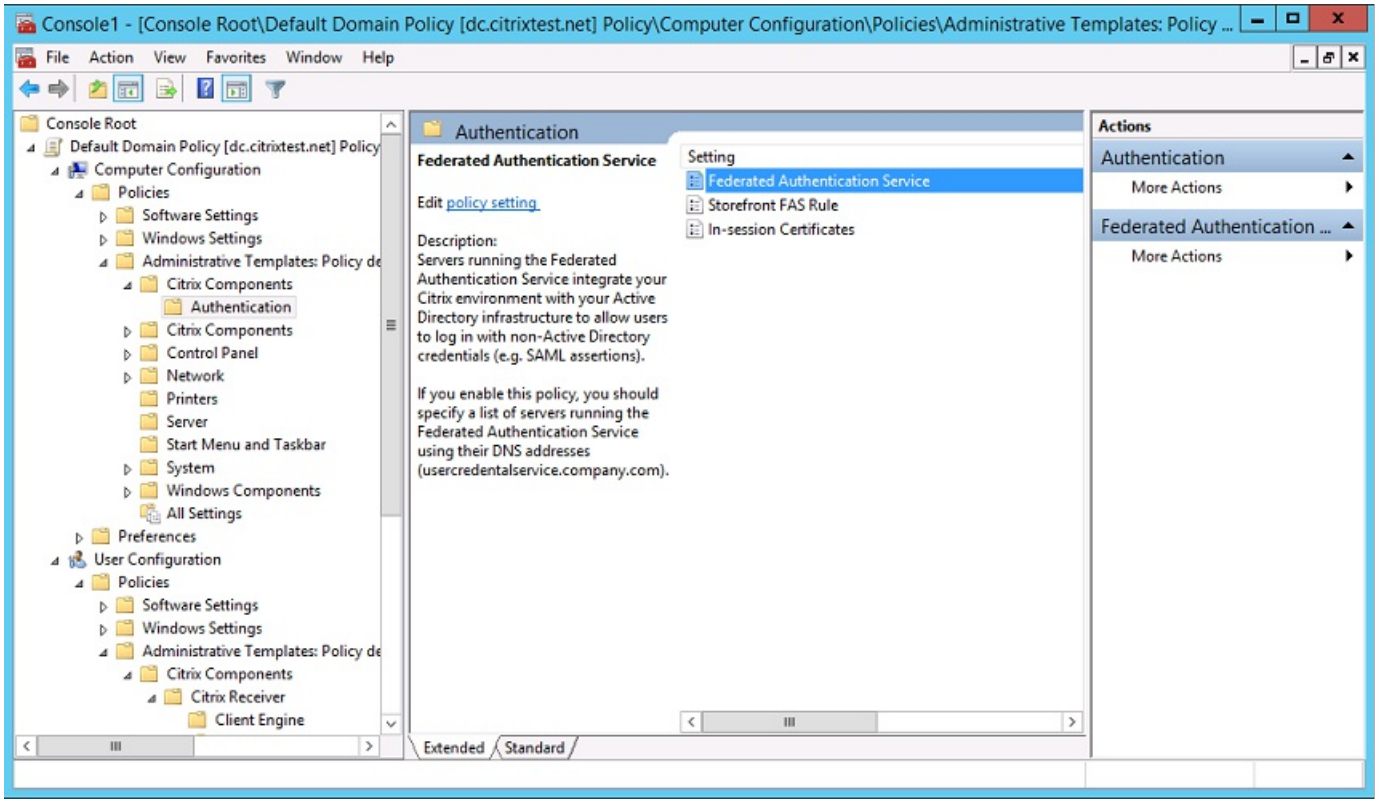
Step 2. Copy these to your domain controller and place them in the C:\Windows\PolicyDefinitions and en-US subfolder.

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**.

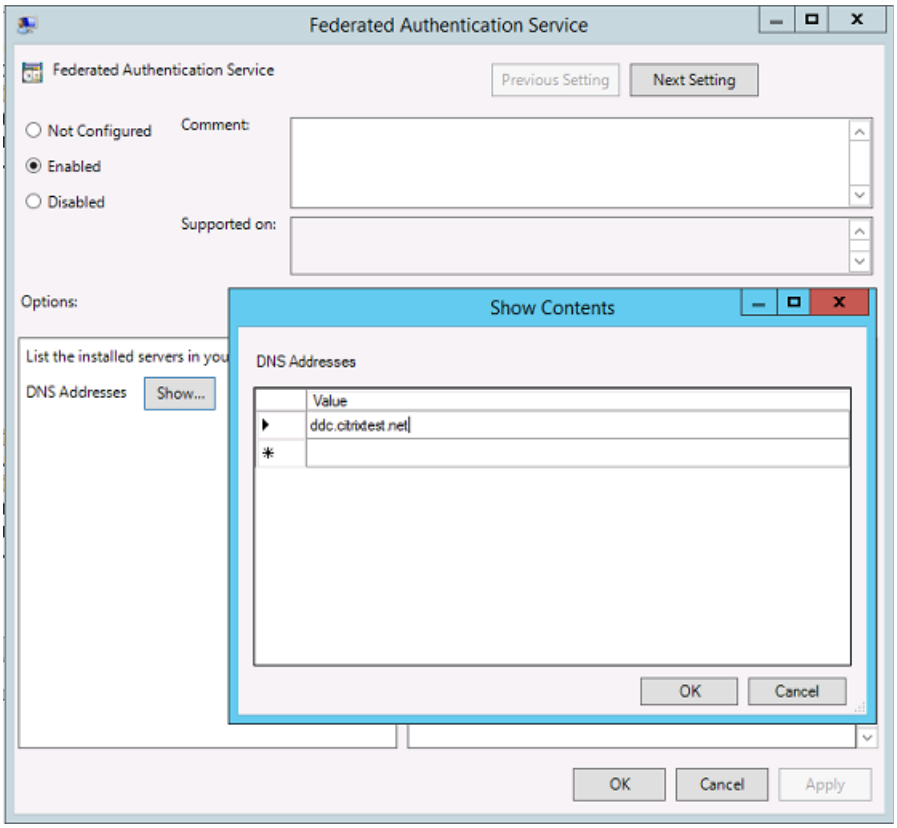
When prompted for a Group Policy Object, select **Browse** and then select **Default Domain Policy**. Alternatively, you can create and select an appropriate policy object for your environment, using the tools of your choice. The policy must be applied to all machines running affected Citrix software (VDAs, StoreFront servers, administration tools).



Step 4. Navigate to the Federated Authentication Service policy located in Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentication.



Step 5. Open the Federated Authentication Service policy and select **Enabled**. This allows you to select the **Show** button, where you configure the DNS addresses of your FAS servers.



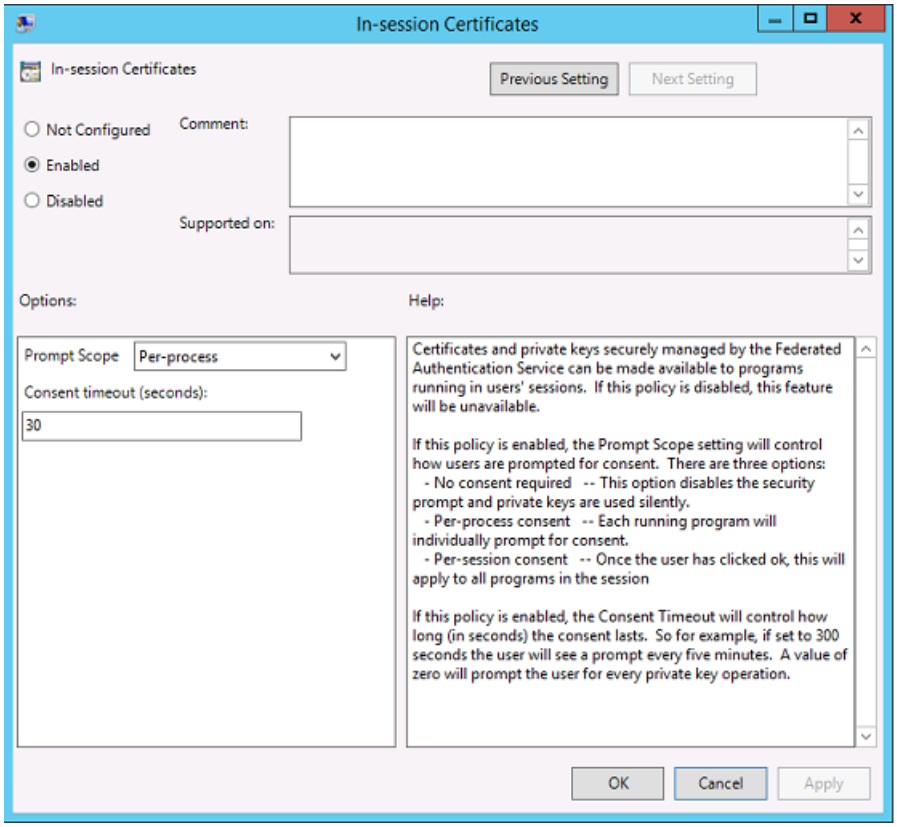
Step 6. Enter the DNS addresses of the servers hosting your Federated Authentication Service.

Remember: If you enter multiple addresses, the order of the list must be consistent between StoreFront servers and VDAs. This includes blank or unused list entries.

Step 7. Click **OK** to exit the Group Policy wizard and apply the group policy changes. You may need to restart your machines (or run **gpupdate /force** from the command line) for the change to take effect.

Enable in-session certificate support

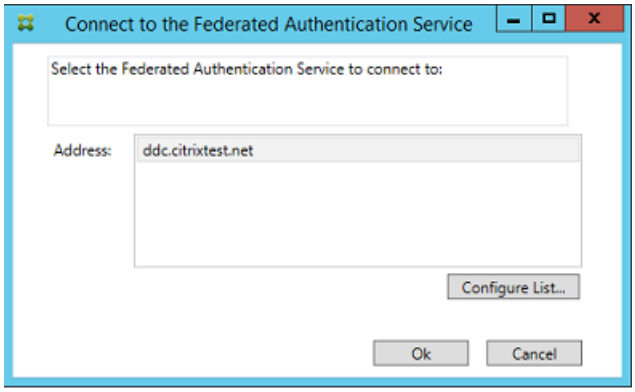
The Group Policy template includes support for configuring the system for in-session certificates. This places certificates in the user's personal certificate store after logon for application use. For example, if you require TLS authentication to web servers within the VDA session, the certificate can be used by Internet Explorer. By default, VDAs will not allow access to certificates after logon.



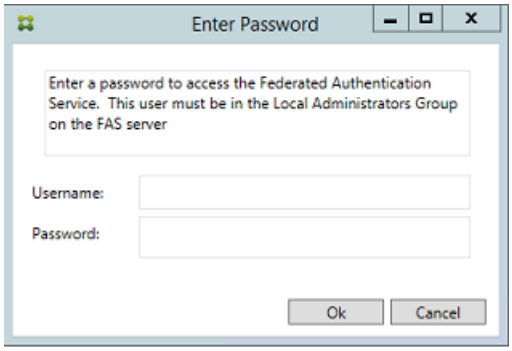
Using the Federated Authentication Service administration console

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.

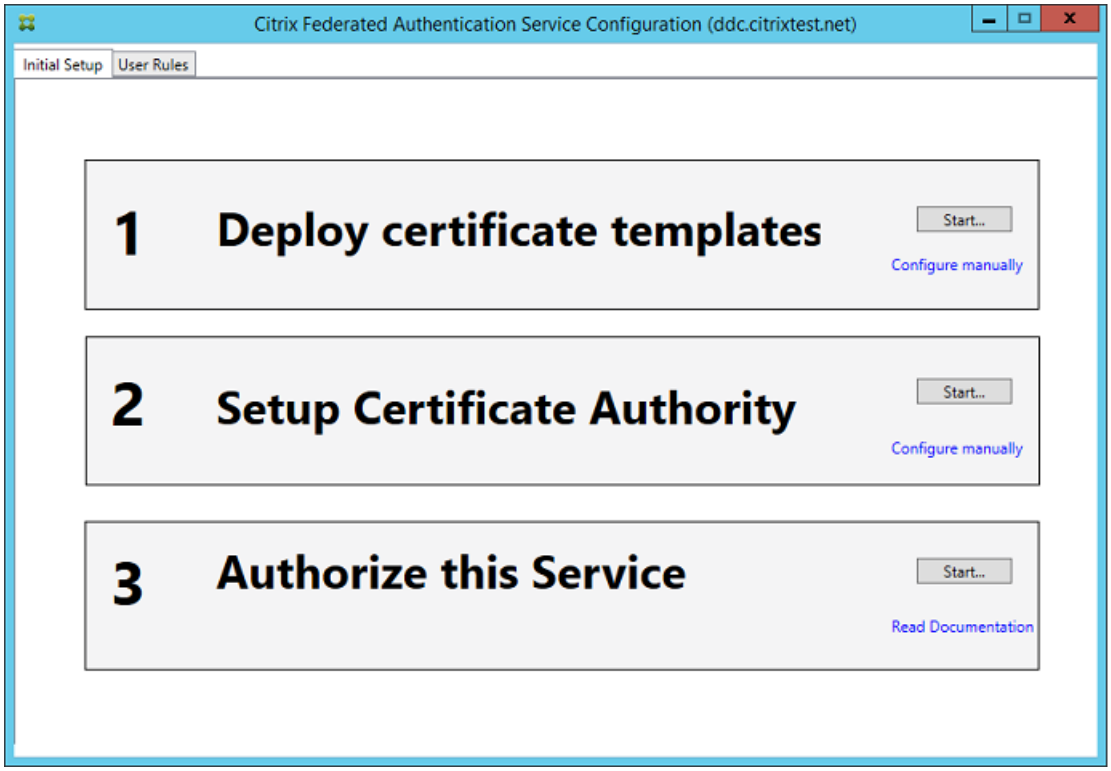
The console attempts to automatically locate the FAS servers in your environment using the Group Policy configuration. If this fails, see the Configure Group Policy section.



If your user account is not a member of the Administrators group on the machine running the Federated Authentication Service, you will be prompted for credentials.



The first time the administration console is used, it guides you through a three-step process that deploys certificate templates, sets up the certificate authority, and authorizes the Federated Authentication Service to use the certificate authority. Some of the steps can alternatively be completed manually using OS configuration tools.

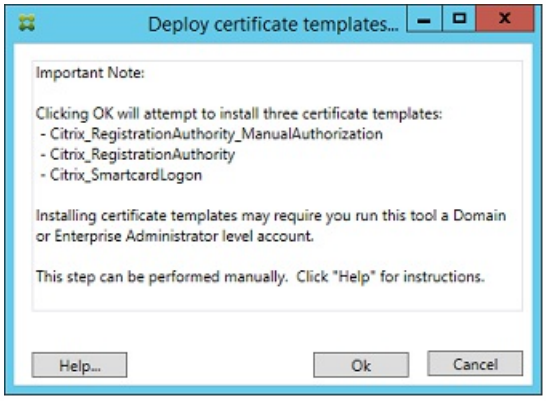


Deploy certificate templates

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 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.



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:

command COPY

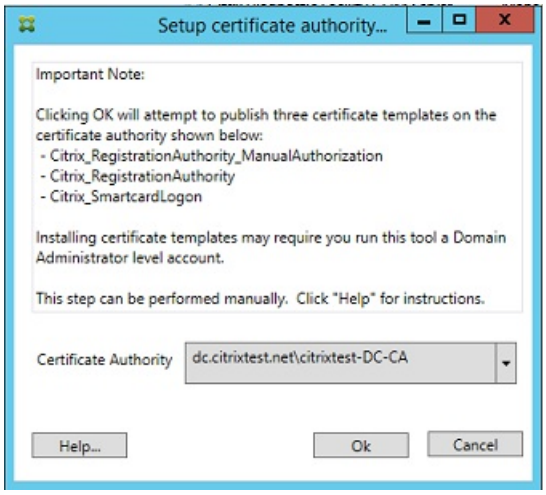
```
<p>$template = [System.IO.File]::ReadAllBytes(&amp;quot;$Pwd\Citrix_SmartcardLogon.certificatetemplate&amp;quot;)<br>
$CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService<br>
$CertEnrol.InitializeImport($template)<br>
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)</p>
<p>$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable<br>
$writabletemplate.Initialize($comtemplate)<br>
$writabletemplate.Commit(1, $NULL)</p>
```

Set up Active Directory Certificate Services

After installing the Citrix certificate templates, they must be published on one or more Microsoft Certification Authority servers. Refer to the Microsoft documentation on how to deploy Active Directory Certificate Services.

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.

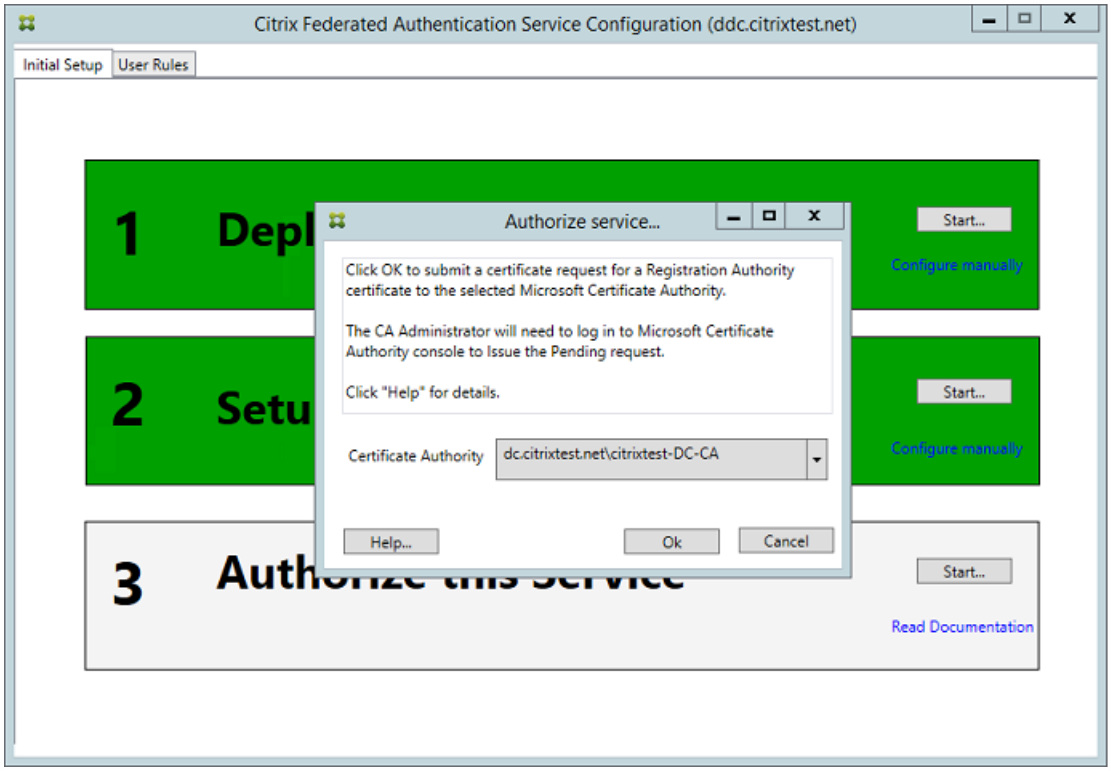
(Certificate templates can also be published using the Microsoft Certification Authority console.)



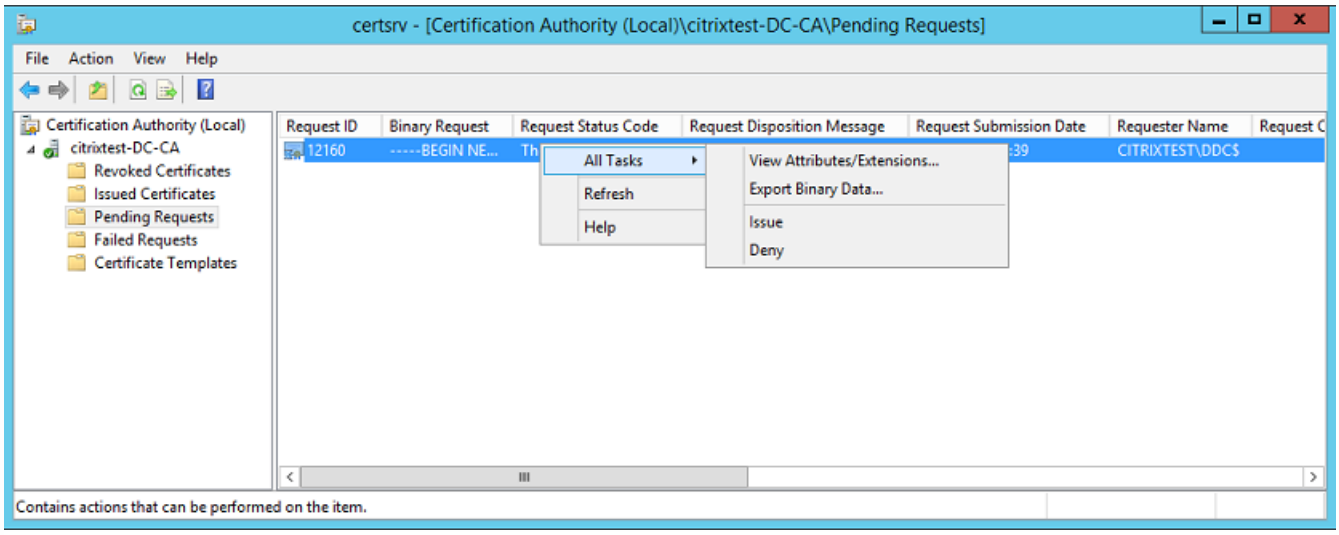
Authorize the Federated Authentication Service

The final setup step in the console initiates the authorization of the Federated Authentication Service. The administration

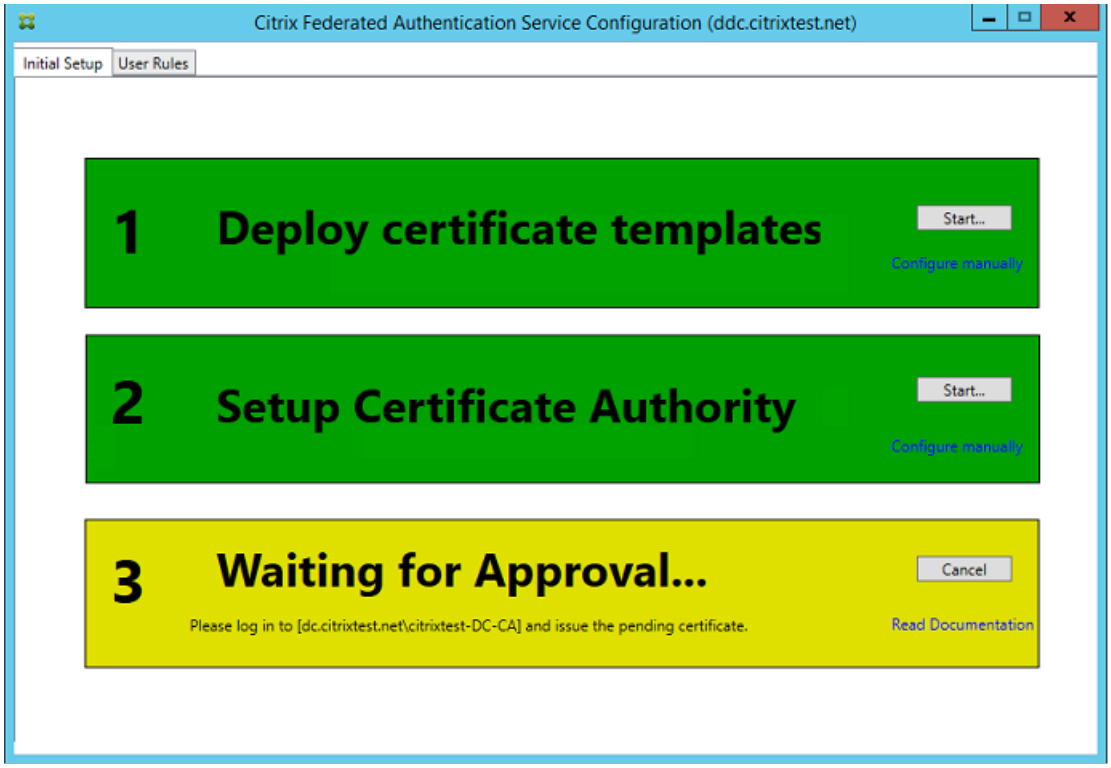
console uses the Citrix_RegistrationAuthority_ManualAuthorization template to generate a certificate request, and then sends it to one of the certificate authorities that publish that template.



After the request is sent, it appears in the **Pending Requests** list of the Microsoft Certification Authority console. The certificate authority administrator must choose to **Issue** or **Deny** the request before configuration of the Federated Authentication Service can continue. Note that the authorization request appears as a **Pending Request** from the FAS machine account.



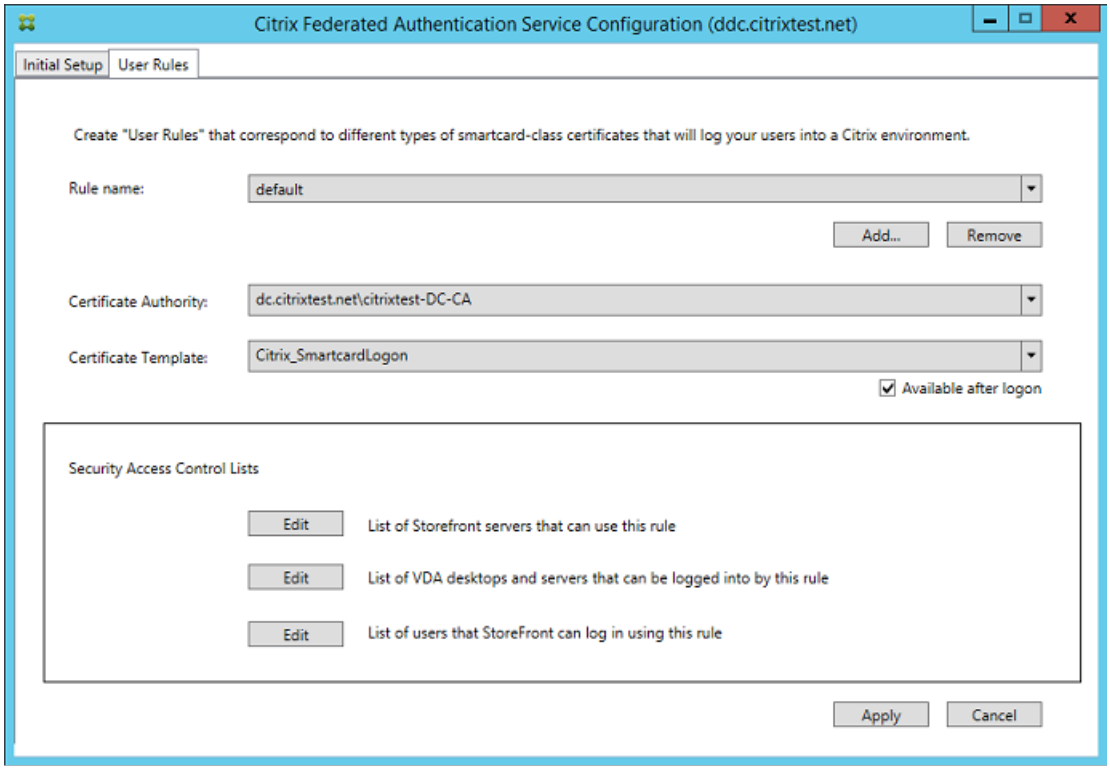
Right-click **All Tasks** and then select **Issue** or **Deny** for the certificate request. The Federated Authentication Service administration console automatically detects when this process completes. This can take a couple of minutes.



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 StoreFront servers that are trusted to request certificates, the set of users for which they can be requested, and the set of VDA machines permitted to use them.

To complete the setup of the Federated Authentication Service, the administrator must define the default rule by switching to the User Rules tab of the FAS administration console, selecting a certificate authority to which the Citrix_SmartcardLogon template is published, and editing 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.



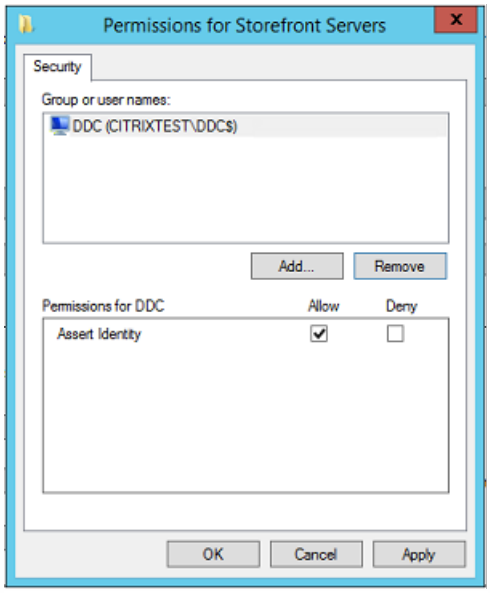
Fields:

Certificate Authority and Certificate Template: The certificate template and certificate authority that will be used to issue user certificates. This should be the Citrix_SmartcardLogon template, or a modified copy of it, on one of the certificate authorities that the template is published to.

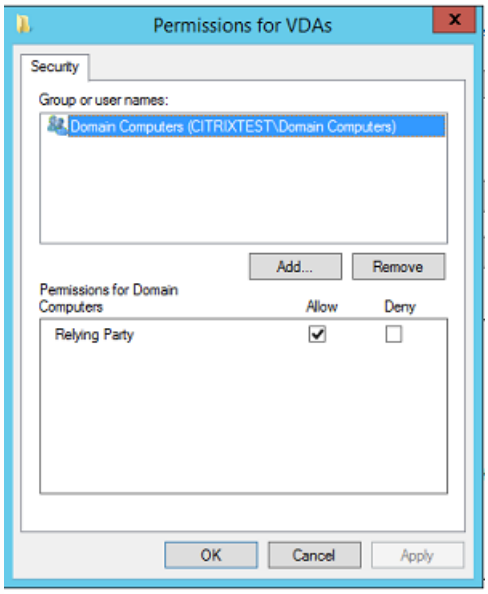
The FAS supports adding multiple certificate authorities for failover and load balancing, using PowerShell commands. Similarly, more advanced certificate generation options can be configured using the command line and configuration files. See the PowerShell and Hardware security modules sections.

In-Session Certificates: The **Available after logon** check box controls whether a certificate can also be used as an in-session certificate. If this check box is not selected, the certificate will be used only for logon or reconnection, and the user will not have access to the certificate after authenticating.

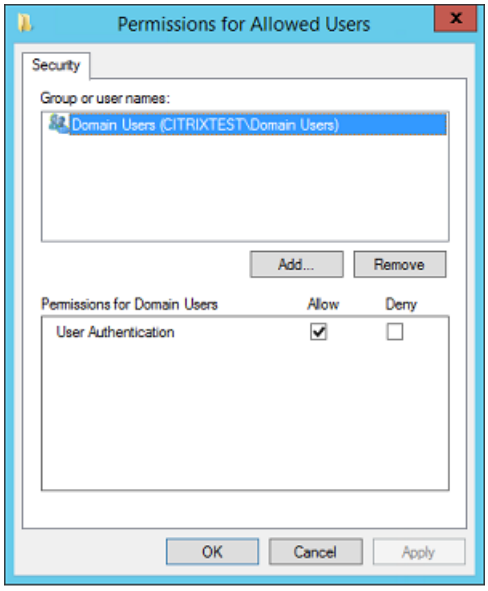
List of StoreFront servers that can use this rule: The list of trusted StoreFront server machines that are authorized to request certificates for logon or reconnection of users. Note that this setting is security critical, and must be managed carefully.



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.



Advanced use

You can create additional rules to reference different certificate templates and authorities, which may be configured to have different properties and permissions. These rules can be configured for use by different StoreFront servers, which will need to be configured to request the new rule by name. By default, StoreFront requests **default** when contacting the Federated Authentication Service. This can be changed using the Group Policy Configuration options.

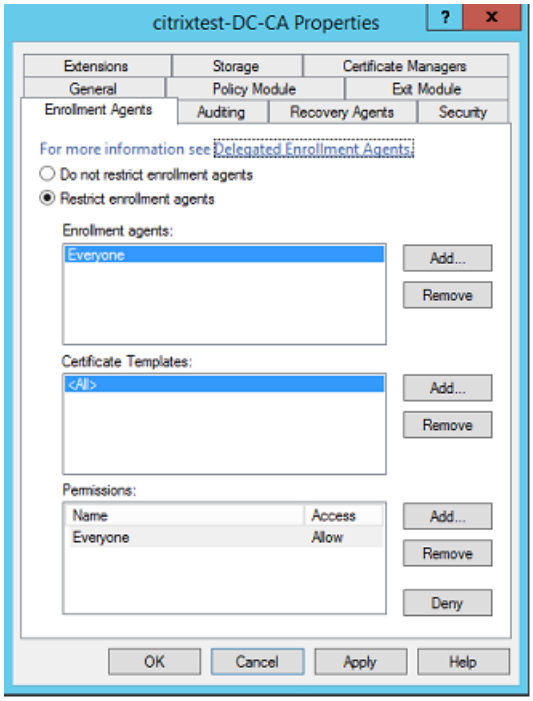
To create a new certificate template, duplicate the Citrix_SmartcardLogon template in the Microsoft Certification Authority console, rename it (for example, Citrix_SmartcardLogon2), and modify it as required. Create a new user rule by clicking **Add** to reference the new certificate template.

Security considerations

The Federated Authentication Service has a registration authority certificate that allows it to issue certificates autonomously on behalf of your domain users. As such, it is important to develop and implement a security policy to protect the the FAS servers, and to constrain their permissions.

Delegated Enrollment Agents

The Microsoft Certification Authority allows control of which templates the FAS server can use, as well as limiting which users the FAS server can issue certificates for.



Citrix strongly recommends configuring these options so that the Federated Authentication Service can only issue certificates for the intended users. For example, it is 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 roles 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 will be issued certificates, and which VDA machines they can authenticate to. This 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 can be used for monitoring and auditing information. The Event logs section lists event log entries that may be generated.

Hardware security modules

All private keys, including those of user certificates 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.

Parameter	Description
ProviderLegacyCsp	When set to true, FAS will use the Microsoft CryptoAPI (CAPI). Otherwise, FAS will use 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. Should 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).

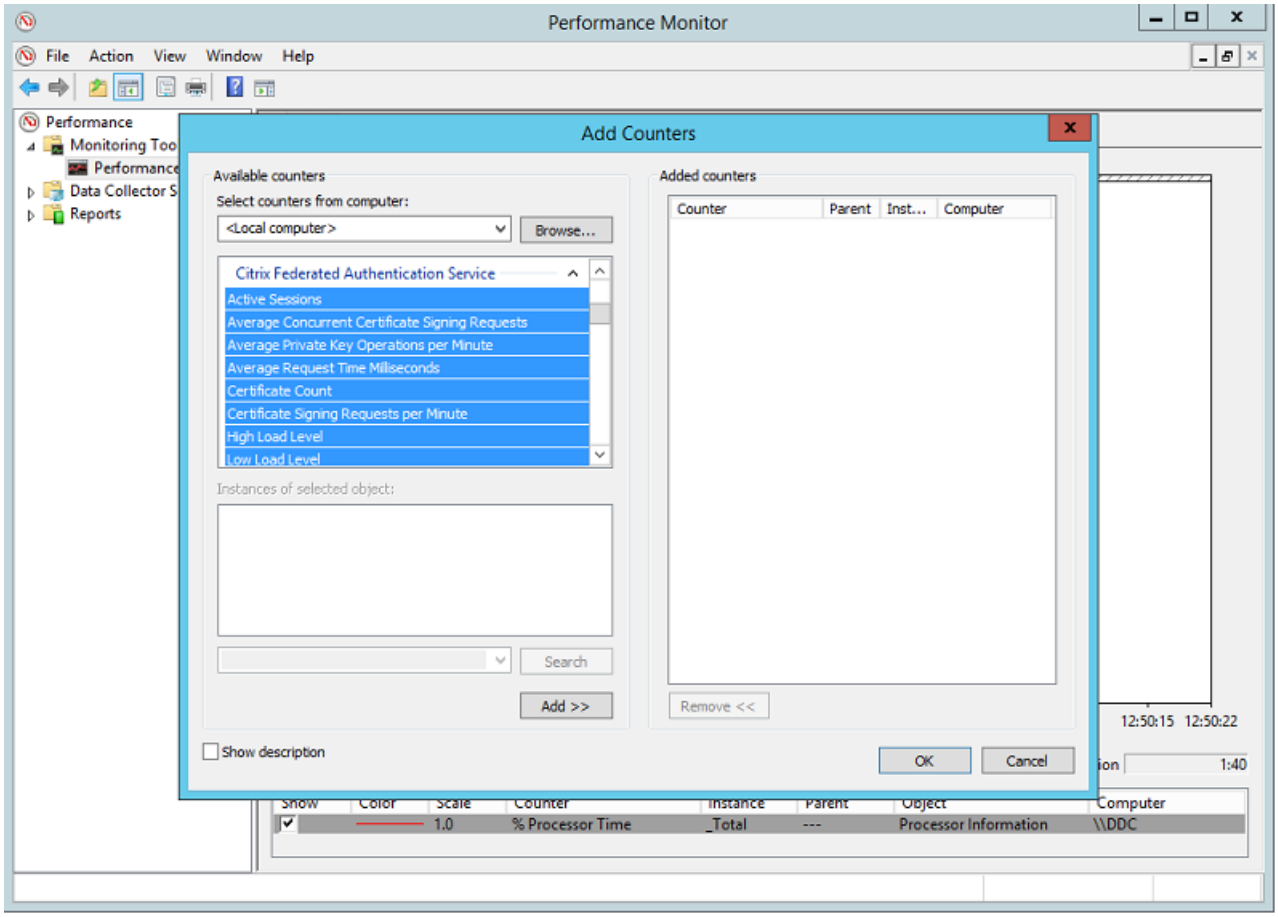
Commands	Overview
*-FasServer	Lists and reconfigures the FAS servers in the current environment.
*-FasAuthorizationCertificate	Manages the Registration Authority certificate.
*-FasCertificateDefinition	Controls the parameters that the FAS uses to generate certificates.
*-FasRule	Manages User Rules configured on the Federated Authentication Service.
*-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 containing 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.

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 may 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]

These events are logged in response to a configuration change in the Federated Authentication Service 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}]
[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}].

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.

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
[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}

[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

Jun 09, 2016

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 various authentication architectures that may be 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 technologies, and is easily extensible using the StoreFront SDK or third-party IIS plugins. The basic design goal is that any authentication technology that can authenticate a user to a web site 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 who are 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

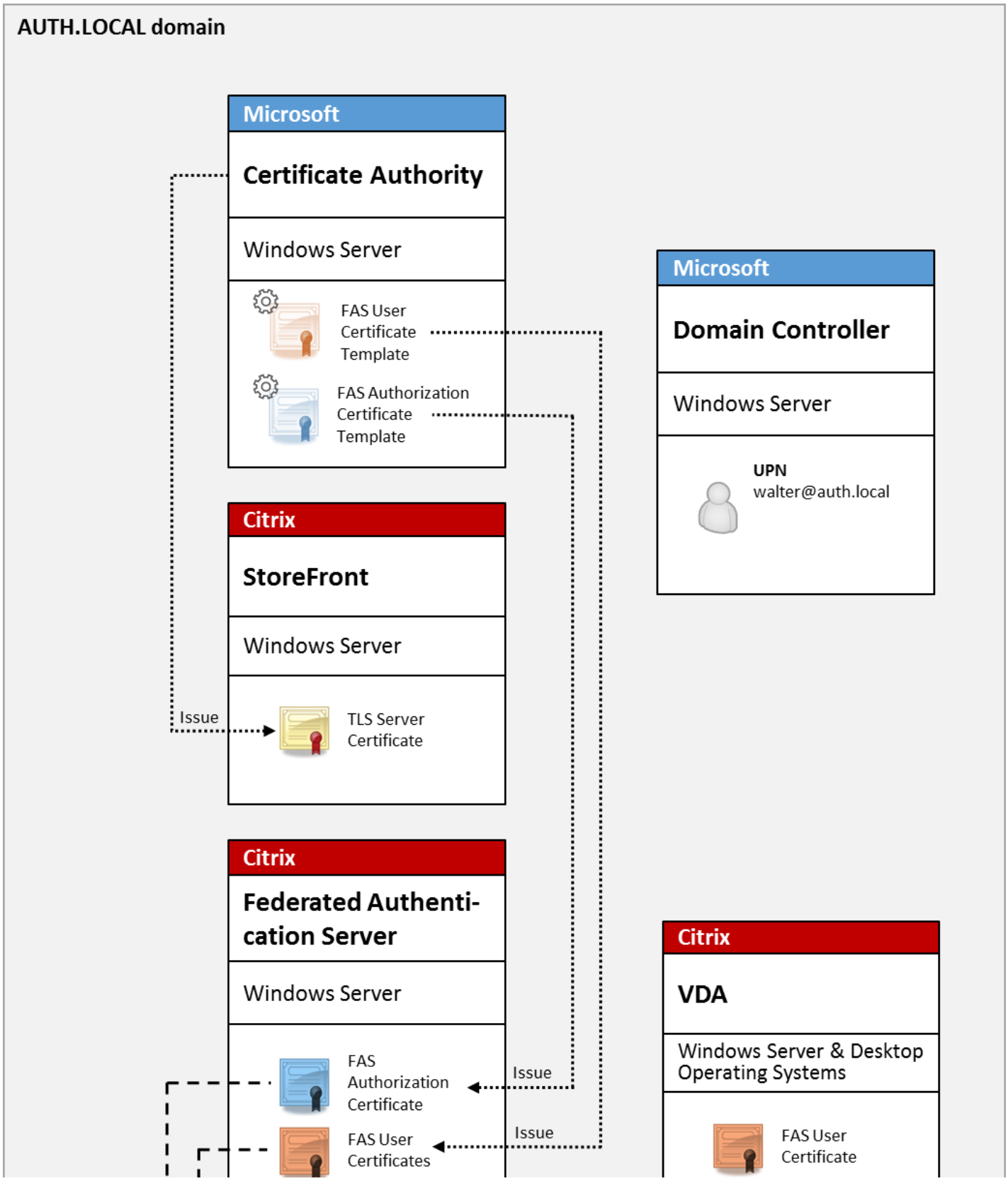
The FAS allows users to securely authenticate to StoreFront using a variety of authentication options (including Kerberos single sign-on) and connect through to a fully authenticated Citrix HDX session.

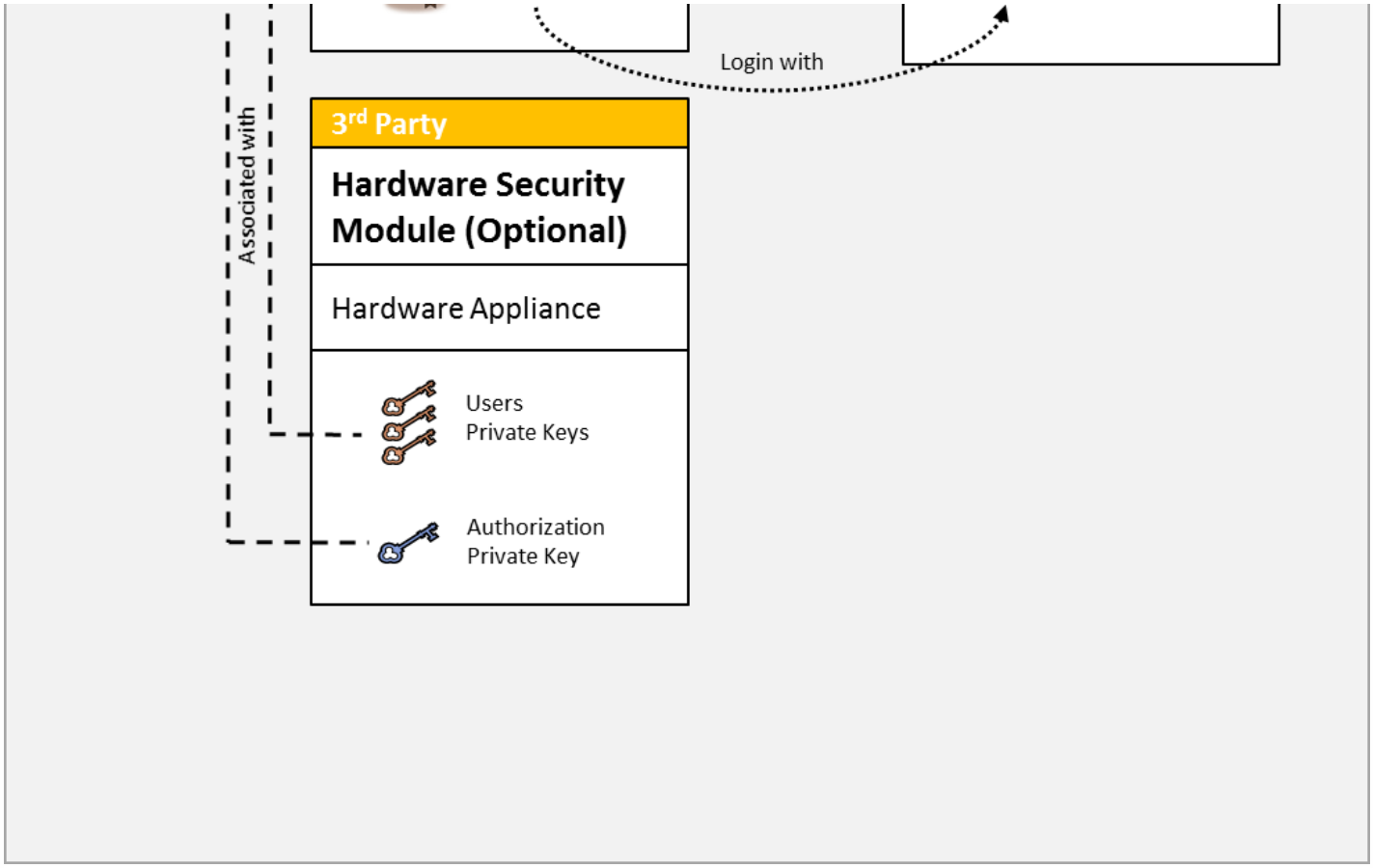
This allows Windows authentication without prompts to enter user credentials or smart card PINs, and without using “saved password management” features such as the Single Sign-on Service. This can be used to replace the Kerberos Constrained Delegation logon features available in earlier versions of XenApp.

All users have access to public key infrastructure (PKI) certificates within their session, regardless of whether or not 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 new 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.





The XenApp or XenDesktop environment must be configured in a similar manner as 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.)

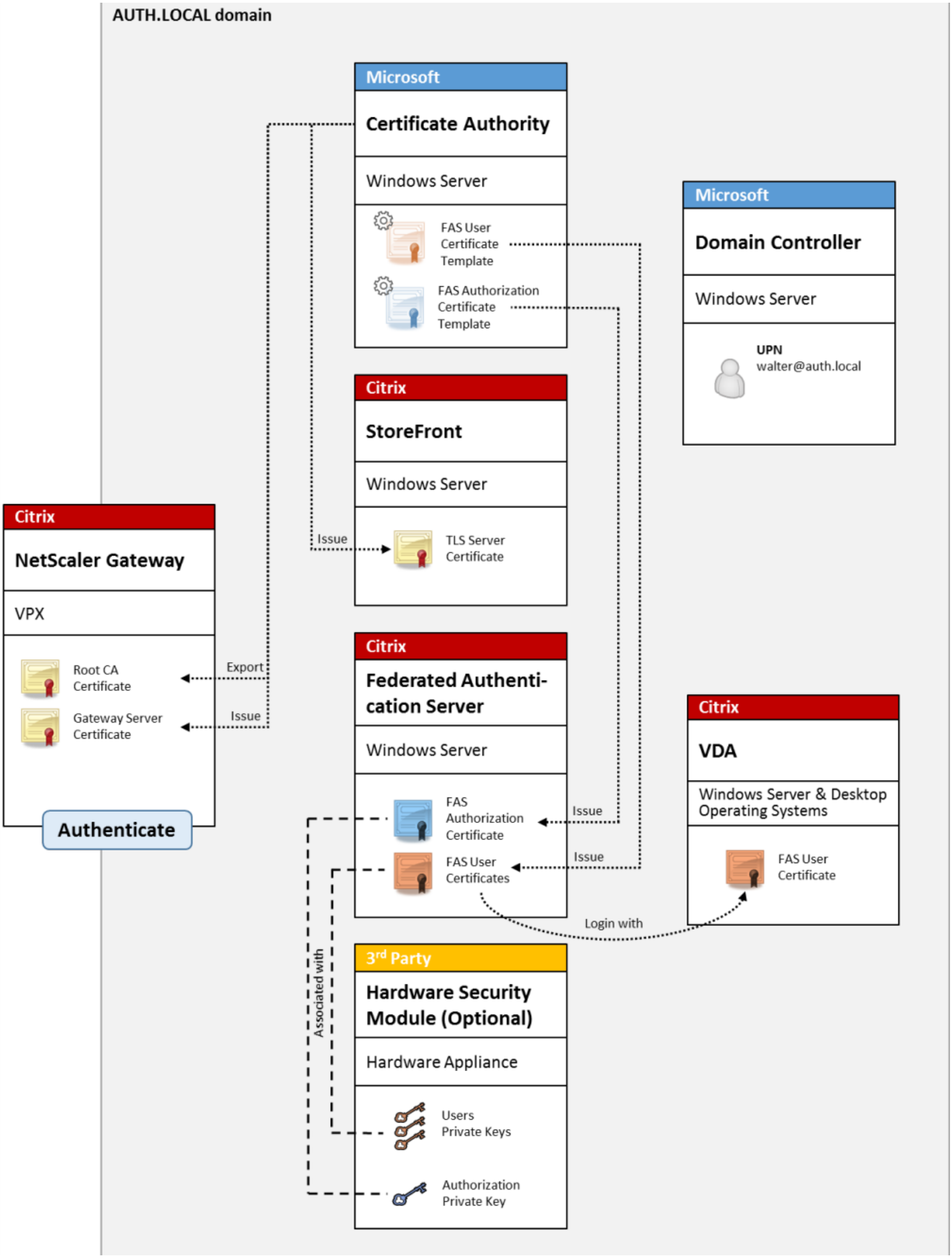
Related information:

- 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 web sites.

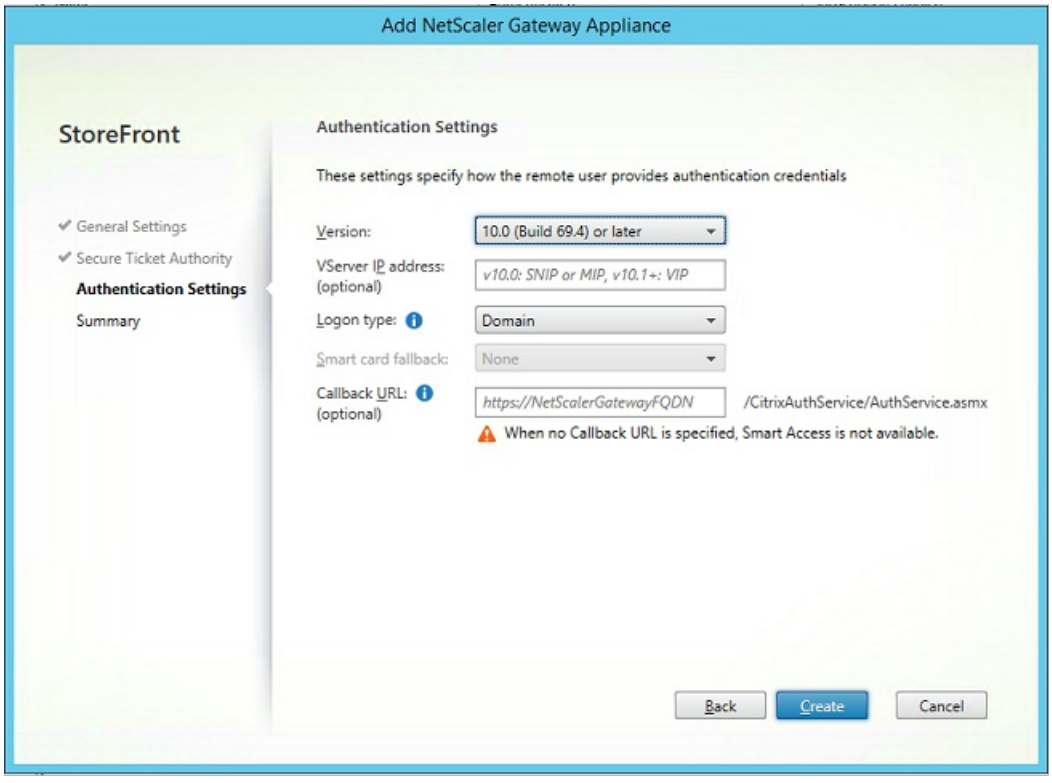
This deployment can be used to avoid multiple PIN prompts that occur when authenticating first to NetScaler and then logging in to a user session. It also allows use of advanced NetScaler authentication technologies without additionally requiring AD passwords or smart cards.



The XenApp or XenDesktop environment must be configured in a similar manner as 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 between 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.

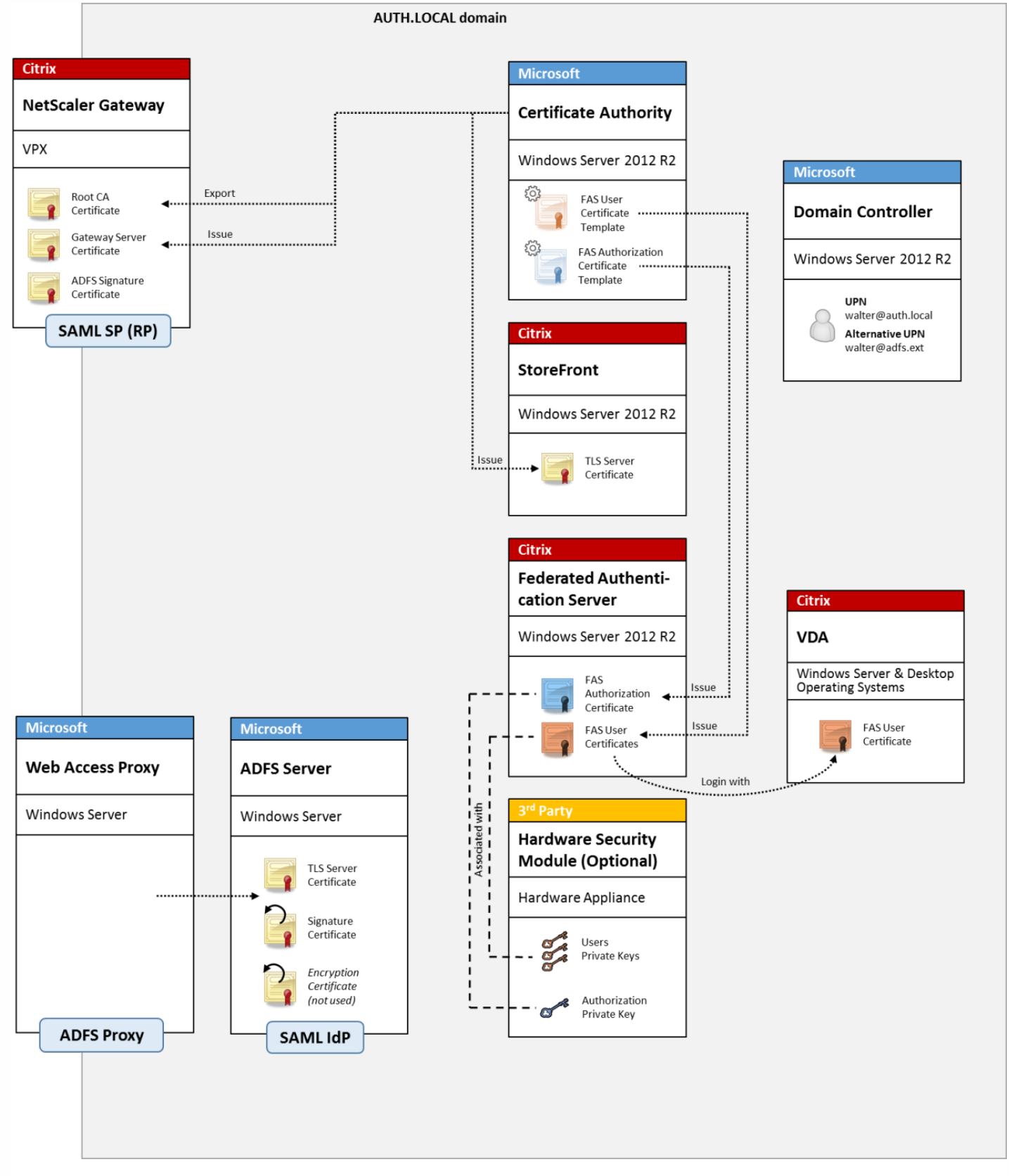


Related information:

- 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. This 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).



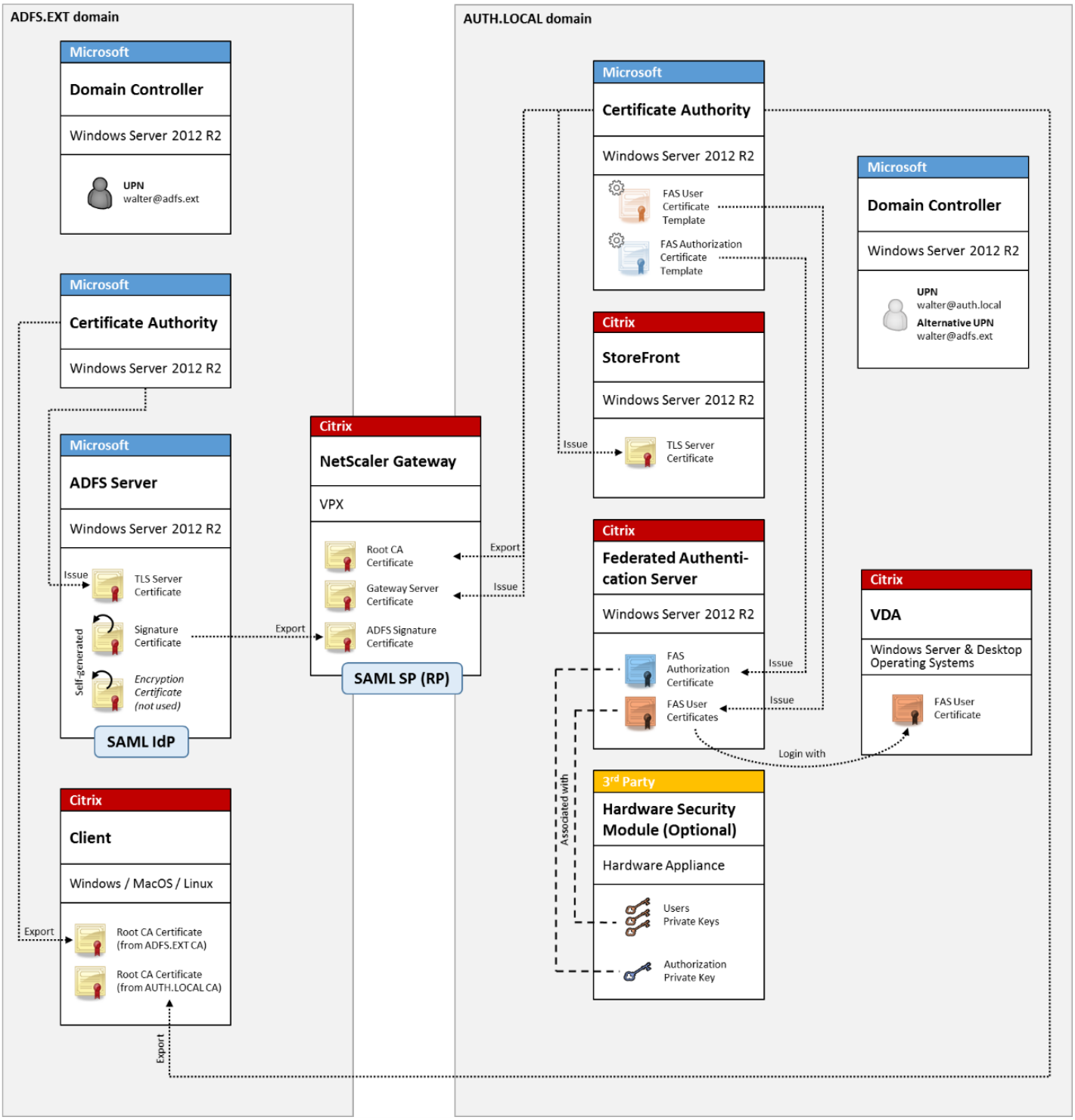
ADFS is commonly used to securely authenticate users to corporate resources remotely over the Internet; for example, it is often used for Office 365 integration.

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 cntains configuration considerations.

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.



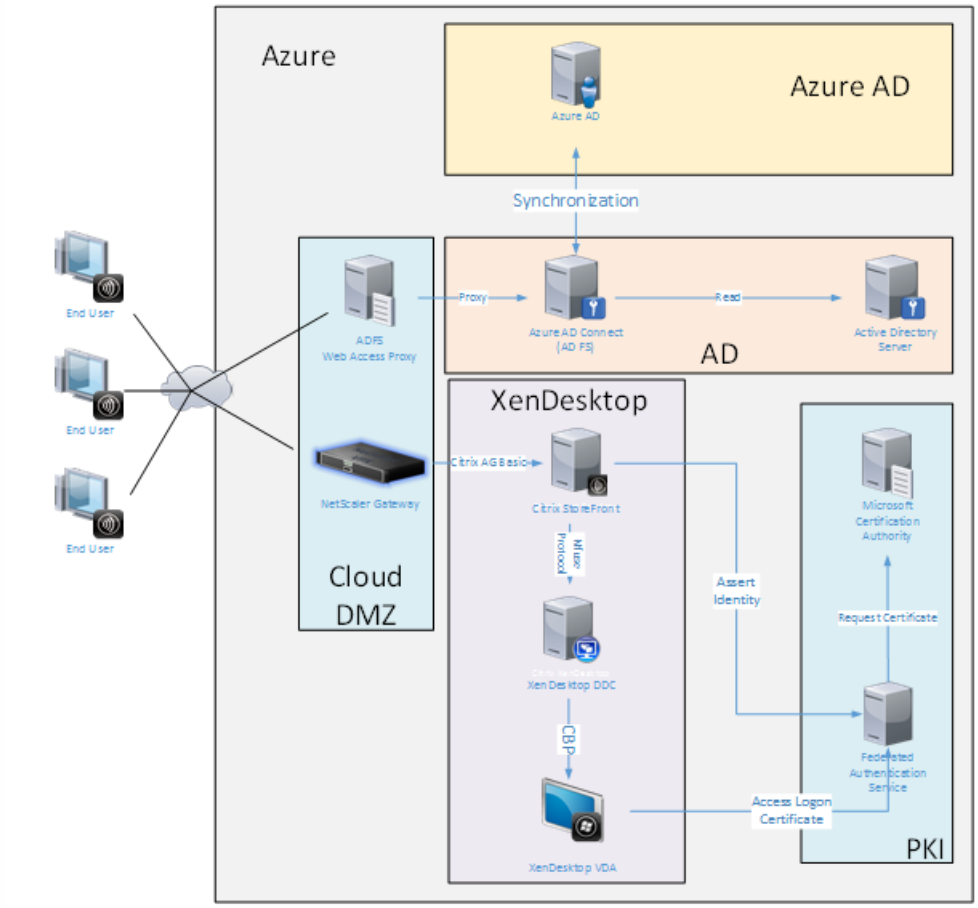
Related information:

- The Federated Authentication Service article describes how to install and configure FAS.

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 single sign-on 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.

Note that 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.

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

Aug 10, 2016

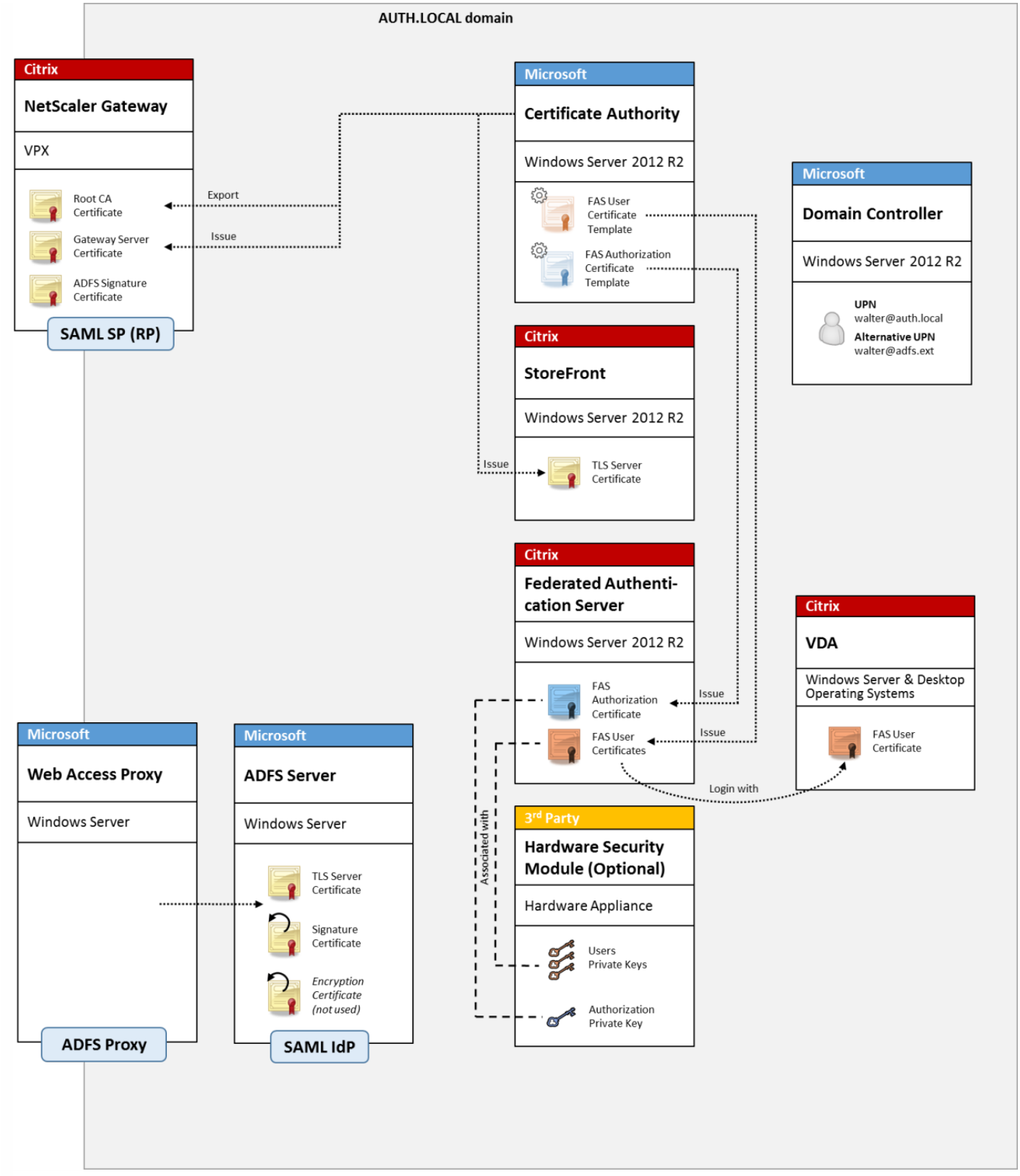
Introduction

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.



SAML overview

Security Assertion Markup Language (SAML) is a simple "redirect to a logon page" web browser logon system. Configuration includes the following items:

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.

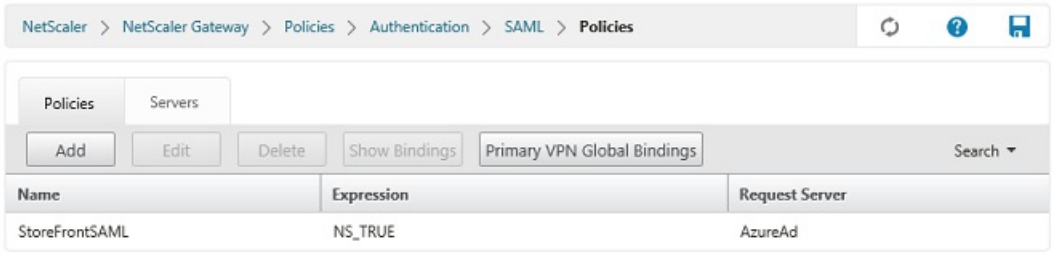
Single sign-out Url [Single Logout URL]

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.

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.)

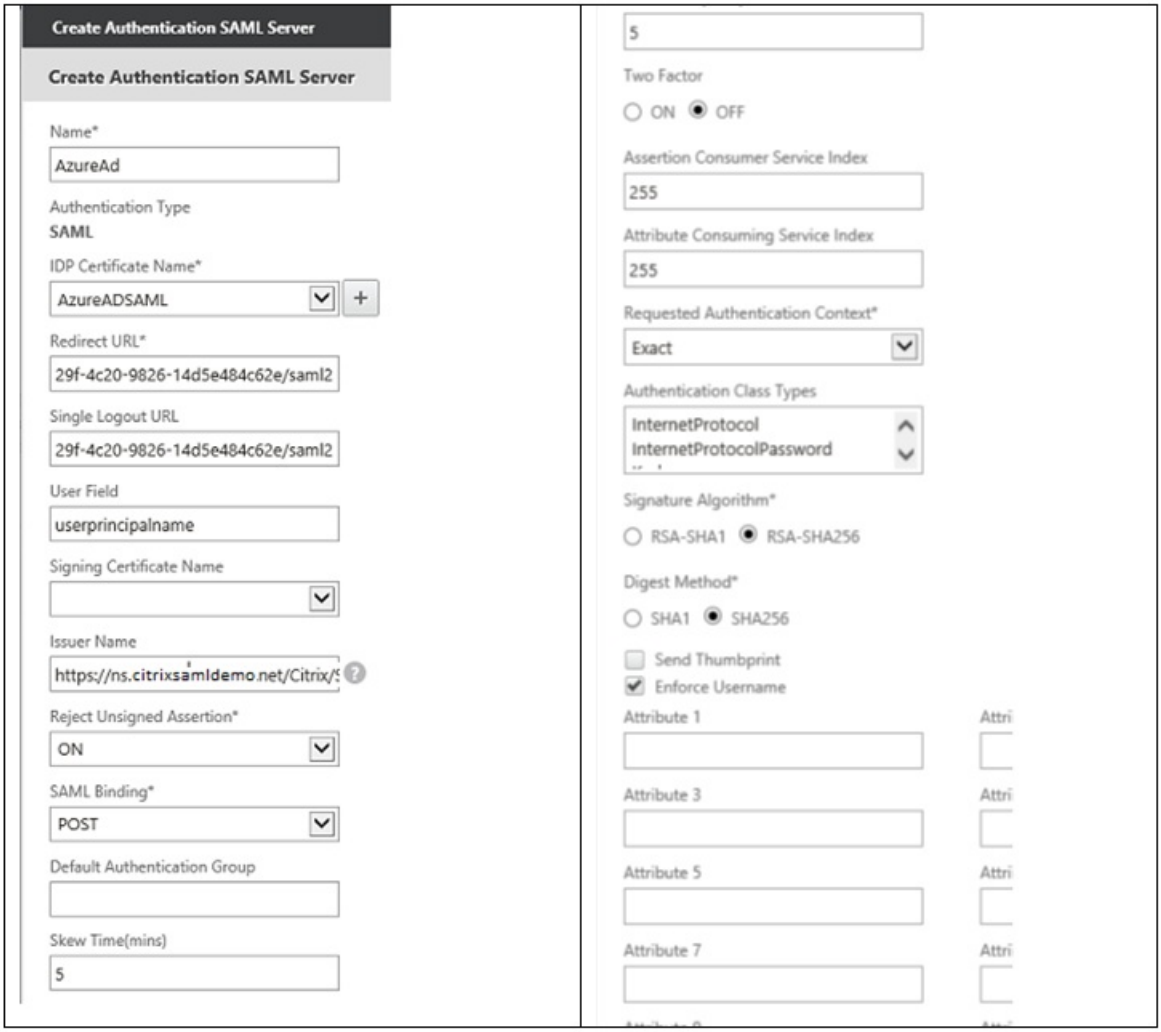
Configuration

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.



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 Service Azure AD integration

Aug 22, 2016

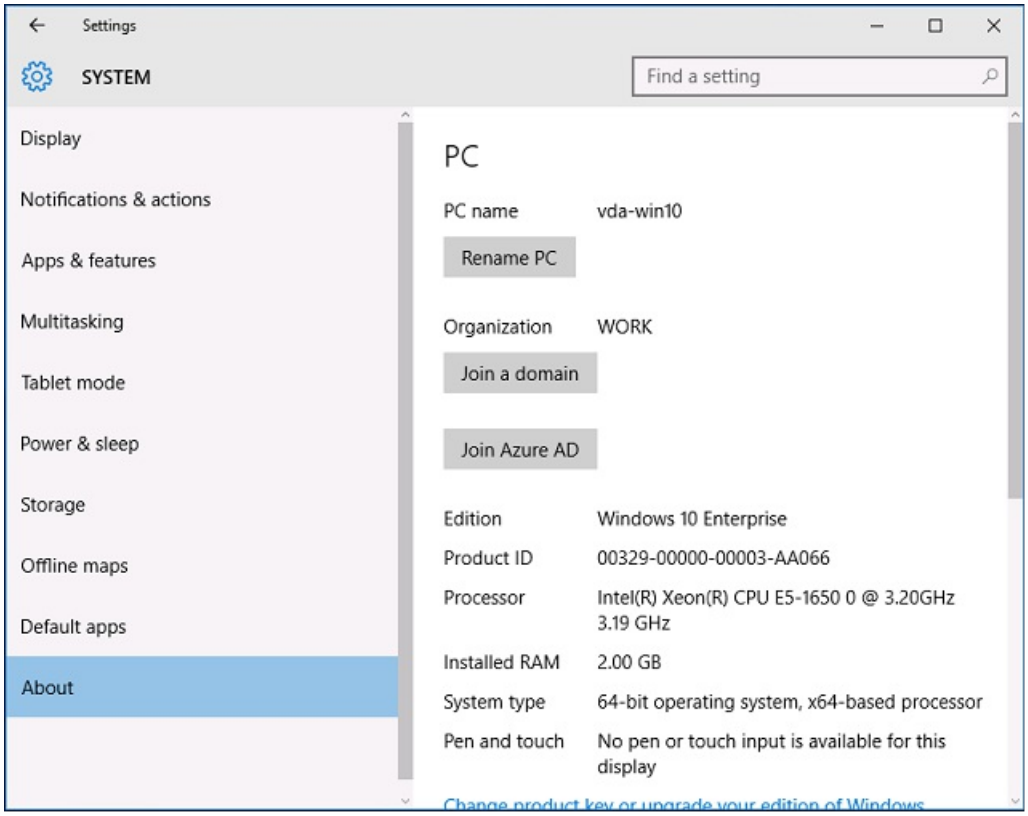
In this article:

Introduction

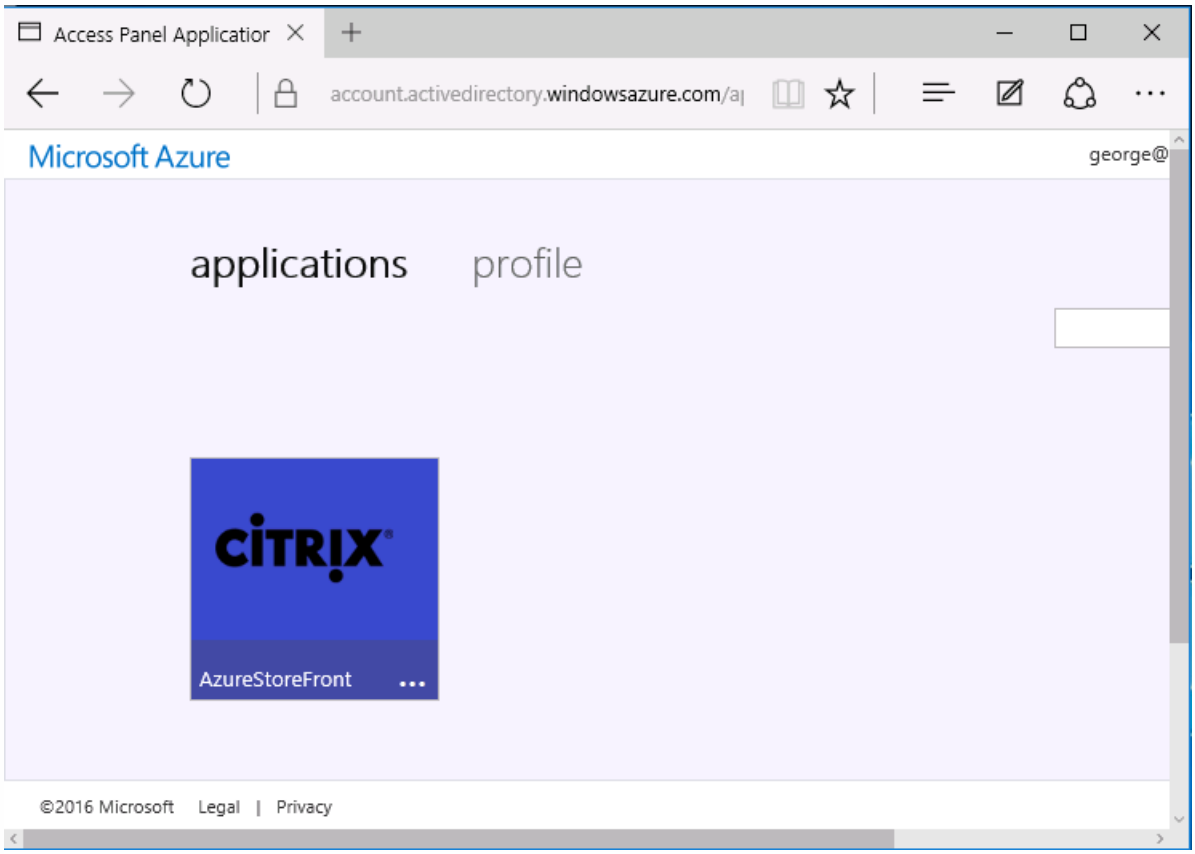
This document describes how to integrate a Citrix environment with the Windows 10 Azure AD feature.

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.



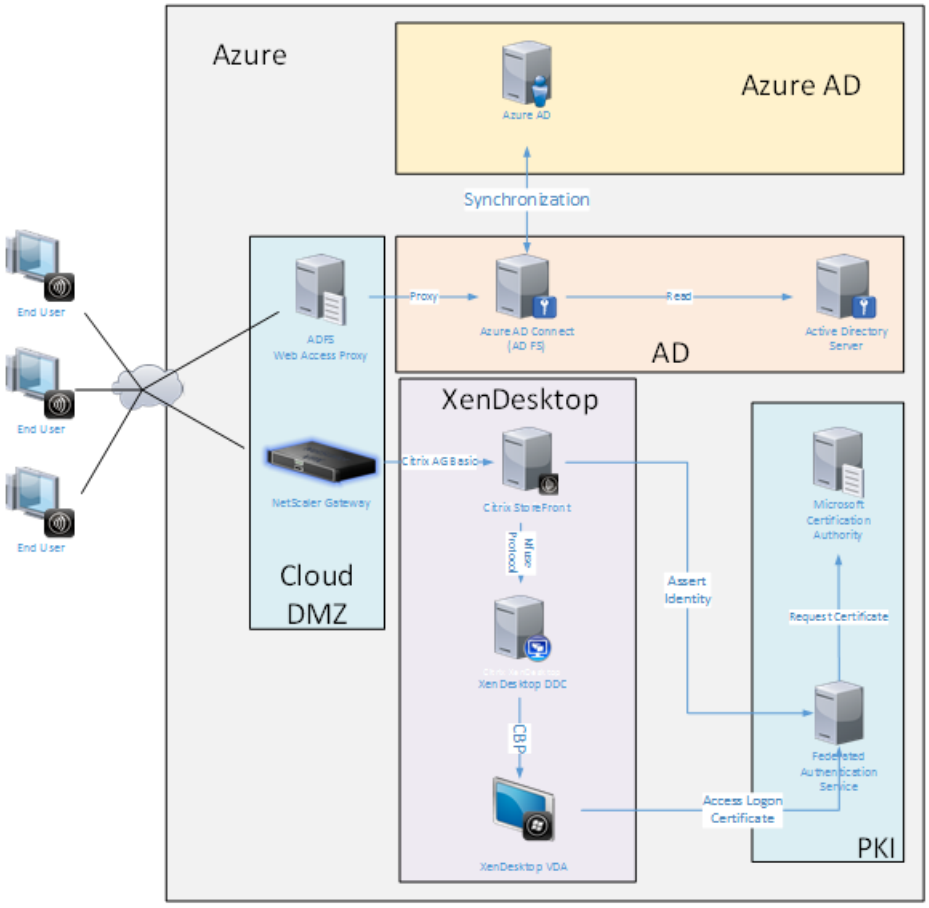
After the laptop is enrolled, the Microsoft Edge web browser automatically signs on to company web sites and Citrix published applications through the Azure SaaS applications web page, with other Azure applications such as Office 365.



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.



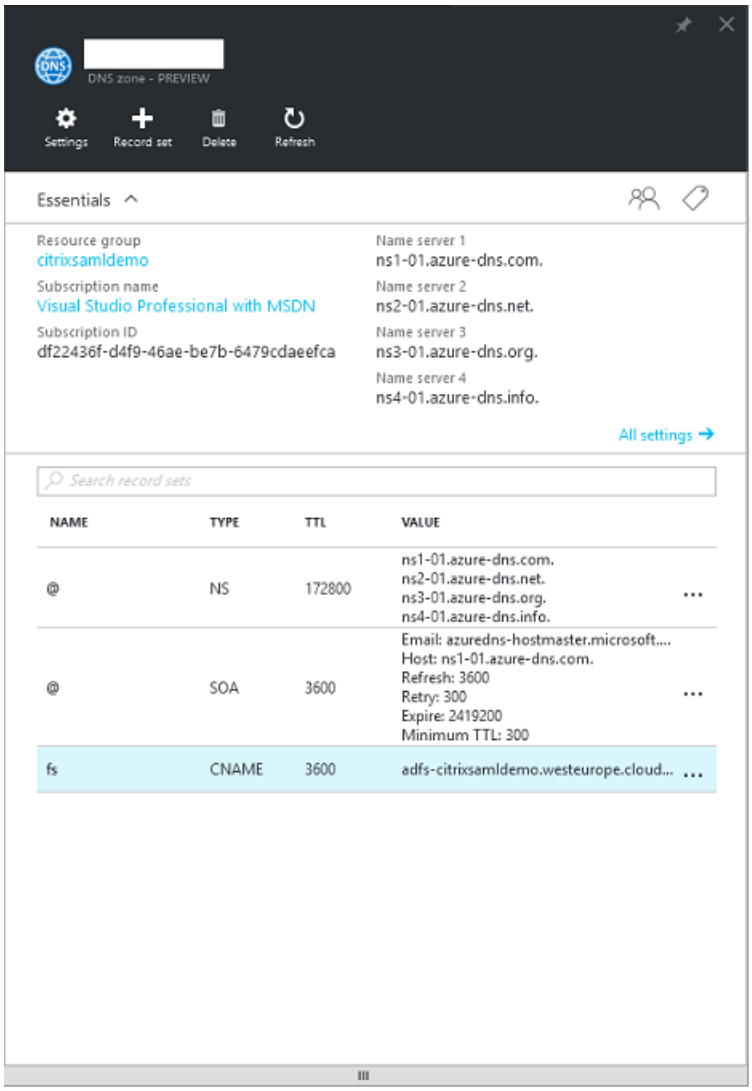
Secure connections and single sign-on, which would traditionally have been firewalled-LAN and Kerberos/NTLM authentication, are replaced in this architecture by TLS connections to Azure and SAML. New services are built as Azure applications joined to Azure AD. Existing applications that require Active 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.

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 registrar’s NS entries for the zone (for example, citrixsamldemo.net. NS n1-01.azure-dns.com)

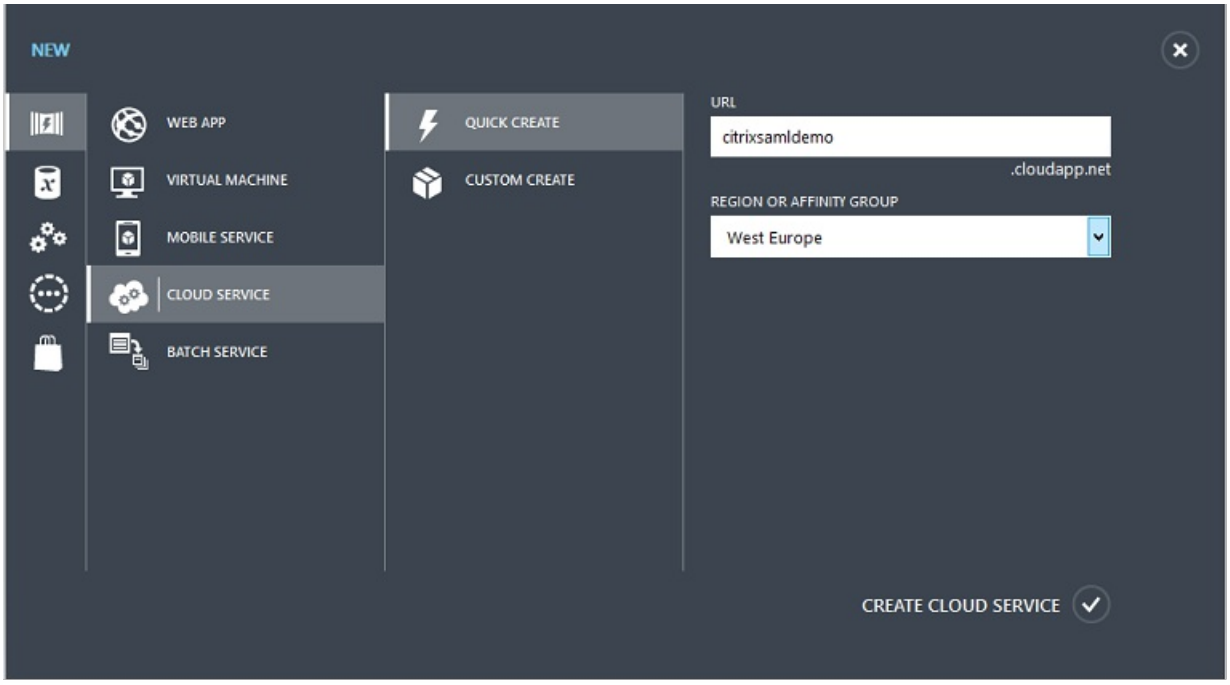
When adding references to VMs running in Azure, it is easiest to use a CNAME pointer to the Azure-managed DNS record for the VM. If the IP address of the VM changes, you will not need to manually update the DNS zone file.

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

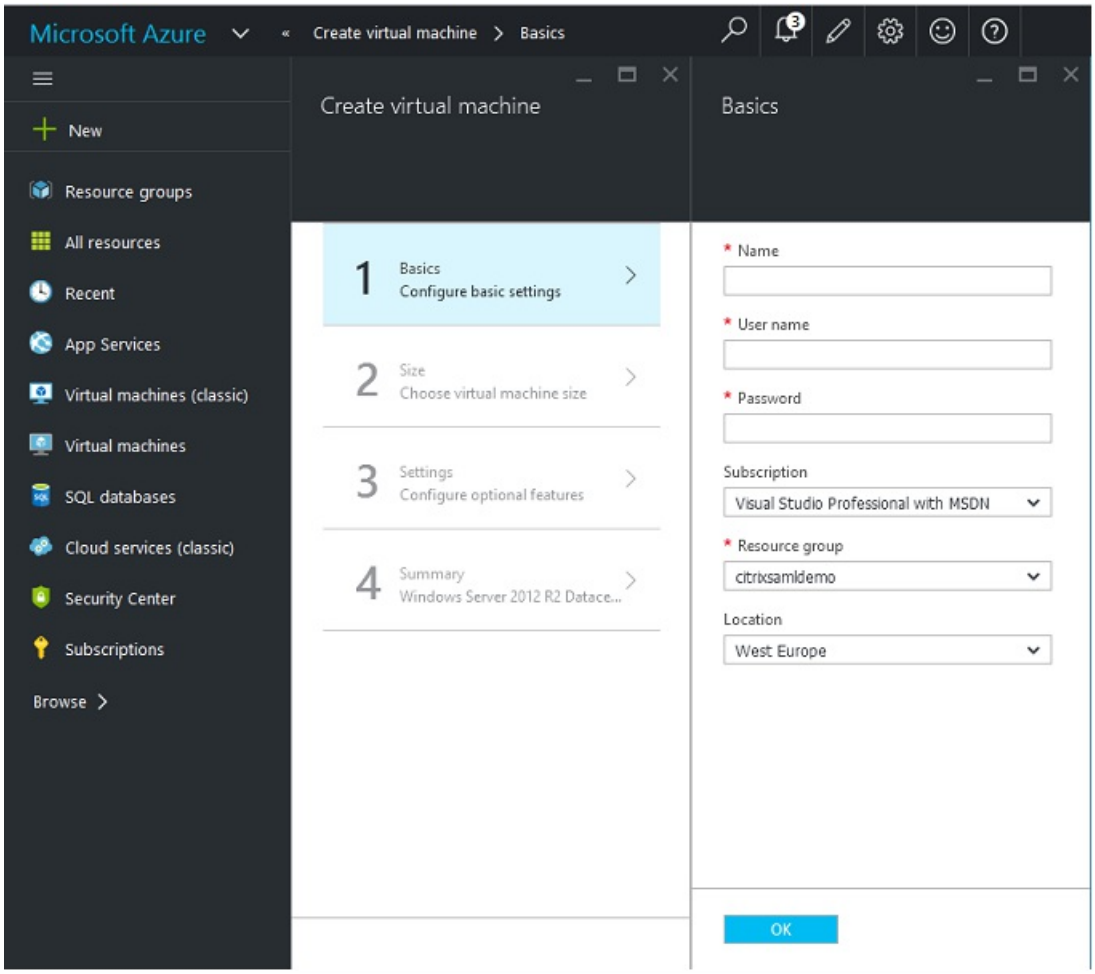
This example configures a Citrix environment, including an AD environment with an ADFS server running in Azure. A Cloud Service is created, named "citrixsamldemo."



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)
- 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.)

ADFS controller and Web Application Proxy server

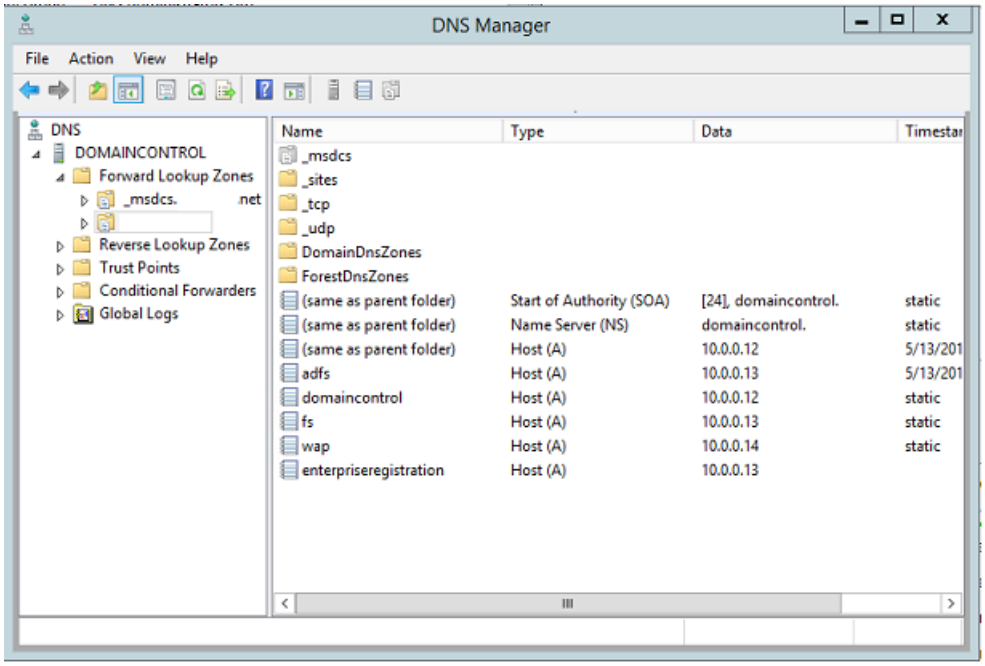
- Join the ADFS server to the citrixsamldemo domain. The Web Application Proxy server should remain in an isolated workgroup, so manually register a DNS address with the AD DNS.
- Run the **Enable-PSRemoting –Force** cmdlet on these servers, to allow PS remoting through firewalls from the AzureAD Connect 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

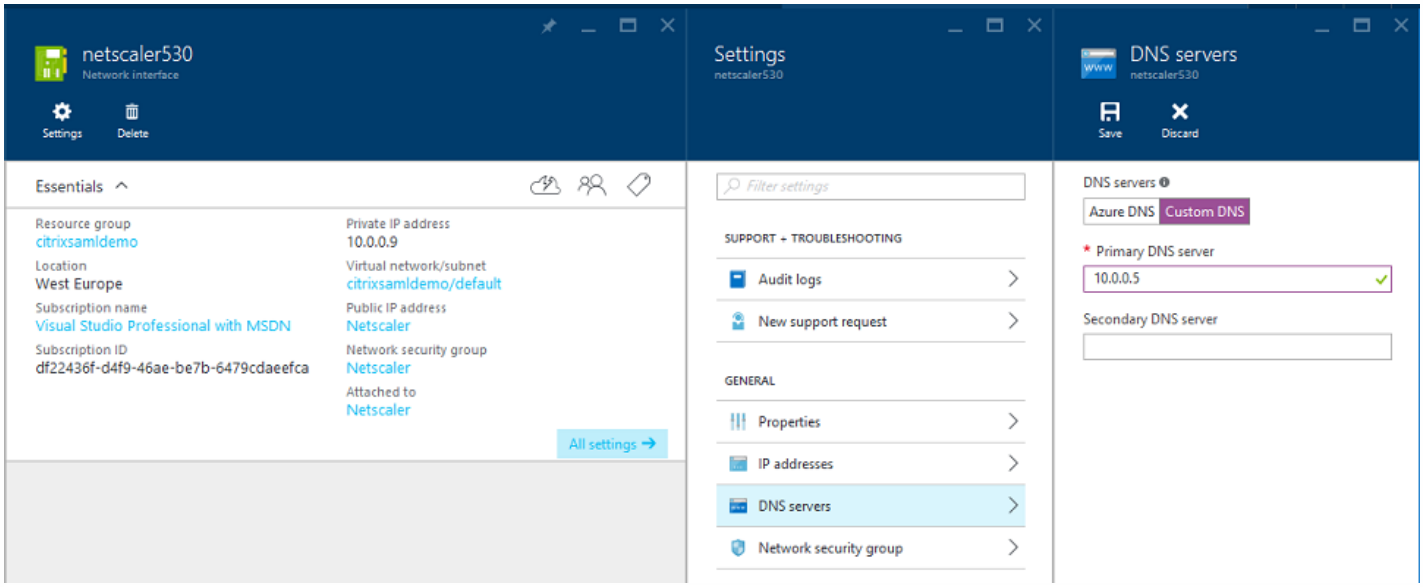
After the domain controller is installed, configure the DNS server to handle the internal view of citrixsamldemo.net, and act as a forwarder to an external DNS server (for example: 8.8.8.8).



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]
- enterpriseregistration.citrixsaml.net [same as fs.citrixsamldemo.net]

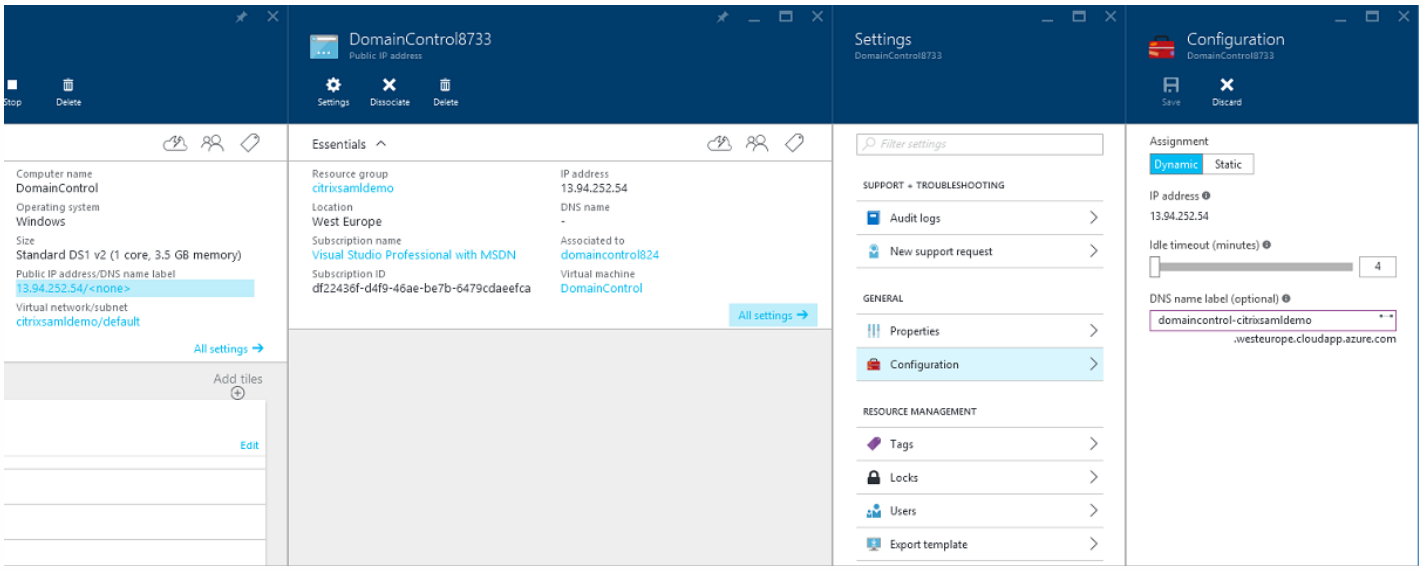
All VMs running in Azure should be configured to use only this DNS server. You can do this through the Network Interface GUI.



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.

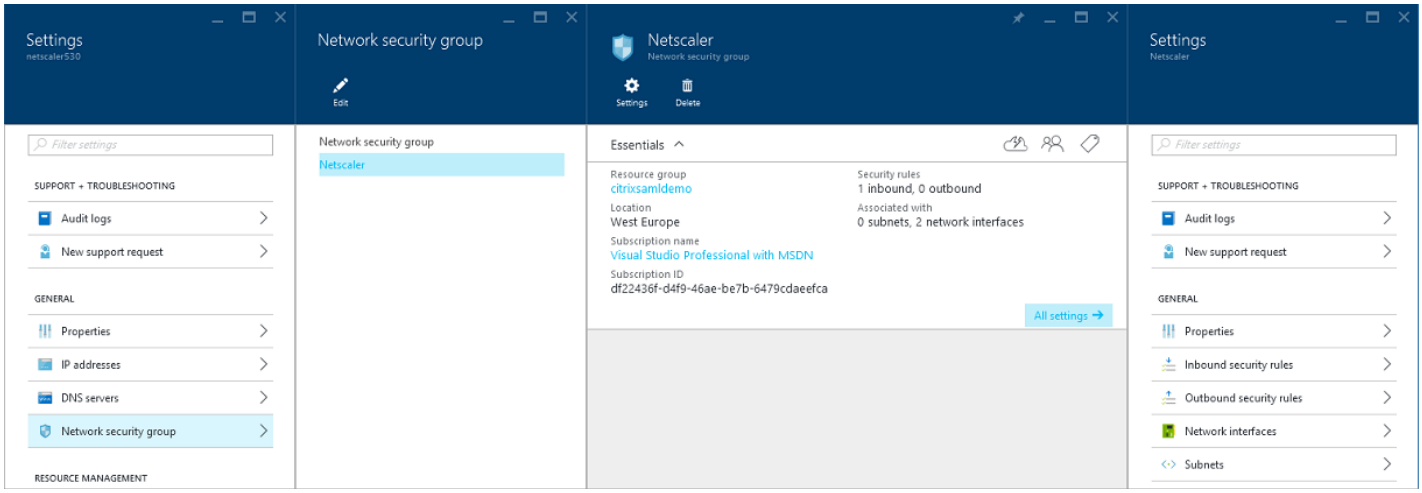


This example assigns a DNS address of domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com to the domain controller.

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.

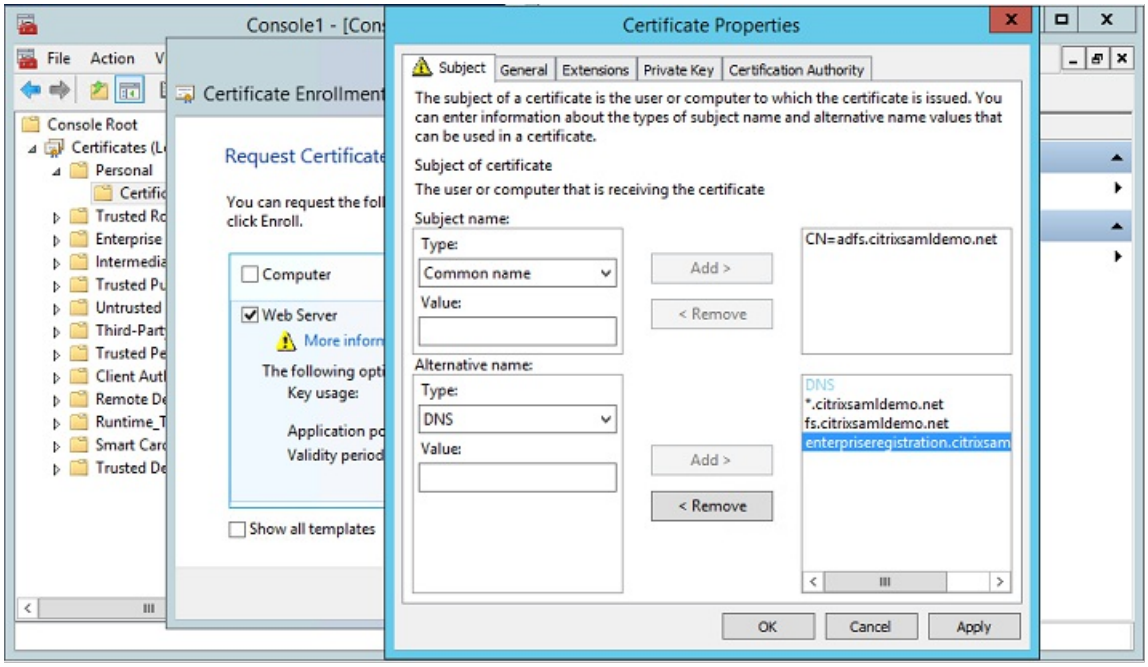


Create an ADFS certificate

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



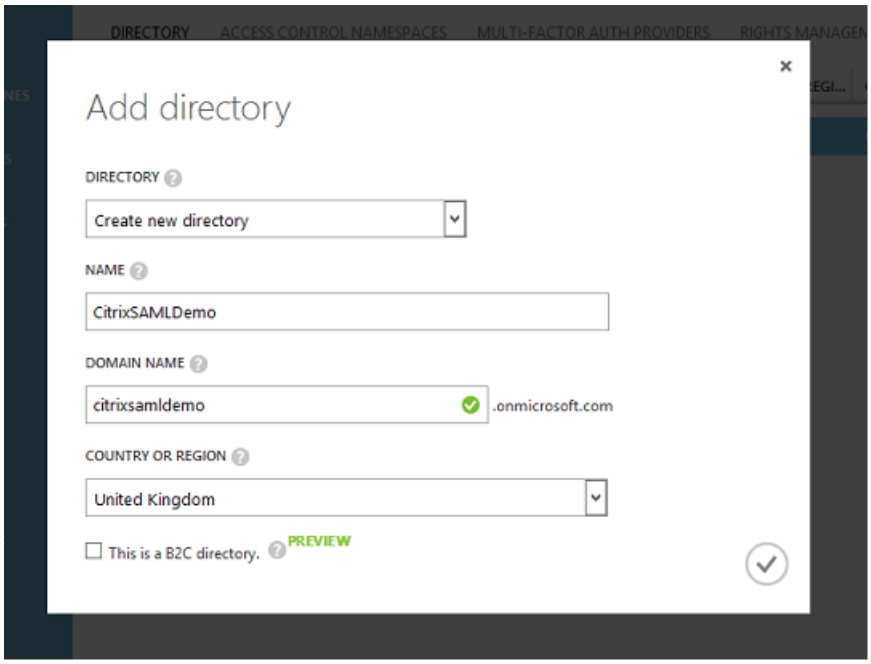
Export the certificate to a pfx file, including a password-protected private key.

Set up Azure AD

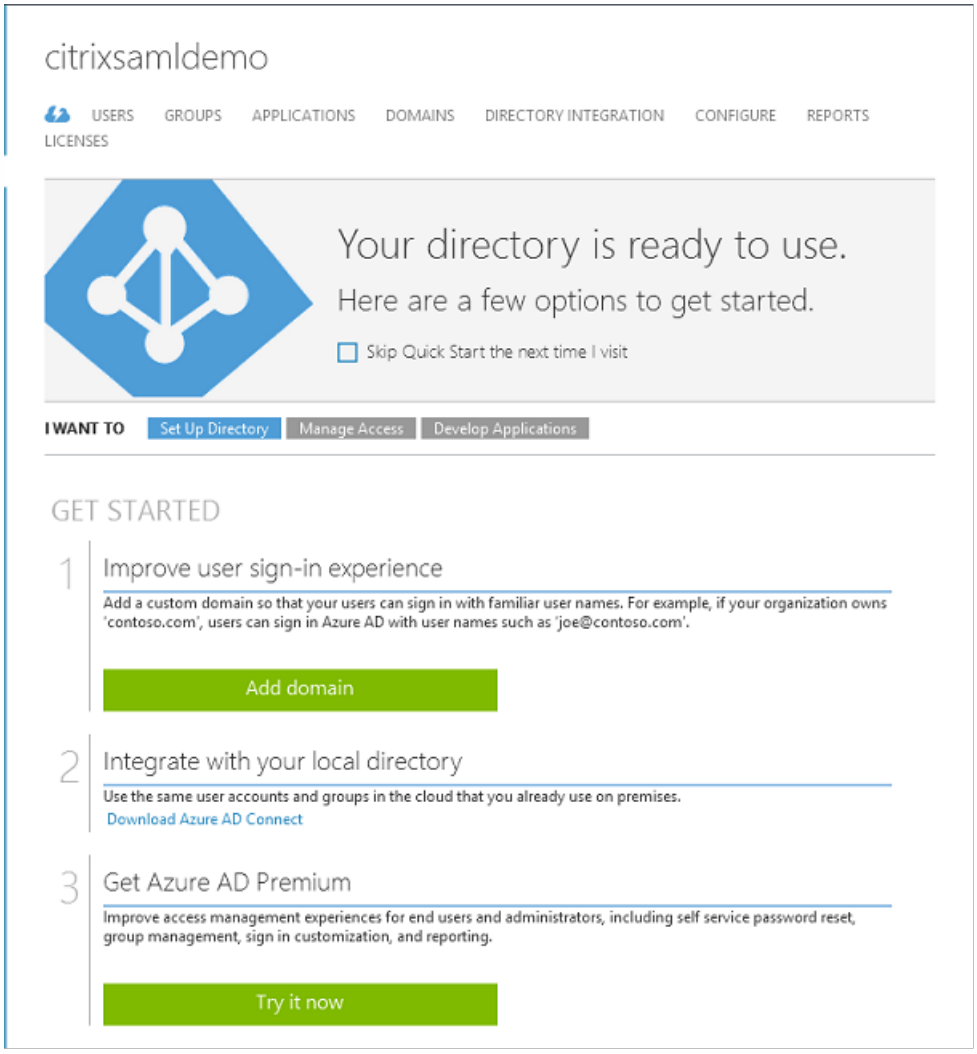
This section details the process of setting up a new Azure AD instance and creating user identities that can be used to join Windows 10 to Azure AD.

Create a new directory

Log on to the classic Azure portal and create a new directory.

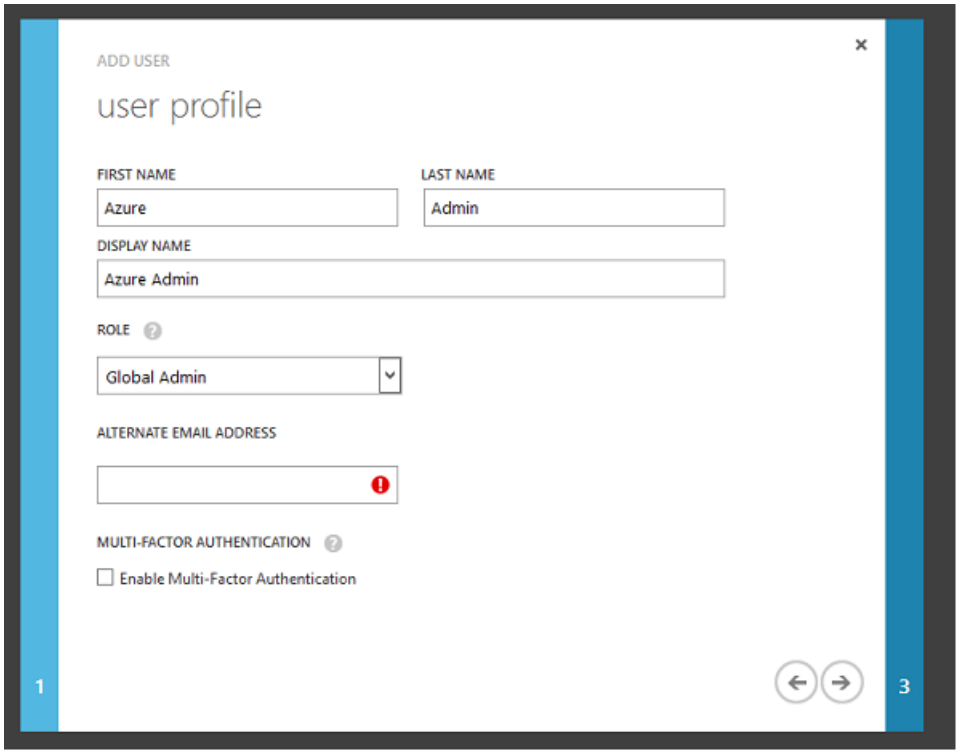


When complete, a summary page appears.



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.



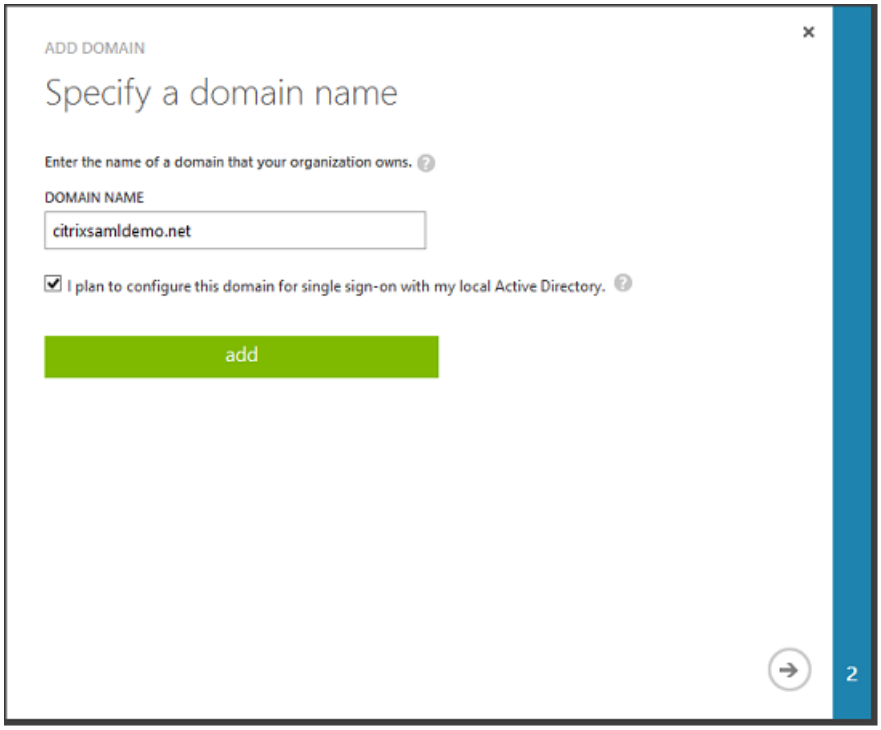
Register your domain with Azure AD

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

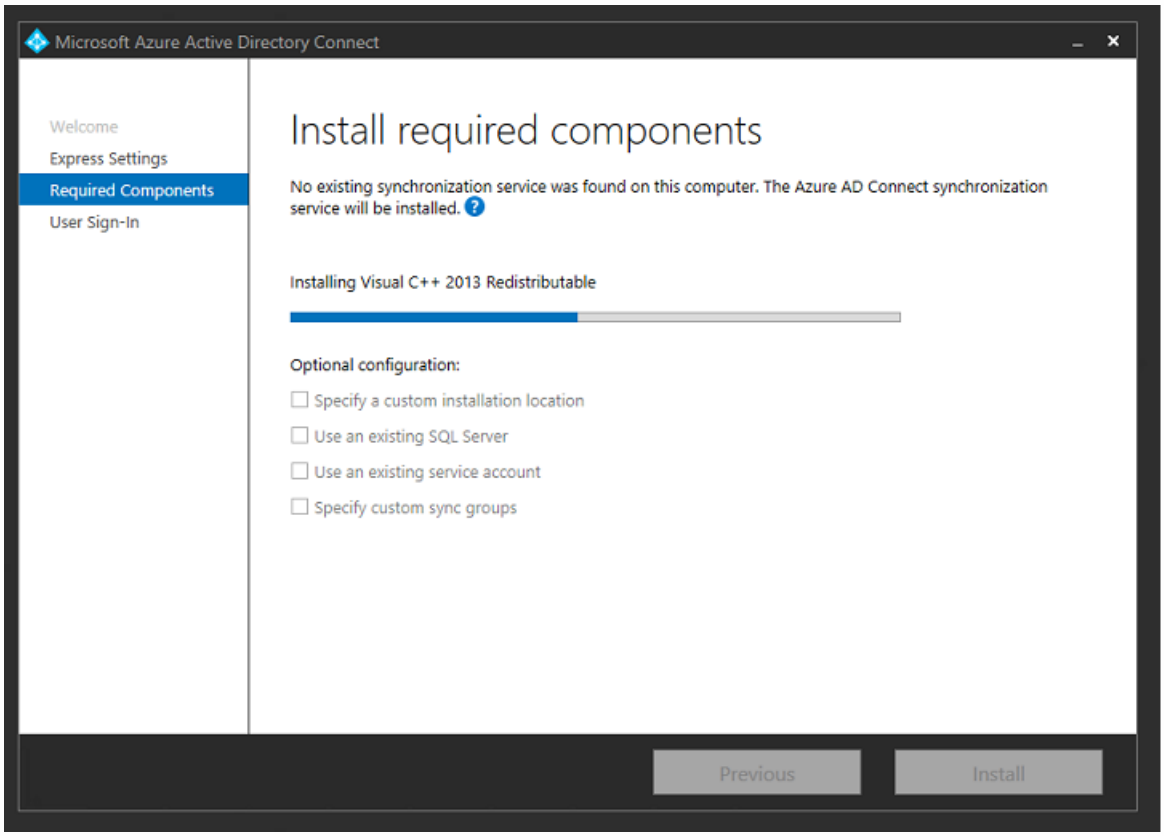
The **Add domain** action configures a redirect from your real company domain. The example uses citrixsamldemo.net.

If you are setting up ADFS for single sign-on, enable the check box.

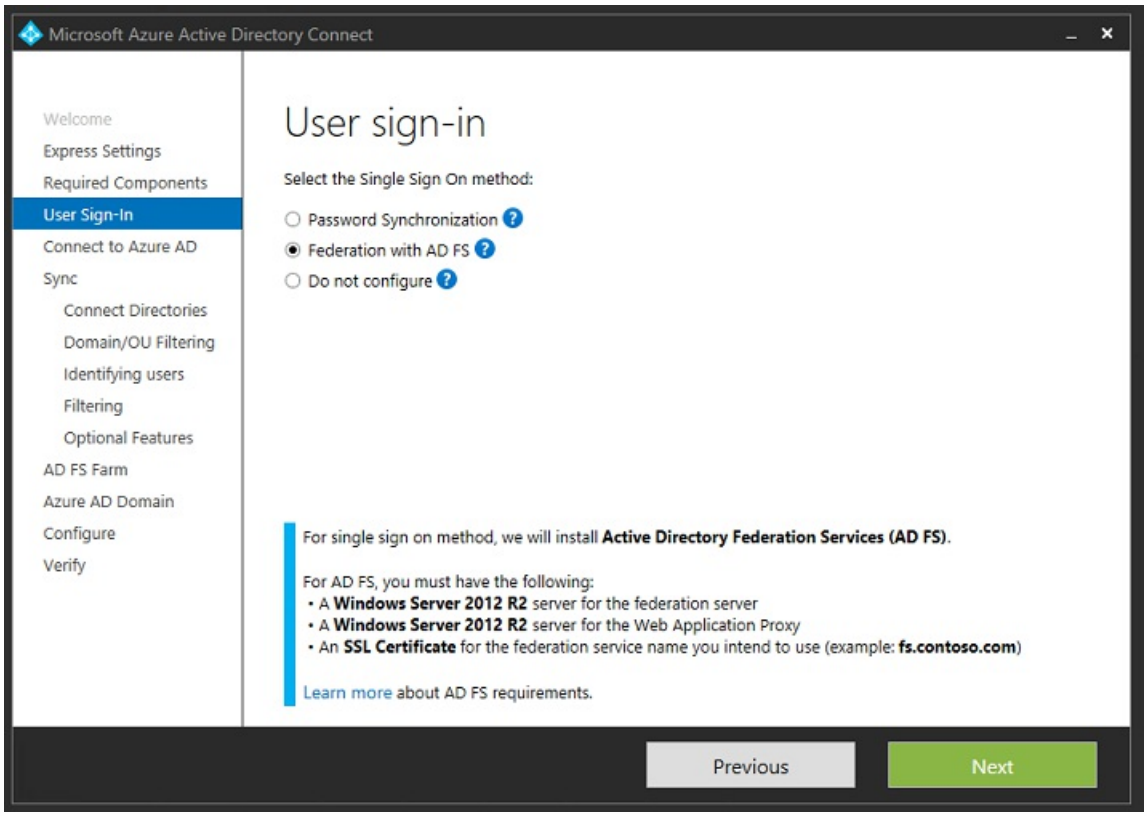


Install Azure AD Connect

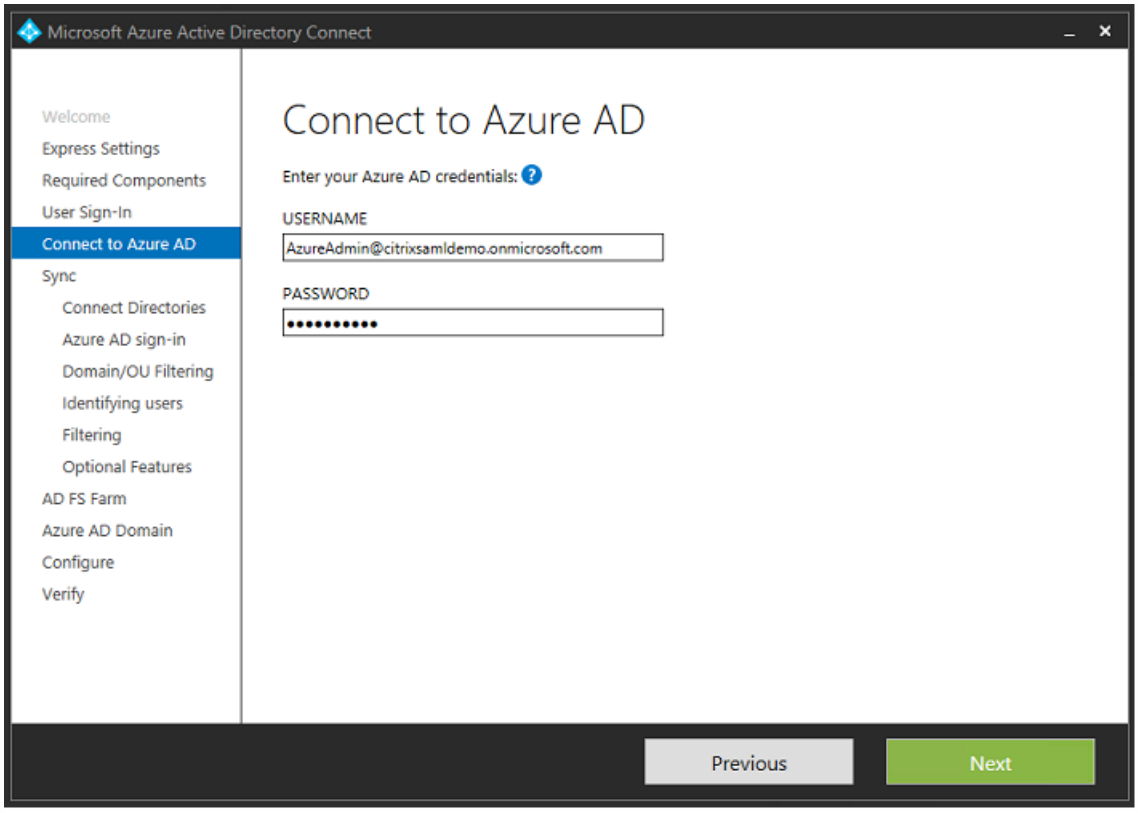
Step 2 of the Azure AD configuration GUI redirects to the Microsoft download page for Azure AD Connect. Install this on the ADFS VM. Use **Custom install**, rather than **Express Settings**, so that ADFS options are available.



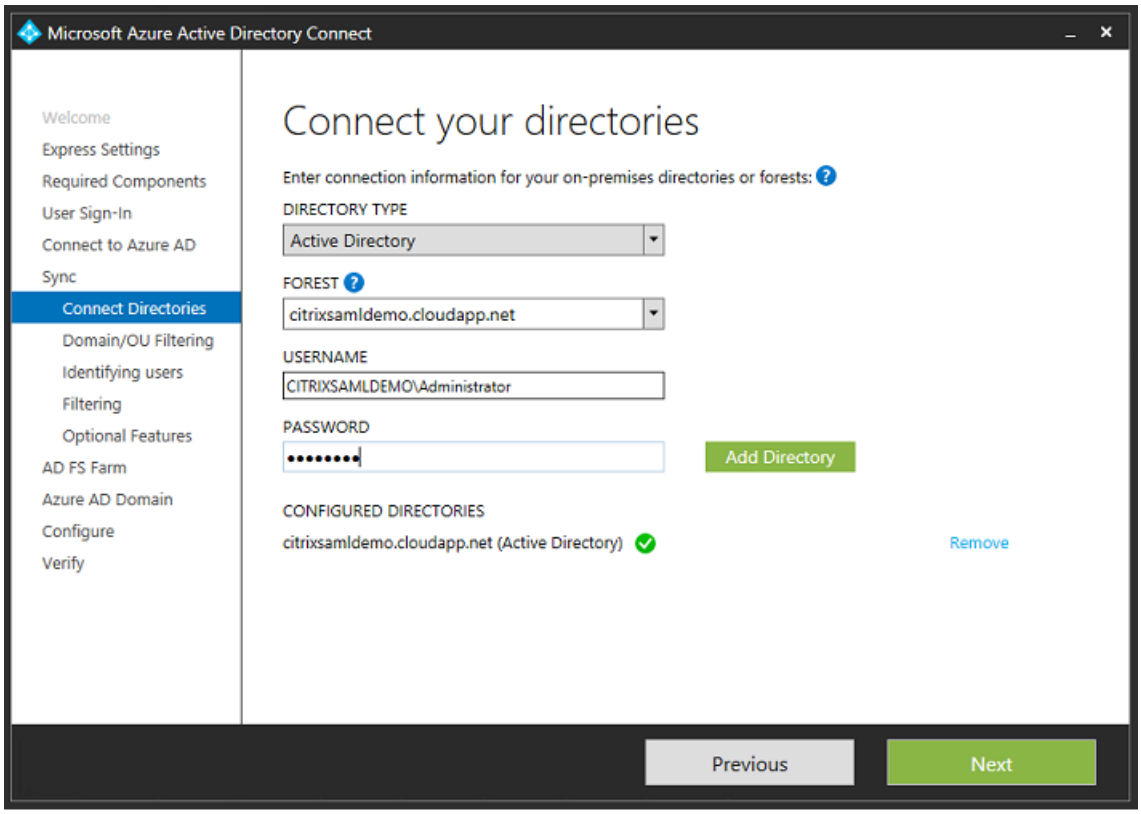
Select the **Federation with AD FS** Single sign-On option.



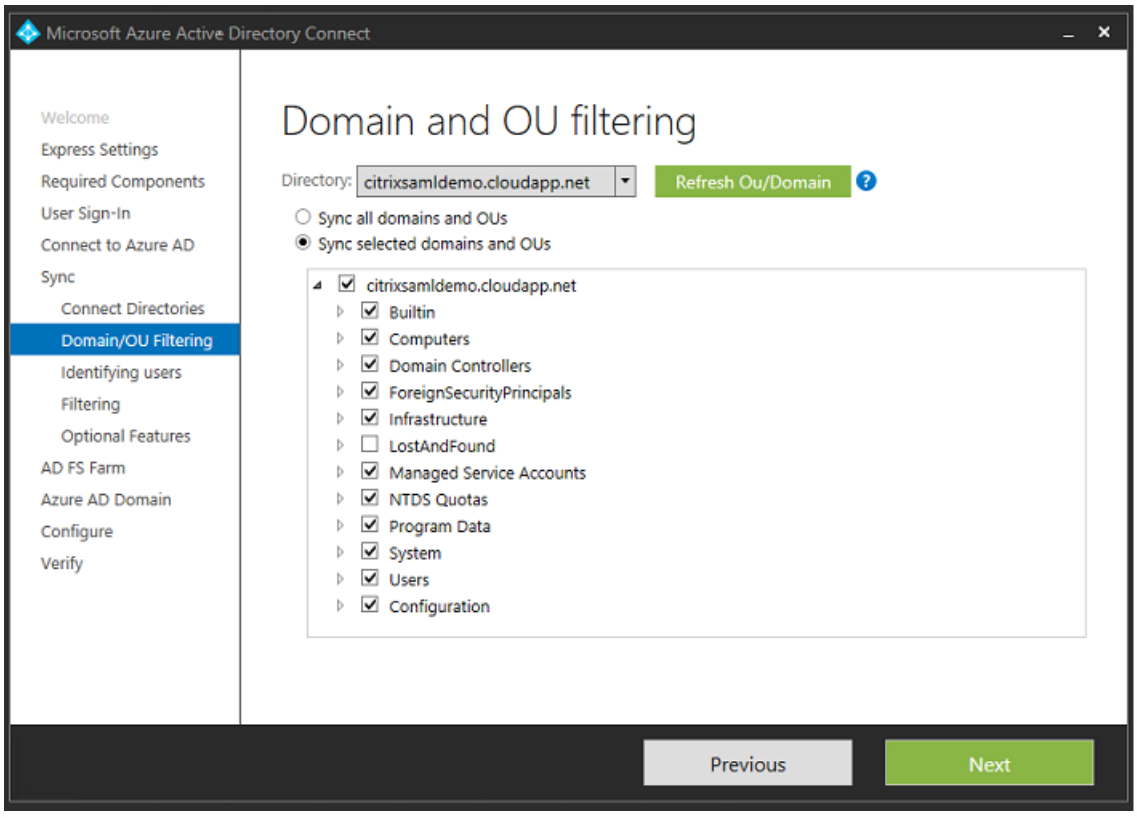
Connect to Azure with the administrator account you created earlier.



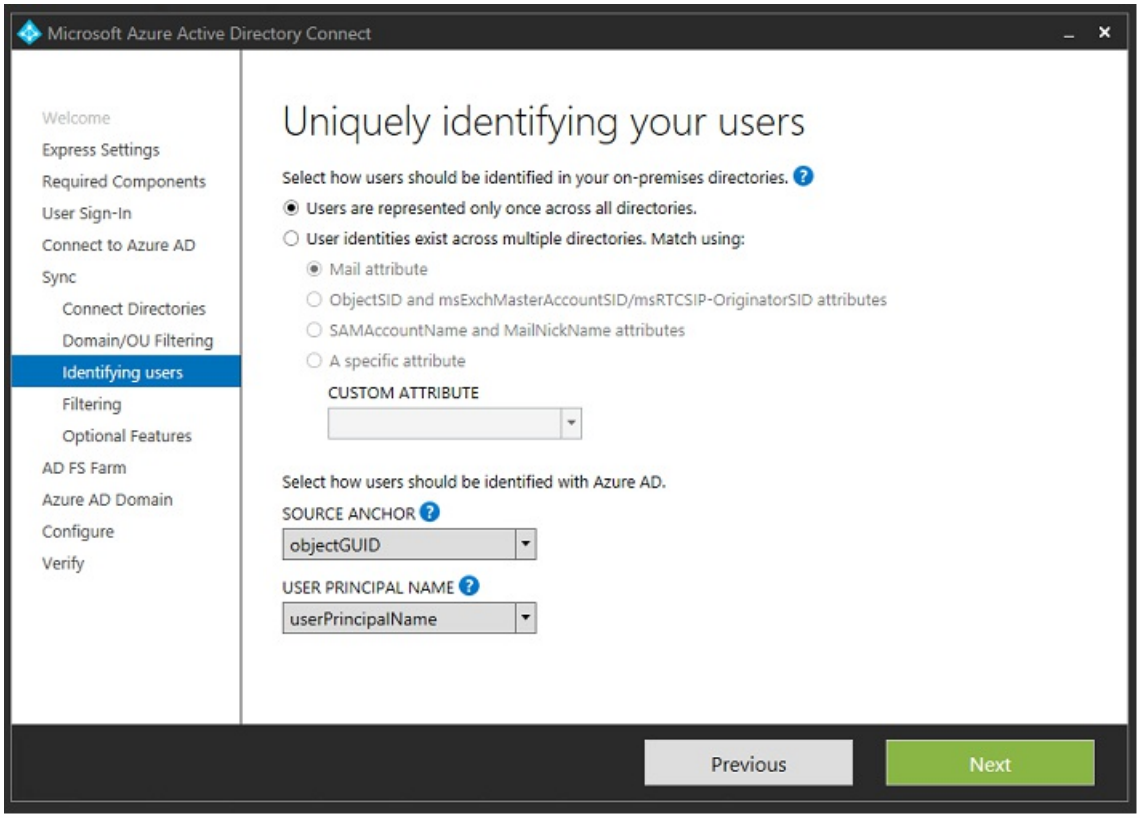
Select the internal AD forest.



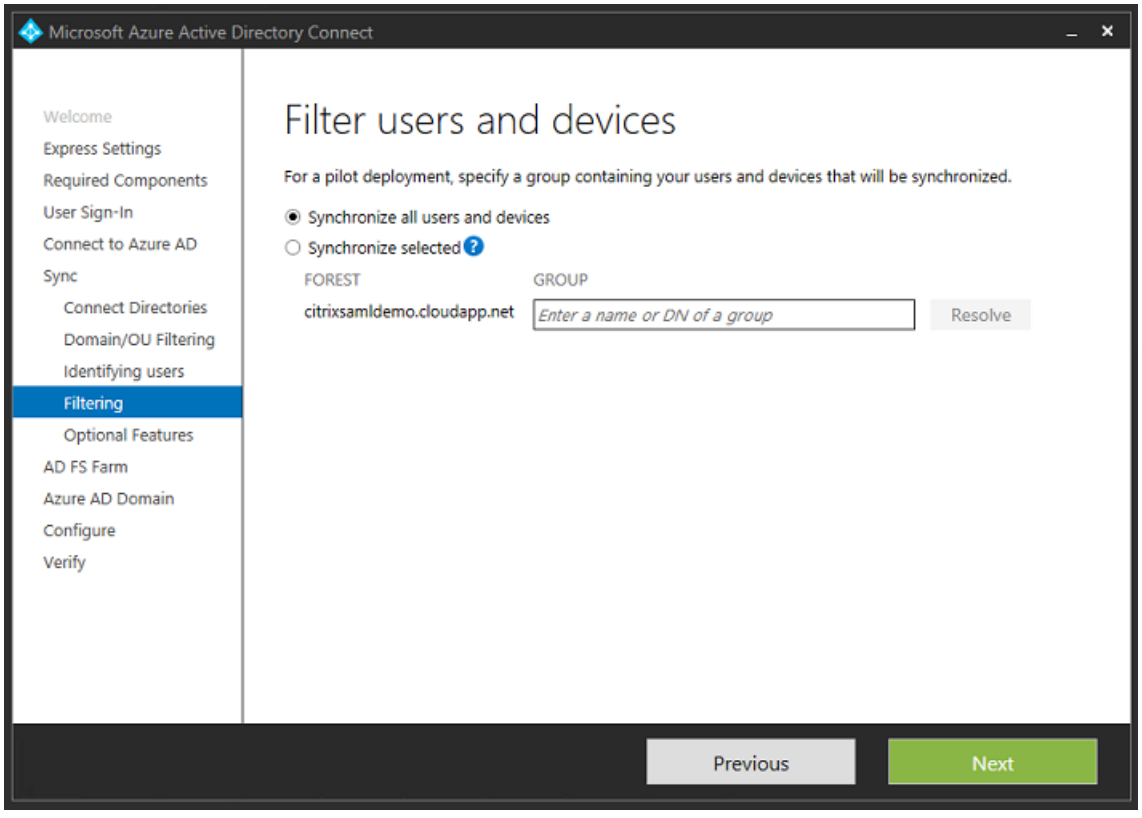
Synchronize all legacy Active Directory objects with Azure AD.



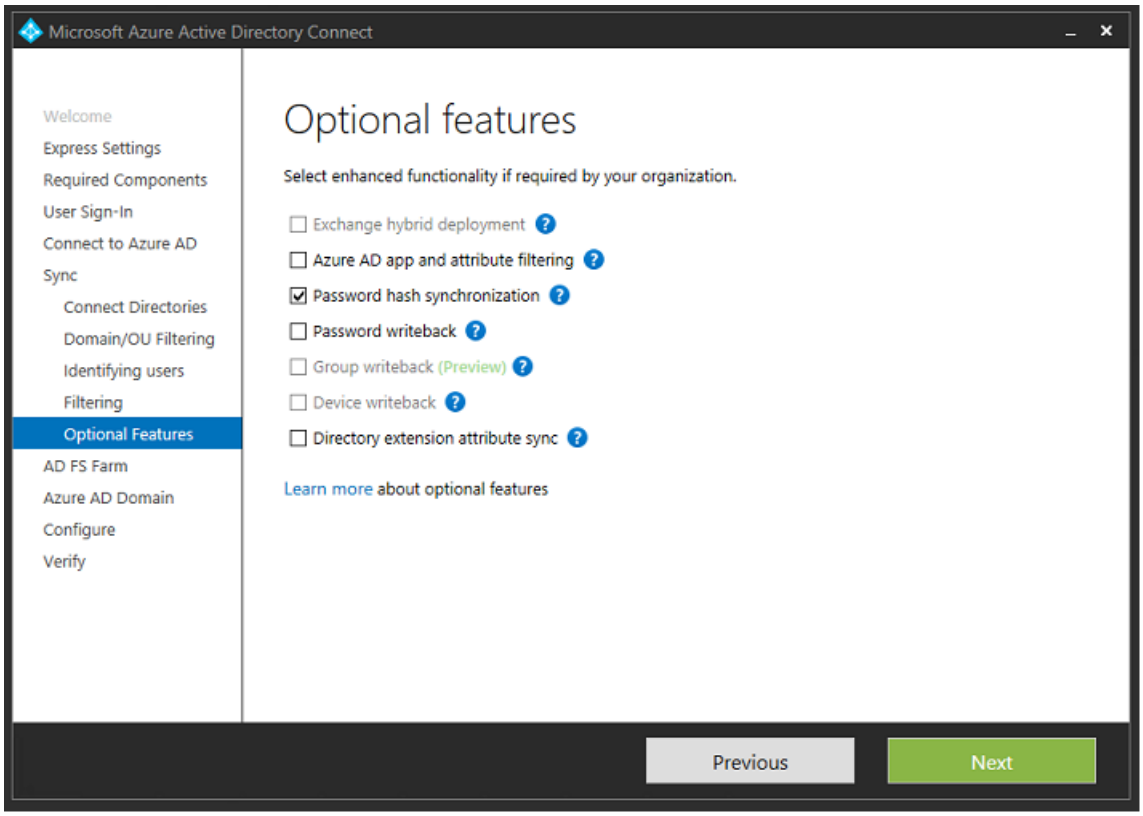
If the directory structure is simple, you can rely on the usernames being sufficiently unique to identify a user who logs on.



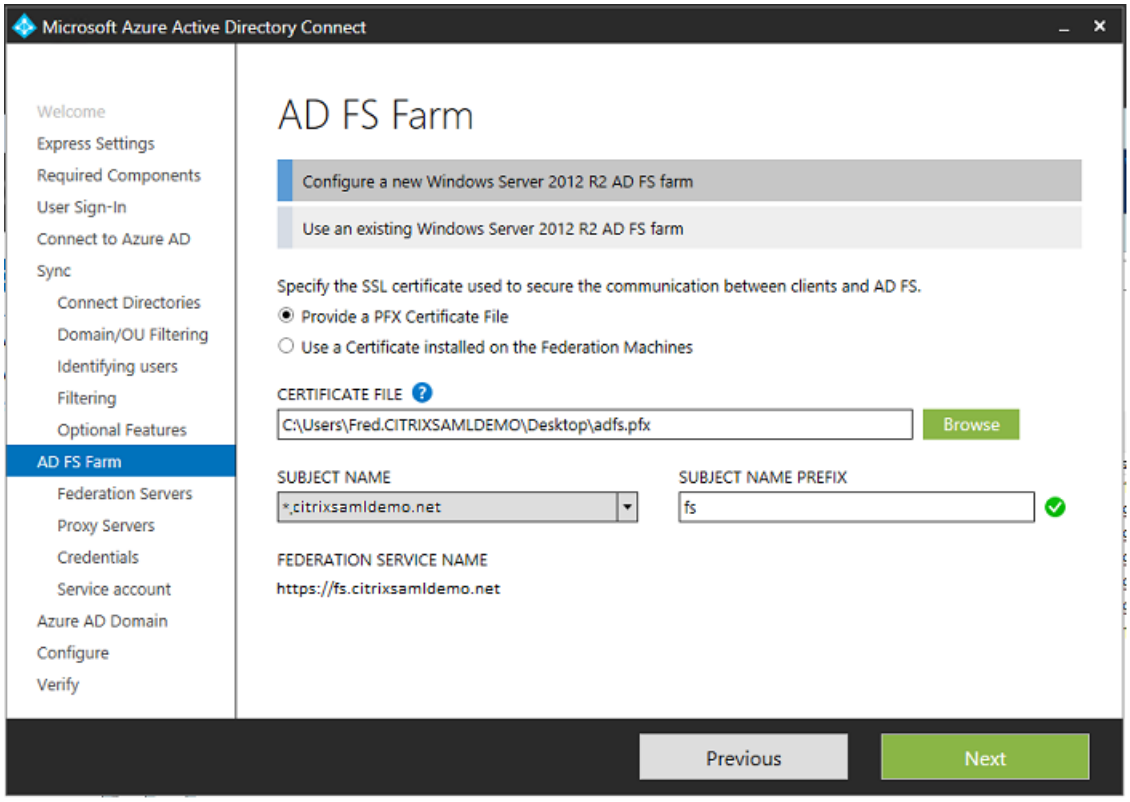
Accept the default filtering options, or restrict users and devices to a particular set of groups.



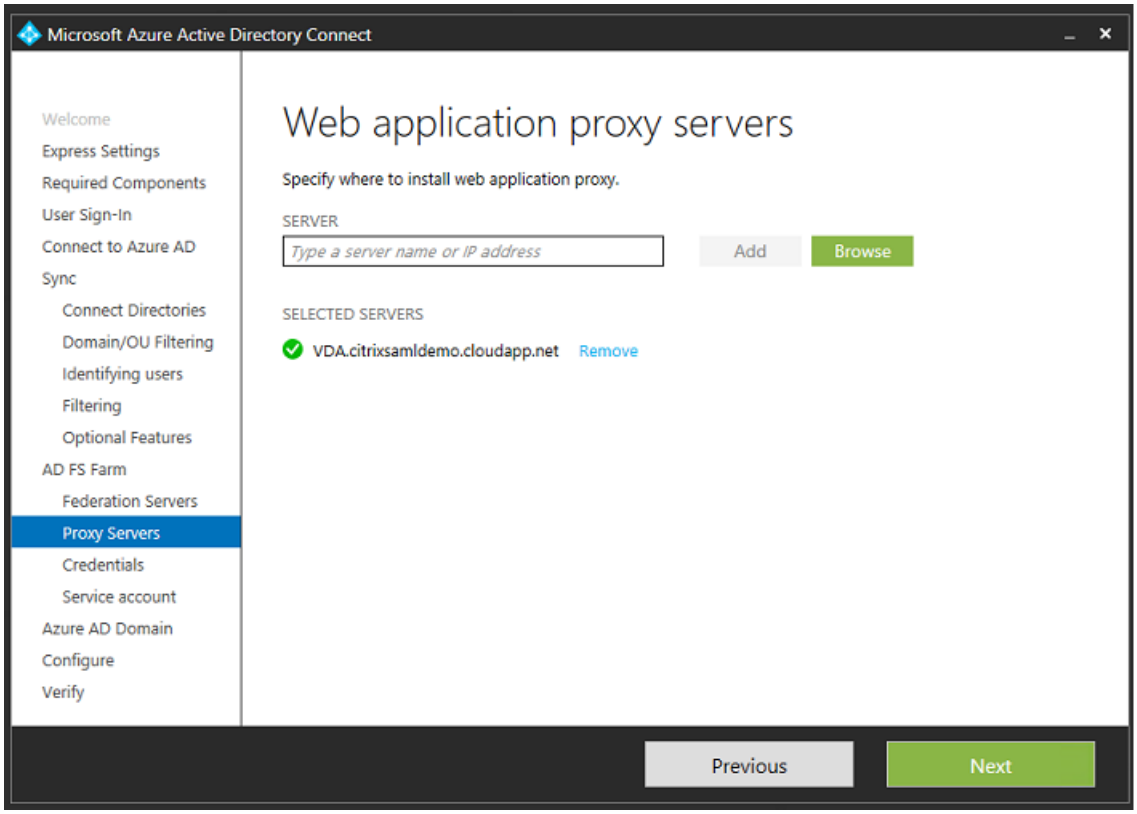
If desired, you can synchronize the Azure AD passwords with Active Directory. This is usually not required for ADFS-based authentication.



Select the certificate PFX file to use in AD FS, specifying fs.citrixsamldemo.net as the DNS name.

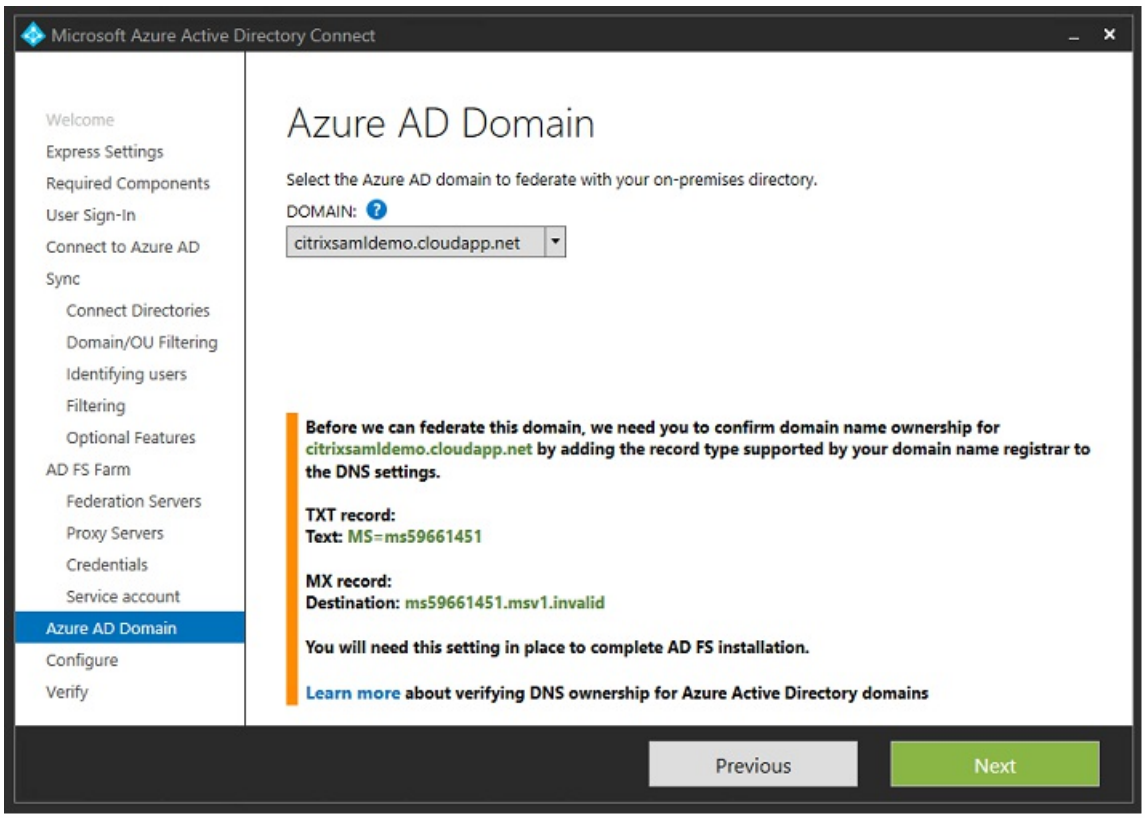


When prompted to select a proxy server, enter the address of the wap.citrixsamldemo.net server. You may need to run the **Enable-PSRemoting –Force** cmdlet as an administrator on the Web Application Proxy server, so that Azure AD Connect can configure it.

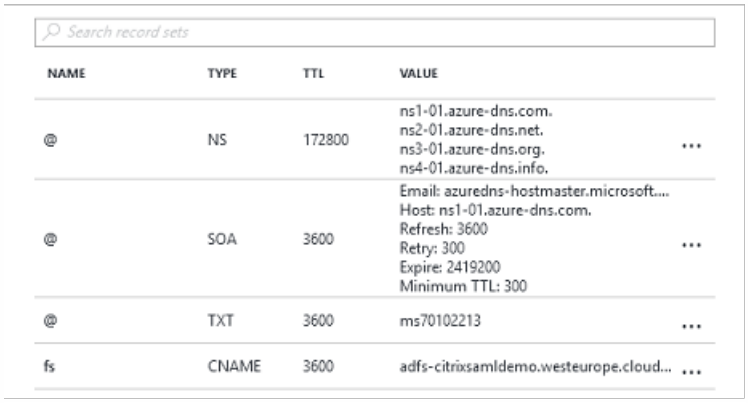


Note: If this step fails due to Remote PowerShell trust problems, try joining the Web Application Proxy server to the domain.

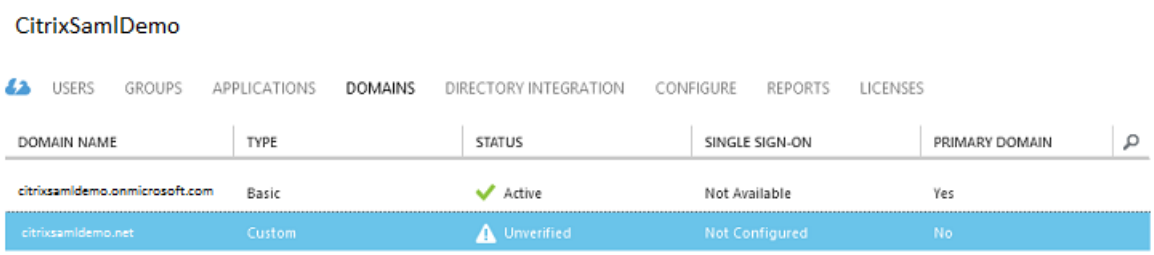
For the remaining steps of the wizard, use the standard administrator passwords, and create a service account for ADFS. Azure AD Connect will then prompt to validate the ownership of the DNS zone.



Add the TXT and MX records to the DNS address records in Azure.

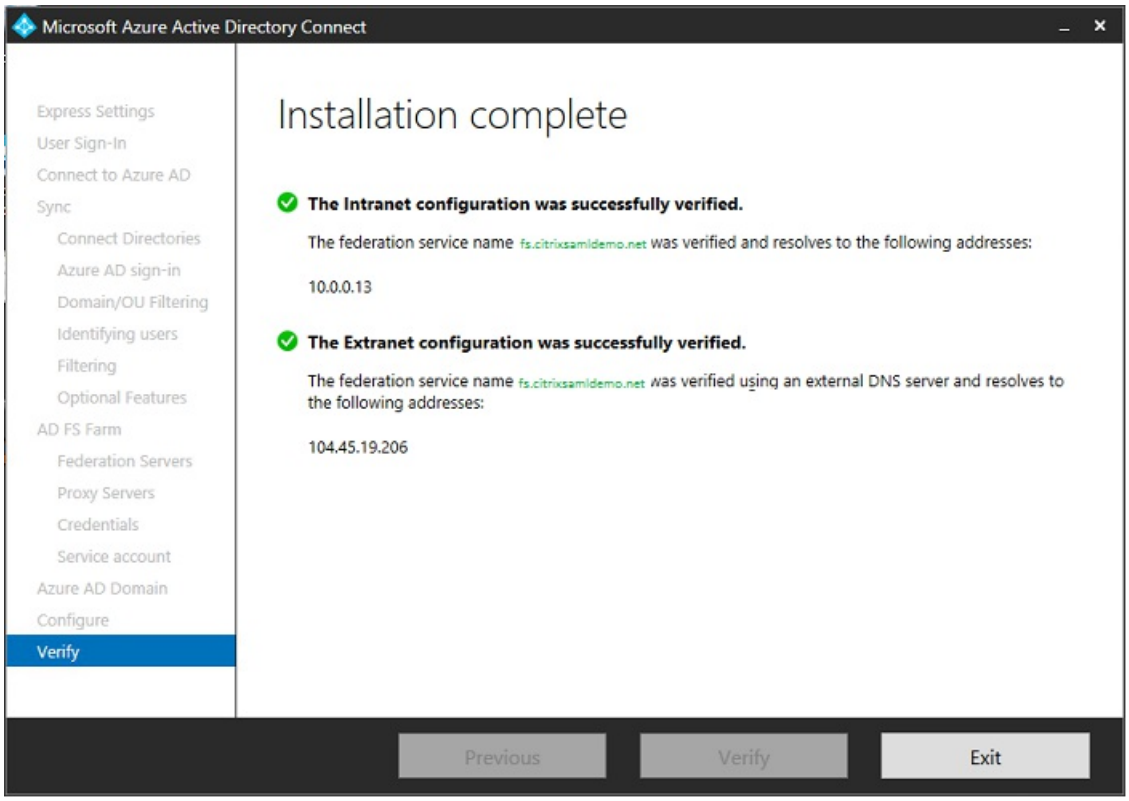


Click **Verify** in the Azure Management Console.



Note: If this step fails, you can verify the domain before running Azure AD Connect.

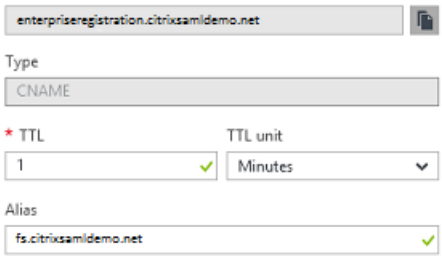
When complete, the external address fs.citrixsamldemo.net is contacted over port 443.



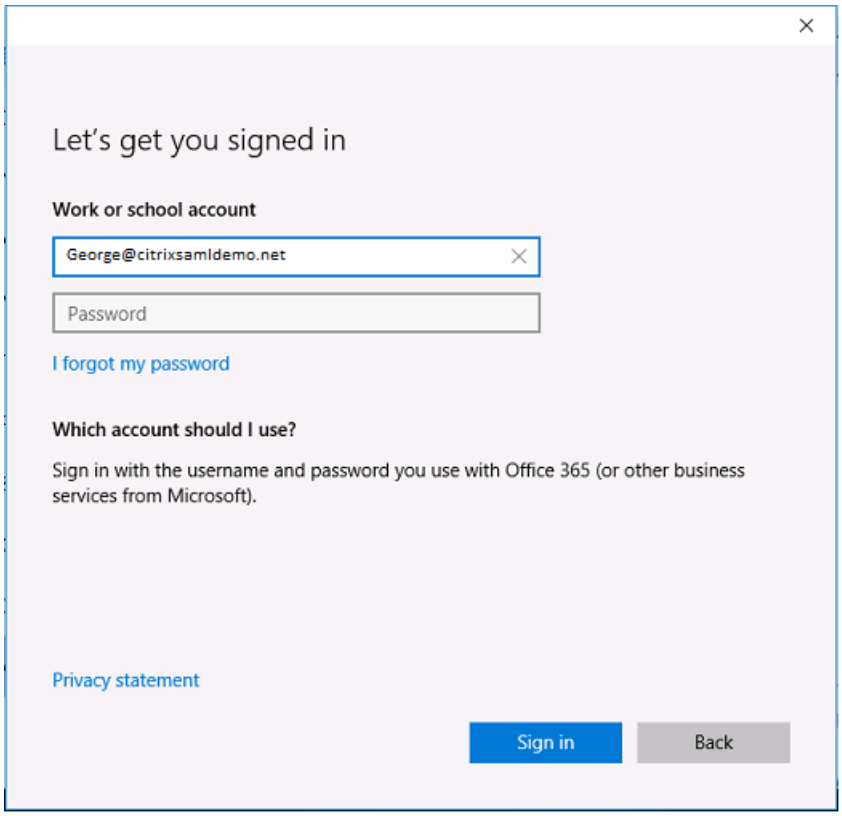
Enable Azure AD Join

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>.

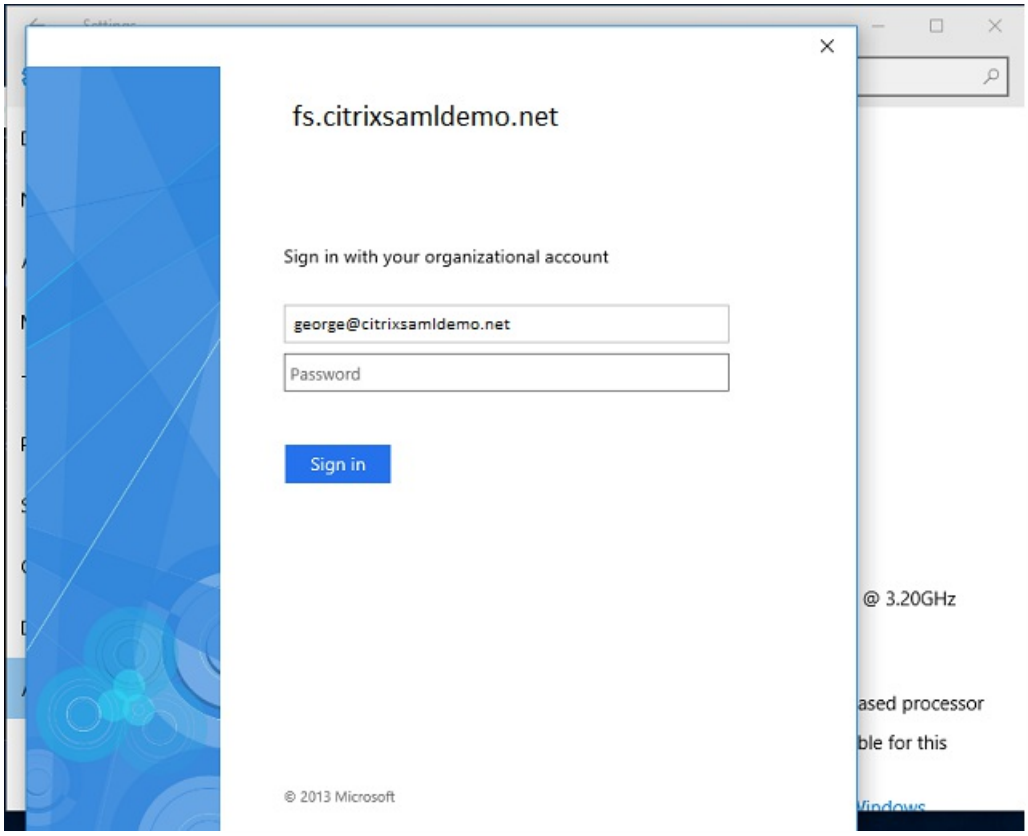
In the example, this is fs.citrixsamldemo.net.

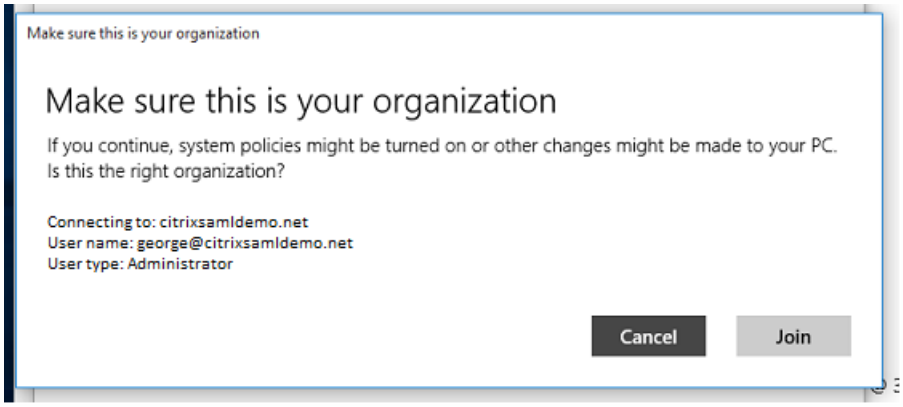


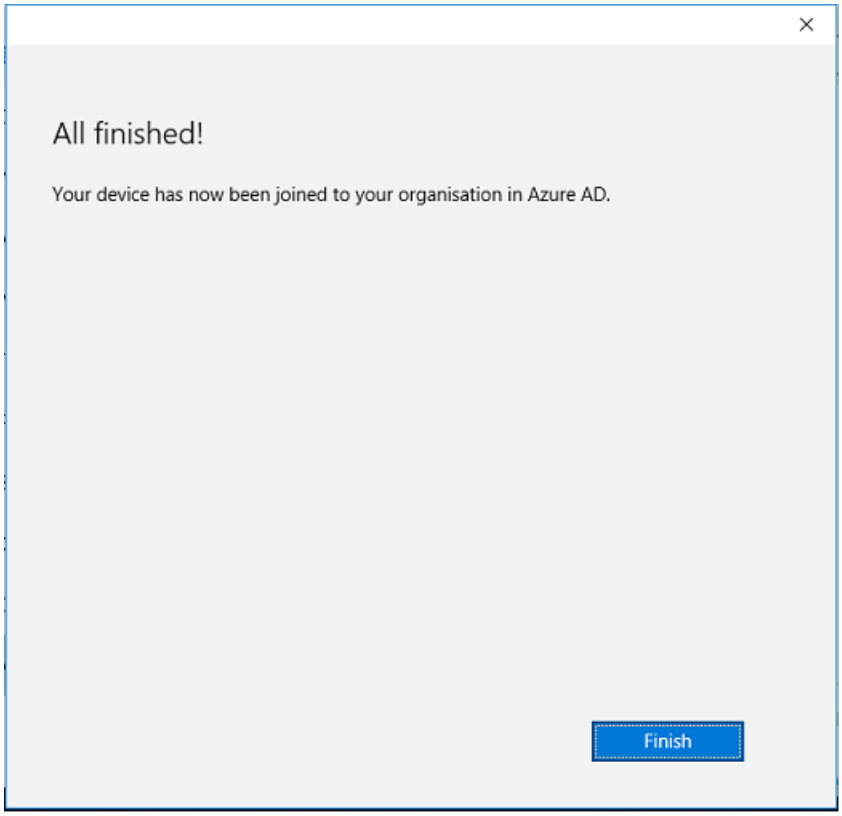
If you are not using a public CA, ensure that the ADFS root certificate is installed on the Windows 10 computer so that Windows trusts the ADFS server. Perform an Azure AD domain join using the standard user account generated earlier.



Note that the UPN must match the UPN recognized by the ADFS domain controller.





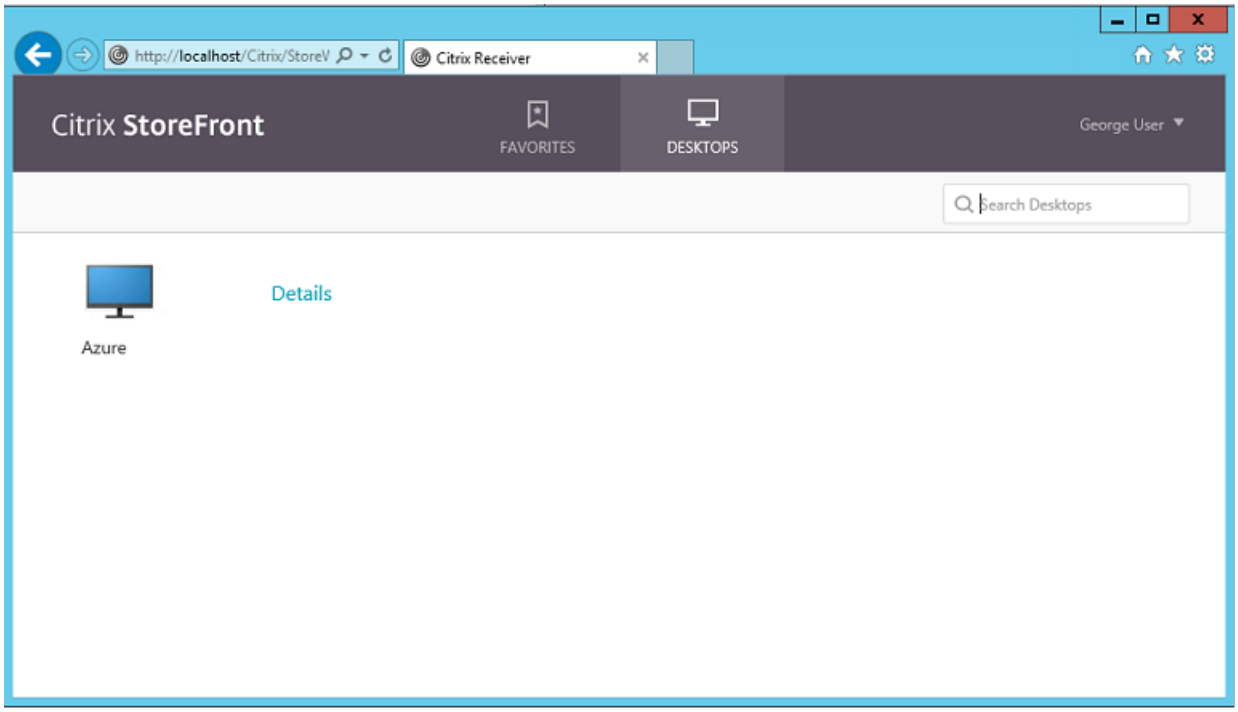


Verify that the Azure AD join was successful by restarting the machine and logging on, using the user's email address. When logged on, launch Microsoft Edge and connect to http://myapps.microsoft.com. The web site should use single sign-on automatically.

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.

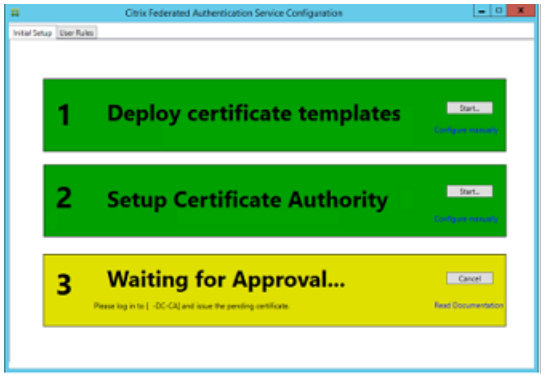
In this example, StoreFront is installed on the same server as the Delivery Controller. The VDA is installed as a standalone Windows 2012 R2 RDS worker, without integrating with Machine Creation Services (although that can optionally be configured). Check that the user George@citrixsamldemo.net can authenticate with a password, before continuing.

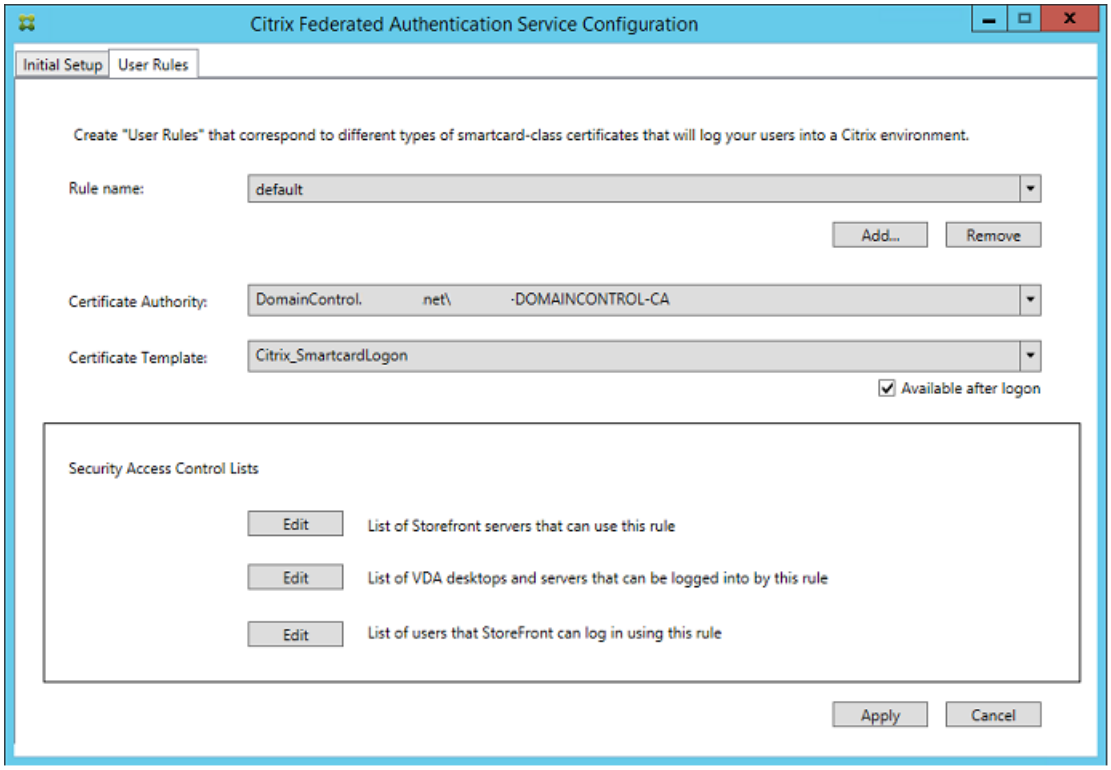


Run the **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet on the Controller to allow StoreFront to authenticate without the users' credentials.

Install the Federated Authentication Service

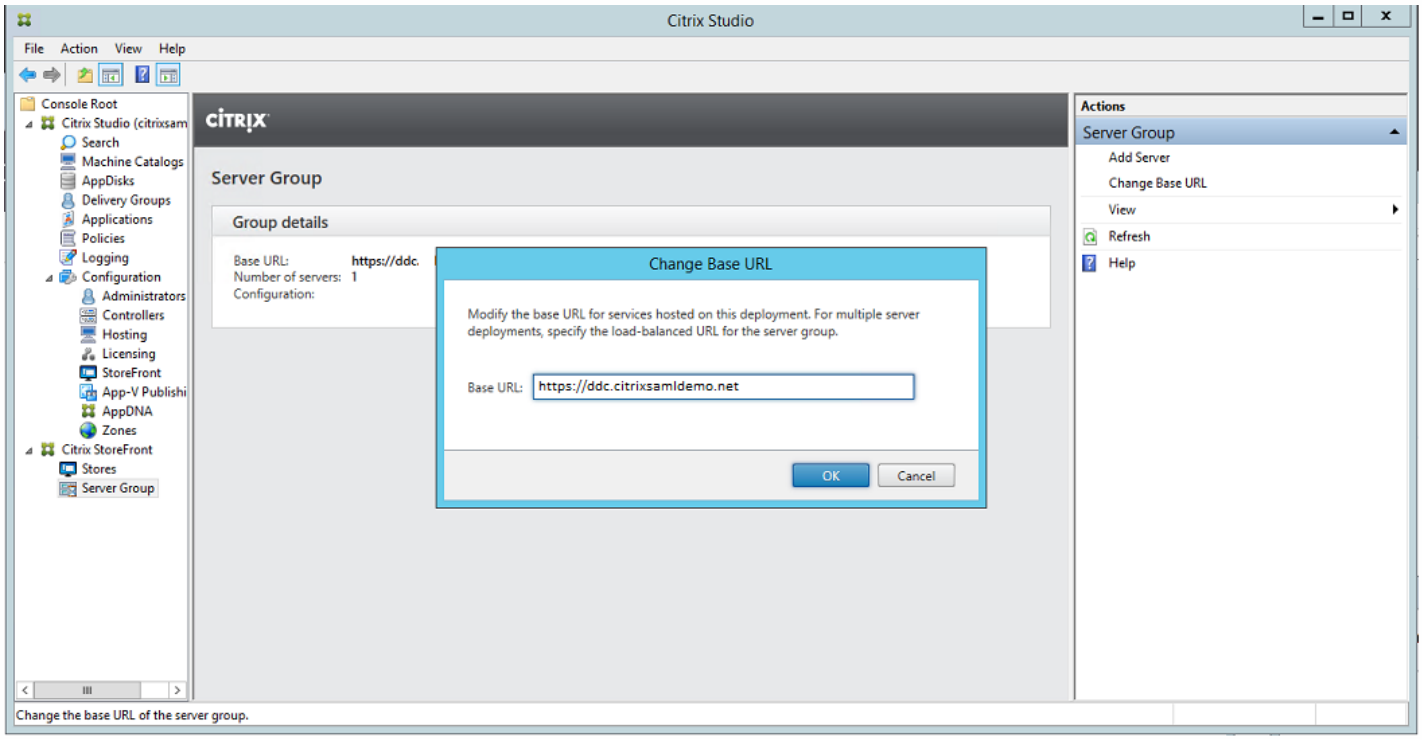
Install the Federated Authentication Service (FAS) component on the ADFS server and configure a rule for the Controller to act as a trusted StoreFront.





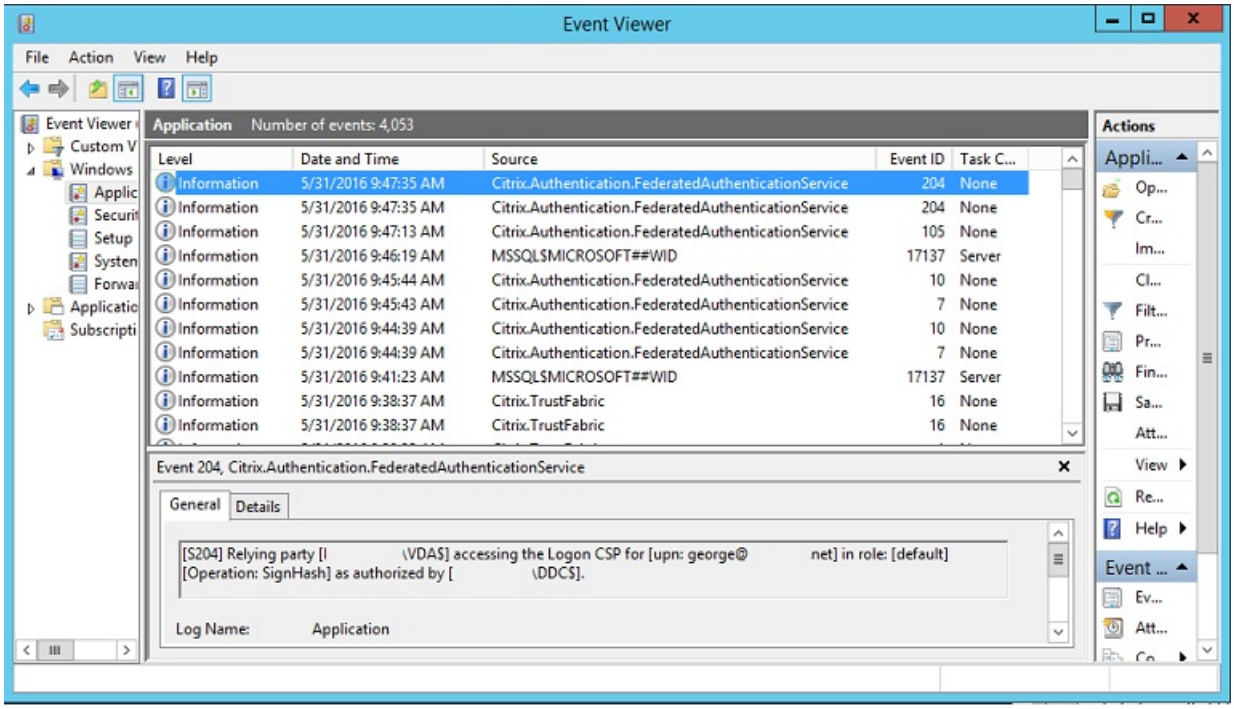
Configure StoreFront

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:.



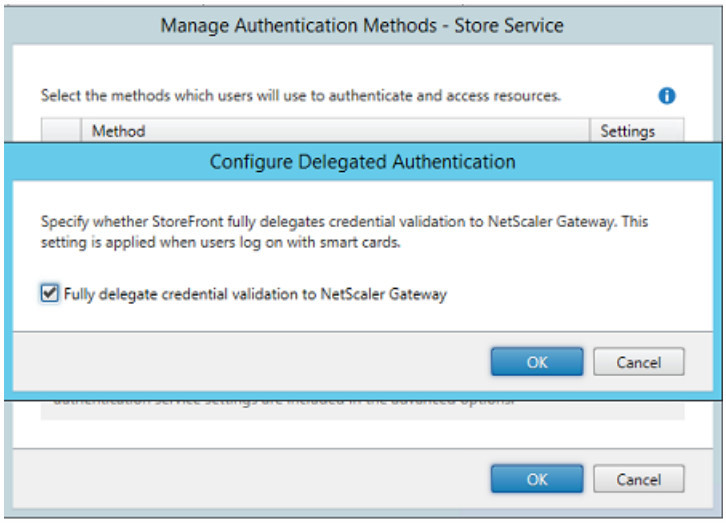
Configure StoreFront to use the FAS server (use the PowerShell script in the Federated Authentication Service article), and

test internally within Azure, ensuring that the logon uses the FAS by checking the event viewer on the FAS server.

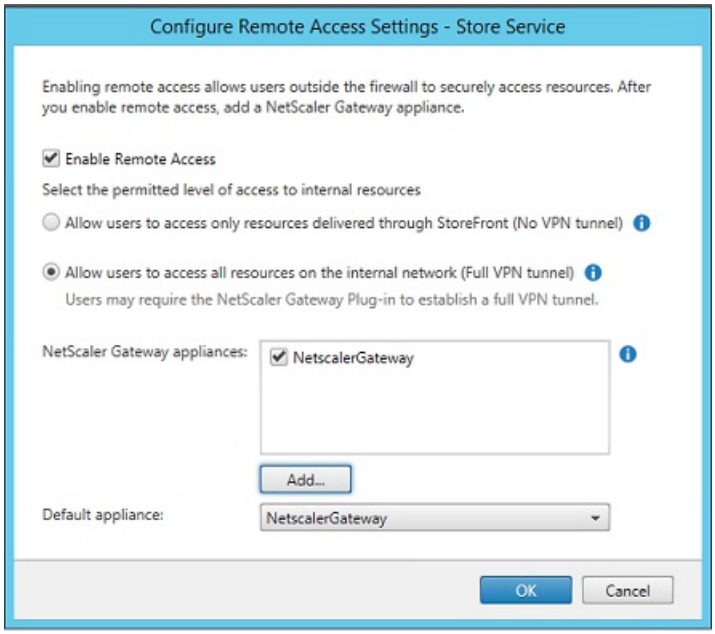


Configure StoreFront to use NetScaler

Using the **Manage Authentication Methods** GUI in the StoreFront management console, configure StoreFront to use NetScaler to perform authentication.

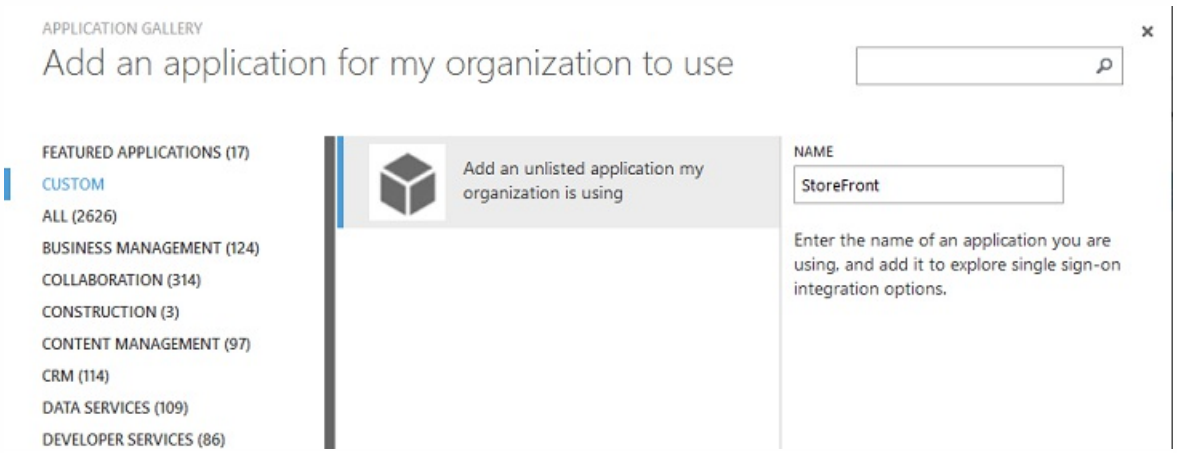


To integrate NetScaler authentication options, configure a Secure Ticket Authority (STA) and configure the NetScaler Gateway address.



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**.



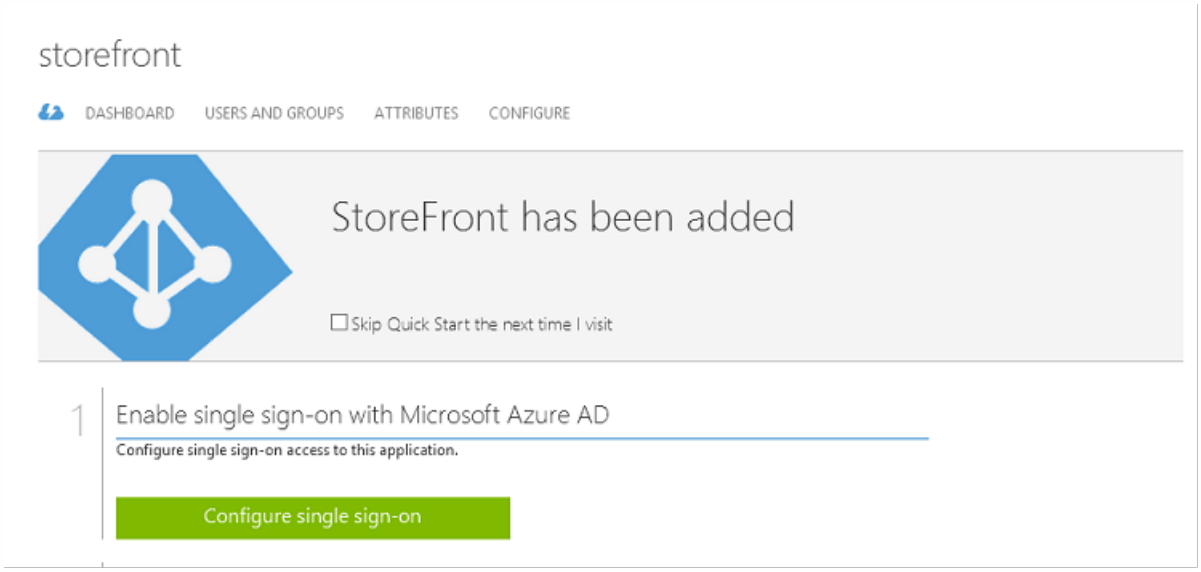
Select **CUSTOM > Add an unlisted application my organization is using** to create a new custom application for your users.

Configure an icon

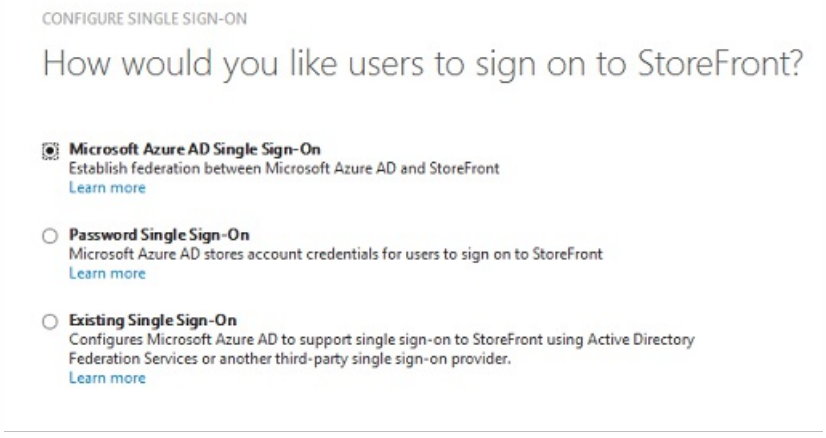
Create an image 215 by 215 pixels in size and upload it on the CONFIGURE page to use as an icon for the application.

Configure SAML authentication

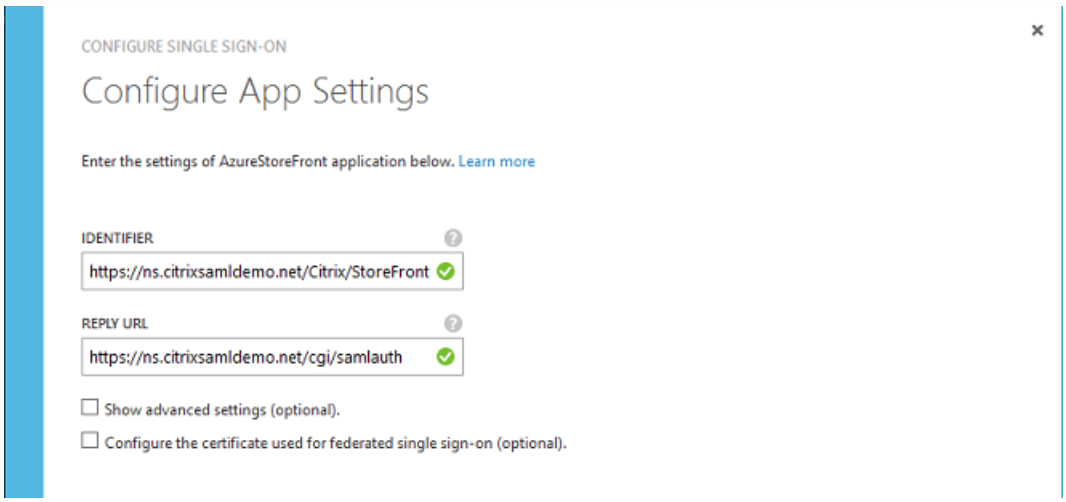
Return to the Application dashboard overview page and select **Configure Single sign-on**.



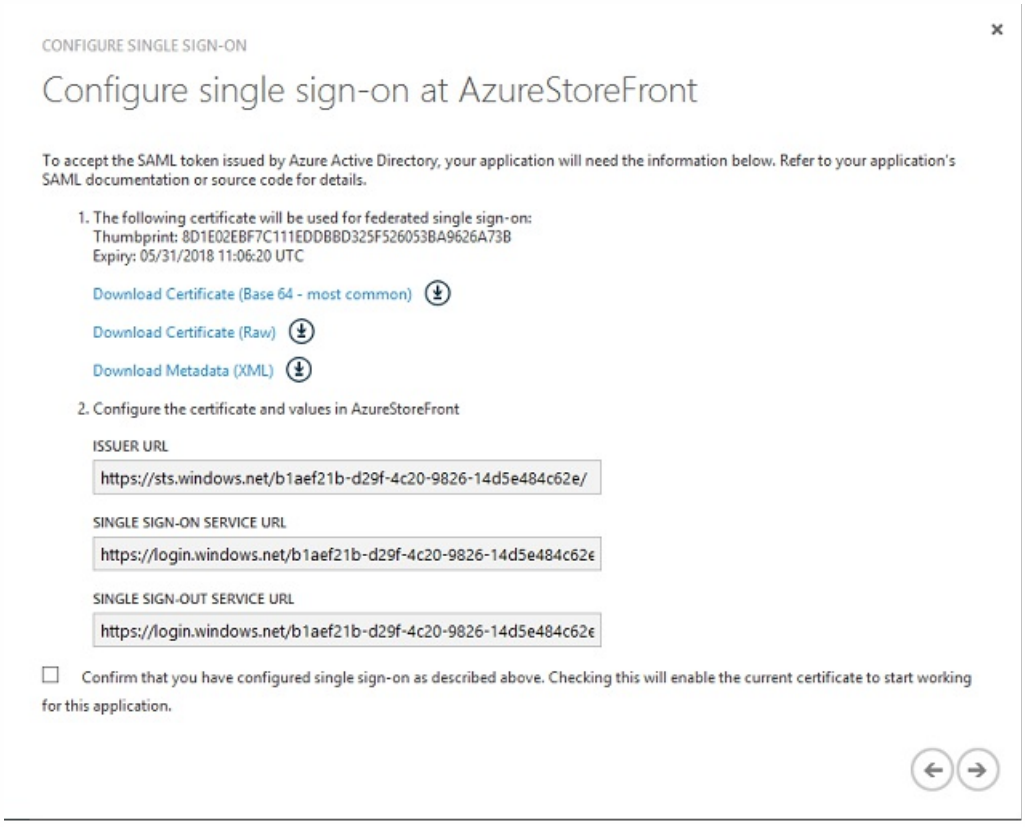
This deployment will use SAML 2.0 authentication, which corresponds to **Microsoft Azure AD Single Sign-On**.



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.

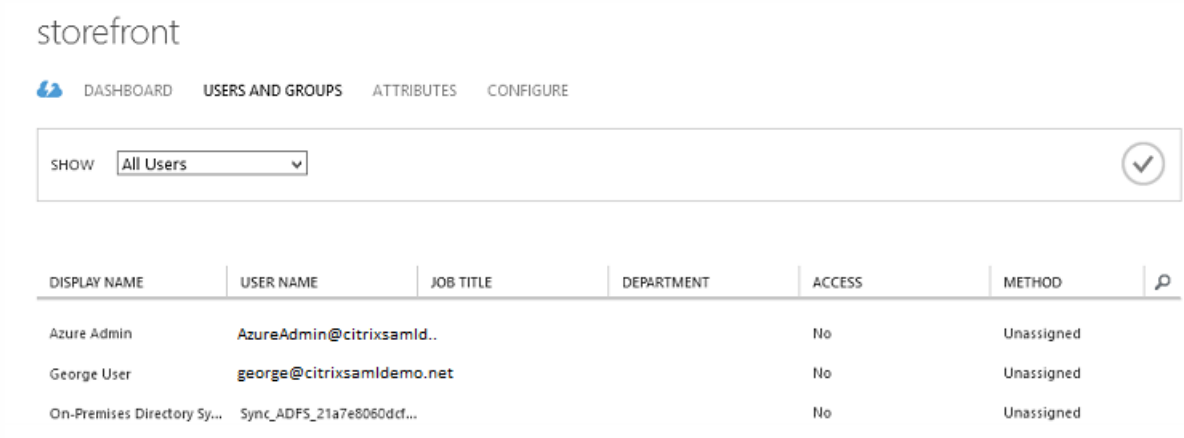


Download the base 64 trusted signing certificate and copy the sign-on and sign-out URLs. You will paste these in NetScaler configuration screens later.

Assign the application to users

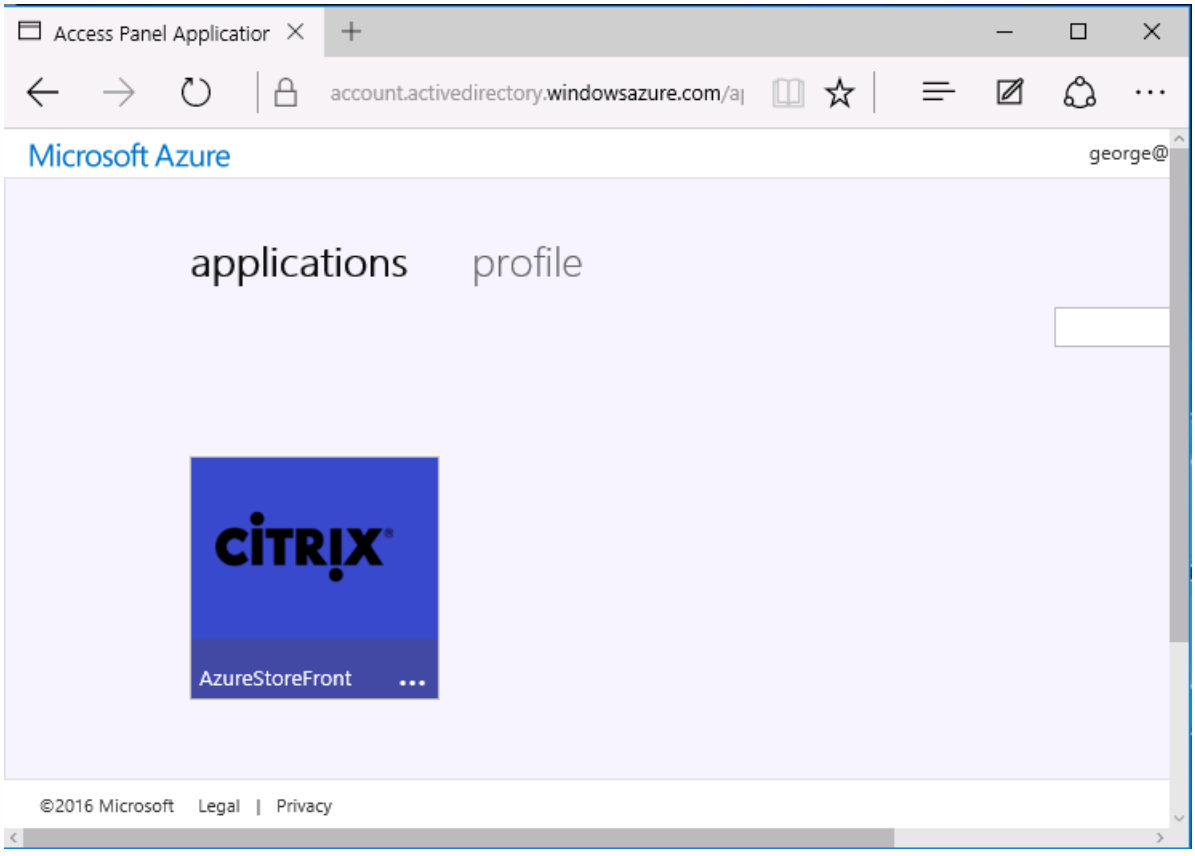
The final step is to enable the application so that it appears on users' "myapps.microsoft.com" control page. This is done on

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.



MyApps page

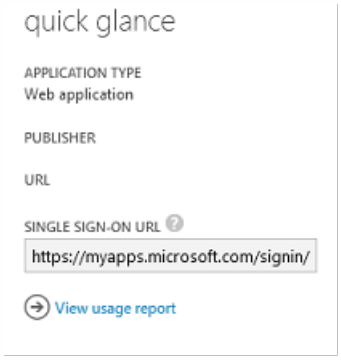
When the application has been configured, it appears on the users' lists of Azure applications when they visit https://myapps.microsoft.com.



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.

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

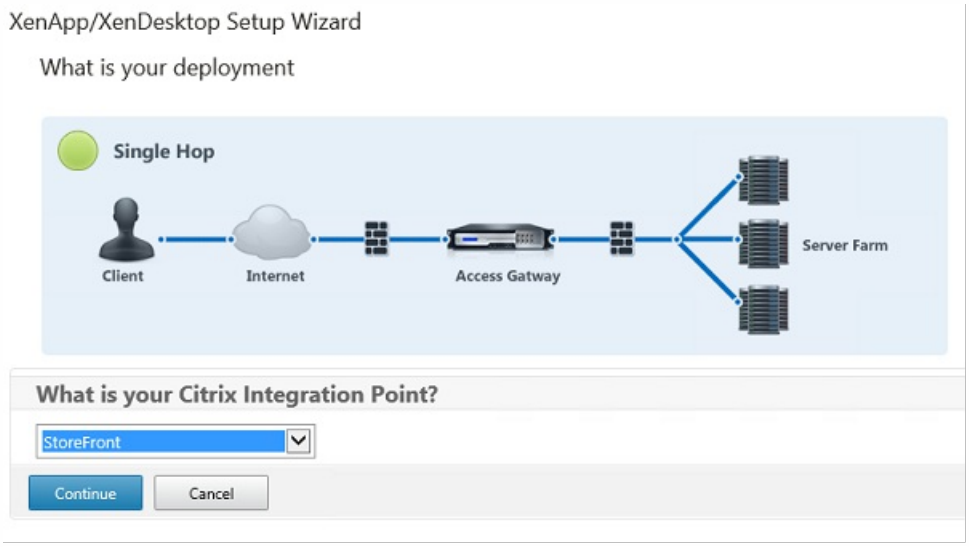
To remotely access the deployment, this example uses a separate VM running NetScaler. This can be purchased from the Azure Store. This example uses the "Bring your own License" version of NetScaler 11.0.

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.

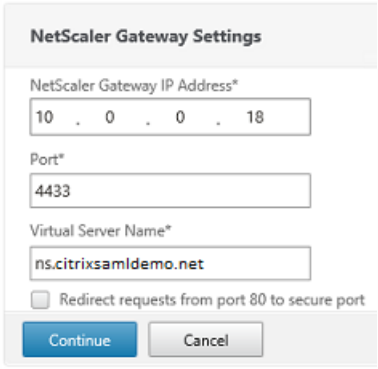
Add licenses, selecting **reboot** after each license file is added, and point the DNS resolver to the Microsoft domain controller.

Run the XenApp and XenDesktop setup wizard

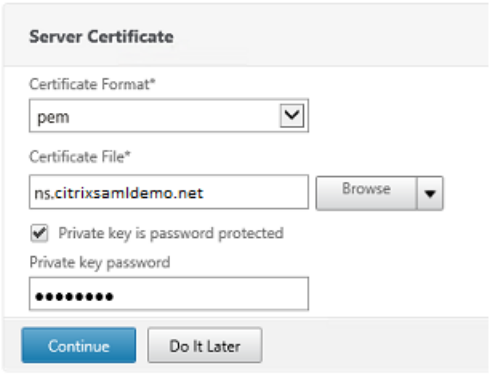
This example starts by configuring a simple StoreFront integration without SAML. After that deployment is working, it adds a SAML logon policy.



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.

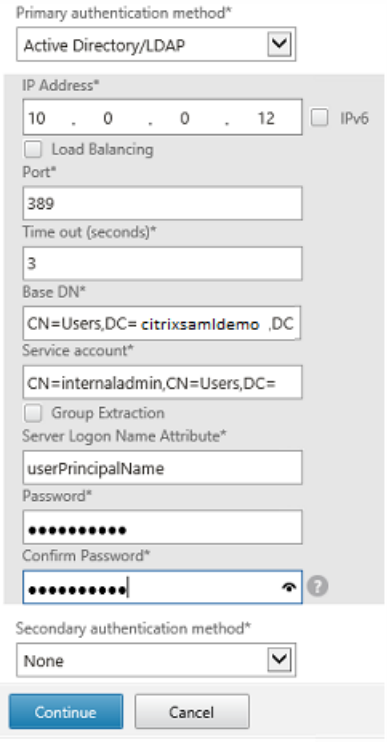


For simplicity, the example uploads an existing server certificate and private key stored in a file.



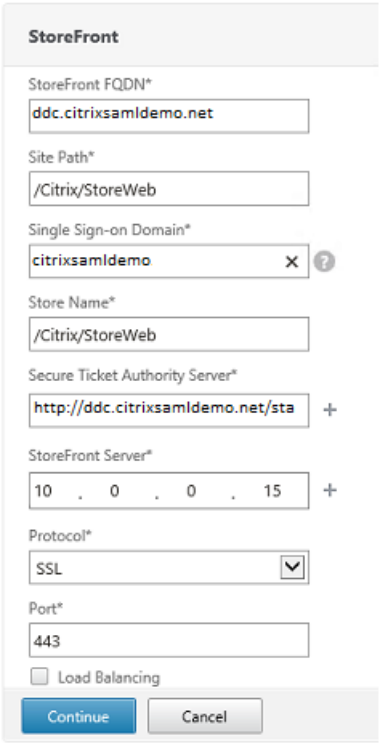
Configure the domain controller for AD account management

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.



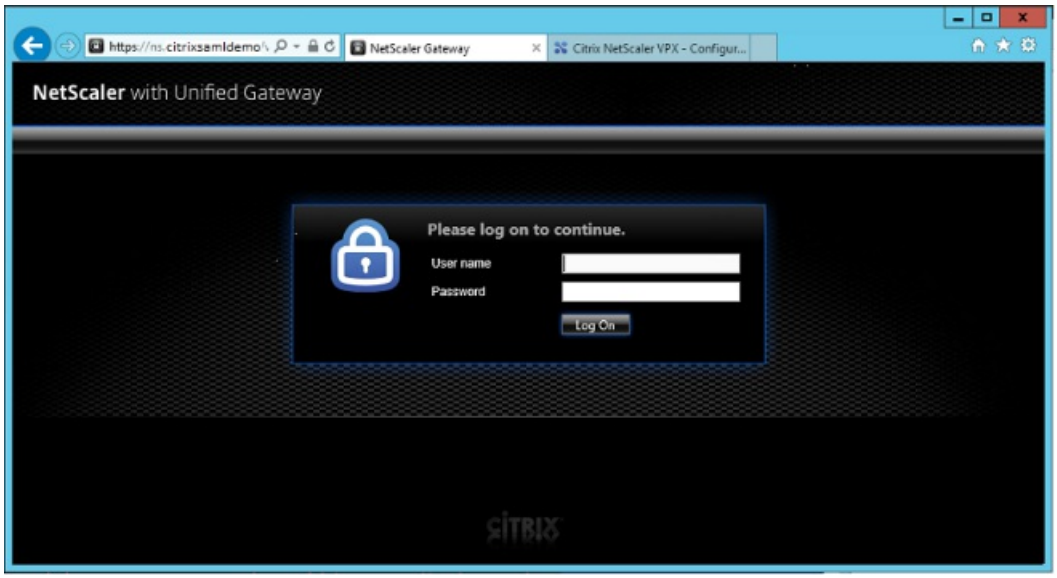
Configure the StoreFront address

In this example, StoreFront has been configured using HTTPS, so select the SSL protocol options.



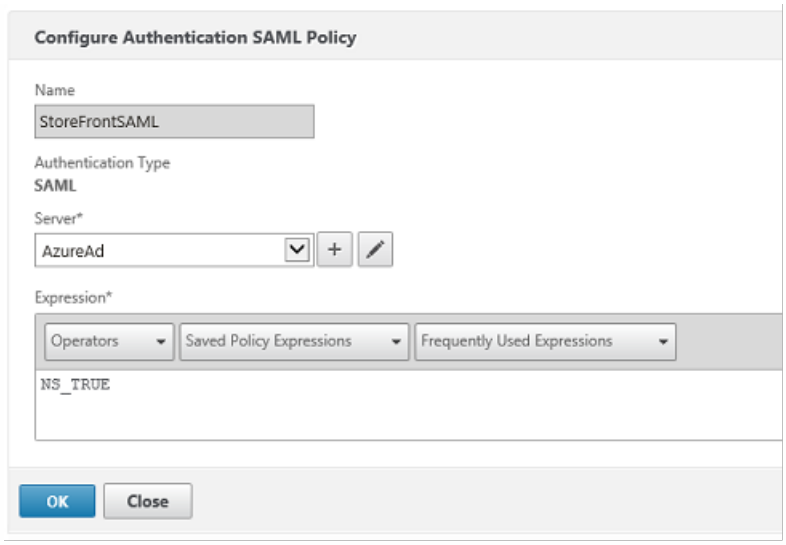
Verify the NetScaler deployment

Connect to NetScaler and check that authentication and launch are successful with the username and password.

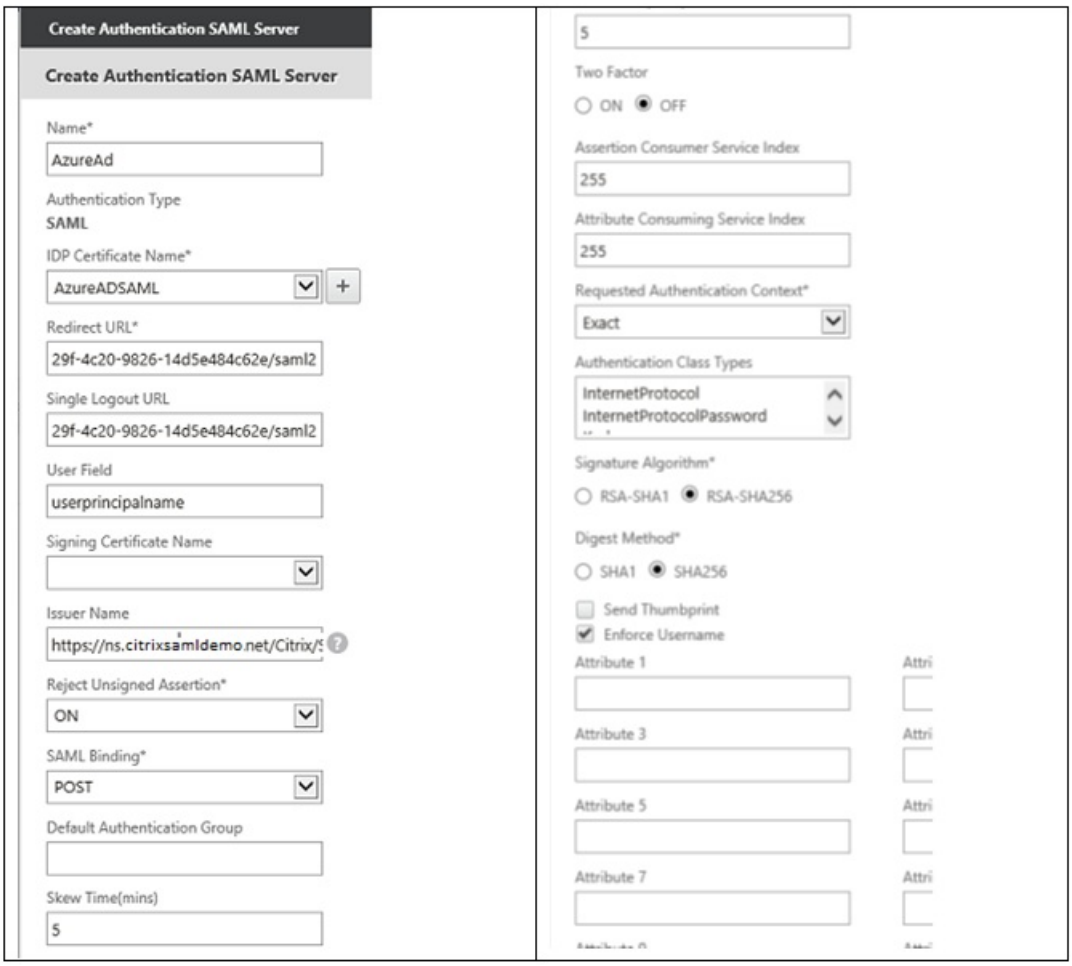


Enable NetScaler SAML authentication support

Using SAML with StoreFront is similar to using SAMl with other web sites. Add a new SAML policy, with an expression of **NS_TRUE**.



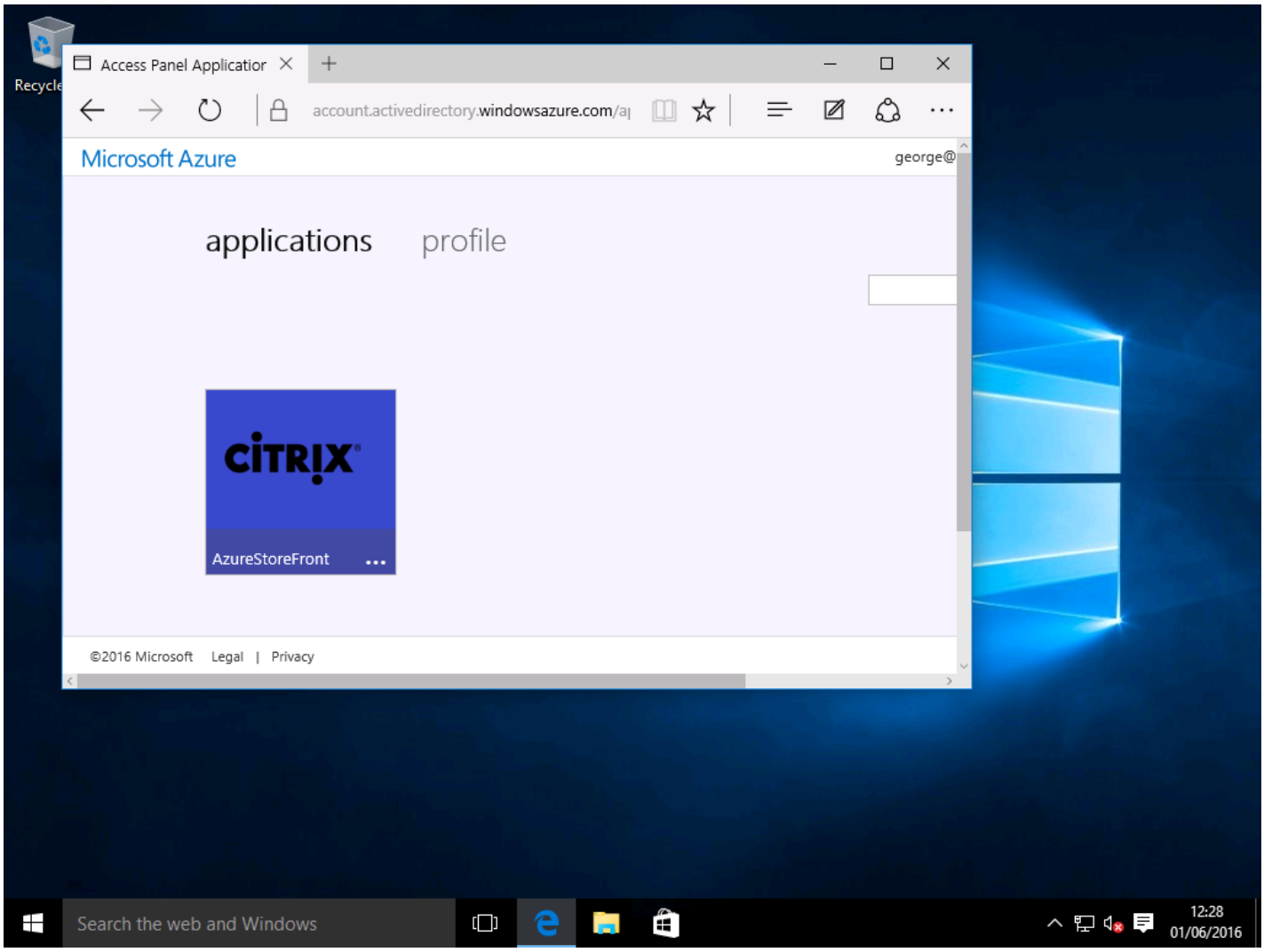
Configure the new SAML IdP server, using information obtained from Azure AD earlier.



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.



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.

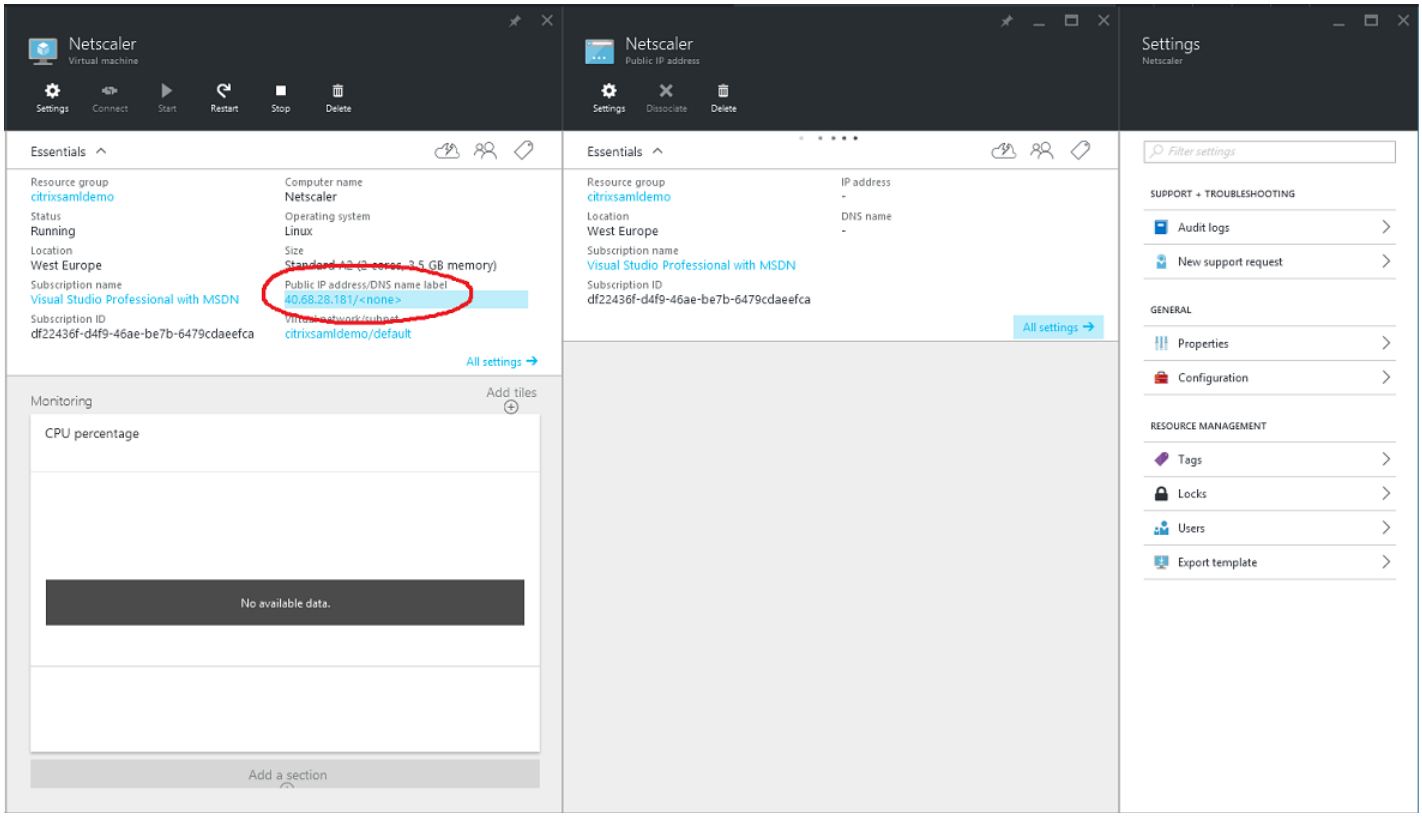
Finally, verify that non-Azure AD joined machines also function with the same URLs (although there will be a single explicit sign-on to Azure AD for the first connection).

Appendix

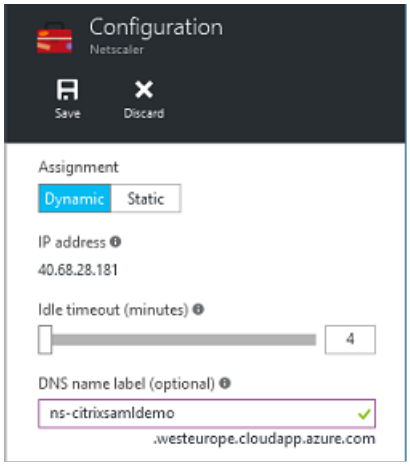
Several standard options should be configured when setting up a VM in Azure.

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.



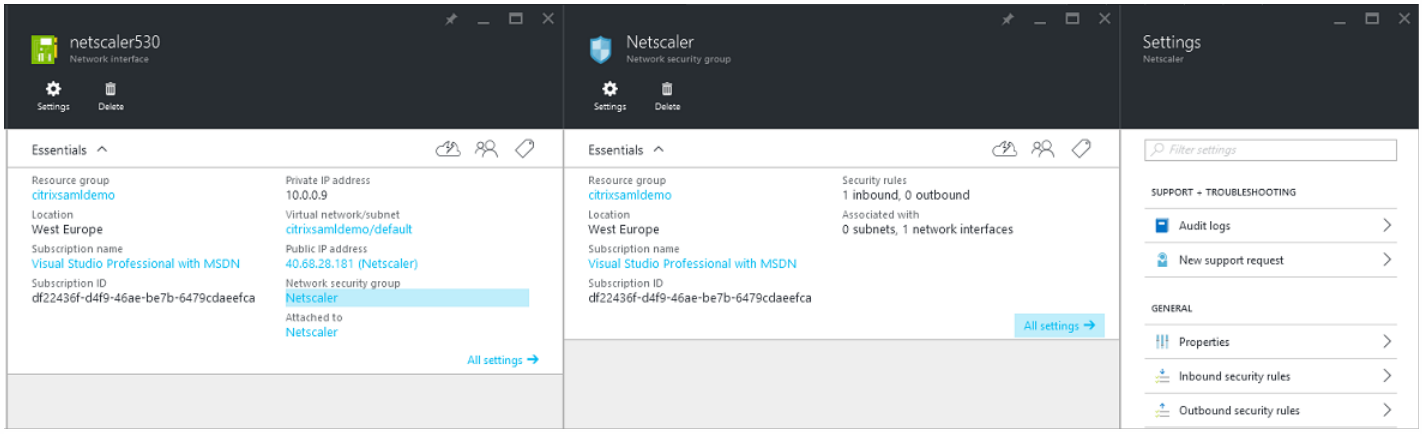
Select **Configuration** of the **Public IP address/DNS name label**. Choose a public DNS address for the VM. This can be used for CNAME references in other DNS zone files, ensuring that all DNS records remain correctly pointing to the VM, even if the IP address is reallocated.



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 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

Jul 18, 2016

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:

- 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

Jun 01, 2016

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.

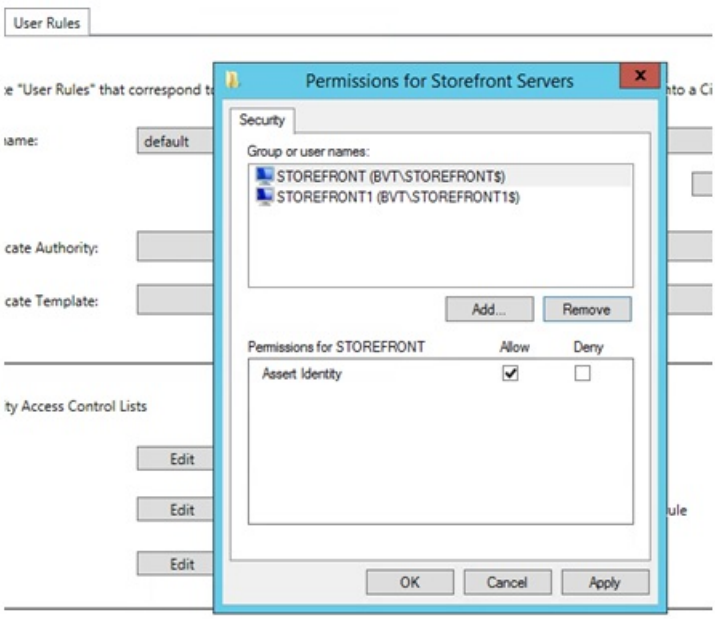
Step 1: Find out how many CA servers FAS is able to locate

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

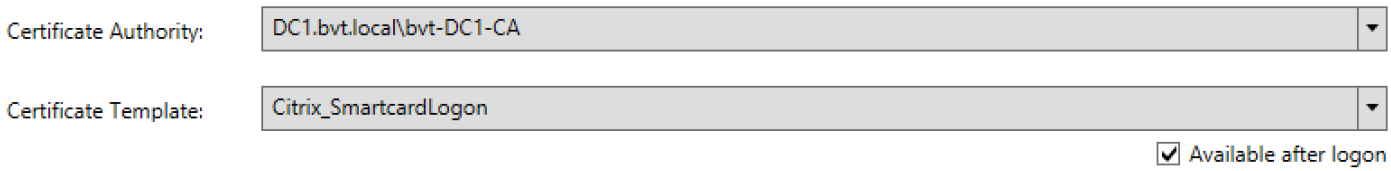
Citrix recommends that you create a role using the FAS administration console, rather than using PowerShell to create the role. This avoids the complication of having to add the SDL manually later. In the following example, a role named 'default' is created, with the access rule configured:



To add multiple CAs to the certificate authority field (which is not supported in this release), you must configure the certificate definition. 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:



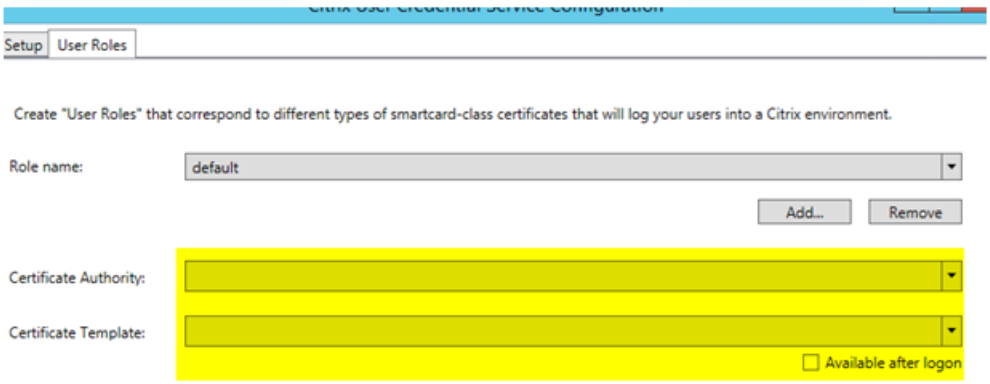
After you have the certificate definition name, modify the certificate definition to have a list of CertificateAuthorities, rather than just one:

```
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
```

Note: Your FAS administration console will not be functional after doing this. You will see an empty field in both 'Certificate Authority" and "Certificate Template" upon loading:



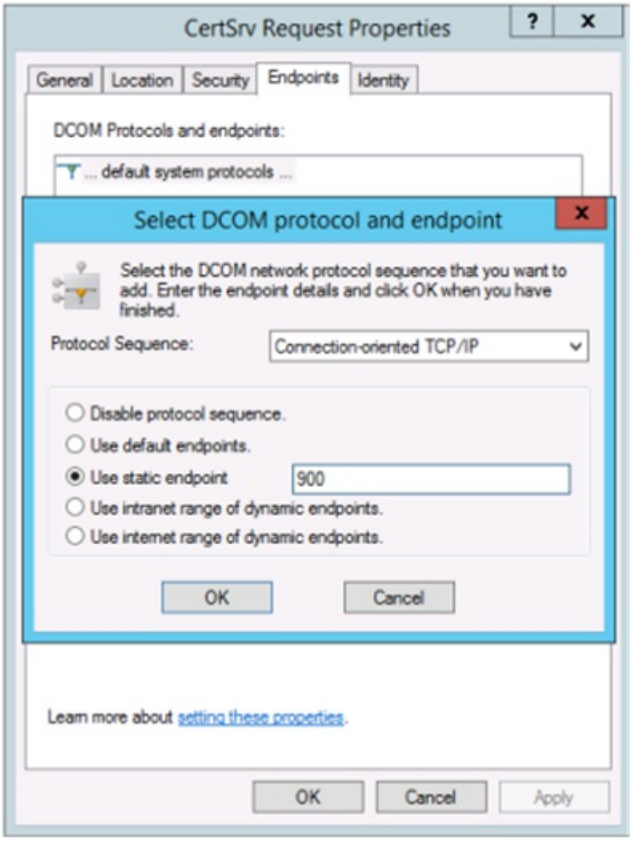
Functionally, FAS is still fine. If you use the console to modify the access rule, just repeat step 2 to display all the certificate authorities.

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, open the DCOM configuration panel and edit the properties of the "CertSrv Request" DCOM application:



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.

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

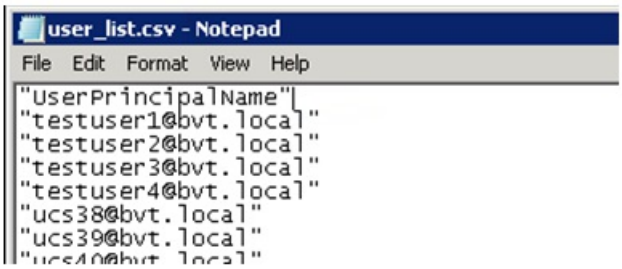
You can improve certificate generation by querying the AD and storing the list of users into a file (for example, a .csv file), as shown in the following example.

```
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
}
```

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:



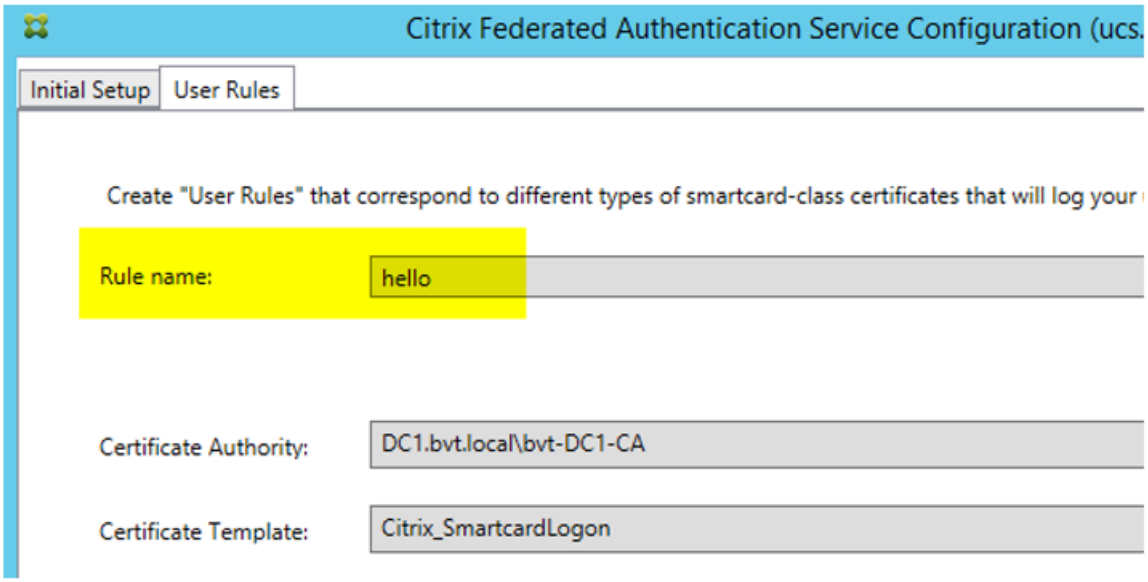
FAS server

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
  }
}
```

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.



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-FasAuthorizationCertificate

3. Place the FAS server into maintenance mode:

    Set-FasServer –Address <FAS server> -MaintenanceMode $true

4. Swap the new authorization certificate:

    Set-FasCertificateDefinition –AuthorizationCertificate <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.
- 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

Jun 01, 2016

Introduction

Private keys are stored by means of the Network Service account 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:

- 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.FederatedAuthenticationService.exe.config 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

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.

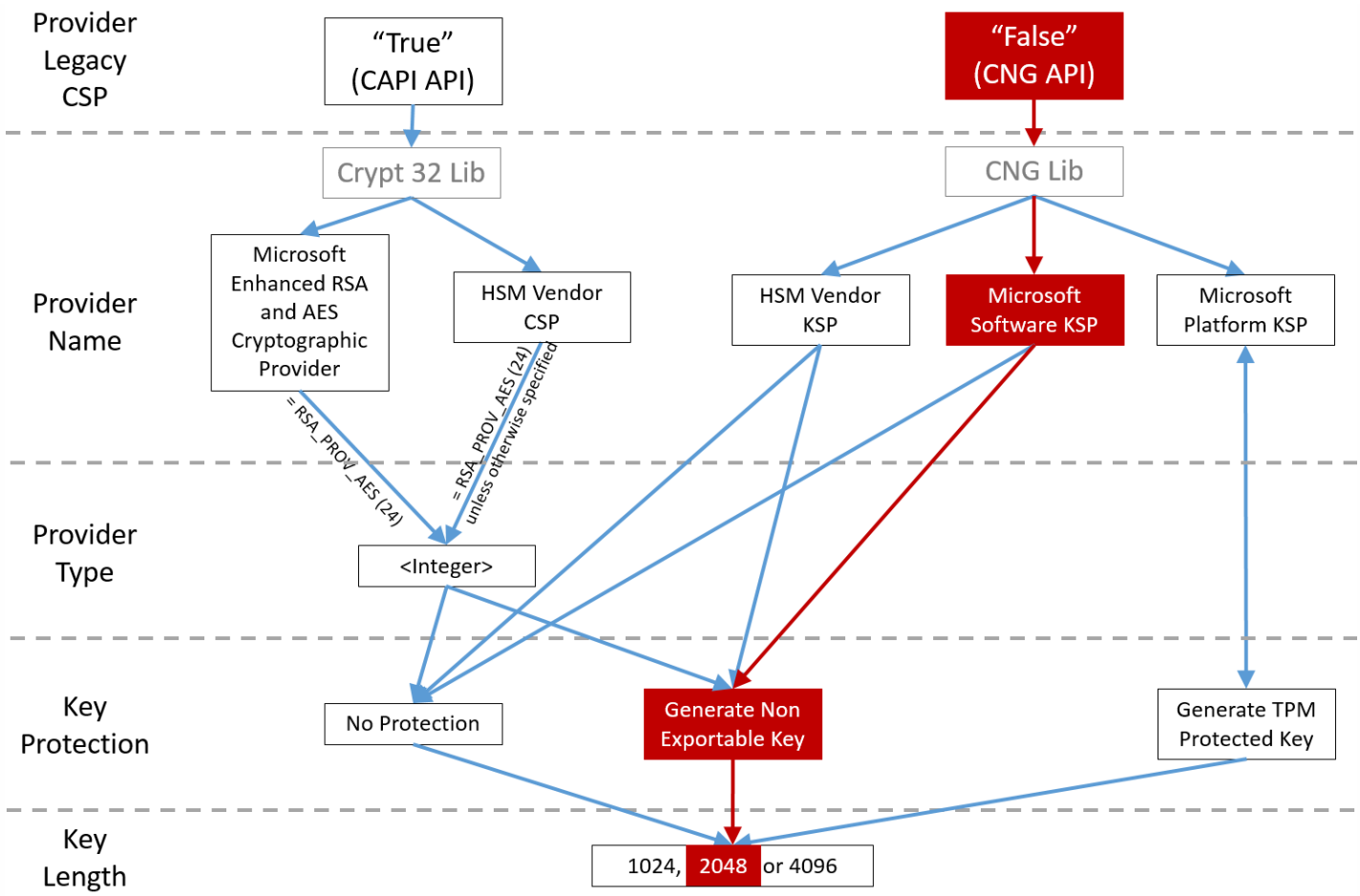
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (When FAS needs to perform a private key operation, it uses the value specified here) Controls the "exportable" flag of private keys. Allows the use of TPM key storage, if supported by the hardware.

Value	Comment
NoProtection	Private key can be exported.
GenerateNonExportableKey	Default. Private key cannot be exported.
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):



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.

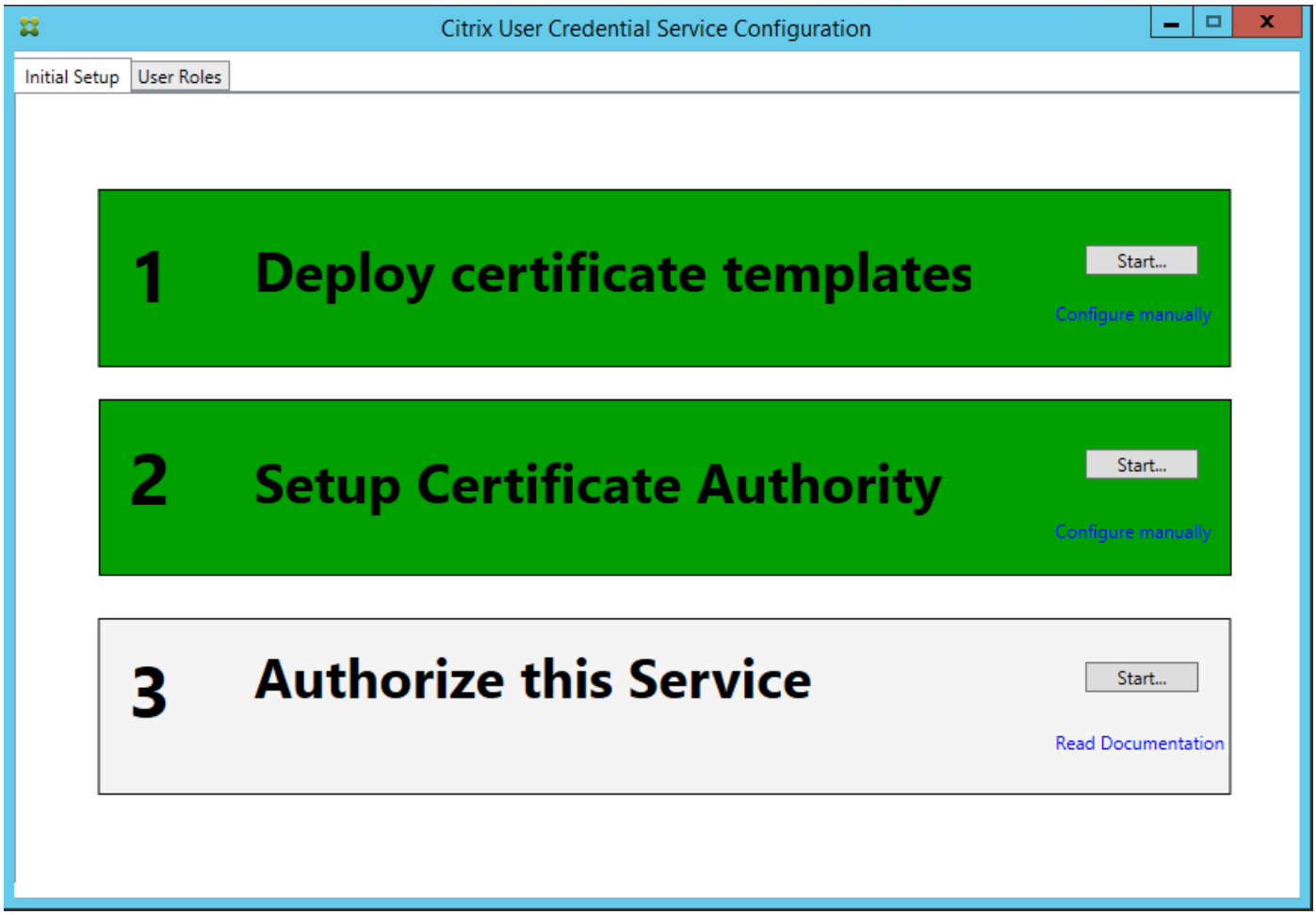
This scenario assumes that the TPM on your FAS server motherboard has been enabled in the BIOS according to the TPM manufacturer's documentation and then initialized in Windows; see https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx.

Using PowerShell (recommended)

The RA certificate can be requested offline using PowerShell. This is recommended for organizations that do not want

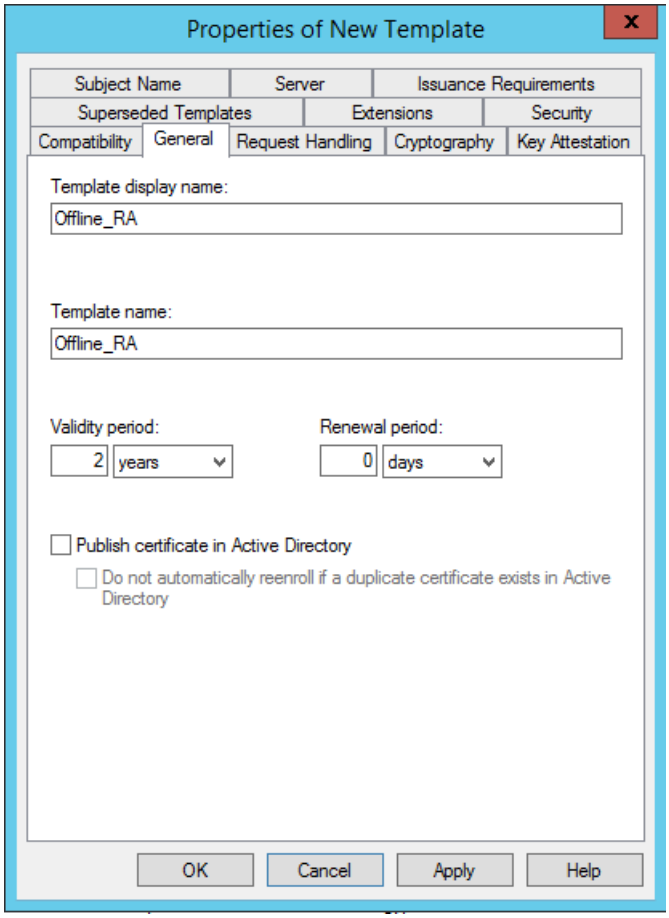
their CA to issue a RA certificate through an online CSR. An offline RA CSR cannot be made using the FAS administration console.

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.”



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:



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:

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationServices.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
```

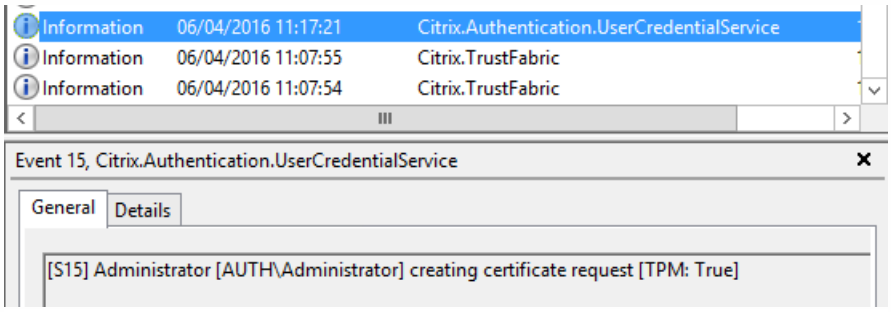
The following is displayed:

```
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
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPBgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVDsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TD15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

Notes:

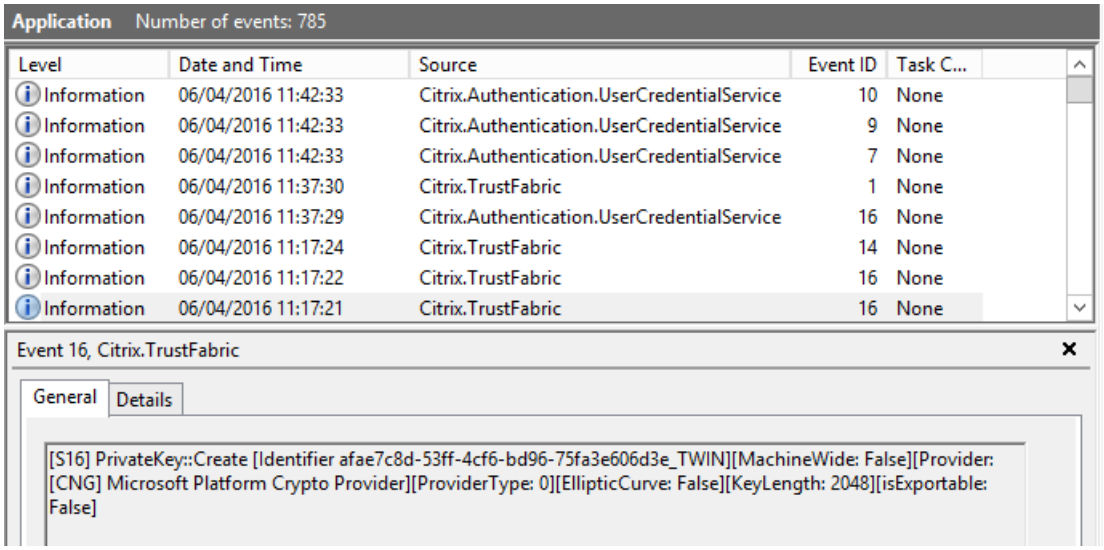
- The Id GUID (in this example, “5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39”) is required in a subsequent step.
- Think of this PowerShell cmdlet as a one-time “override” that is used to generate the private key for the RA certificate.
- When running this cmdlet, the values that are read from the config file 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.



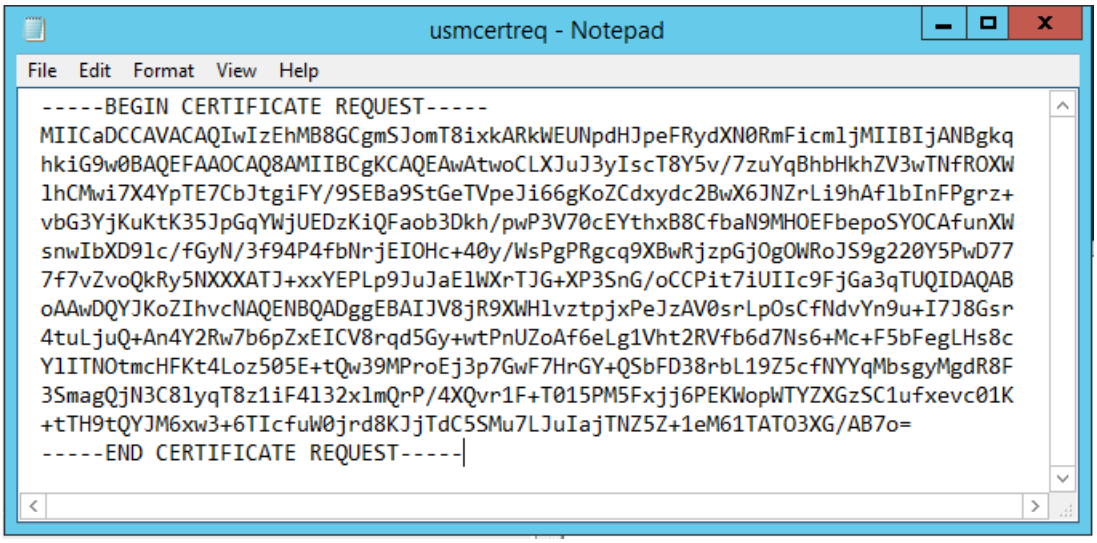
Note “[TPM: True]”

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.



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>

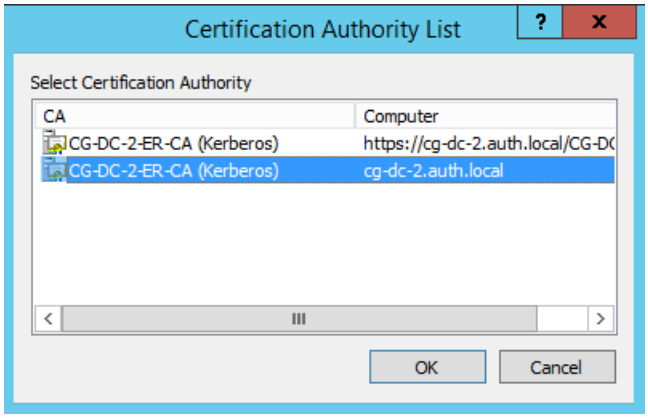
For example:

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-0B0C-4D21-A4FD-2E29502177C2}
  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:

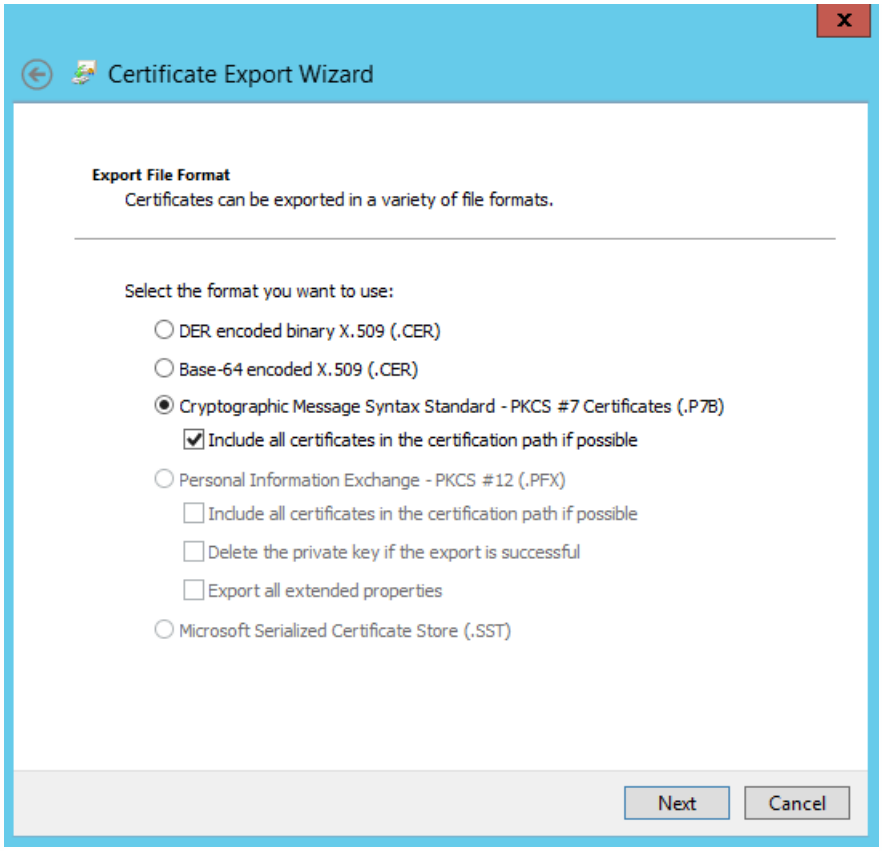


After the CA has been specified, PowerShell displays the RequestID:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E2950177C2}
  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:



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>
```

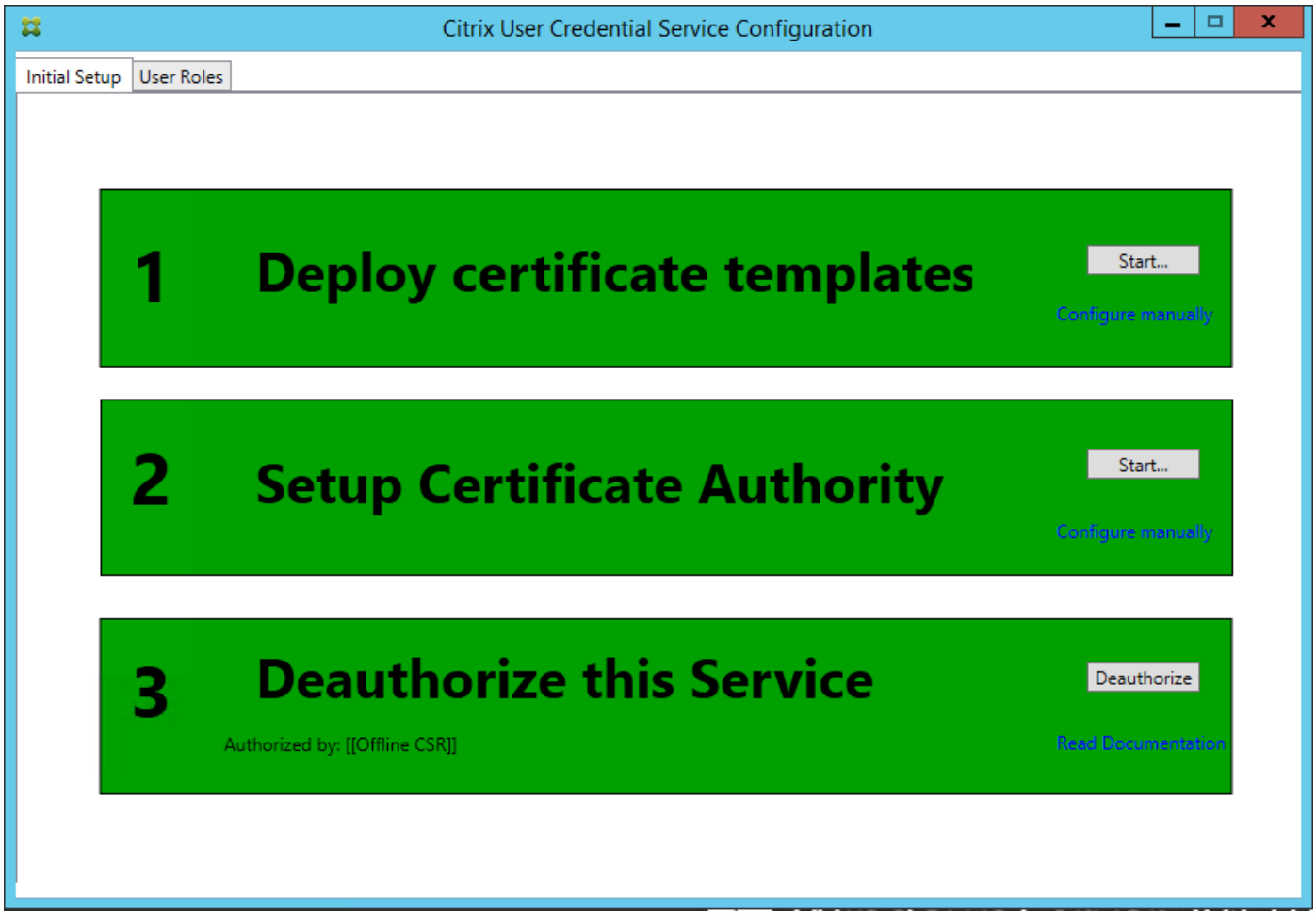
For example:

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

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-8963-16ec311020fc
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):

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.

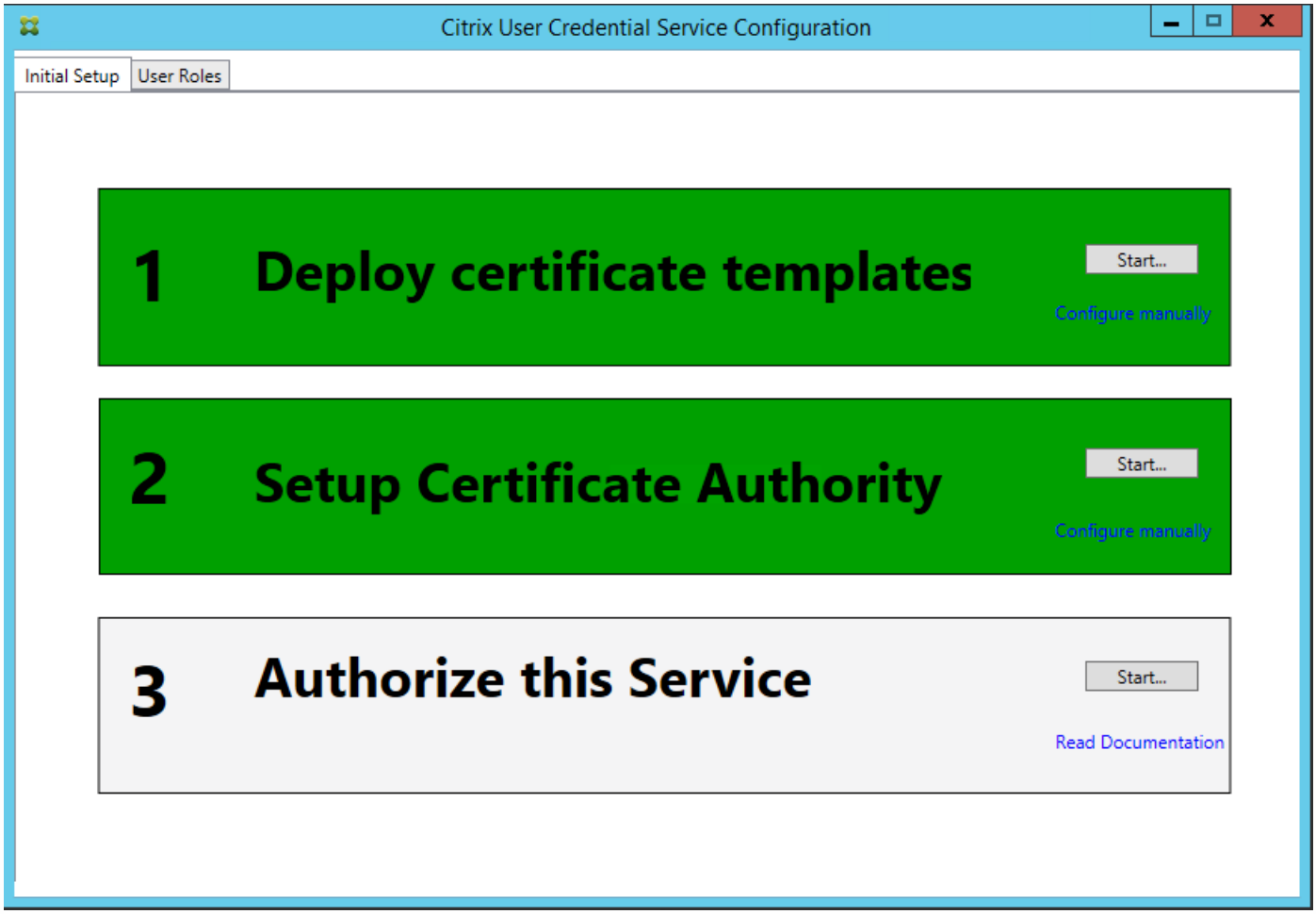
Example 3

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:

```
<?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]
```

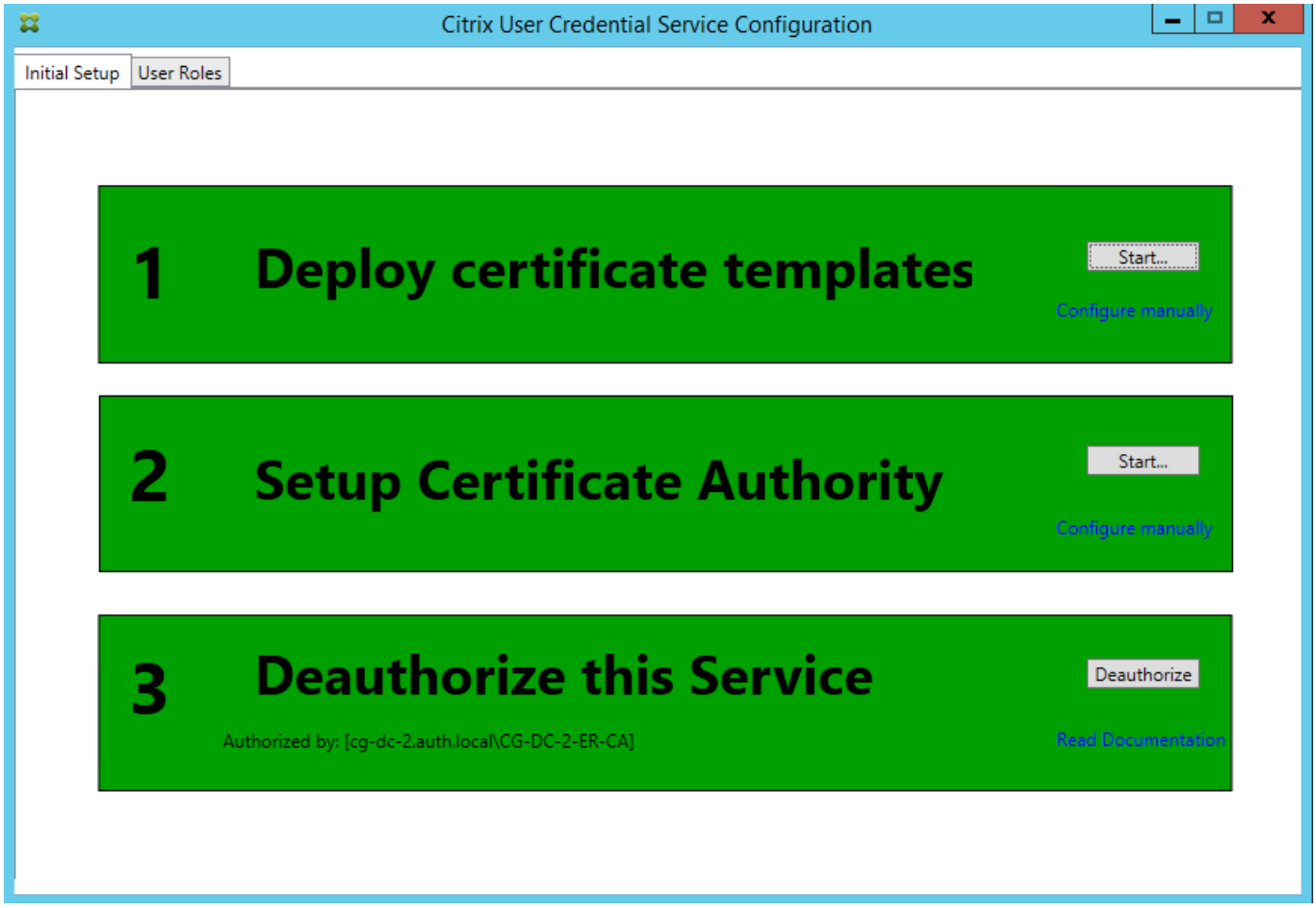
Note: [Provider: [CNG] HSM_Vendor's Key Storage Provider]

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>]"



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

```
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-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/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

Jun 15, 2016

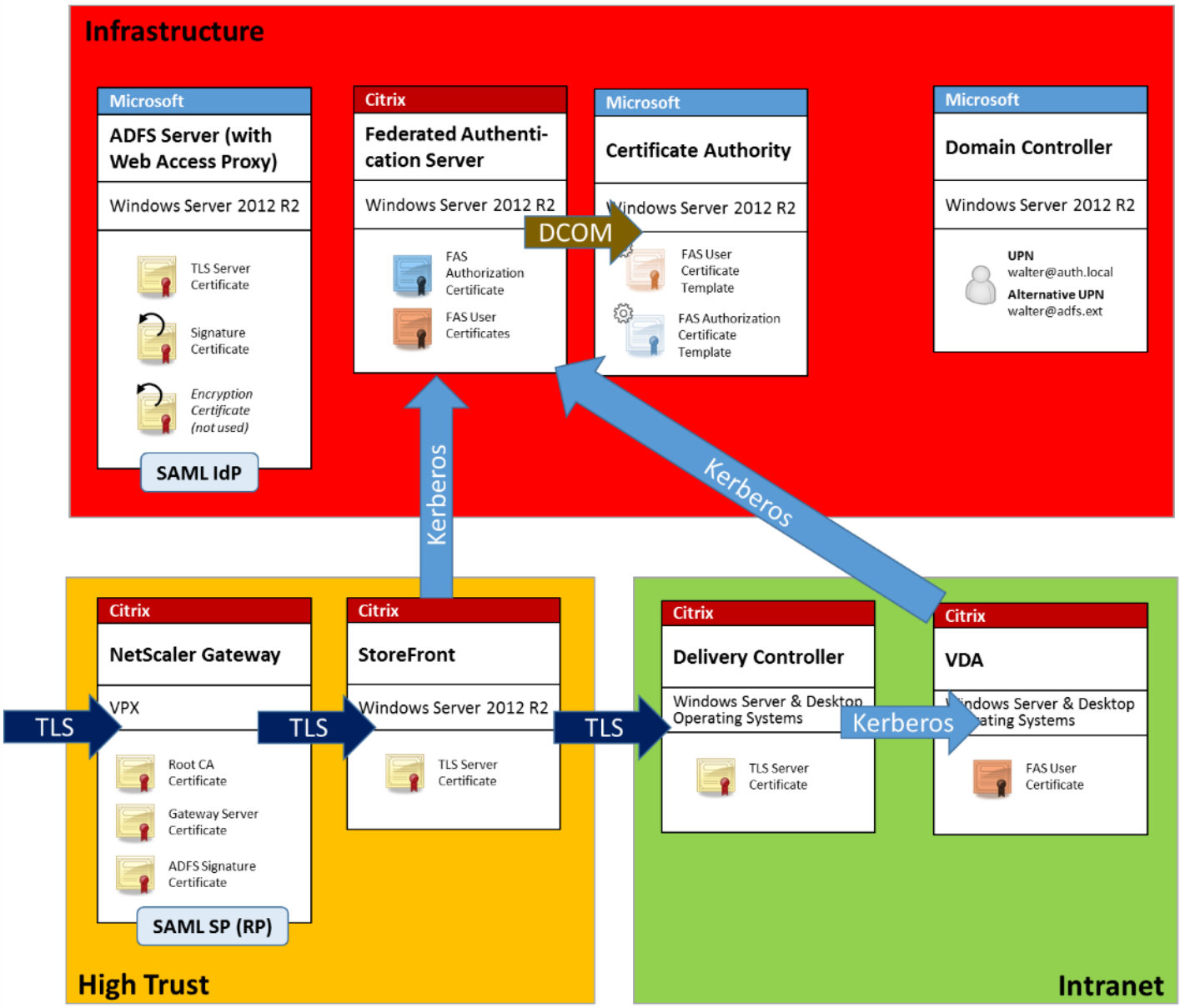
The Citrix Federated Authentication Service (FAS) is tightly integrated with Microsoft Active Directory and the Microsoft certification authority (CA). It is essential to ensure that the system is managed and secured appropriately, developing a security policy as you would for a domain controller or 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.



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:

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

Certificate templates are installed "forest-wide" by the enterprise administrator. There are four main security considerations.

Installation of registration authority templates

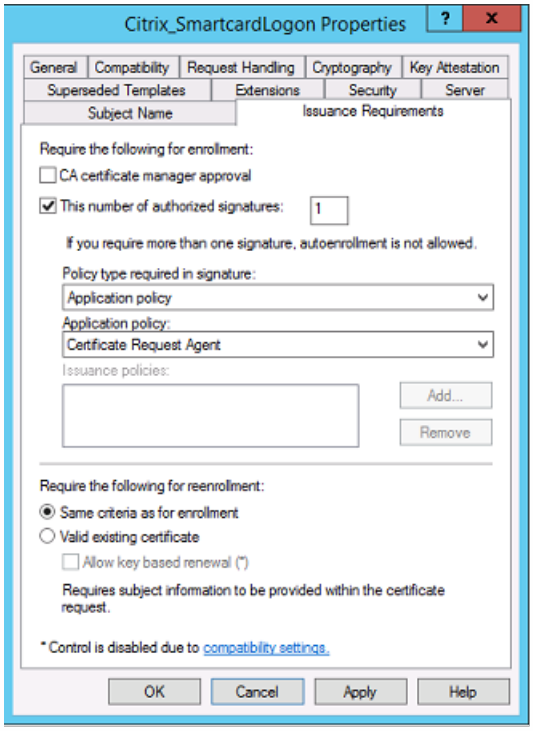
The FAS installer provides two types of certificate templates: the registration authority (RA) templates and the smart card logon template.

Only the smart card logon template is needed at run time, so the other RA templates can either not be installed (meaning that RA certificates must be issued manually using a separate offline CA), or the RA templates can be disabled after an FAS server has been authorized.

Application policy OID

RA certificates are identified by including a "Certificate Request Agent" object identifier (OID) in the Enhanced Key Usage extensions. If there is potential for this OID to be in use by a different system, this can be changed to a completely

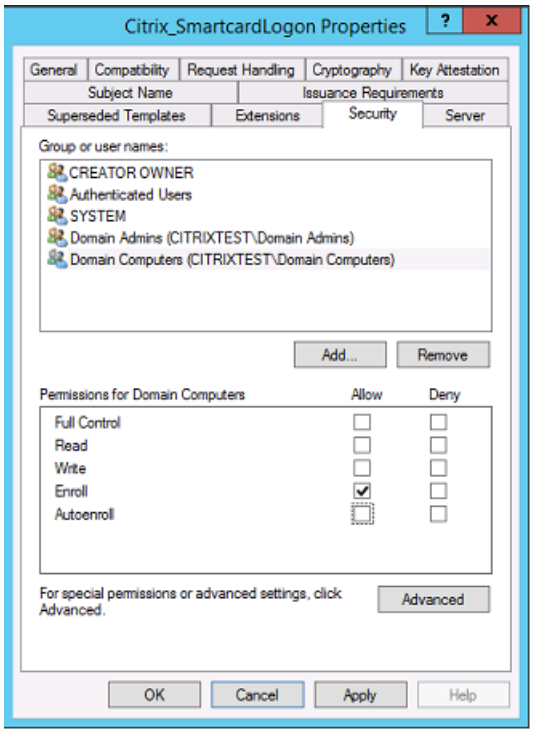
custom OID.



Access Control List (ACL)

Each template has an ACL that controls which users and computers can issue certificates.

Citrix recommends that this ACL be reconfigured to explicitly allow only the machine accounts of the FAS servers to request certificates. This can be further restricted using network firewall policies.



Subject name, extensions, and path name constraints

The standard subject name and extensions can be configured using standard RFC 5280 features to control which purposes the issued certificates can be used for. This provides a basic level of control over what certificates issued through the public key infrastructure (PKI) can be used for.

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.

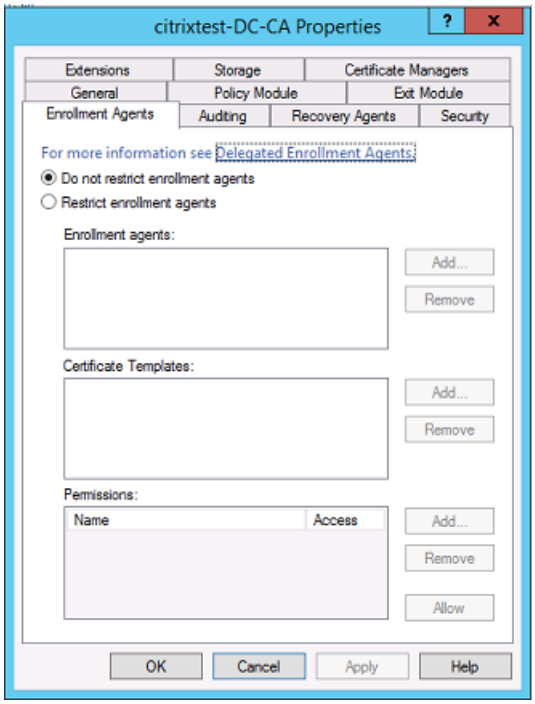
A simple security practice is to publish only the RA certificate templates when the FAS servers are being installed, or to insist on a completely offline issuance process. In either case, the CA administrator should maintain complete control over authorizing RA certificate requests, and have a policy 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.



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:

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.

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.

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

Jul 18, 2016

In this article:

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://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx.

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.

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.

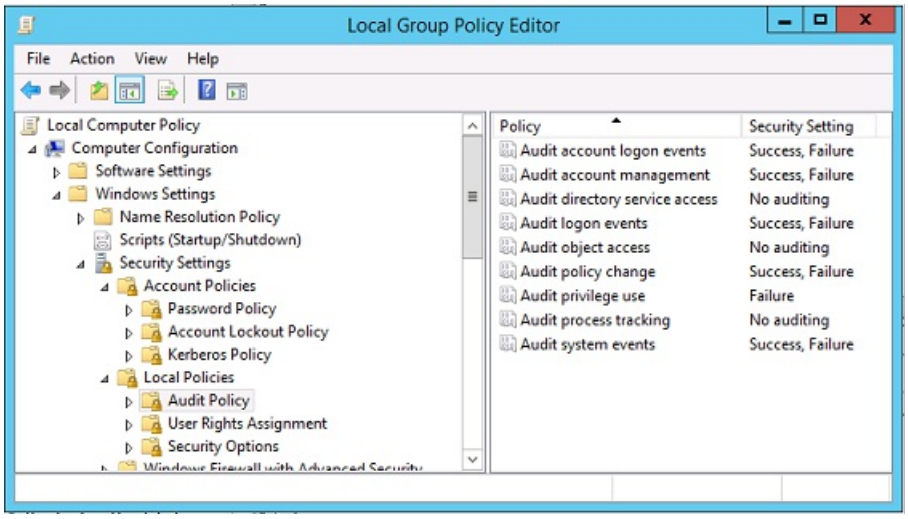
Identify the domain controller in use

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.

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)
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.

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

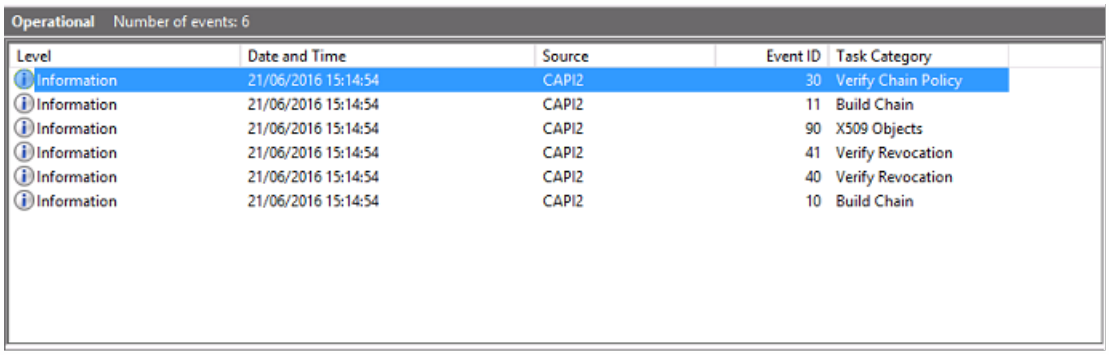
This section describes the expected log entries on the domain controller and workstation when the user logs on with a certificate.

- 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.



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

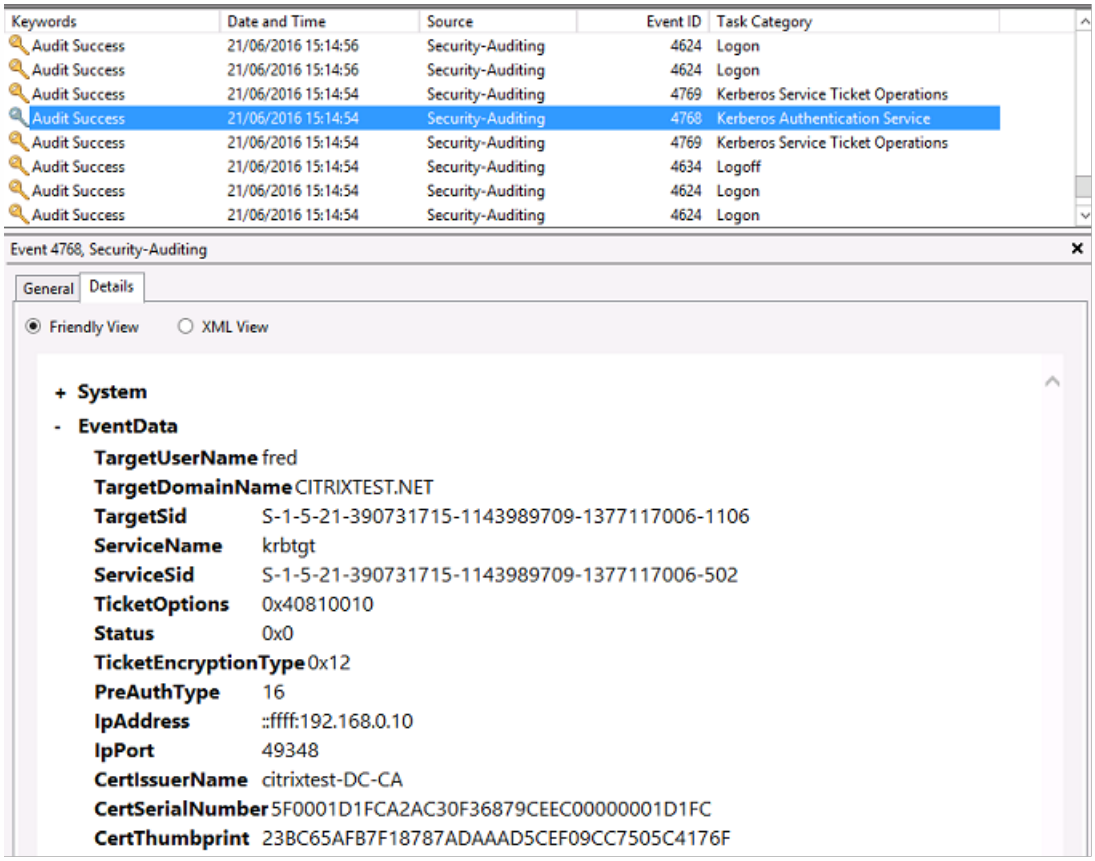
The final event log message shows lsass.exe on the domain controller constructing a chain based on the certificate provided by the VDA, and verifying it for validity (including revocation). The result is returned as "ERROR_SUCCESS".

- **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

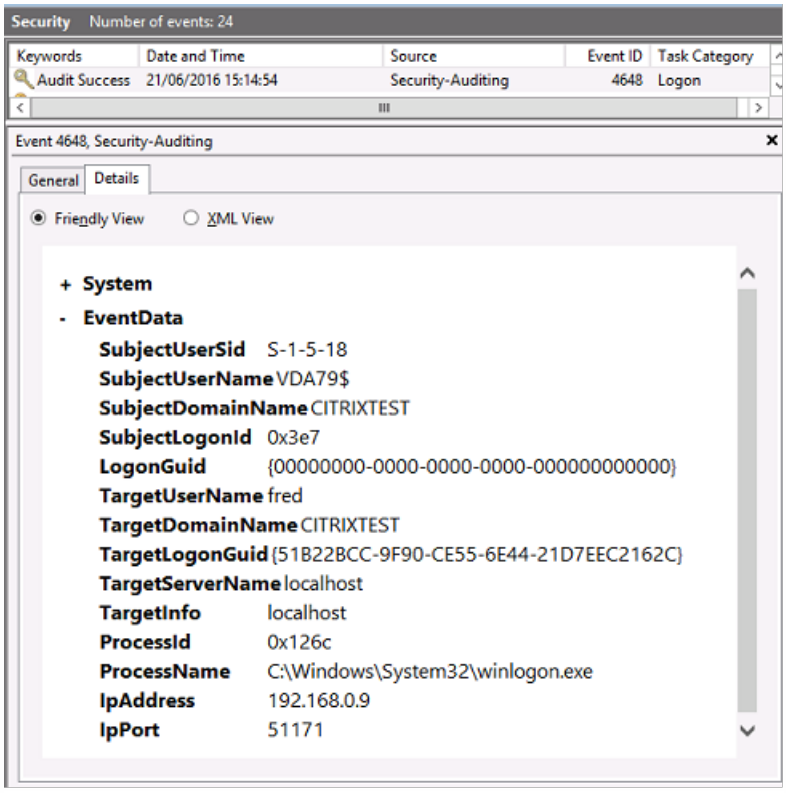
The domain controller shows a sequence of logon events, the key event being 4768, where the certificate is used to issue the Kerberos Ticket Granting Ticket (krbtgt).

The messages before this show the machine account of the server authenticating to the domain controller. The messages following this show the user account belonging to the new krbtgt being used to authenticate to the domain controller.



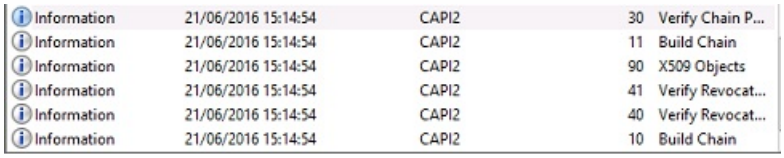
VDA security log

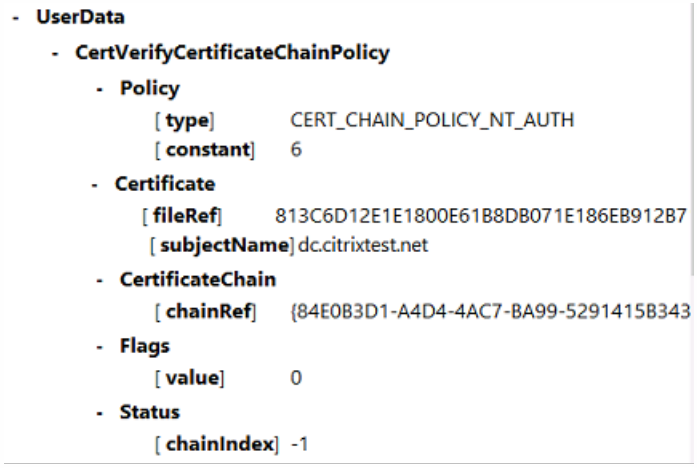
The VDA security audit log corresponding to the logon event is the entry with event ID 4648, originating from winlogon.exe.



VDA CAPI log

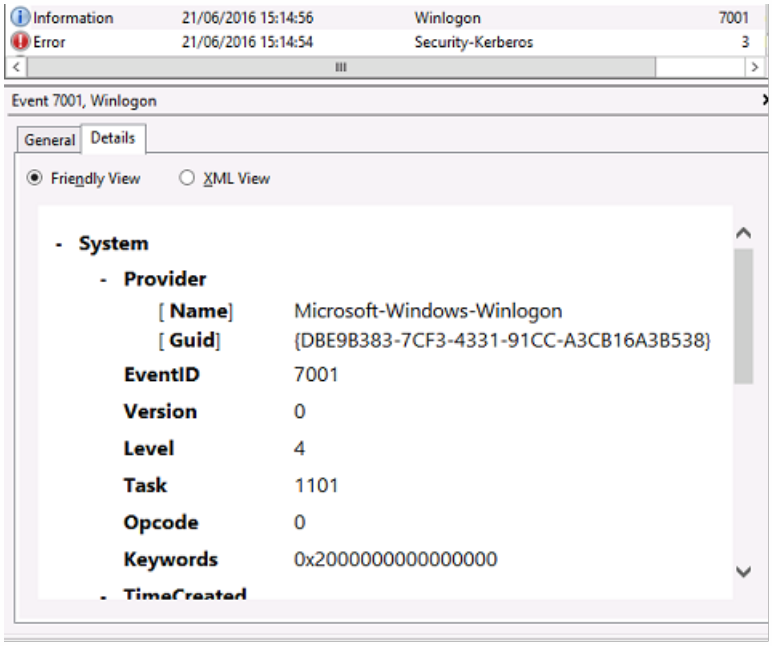
This example VDA CAPI log shows a single chain build and verification sequence from lsass.exe, validating the domain controller certificate (dc.citrixtest.net).





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.



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 request is not supported	The domain controller cannot be contacted, or the domain controller does not have appropriate certificates installed. 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.
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: http://support.citrix.com/article/CTX206156
- Smartcard logon policies: https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- Enabling CAPI logging: http://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

Jul 19, 2016

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.

ZIP Federated Authentication Service PowerShell cmdlet help files

Print

Jul 08, 2016

Managing printers in your environment is a multistage process:

1. Become familiar with printing concepts, if you are not already.
2. Plan your printing architecture. This includes analyzing your business needs, your existing printing infrastructure, how your users and applications interact with printing today, and which printing management model best applies to your environment.
3. Configure your printing environment by selecting a printer provisioning method and then creating policies to deploy your printing design. Update policies when new employees or servers are added.
4. Test a pilot printing configuration before deploying it to users.
5. Maintain your Citrix printing environment by managing printer drivers and optimizing printing performance.
6. Troubleshoot issues that may arise.

Printing concepts

Before you begin planning your deployment, make sure that you understand these core concepts for printing:

- The types of printer provisioning available
- How print jobs are routed
- The basics of printer driver management

Printing concepts build on Windows printing concepts. To configure and successfully manage printing in your environment, you must understand how Windows network and client printing works and how this translates into printing behavior in this environment.

Print process

In this environment, all printing is initiated (by the user) on machines hosting applications. Print jobs are redirected through the network print server or user device to the printing device.

When a user prints:

- Determines what printers to provide to the user. This is known as printer provisioning.
- Restores the user's printing preferences.
- Determines which printer is the default for the session.

You can customize how to perform these tasks by configuring options for printer provisioning, print job routing, printer property retention, and driver management. Be sure to evaluate how the various option settings might change the performance of printing in your environment and the user experience.

Printer provisioning

The process that makes printers available in a session is known as provisioning. Printer provisioning is typically handled dynamically. That is, the printers that appear in a session are not predetermined and stored. Instead, the printers are assembled, based on policies, as the session is built during log on and reconnection. As a result, the printers can change according to policy, user location, and network changes, provided they are reflected in policies. Thus, users who roam to a different location might see changes to their workspace.

The system also monitors client-side printers and dynamically adjusts in-session auto-created printers based on additions, deletions, and changes to the client-side printers. This dynamic printer discovery benefits mobile users as they connect from various devices.

The most common methods of printer provisioning are:

- **Universal Print Server** - The Citrix Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal print driver. This solution enables you to use a single driver on a 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.

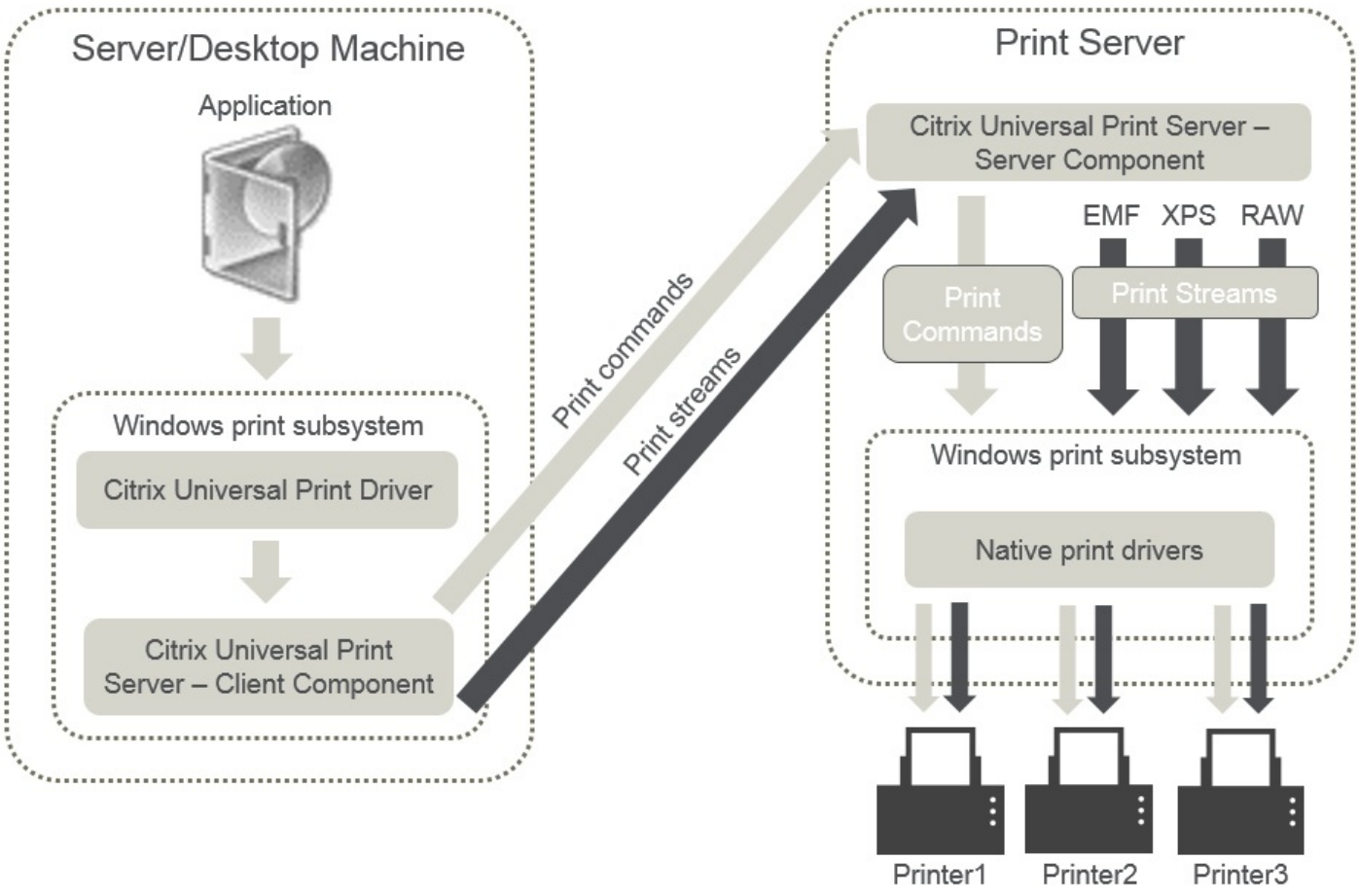
  The Universal Print Server feature comprises:

  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.



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.

  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.

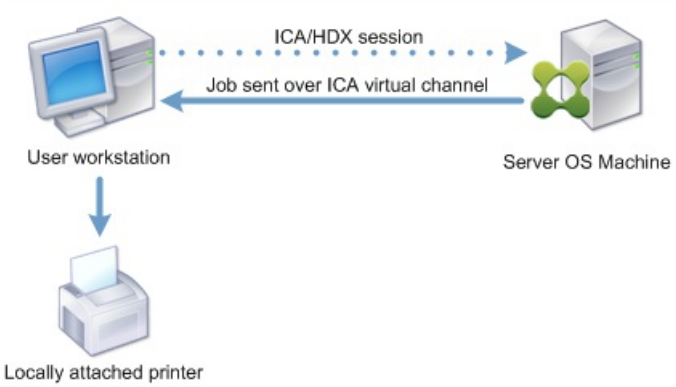
Print job routing

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.



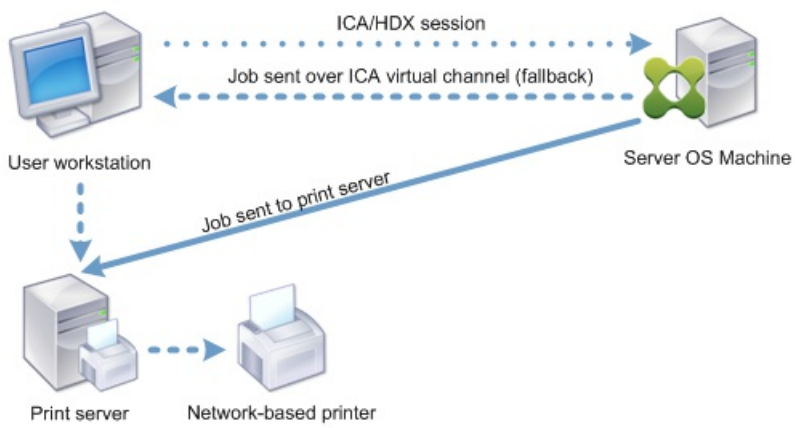
Network-based printers

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:

- 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.

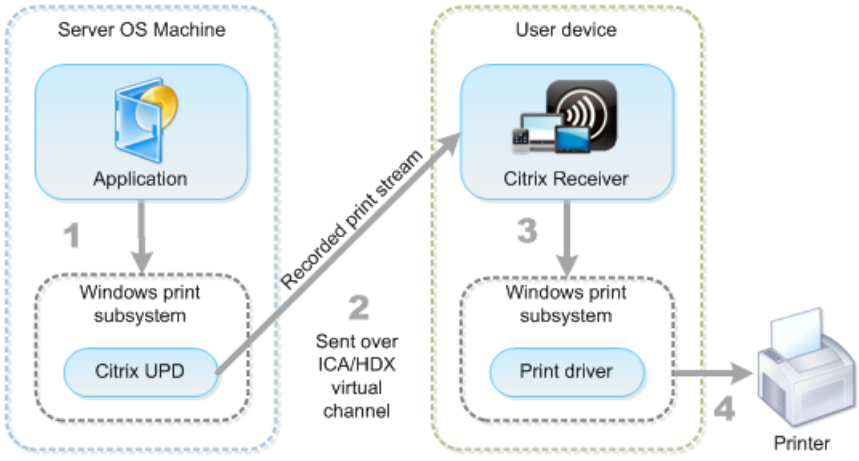


Print driver management

To simplify printing in this environment, Citrix recommends using Citrix Universal print driver. The Universal print driver is a device-independent driver that supports any print device and thus simplifies administration by reducing the number of drivers required.

The Citrix XPS Universal print driver 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 will not be available using Citrix XPS Universal print driver.

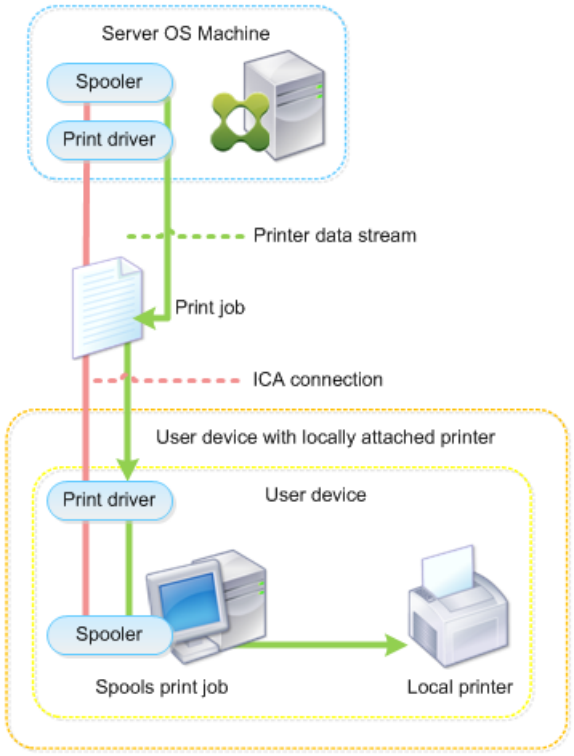
The following illustration shows the Universal print driver components and a typical workflow for a printer locally attached to a device.



When planning your driver management strategy, determine if you will support the Universal print driver, device-specific drivers, or both. If you support standard drivers, you need to 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
- Best practices, security considerations, and default operations
- Print policies and preferences
- Provision printers
- Maintain the printing environment

Printing configuration example

Sep 09, 2015

Choosing the most appropriate printing configuration options for your needs and environment can simplify administration. Although the default print configuration enables users to print in most environments, the defaults might not provide the expected user experience or the optimum network usage and management overhead for your environment.

Your printing configuration depends upon:

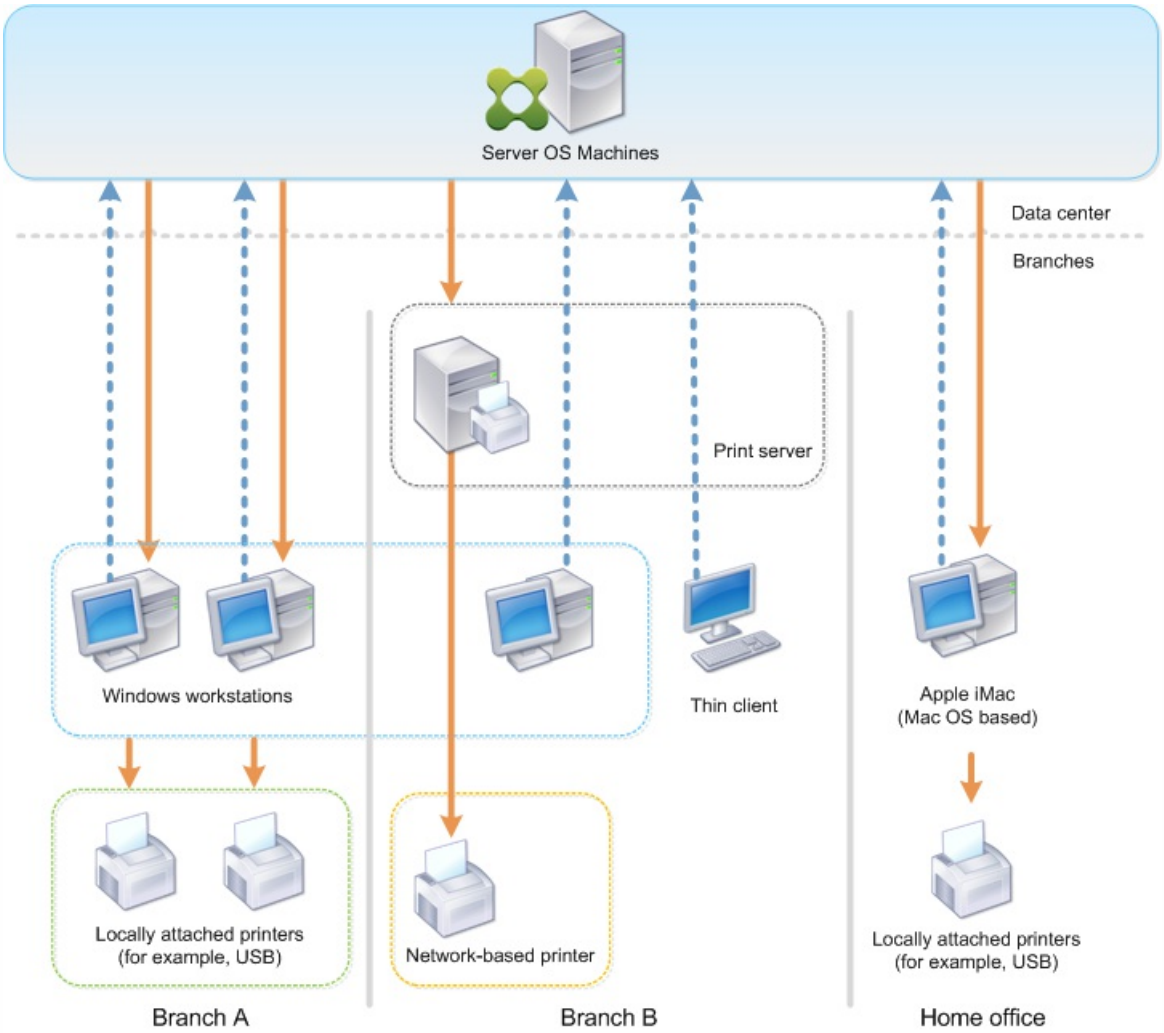
- Your business needs and your existing printing infrastructure.
  Design your printing configuration around the needs of your organization. Your existing printing implementation (whether users can add printers, which users have access to what printers, and so on) might be a useful guide when defining your printing configuration.
- Whether your organization has security policies that reserve printers for certain users (for example, printers for Human Resources or payroll).
- Whether users need to print while away from their primary work location, such as workers who move between workstations or travel on business.

When designing your printing configuration, try to give users the same experience in a session as they have when printing from local user devices.

Example print deployment

The following illustration shows the print deployment for these use cases:

- **Branch A -** A small overseas branch office with a few Windows workstations. Every user workstation has a locally attached, private printer.
- **Branch B -** A large branch office with thin clients and Windows-based workstations. For increased efficiency, the users of this branch share network-based printers (one per floor). Windows-based print servers located within the branch manage the print queues.
- **Home office -** A home office with a Mac OS-based user device that accesses the company's Citrix infrastructure. The user device has a locally attached printer.



The following sections describe the configurations which minimize the complexity of the environment and simplify its management.

Auto-created client printers and Citrix Universal printer driver

In Branch A, all users work on Windows-based workstations, therefore auto-created client printers and the Universal printer driver are used. Those technologies provide these benefits:

- Performance - Print jobs are delivered over the ICA printing channel, thus the print data can be compressed to save bandwidth.
  To ensure that a single user printing a large document cannot degrade the session performance of other users, a Citrix policy is configured to specify the maximum printing bandwidth.

  An alternative solution is to leverage a multi-stream ICA connection, in which the print traffic is transferred within a separate low priority TCP connection. Multi-stream ICA is an option when Quality of Service (QoS) is not implemented on the WAN connection.

- Flexibility - Use of the Citrix Universal printer driver ensures that all printers connected to a client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center.

Citrix Universal Print Server

In Branch B, all printers are network-based and their queues are managed on a Windows print server, thus the Citrix Universal Print Server is the most efficient configuration.

All required printer drivers are installed and managed on the print server by local administrators. Mapping the printers into the virtual desktop or application session works as follows:

- For Windows-based workstations - The local IT team helps users connect the appropriate network-based printer to their Windows workstations. This enables users to print from locally-installed applications.
  During a virtual desktop or application session, the printers configured locally are enumerated through autocreation. The virtual desktop or application then connects to the print server as a direct network connection if possible.

  The Citrix Universal Print Server components are installed and enabled, thus native printer drivers are not required. If a driver is updated or a printer queue is modified, no additional configuration is required in the data center.

- For thin clients - For thin client users, printers must be connected within the virtual desktop or application session. To provide users with the simplest printing experience, administrators configure a single Citrix Session Printer policy per floor to connect a floor's printer as the default printer.
  To ensure the correct printer is connected even if users roam between floors, the policies are filtered based on the subnet or the name of the thin client. That configuration, referred to as proximity printing, allows for local printer driver maintenance (according to the delegated administration model).

  If a printer queue needs to be modified or added, Citrix administrators must modify the respective Session printer policy within the environment.

Because the network printing traffic will be sent outside the ICA virtual channel, QoS is implemented. Inbound and outbound network traffic on ports used by ICA/HDX traffic are prioritized over all other network traffic. That configuration ensures that user sessions are not impacted by large print jobs.

Auto-created client printers and Citrix Universal printer driver

For home offices where users work on non-standard workstations and use non-managed print devices, the simplest approach is to use auto-created client printers and the Universal printer driver.

Deployment summary

In summary, the sample deployment is configured as follows:

- No printer drivers are installed on 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

Sep 09, 2015

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.
- 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 to ensure 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.

- 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

Jun 01, 2016

When users access printers from published applications, you can configure Citrix policies to specify:

- How printers are provisioned (or added to sessions)
- How print jobs are routed
- How printer drivers are managed

You can have different printing configurations for different user devices, users, or any other objects on which policies are filtered.

Most printing functions are configured through the Citrix Printing policy settings. Printing settings follow standard Citrix policy behavior.

The system can write printer settings to the printer object at the end of a session or to a client printing device, provided the user's network account has sufficient permissions. By default, Citrix 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 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

Jul 08, 2016

There are three printer provisioning methods:

- Citrix Universal Print Server
- Auto-created client printers
- Administrator-assigned session printers

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.

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 using the graphical interface 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 Use the standalone VDA installer.
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 pre-requisite from the \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
   - Cdf_x64 / Cdf_x86
     - x86 for 32-bit, x64 for 64-bit
5. Find the UPClient component in \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
6. Install the UPClient component by extracting and then launching the component's MSI.

7. A restart is required after installing the UPClient component.

Opt out of CEIP for the Universal Print Server

You are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP) when you install the Universal Print Server. The first upload of data occurs after seven days from the date and time of installation.

To opt out of CEIP, edit the registry key **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** and set the **DWORD** value to **0**.

To opt back in, set the DWORD value to 1.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

For more information, see Citrix Insight Services.

Configure the Universal Print Server

Use the following Citrix policy settings to configure the Universal Print Server. For more information, refer to the on-screen policy settings help.

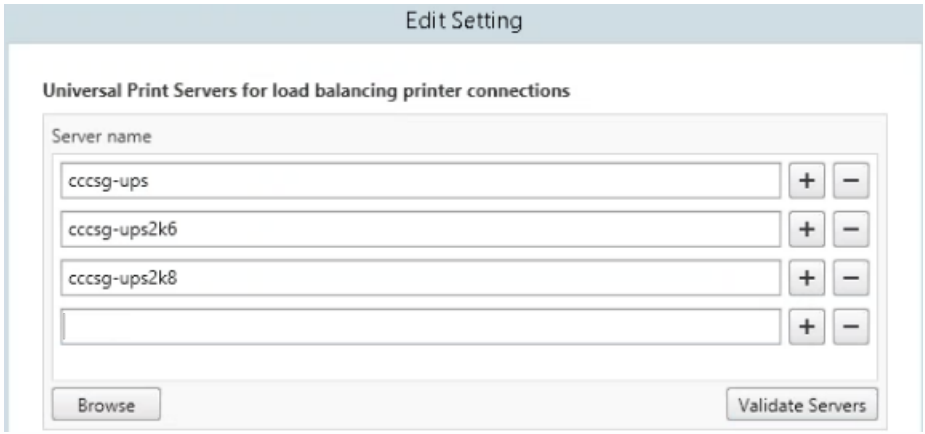
- **Universal Print Server enable**. Universal Print Server is disabled by default. When you enable Universal Print Server, you choose whether to use the Windows Print Provider if the Universal Print Server is unavailable. After you enable the Universal Print Server, a user can add and enumerate network printers through the Windows Print Provider and Citrix Provider interfaces.
- **Universal Print Server print data stream (CGP) port**. Specifies the TCP port number used by the Universal Print Server print data stream CGP (Common Gateway Protocol) listener. Defaults to **7229**.
- **Universal Print Server web service (HTTP/SOAP) port**. Specifies the TCP port number used by the Universal Print Server listener for incoming HTTP/SOAP requests. Defaults to **8080**.

To change the default port of HTTP 8080 for Universal Print Server communication to 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. 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.



- **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. For more information, see Universal Print Server policy settings.

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.

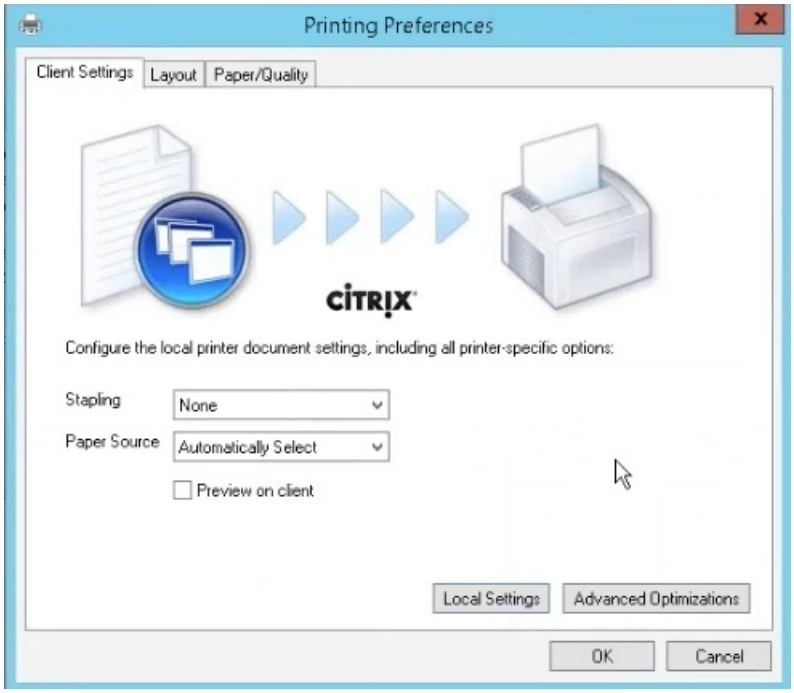
Policy setting	Interaction
Client printer redirection, Auto-create client printers	After the Universal Print Server is enabled, client network printers are created using the Universal print driver instead of the native drivers. Users see the same printer name as before.
Session printers	When you use 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 can be created to the print server, using the Universal print driver.
UPD preference	Supports EMF and XPS drivers.

Effects on user interfaces - The Citrix Universal print driver used by the Universal Print Server disables the following user interface controls:

- In the Printer Properties dialog box, the Local Printer Settings button
- In the Document Properties dialog box, the Local Printer Settings and Preview on client buttons

The Citrix XPS Universal print driver 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.

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 XPS 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.
- Auto-create generic universal printer. Enables or disables auto-creation of the generic Citrix Universal Printer object for sessions when a user device compatible with Universal Printing is in use. By default, the generic Universal Printer object is not auto-created.
- Universal driver preference. Specifies the order in which the system attempts to use Universal print drivers, beginning with the first entry in the list. You can add, edit, or remove drivers and change the order of the drivers in the list.
- Universal printing preview preference. Specifies whether to use the print preview function for auto-created or generic universal printers.
- Universal printing EMF processing mode. Controls the method of processing the EMF spool file on the Windows user device. By default, EMF records are spooled directly to the printer. Spooling directly to the printer allows the spooler to process the records faster and uses fewer CPU resources.

For more policies, see Optimize printing performance. To change the defaults for settings such as paper size, print quality, color, duplex, and the number of copies, see CTX113148.

Auto-create printers from the user device - At the start of a session, the system auto-creates all printers on the user device by default. You can control what, if any, types of printers are provisioned to users and prevent autocreation.

Use the Citrix policy setting Auto-create client printers to control autocreation. You can specify that:

- All printers visible to the user device, including network and locally attached printers, are created automatically at the start of each session (default)
- All local printers physically attached to the user device is created automatically
- Only the default printer for the user device is created automatically
- Autocreation is disabled for all client printers

The Auto-create client printers setting requires that the Client printer redirection setting is Allowed (the default).

Assign network printers to users

By default, network printers on the user device are created automatically at the beginning of sessions. The system enables you to reduce the number of network printers that are enumerated and mapped by specifying the network printers to be created within each session. Such printers are referred to as session printers.

You can filter session printer policies by IP address to provide proximity printing. Proximity printing enables users within a specified IP address range to automatically access the network printing devices that exist within that same range. Proximity printing is provided by the Citrix Universal Print Server and does not require the configuration described in this section.

Proximity printing might involve the following scenario:

- The internal company network operates with a DHCP server which automatically designates IP addresses to users.
- All departments within the company have unique designated IP address ranges.

- Network printers exist within each department's IP address range.

When proximity printing is configured and an employee travels from one department to another, no additional printing device configuration is required. Once the user device is recognized within the new department's IP address range, it will have access to all network printers within that range.

Configure specific printers to be redirected in sessions - To create administrator-assigned printers, configure the Citrix policy setting Session printers. Add a network printer to that policy using one of the following methods:

- Enter the printer UNC path using the format \\servername\printername.
- Browse to a printer location on the network.
- Browse for printers on a specific server. Enter the server name using the format \\servername and click Browse.

Important: The server merges all enabled session printer settings for all applied policies, starting from the highest to lowest priorities. When a printer is configured in multiple policy objects, custom default settings are taken from only the highest priority policy object in which that printer is configured.
Network printers created with the Session printers setting can vary according to where the session was initiated by filtering on objects such as subnets.

Specify a default network printer for a session - By default, the user's main printer is used as the default printer for the session. Use the Citrix policy setting Default printer to change how the default printer on the user device is established in a session.

1. On the Default printer settings page, select a setting for Choose client's default printer:
   - Network printer name. Printers added with the Session printers policy setting appear in this menu. Select the network printer to use as the default for this policy.
   - Do not adjust the user's default printer. Uses the current Terminal Services or Windows user profile setting for the default printer. For more information, refer to the on-screen policy settings help.
2. Apply the policy to the group of users (or other filtered objects) you want to affect.

Configure proximity printing - Proximity printing is also provided by the Citrix Universal Print Server, which does not require the configuration described here.

1. Create a separate policy for each subnet (or to correspond with printer location).
2. In each policy, add the printers in that subnet's geographic location to the Session printers setting.
3. Set the Default printer setting to Do not adjust the user's default printer.
4. Filter the policies by client IP address. Be sure to update these policies to reflect changes to the DHCP IP address ranges.

Maintain the printing environment

Jun 01, 2016

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.

Map client printer drivers - Each client provides information about client-side printers during logon, including the printer driver name. During client printer autocreation, Windows server printer driver names are selected that correspond to the printer model names provided by the client. The autocreation process then uses the identified, available printer drivers to construct redirected client print queues.

Here is the general process for defining driver substitution rules and editing print settings for mapped client printer drivers:

1. To specify driver substitution rules for auto-created client printers, configure the Citrix policy setting Printer driver mapping and compatibility by adding the client printer driver name and selecting the server driver that you want to substitute for the client printer driver from the Find printer driver menu. You can use wildcards in this setting. For example, to force all HP printers to use a specific driver, specify HP* in the policy setting.
2. To ban a printer driver, select the driver name and choose the Do not create setting.
3. As needed, edit an existing mapping, remove a mapping, or change the order of driver entries in the list.
4. To edit the printing settings for mapped client printer drivers, select the printer driver, click Settings, and specify settings such as print quality, orientation, and color. If you specify a printing option that the printer driver does not support, that option has no effect. This setting overrides retained printer settings the user set during a previous session.
5. Citrix recommends testing the behavior of the printers in detail after mapping drivers, since some printer functionality can be available only with a specific driver.

When users log on the system checks the client printer driver compatibility list before it sets up the client printers.

Optimize printing performance

To optimize printing performance, use the Universal Print Server and Universal print driver. The following policies control printing optimization and compression:

- Universal printing optimization defaults. Specifies default settings for the Universal Printer when it is created for a session:
  - Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
  - Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.
  - Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached.
  - Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.
- Universal printing image compression limit. Defines the maximum quality and the minimum compression level available for images printed with the Universal print driver. By default, the image compression limit is set to Best Quality (lossless compression).
- Universal printing print quality limit. Specifies the maximum dots per inch (dpi) available for generating printed output in the session. By default, no limit is specified.

By default, all print jobs destined for network printers route from the 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.

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	UAC Enabled?	Location
Client printers (Printers attached to the user device)	Client printing pathway	On	Print Management snap-in located in the Microsoft Management Console
		Off	Pre-Windows 8: Control Panel Windows 8: Print Management snap-in
Network printers (Printers on a network print server)	Network printing pathway	On	Print Server > Print Management snap-in located in the Microsoft Management Console
		Off	Print Server > Control Panel
Network printers (Printers on a network print server)	Client printing pathway	On	Print Server > Print Management snap-in located in the Microsoft Management Console
		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	On	Print Server > Control Panel

	Printing Pathway	UAC Enabled?	Location
		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.

HDX

Jun 01, 2016

Citrix HDX includes a broad set of technologies that provide a high-definition user experience.

At the device	HDX leverages the computing capacity of user devices to enhance and optimize the user experience. HDX MediaStream technology ensures 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, balancing performance and bandwidth by applying the best technologies for each unique user scenario, whether the desktop or application is accessed locally on the corporate network or remotely from outside the corporate firewall.
In the datacenter	HDX leverages the processing power and scalability of servers to deliver advanced graphical performance, regardless of the capabilities of the client device. Compressed multimedia information is sent directly to the user device in its native format. HDX channel monitoring provided by Citrix Director displays the status of connected HDX channels on user devices. HDX Insight, the integration of Network Inspector and Performance management with Director, captures data about ICA traffic and provides a dashboard view of real-time and historical details such as client-side and server-side ICA session latency, bandwidth use of ICA channels, and the ICA round trip time value of each session.

To experience HDX capabilities from your virtual desktop:

- See how HDX delivers rich video content to virtual desktops: View a video on a web site containing high definition videos, such as http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.
- See how Flash Redirection accelerates delivery of Flash multimedia content:
  1. Download Adobe Flash player (http://get.adobe.com/flashplayer/) and install it on both the virtual desktop and the user device.
  2. On the Desktop Viewer toolbar, click Preferences. In the Desktop Viewer Preferences dialog box, click the Flash tab and select Optimize content.
  3. To experience how Flash Redirection accelerates the delivery of Flash multimedia content to virtual desktops, view a video on your desktop from a web site containing Flash videos, such as YouTube. Flash Redirection is designed to be seamless so that users do not know when it is running. You can check to see whether Flash Redirection is being used by looking for a block of color that appears momentarily before the Flash player starts.
- 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, with no configuration required. Citrix

policy settings that provide the best out-of-the-box experience for the majority of 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 delivers a Windows Aero experience to virtual desktop users on any client.
- 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 Windows Media redirection to play media run-time files on user devices rather than the host server. In most cases, no adjustments to the Windows Media feature policies are needed.

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 further optimize the user experience, improve server scalability, or reduce bandwidth requirements. For information about working with Citrix policies and policy settings, see the *— Citrix policies* documents for this release.
- For instructions that include working with 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.

Reduce the bandwidth needed for Windows desktops

By default, HDX delivers a highly responsive Windows Aero or Windows 8 desktop experience to virtual desktops accessed from supported Windows user devices. To do that, HDX leverages the graphics processing unit (GPU) or integrated graphics processor (IGP) on the user devices for local DirectX graphics rendering. This feature, named desktop composition redirection, maintains high scalability on the server. For details, see What to do with all these choices in http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/.

To reduce the bandwidth required in user sessions, consider adjusting the following Citrix policy settings. Keep in mind that changing these settings can reduce the quality of the user experience.

- **Desktop Composition Redirection**. Applies only to Windows Desktop OS machines accessed from Windows user devices and applies only to the composition of the Windows desktop. Application windows are rendered on the server unless the Citrix policy setting Allow local app access is Allowed.
- **Desktop Composition Redirection graphics quality**. Uses high-quality graphics for desktop composition unless seamless applications or Local App Access are enabled. To reduce bandwidth requirements, lower the graphics quality.
- **Dynamic windows preview**. Controls the display of seamless windows in Flip, Flip 3D, taskbar preview, and peek window preview modes. To reduce bandwidth requirements, disable this policy setting.

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).
- Target frame rate. Specifies the maximum number of frames per second that are sent from the virtual desktop to the user device (default = 30). In many circumstances, you can improve the user experience by specifying a higher value. For devices with slower CPUs, specifying a lower value can improve the user experience.

- 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. Color depths other than 32-bit are available only if the Legacy graphics mode policy setting is enabled.

Improve video conference performance

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 uses significantly less bandwidth compared to the isochronous HDX Plug-n-Play support, and works well over WAN connections.

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 with the policy settings under ICA policy settings > USB Devices policy settings.

HDX webcam video compression is enabled by default on Citrix Receiver for Windows but must be configured on Citrix Receiver for Linux. For more information, refer to the Citrix Receiver documentation. 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 uses additional bandwidth and is not suitable for a low bandwidth network. To force software compression over low bandwidth networks, add the following DWORD key value to the registry key: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Choose server scalability over user experience

For deployments where server scalability is of greater concern than user experience, you can use the legacy graphics system by adding the Legacy graphics mode policy setting and configuring the individual legacy graphics policy settings. Use of the legacy graphics system affects the user experience over WAN and mobile connections.

Thinwire Compatibility Mode

Oct 06, 2015

Thinwire Compatibility Mode uses new screen decomposition and caching techniques, which achieve low bandwidth usage and high server scalability without compromising the end-user experience.

Thinwire Compatibility Mode includes the following features:

- Intelligent bitmap matching for a bitmap-only provider.
  - Bitmap translation analysis for efficient window movement and scrolling.
- Backwards compatible. There is no requirement for client or Citrix Receiver upgrades or hardware acceleration.
  - Tested on a range of older thin clients up to and over 5 years old.
- Optimized for very low server CPU usage and improved server scalability.
- An emulated 16-bit mode, which reduces bandwidth by a further 15-20% for typical workloads.
- Transient detection for server-rendered video content.
  - Multi-transient handling for an improved multimedia experience. For example, when watching multiple videos or ticker tapes.
  - Selective sharpening for regions that leave a transient state.
- Optimized for CloudBridge acceleration. In tests, we have seen up to a 6:1 ratio of bandwidth reduction on Office-type workloads.
- Adaptive display, which can be tuned through policy settings. For more information see **Moving image compression** in Moving image policy settings.
- VDA's and Windows OS's up to and including Windows 10 VDA are supported.
- New "Build to Lossless" mode for 3D Pro, which improves responsiveness, interactivity, and interruptible sharpening for a better user experience on low bandwidth.
- Default static photographic imagery quality is higher than in Legacy Graphics Mode.

For Visual Quality settings "Low", "Medium" (default) and "High", the transient detector dynamically evaluates screen updates to decide whether highly-animated areas should be sent at lower quality, in accordance with the Adaptive Display policy, to improve client performance and reduce bandwidth usage.

For the **Build to lossless** visual quality, Thinwire Compatibility Mode uses a "fuzzy-first" approach for large screen updates. This setting is targeted at 3D Pro users who are manipulating 3D models or other graphic-intensive applications. If the activity continues, a transient mode is assumed and the affected area is sharpened and cached once transient activity stops. For the initial large change, some lightweight image analysis is performed on the change area to determine whether to use "fuzzy transient" or "sharp transient" (lossless) - for example, when rotating a wireframe. It is more efficient, for FPS (Frames Per Second) and bandwidth, to encode simple imagery using the Citrix lossless codec and no loss in quality occurs.

The sharpen-to-lossless step in Build to lossless is also different. Rather than sharpening the affected area in one step, the area is sharpened in pre-determined blocks to help maintain interactivity and a smooth user experience. Sharpening a large change area mid-transient, for example moving a 3D model which is stopped briefly, then moved again, would previously cause a "stall", especially over a low bandwidth line. The size of the sharpening blocks depends on how far the quality was reduced to try and maintain the target minimum frame rate, which is an Adaptive Display policy setting. If the quality was significantly reduced, the sharpening block size will be smaller, with a minimum size of 128 x 128 pixels. If the quality was not reduced, for example, when the client has adequate processing power and bandwidth, the sharpening block size can be a maximum size of 384 x 384 pixels.

Framehawk virtual channel

Feb 24, 2016

Introduction

The Framehawk virtual channel optimizes the delivery of virtual desktops and applications to users on broadband wireless and lossy long-haul broadband network connections, when high packet loss or congestion occurs. You can use Citrix policies to implement either Framehawk or Thinwire for a set of users in a way that is appropriate for your network characteristics, and is aligned with overall scalability and performance expectations.

Generally, user experience has focused on frame rate and visual quality as a basis for a positive user experience. Framehawk enhances the definition to account for linearity. Users need to enjoy the experience, not be distracted by it. Under degraded network circumstances, users struggle with the "rubber band" effect that plagues all protocols. This effect includes the tapping-waiting-tapping syndrome where a user isn't sure if the screen will respond, resulting in extra errant clicks by the user, creating more and more undesirable results. Framehawk smooths out those experiences, especially under strenuous network conditions.

High-speed home Internet connections frequently exhibit performance issues, whether due to collisions with neighboring Wi-Fi signals or spectral interference from cordless devices, among others. More and more users are connecting to hosted apps and data via 3G or 4G/LTE cellular networks, or using inflight Internet services. Others like to take advantage of public Wi-Fi hotspots while stopping for a coffee break or at hotels where congestion is a common problem.

With Framehawk, users notice a more interactive experience (a more linear echoback of characters) at high latencies.

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 it comes to areas of the screen that are changing rapidly, like video or moving graphics, it doesn't matter to the human eye if some pixels are lost along the way because they are quickly overwritten with new data.

But when it comes to static areas of the screen, such as the icons in the systray or a toolbar, or text after scrolling to where the user wants to start reading, the human eye is very fussy; a user expects those areas to be pixel perfect. Unlike protocols that aim 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 QoS 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).

The Framehawk Intent Engine distinguishes between scrolling up or down, zooming, moving to the left or right, reading, typing, and other common actions, and 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 needs to be excellent. If the user is scrolling, it

should 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 (which we call "gearing", analogous to the tension on a bicycle chain), the Framehawk logic can react 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 well-suited to a broad range of access scenarios and network conditions, it is TCP-based for reliable data communications and therefore must retransmit packets on a lossy or overburdened network, leading to lag in the user experience.

Framehawk is UDP based, taking a best-effort approach at data transmission. UDP is just a small part of how Framehawk overcomes lossiness, as can be seen when comparing the performance of Framehawk with other UDP-based protocols, but it provides an important foundation to the human-centric techniques that sets 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 or 5 Mbps plus about 150 Kbps per concurrent user.

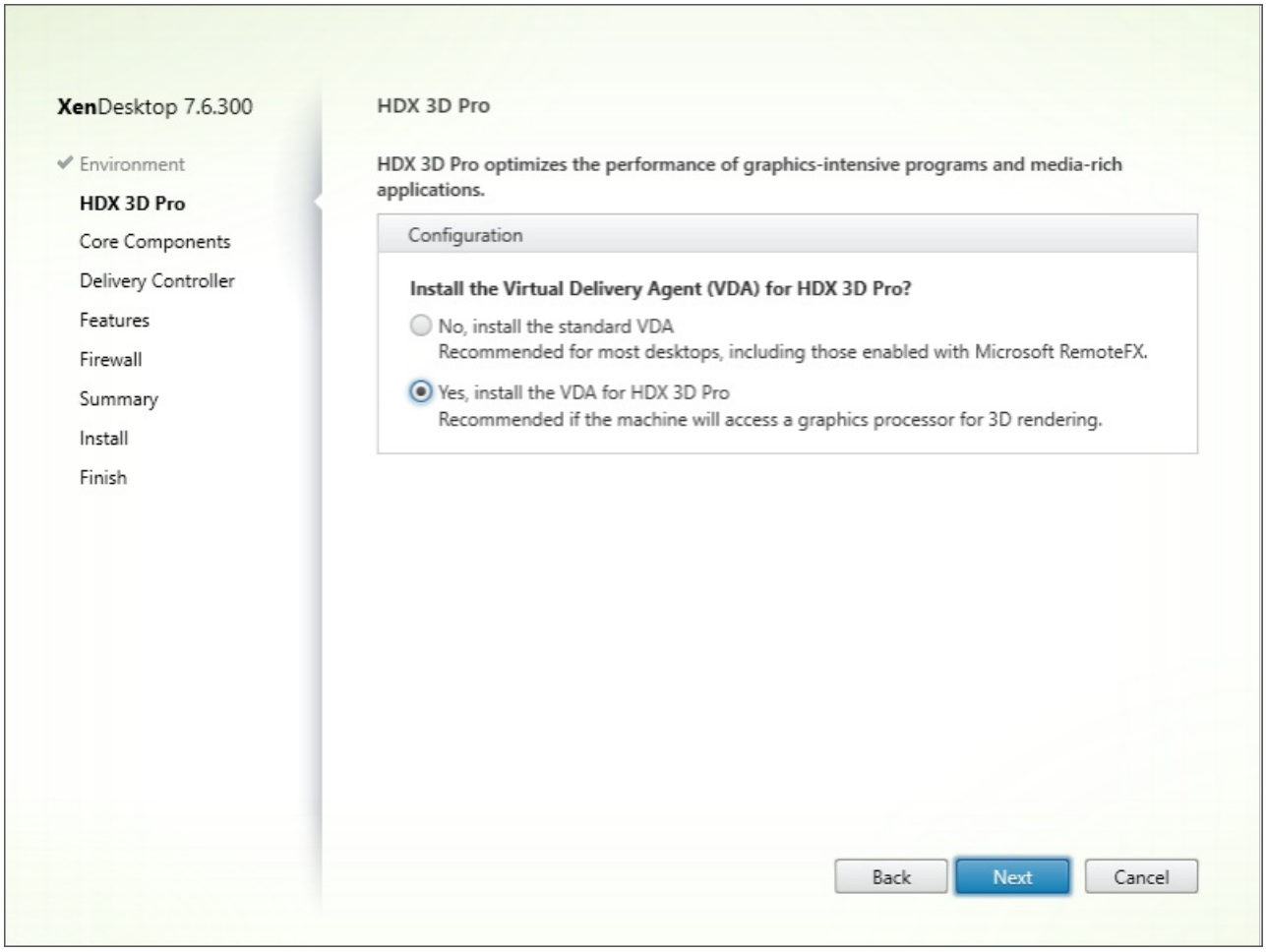
The Citrix bandwidth recommendation for Thinwire is generally a base of 1.5 Mbps plus 150 Kbps per user (for more detail, refer to XenApp and XenDesktop bandwidth blog), but at 3% packet loss you will find that Thinwire needs much more bandwidth than Framehawk to maintain a positive user experience.

Note: 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.

Framehawk and HDX 3D Pro

Framehawk now supports all the HDX 3D Pro use cases, both for XenApp (server OS) and XenDesktop (desktop OS) apps. In early previews, it has been validated in customer environments with 400-500 ms latency and 1-2% packet loss, 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.

Enabling this functionality doesn't require any additional configuration tasks. When installing the VDA, select the 3DPro option at the beginning of the installation:



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 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, you need to 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.

Consider the following best practices before implementing Framehawk virtual channels:

- 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.
- In many cases, NetScaler Gateway might be installed in the DMZ, flanked by firewalls on both the external as well as the internal side. Ensure UDP port 443 is open on the external firewall, and 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 experiencing high packet loss. It is also recommended that you do not enable Framehawk as a universal policy for all objects in the Site.

The Framehawk virtual channel is disabled by default. When enabled, the server attempts to use the Framehawk virtual channel for users' 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:

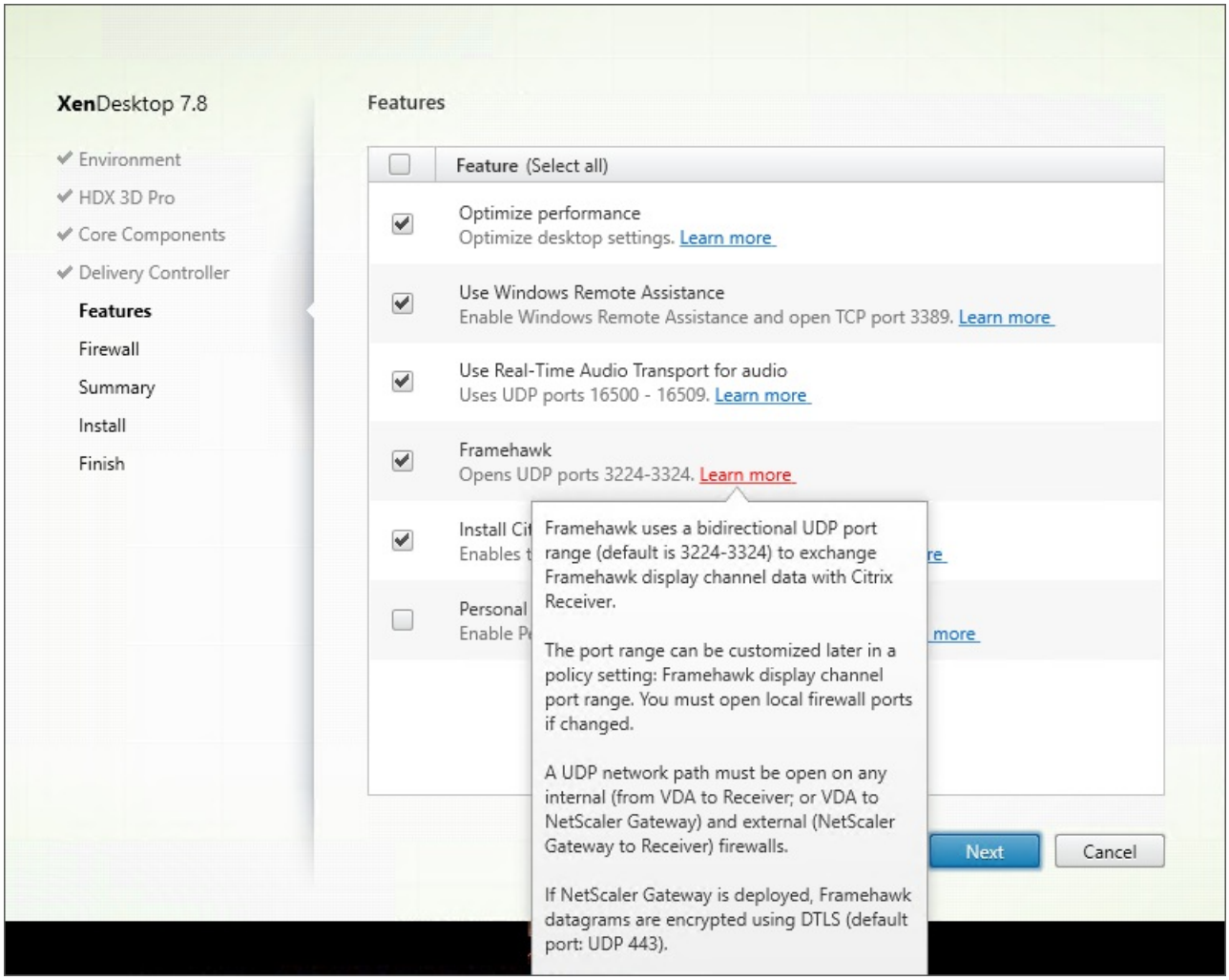
- Framehawk display channel: Enables or disables the feature.
- Framehawk display channel port range: Specifies the range of UDP port numbers (lowest port number to highest port number) that the VDA uses to exchange Framehawk display channel data with the user device. The VDA attempts to use each port, starting with the lowest port number and incrementing for each subsequent attempt. The port handles inbound and outbound traffic.

Opening ports for the Framehawk display channel

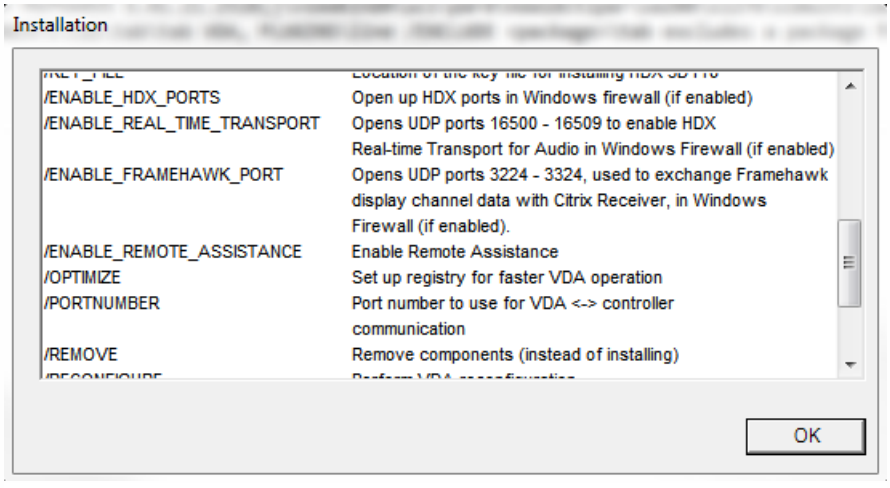
In release 7.8, a new option is available to reconfigure the Firewall during the **Features** step of the VDA installer. This checkbox opens UDP ports 3224-3324 on the Windows Firewall, if selected. Please note that manual Firewall configuration is required in some circumstances:

- for any network Firewalls, or
- if the default port range is customized.

To open these UDP ports, select the **Framehawk** checkbox:

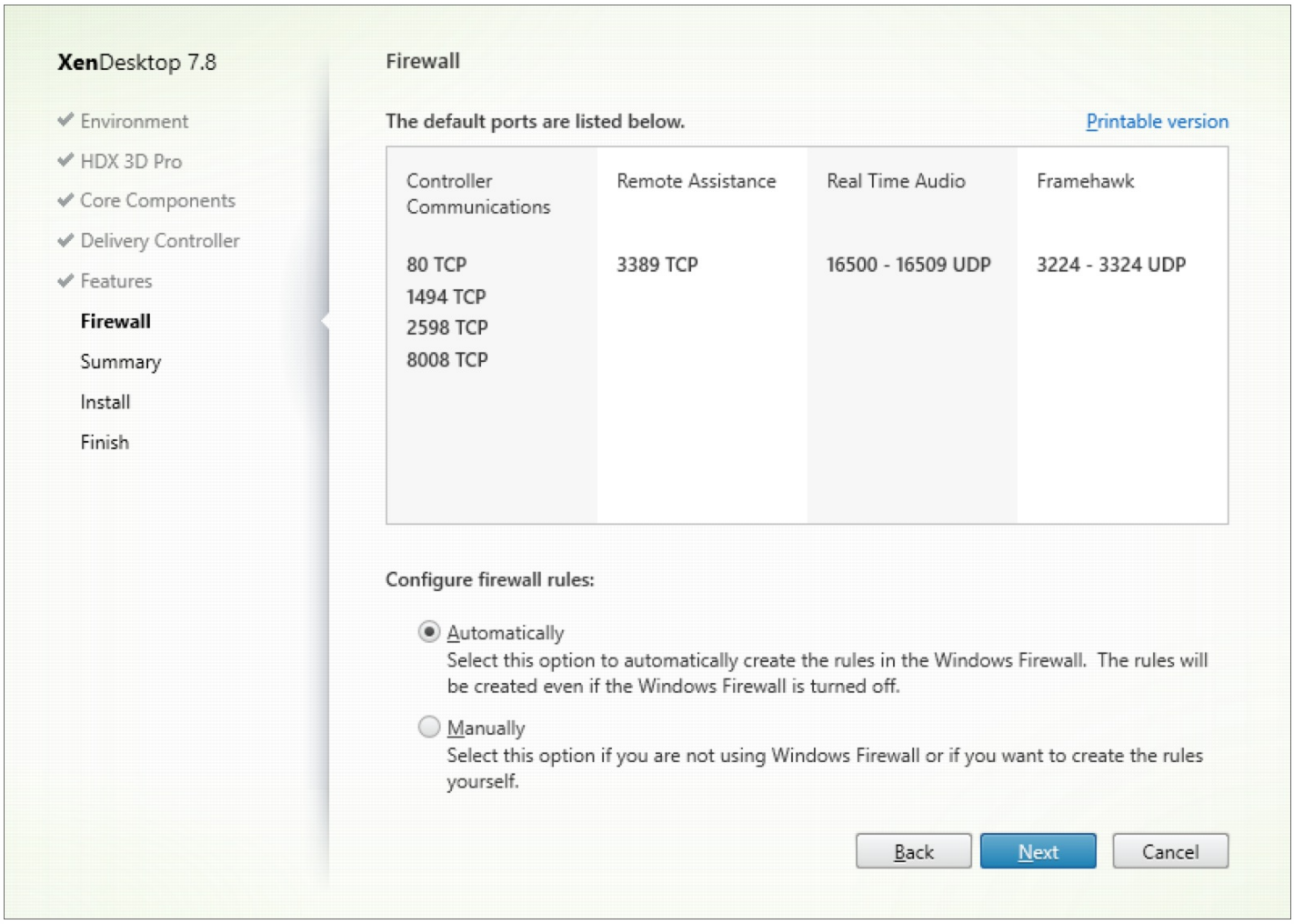


You can also use the command line to open UDP ports for the Framehawk virtual channel using **/ENABLE_FRAMEHAWK_PORT**:

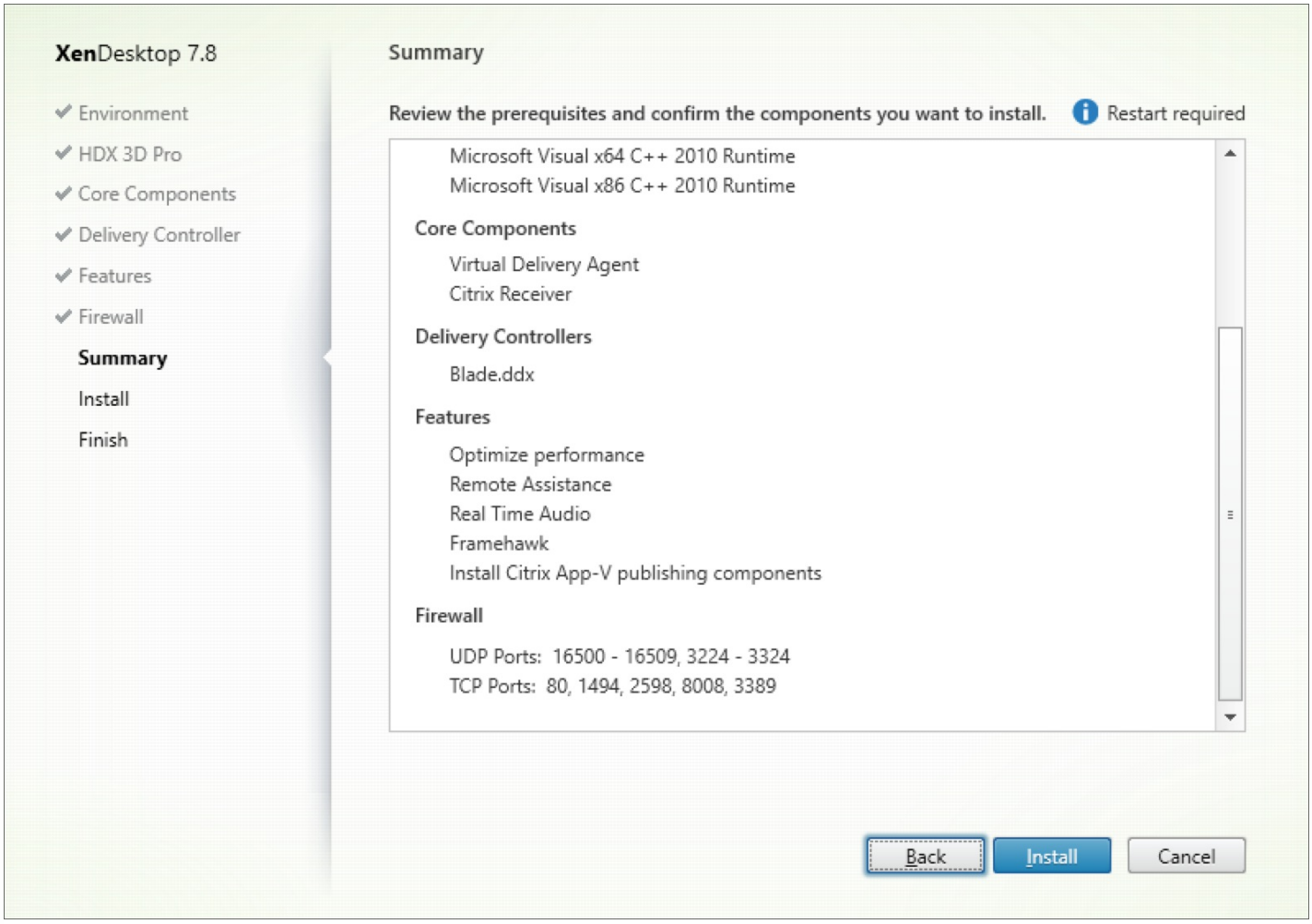


Verifying Framehawk UDP port assignments

During installation, you can verify the UDP ports assigned to the Framehawk virtual channel in the **Firewall** screen:



The **Summary** screen indicates if the Framehawk virtual channel feature is enabled:



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 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 will have the public IP and the Gateway VPN vServer will have a dummy IP.

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.

The following scenarios are not supported with Framehawk:

- HDX Insight
- NetScaler Gateway in IPv6 mode
- NetScaler Gateway Double Hop
- Multiple Secure Ticket Authority (STA) on NetScaler Gateway
- NetScaler Gateway with High Availability (HA)
- 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 (STA) on NetScaler Gateway	No
NetScaler Gateway with High Availability (HA)	No
NetScaler Gateway with Cluster setup	No

Configuring NetScaler for Framehawk support

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.

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; note that this is not required if you are using NetScaler version 11.0.64.34 or

later.

To configure NetScaler Gateway for Framehawk support:

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 additional 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.

Additional 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 configurd. For additional information, refer to the 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*.

Support for other VPN products

NetScaler Gateway is the only SSL VPN product to support the UDP encryption required by Framehawk. The Framehawk policy may fail to apply if another SSL VPN or an incorrect version of NetScaler Gateway is used. Traditional IPSec VPN products will support Framehawk without any modifications.

Configure Citrix Receiver for iOS to support Framehawk

To configure 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 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.

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 the Framehawk virtual channel in any session. To view Framehawk-related metrics, select **Graphics-Framehawk**.

If the Framehawk connection is established, you will 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

Jun 01, 2016

HDX 3D Pro enables you to deliver desktops and applications that perform best with a graphics processing unit (GPU) for hardware acceleration, including 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 What to specify when installing a VDA in the Prepare to install article.

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 wide area network (WAN) connections: Deliver an interactive user experience over WAN connections with bandwidths as low as 1.5 Mbps.
- On local area network (LAN) connections: Deliver a user experience equivalent to that of a local desktop on LAN connections with bandwidths of 100 Mbps.
  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. When used with Citrix XenServer and NVIDIA GRID GPUs, HDX 3D Pro provides Virtual GPU (vGPU) acceleration for Windows Desktop OS machines. For the supported XenServer versions, see Citrix Virtual GPU Solution.

Use the HDX Monitor tool (which replaces the Health Check 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/.

Flash Redirection

Sep 29, 2015

Flash Redirection offloads the processing of most Adobe Flash content (including animations, videos, and applications) to users' LAN- and WAN-connected Windows 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 Flash Player to be installed on the user device, enable this feature only if the Flash Player itself is secured.

The legacy and second generation versions of Flash Redirection are independent solutions and run in separate virtual channels.

- Legacy Flash Redirection features are supported on the client side only. If an earlier version of the Flash Player is installed on the user device, or if the Flash Player cannot be installed, Flash content renders on the server.
- Second generation Flash Redirection is supported on both clients and servers. If the client supports second generation Flash Redirection, Flash content renders on the client. Second generation 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 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.

- Flash default behavior establishes the default behavior of Flash acceleration. 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. It 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.
- Flash server-side content fetching URL list allows you to specify websites whose Flash content can be downloaded to the server and then transferred to the user device for rendering. (By default, Flash Redirection downloads Flash content to the user device, where it is played.) This setting works with (and requires) the Enable server-side content fetching setting on the user device and is intended 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.

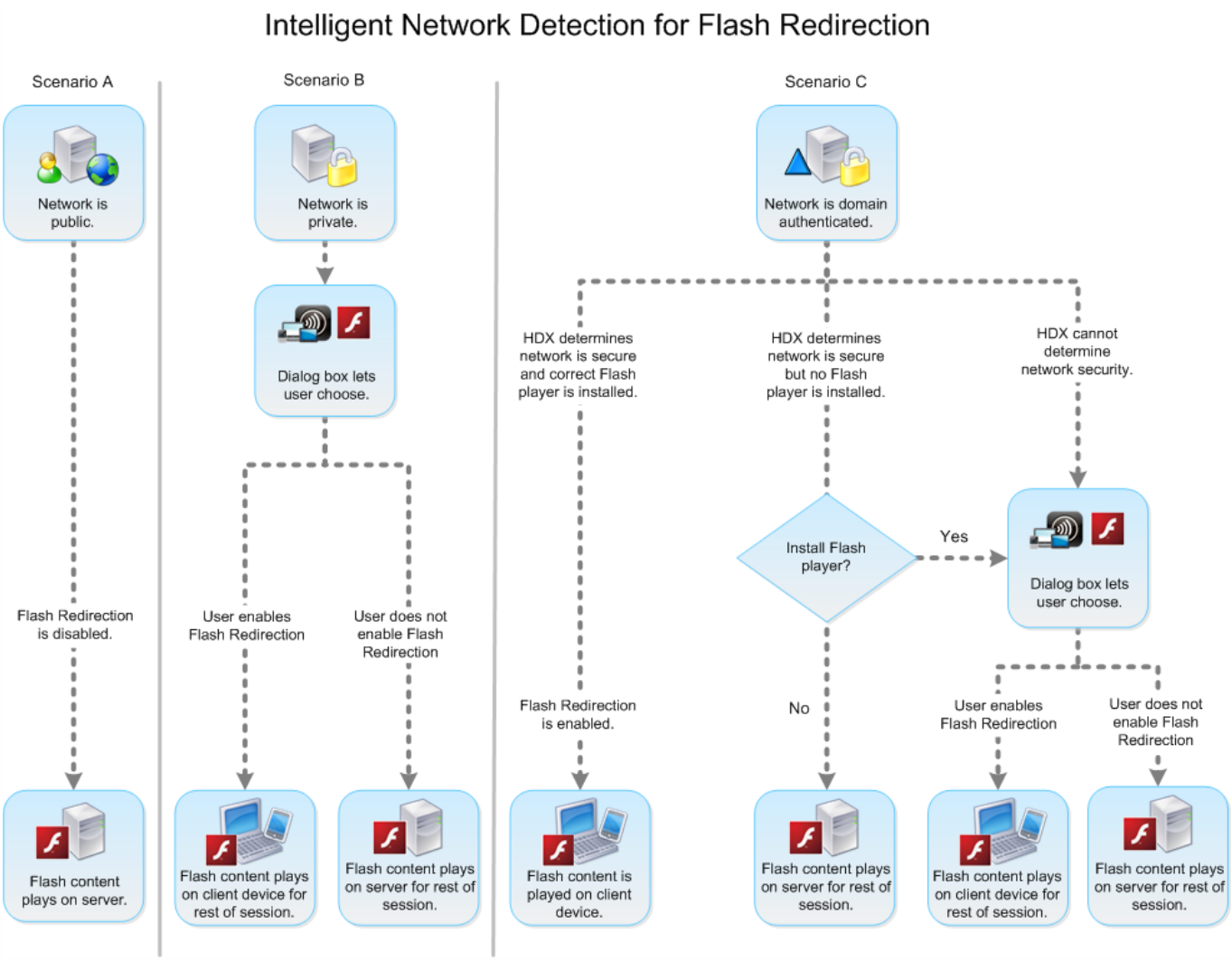
Change when Flash Redirection is used

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.

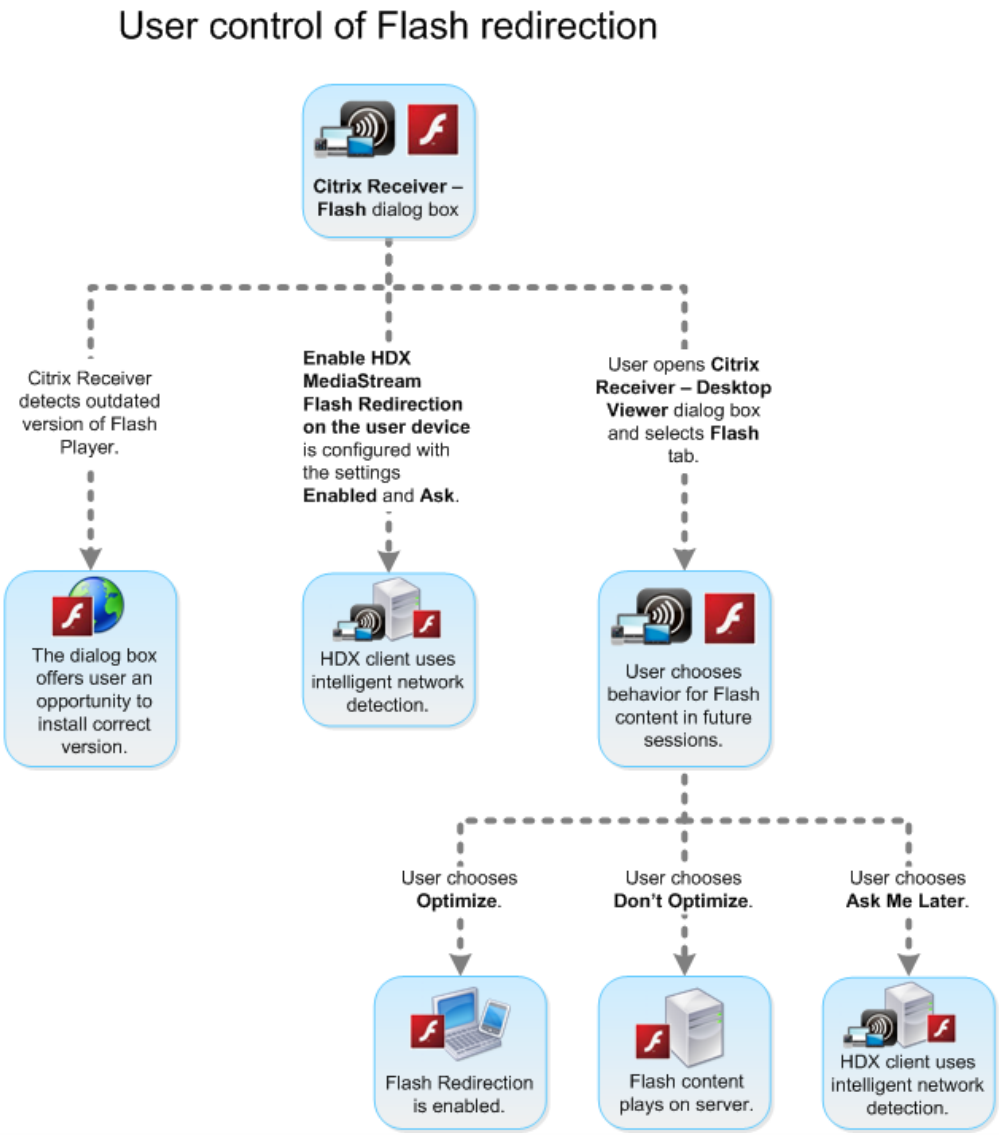
If no configuration is set and Desktop Lock is used, Flash Redirection is enabled on the user device by default.

To change when Flash Redirection is used or to disable Flash Redirection on the user device:

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 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 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 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.
Second generation 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.

With second generation Flash redirection, 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.
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.
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

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.

> **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.

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". Currently, 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.

In order for redirection to occur the client and server minimum checks need to be successful in addition to the check using the comparison mask.

The subkey ClientID0x51 specifies the Linux ICA Client. The subkey ClientID0x1 specifies the Windows ICA Client. This subkey is named by appending the hexadecimal Client Product ID (without any leading zeros) to the string "ClientID". A full list of Client IDs can be found in the Mobile SDK for Windows Apps documentation
http://www.citrix.com/mobilitysdk/docs/clientdetection.html

32-bit VDA example registry configuration

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] Client agnostic settings

"ClientFlashPlayerVersionMinimum"="13.0" Minimum version required for the ICA client
"ServerFlashPlayerVersionMinimum"="13.0" Minimum version required for the ICA server
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] 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\PseudoServer\ClientID0x51] 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\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0" [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

Host to client redirection

Nov 22, 2016

Content redirection allows you to control whether users access information with applications published on servers or with applications running locally on user devices.

Host to client redirection is one kind 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 located 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.

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 will improve 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 below, rather than host to client redirection; they 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's multimedia player with multimedia redirection.
- The application for the content type is used by only a small number of users who already have the application installed on their user device.
- The VDA cannot access certain web sites (for example, web sites 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 may 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)
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
A web page or document	The VDA cannot access the URL	Host to client redirection
A web page	The web page contains Adobe Flash	Flash redirection

A multimedia file or stream	The VDA has a compatible multimedia player	Multimedia redirection
A multimedia file or stream	The VDA does not have a compatible multimedia player	Host to client redirection
A document	The VDA does not have an application for that document type	Host to client redirection
A document	The document must not be downloaded to the user device	No redirection
A document	The document must not be uploaded to the VDA	Host to client redirection
A custom URL type	The VDA does not have an application for that custom URL type	Host to client redirection

Host to client redirection is supported by Citrix Receiver for Windows, Receiver for Mac, Receiver for Linux, Receiver for HTML5, and Receiver for Chrome.

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 a VDA application's menus or dialogs, provided that the application uses the Windows ShellExecuteEx API.
- Entered in the Windows Run dialog.

Host to client redirection is not used for URLs in a web browser (either in a web page or entered in the address bar of the web browser).

> **Note**
>
> If users change their default web browser on the VDA (for example, by 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 is used to open the URL depends on the configuration of the user device for both the URL type and the content type. For example:

- An HTTP URL with an HTML content type will open in the default web browser.
- An HTTP URL with a PDF content type might open in the default web browser, or it might open in another application.

This user device configuration is not controlled by host to client content redirection. 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)
- 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 with 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 may need to set registry keys and Group Policy for the server VDAs, depending on the VDA's 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 with "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.

ServerFTA.reg COPY

```
<p><b>- Reg file start --</b><br>
Windows Registry Editor Version 5.00<br>
 <br>
[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]<br>
@=&quot;\&quot;C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\&quot; %1&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]<br>
@=&quot;ServerFTA&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]<br>
&quot;ApplicationDescription&quot;=&quot;Server FTA URL.&quot;<br>
&quot;ApplicationIcon&quot;=&quot;C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0&quot;<br>
&quot;ApplicationName&quot;=&quot;ServerFTA&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]<br>
&quot;http&quot;=&quot;ServerFTAHTML&quot;<br>
&quot;https&quot;=&quot;ServerFTAHTML&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]<br>
&quot;Citrix.ServerFTA&quot;=&quot;SOFTWARE\\Citrix\\ServerFTA\\Capabilities&quot;<br>
<b>-- Reg file end --</b></p>
```

Group Policy changes

Create an XML file. Copy the text between **"**xml file start" and "xml file end" below, paste it in the XML file, and then save the file as **ServerFTAdefaultPolicy.xml**.

ServerFTAdefaultPolicy.xml COPY

```
<p><b>-- xml file start --</b><br>
&lt;?xml version=&quot;1.0&quot; encoding=&quot;UTF-8&quot;?&gt;<br>
&lt;DefaultAssociations&gt;<br>
&lt;Association Identifier=&quot;http&quot; ProgId=&quot;ServerFTAHTML&quot; ApplicationName=&quot;ServerFTA&quo
&lt;Association Identifier=&quot;https&quot; ProgId=&quot;ServerFTAHTML&quot; ApplicationName=&quot;ServerFTA&qu
&lt;/DefaultAssociations&gt;<br>
<b>-- xml file end --</b></p>
```

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 remove 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. Enter 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 with semicolons. For example:

customtype1://;customtype2://

Enable host to client redirection for a specific set of web sites

To enable host to client redirection for a specific set of web sites, 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). Enter multiple FQDNs on separate lines. An FQDN may 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

GPU acceleration for Windows Desktop OS

Jul 13, 2016

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 XenServer VMs with GPU Passthrough and XenServer VMs with Virtual GPU (vGPU).

Using XenServer 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 XenServer vGPU, multiple virtual machines can directly access the graphics processing power of a single physical GPU. The true hardware GPU sharing provides full Windows 7 or Windows 10 desktops suitable for users with complex and demanding design requirements. Supported for NVIDIA GRID cards (see NVIDIA GRID), the GPU sharing uses the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems. Also supported for 5th and 6th Generation Intel CPUs with Intel Iris Pro graphics. For more information on these families of Intel processors, see 5th Generation Intel Core Processors and 6th Generation Intel Core i5 Processors.

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 deep compression as the default compression technique for encoding. This provides optimal compression that dynamically adapts to network conditions.
  The H.264-based deep compression codec no longer competes with graphics rendering for CUDA cores on the NVIDIA GPU. The deep compression codec runs on the CPU and provides bandwidth efficiency.

- 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. 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
    - 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 Windows 10, 8 and 7 desktops, 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.

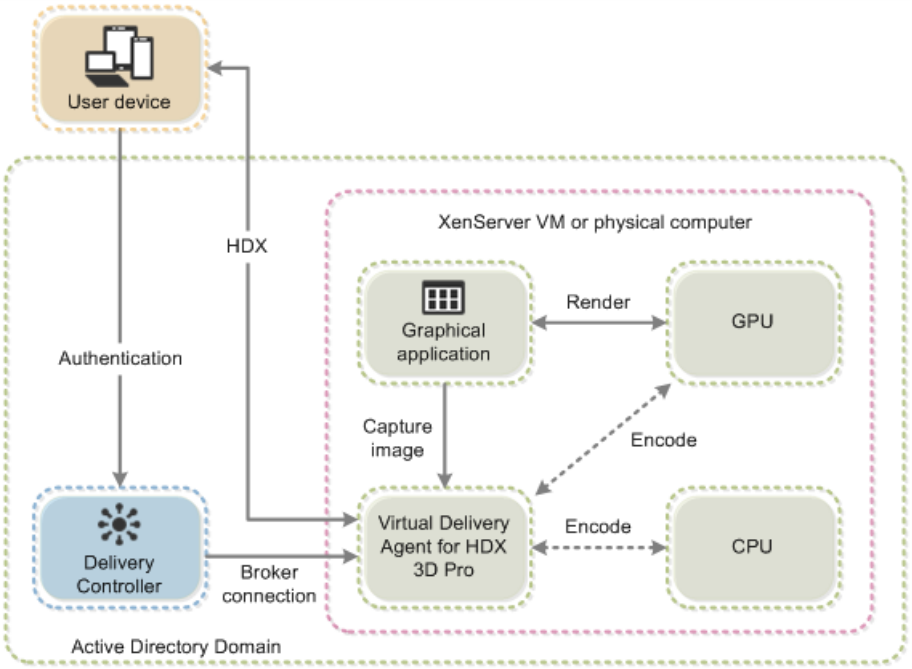
- Support for NVIDIA Kepler architecture. HDX 3D Pro supports NVIDIA GRID cards (see NVIDIA GRID) for GPU passthrough and GPU sharing. NVIDIA GRID vGPU enables multiple VMs to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized 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 5th and 6th Generation Intel CPUs with Intel Iris Pro graphics. HDX 3D Pro supports multi-monitors (up to a maximum of three), console blanking, custom resolution and high frame rate. For more information on the supported families of Intel processors, see 5th Generation Intel Core Processors and 6th Generation Intel Core i5 Processors.

As shown in the following figure:

- The host computer must reside within the same Active Directory domain as the Delivery Controller.
- 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.



Install the VDA for HDX 3D Pro

When you use the installer's graphical interface to install a VDA for Windows Desktop OS, simply 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 for HDX 3D Pro. Similarly, to switch from the standard VDA for Windows Desktop OS to the HDX 3D Pro VDA, uninstall the standard VDA and then install the VDA for HDX 3D Pro.

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.

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: Montereyenable.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 Montereyenable tool provided by NVIDIA.

To disable NVIDIA GRID, run the following command and then restart the VDA: Montereyenable.exe -disable -noreset

Install Intel drivers

This 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.

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.

GPU acceleration for Windows Server OS

Mar 07, 2016

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.

When using HDX 3D Pro, multiple users can share graphics cards. When HDX 3D Pro is used with XenServer GPU Passthrough, a single server hosts multiple graphics cards, one per virtual machine.

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.

Virtual machines require direct passthrough access to a GPU, which is available with Citrix XenServer or VMware vSphere. 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

For example, scalability figures in the range of 8-10 users have been reported on NVIDIA Q6000 and M2070Q cards running applications such as ESRI ArcGIS. These cards offer 6 GB of video RAM. Newer NVIDIA GRID cards offer 8 GB of video RAM and significantly higher processing power (more CUDA cores). With the NVIDIA GRID K2 cards, good performance has been observed with up to 20 users per GRID K2 card. Other applications may scale much higher, achieving 32 concurrent users on a high-end GPU.

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 http://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 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:
  - [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 supported as a Proof of Concept (POC) only. This support is disabled by default, but you can enable it for testing and evaluation purposes.

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

OpenGL Software Accelerator

Sep 11, 2015

The OpenGL Software Accelerator is a software rasterizer for OpenGL applications such as ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD, and CAM. In some cases, the OpenGL Software Accelerator can eliminate the need to use graphics cards to deliver a good user experience with OpenGL applications.

Important: The OpenGL Software Accelerator is provided "as is" and must be tested with all applications. It might not work with some applications and is intended as a solution to try if the Windows OpenGL rasterizer does not provide adequate performance. If the OpenGL Software Accelerator works with your applications, it can be used 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 should you try the OpenGL Software Accelerator?

- If the performance of OpenGL applications running in virtual machines on XenServer or other hypervisors is an issue, try using OpenGL Accelerator. For some applications, the OpenGL Accelerator outperforms the Microsoft OpenGL software rasterizer that is included with Windows because the OpenGL Accelerator leverages 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's graphics adapter. If the graphics card is the latest version, in most cases it will deliver the best performance. If the graphics card is an earlier version or does not delivery satisfactory performance, then try the OpenGL Software Accelerator.
- 3D OpenGL applications that are not adequately delivered using CPU-based software rasterization may benefit from OpenGL GPU hardware acceleration. This feature can be used on bare metal or virtual machines.

Audio features

Jun 01, 2016

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: Most audio features are transported using the ICA stream and are secured in the same way as other ICA traffic. User Datagram Protocol (UDP) audio uses a separate, unsecured, transport mechanism when NetScaler Access Gateway is not in path. If NetScaler Access Gateway is configured to access XenApp and XenDesktop resources, then audio traffic between the endpoint device and NetScaler Access Gateway is secured using DTLS protocol.

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. This 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.

Consider creating separate policies for groups of dial-up users and for those who connect over a LAN or WAN. Over dial-up connections, where bandwidth typically is limited, download speed is often more important to users than sound quality. Therefore, you may want to create one policy for dial-up connections that applies high compression levels to sound, and another for LAN or WAN connections that applies lower compression levels.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device; see Audio setting policies for user devices.

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, add the Client audio redirection setting, which is Allowed by default.

Client audio mapping may cause a heavy 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.

Client microphone redirection

To allow users to record audio using input devices such as microphones on the user device add the Client microphone redirection setting, which is Allowed by default.

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.

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.

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 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.

Audio over UDP Real-time Transport and Audio UDP port range

By default, Audio over 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.
Important: Audio data transmitted with UDP is not encrypted when NetScaler Access Gateway is not in path. If NetScaler Access Gateway is configured to access XenApp and XenDesktop resources then audio traffic between the endpoint device and NetScaler Access Gateway is secured using 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 is16500 - 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.

Audio setting policies for user devices

1. Load the group policy templates by following Configure Receiver with the Group Policy Object 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.
   - **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 Access Gateway, select **Allow Real-Time Transport Through gateway**. NetScaler Access Gateway should 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.

command COPY

```
<p>; This is to enable Real-Time Transport</p>
<p>EnableRtpAudio=true</p>
<p>; This is to Allow Real-Time Transport Through gateway</p>
<p>EnableUDPThroughGateway=true</p>
<p>; This is to set audio quality to Medium</p>
<p>AudioBandwidthLimit=1-</p>
<p>; UDP Port range</p>
<p>RtpAudioLowestPort=16500</p>
<p>RtpAudioHighestPort=16509</p>
```

If UDP Audio is enabled by editing default.ica, then UDP audio will enabled for all users who are using that store.

Avoid echo during multimedia conferences

Users in audio or video conferences may hear an echo. Echoes usually occur when speakers and microphones are too close to each other. For that reason, Citrix recommends 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 should not be too close or too far away from each other.

You can change a registry setting to disable echo cancellation. When working in 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.

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\Advanced\Modules\ClientAudio\EchoCancellation
   - 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.

Network traffic priorities

Sep 29, 2015

Priorities are assigned to network traffic across multiple connections for a session with quality of service (QoS)-supported routers. Four TCP/IP streams (real-time, interactive, background, and bulk) and one UDP/RTP stream (for voice) 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 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. On an internal corporate network, multi-stream connections with TLS are not supported.
To set quality of service for multiple streaming connections, add the following Citrix policy settings to a policy (see Multi-stream connections policy settings for details):

- Multi-Port policy - This setting specifies ports for ICA traffic across multiple connections, and establishes network priorities.
  - Select a priority from the CGP default port priority list; by default, the primary port (2598) has a High priority.
  - Enter additional 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 Cloudbridge 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.

USB and client drive considerations

Jun 01, 2016

Using HDX USB device redirection, a user can connect a flash drive to a local computer and access it remotely from within a virtual desktop or a desktop hosted application. During a session, users can use plug and play devices, including Picture Transfer Protocol (PTP) devices such as digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players, and point-of-sale (POS) devices.

Double-hop USB is not supported for desktop hosted application sessions.

USB redirection is available for the Citrix Receiver for Windows and the Citrix Receiver for Linux.

By default, USB redirection is allowed for certain classes of USB devices, and denied for others; see the Citrix Receiver documentation for details. You can restrict the types of USB devices made available to a virtual desktop by updating the list of USB devices supported for redirection.

> ## Important
>
> In environments where security separation between the user device and server is needed, provide guidance to users about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide performance and bandwidth efficiency over a WAN. The level of support provided depends on the Citrix Receiver installed on the user device. Optimized virtual channels are usually the best option, especially in high latency environments.

For USB redirection purposes, the product handles a SMART board the same as a mouse.

The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports, such as a CDM virtual channel used to view files on a camera or to provide audio to a headset). The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

Specialty devices for which there is no optimized virtual channel are supported by falling back to a Generic USB virtual channel that provides raw USB redirection. For information on USB devices tested with XenDesktop, see CTX123569.

Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, may not work as expected with the optimized virtual channel; if this is an issue, use the Generic USB virtual channel.

Certain devices are not redirected by default, and are available only to the local session. For example, it would not be appropriate to redirect a network interface card that is attached to the user device's system board by internal USB.

The following Citrix policy settings control USB support:

- **Client USB device optimization rules.** The optimization mode is supported for input devices for class=03, for example, signature devices and drawing tablets. If no rule is specified, then the device is handled as Interactive mode (02). Capture mode (04) is the recommended mode for signature devices.
- **Client USB device redirection.** The default is Prohibited.
- **Client USB device redirection rules.** Rules only apply to devices using Generic USB redirection; therefore, the rules do not apply to devices using specialized or optimized redirection, such as CDM.
- **Client USB Plug and Play device redirection.** The default is Allowed, to permit plug-and-play of PTP, MTP, and POS

devices in a user session.

- **Client USB device redirection bandwidth limit.** The default is 0 (no maximum).
- **Client USB device redirection bandwidth limit percent.** The default is 0 (no maximum).

About USB Generic Redirection

Generic USB Redirection is for specialty USB devices for which there is no optimized virtual channel. This functionality redirects arbitrary USB devices from client machines to virtual desktops; with this feature, end users have the ability to interact with a wide selection of generic USB devices in the desktop session as if the devices were physically attached.

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

This feature is supported for desktop sessions from VDA for Desktop OS, minimum version 7.6.

This feature is also supported for desktop sessions from VDA for Server OS, minimum version 7.6, with these restrictions:

- The VDA machine must be running Windows Server 2012 R2
- Only single-hop scenarios are supported
- The USB client drivers must be compatible with RDSH for Windows 2012 R2
- USB storage devices, audio devices, smartcard reader, and devices that are not fully virtualized are not supported

For more information on configuring Generic USB Redirection, see CTX137939.

Enable USB support

1. Add the Client USB device redirection setting to a policy and set its value to Allowed.
2. (Optional) To update the list of USB devices available for remoting, add the Client USB device redirection rules setting to a policy and specify the USB policy rules.
3. Enable USB support when you install Citrix Receiver on user devices. 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.

Update the list of USB devices available for remoting (Citrix Receiver for Windows 4.2)

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. In some instances, however, you might not want to automatically redirect all USB devices. For more information, see CTX123015.

Users can explicitly redirect devices that are not automatically redirected by selecting them from the USB device list. To prevent USB devices from ever being listed or redirected, you can specify device rules on the client and the VDA, as explained below.

You can update the range of USB devices available for remoting by specifying USB device redirection rules for both Citrix Receiver and the VDA to override the default USB policy rules.

- 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.
- 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

> ## 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. 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 http://www.usb.org/ for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating 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.

Important

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

When working with optimized devices such as mass storage, you usually redirect the device using the specialized CDM channel rather than with policy rules. However, you can override this behavior in one of the following ways:

- Manually redirect optimized device using Generic USB redirection, choose Switch to Generic from the Devices tab of the Preferences dialog box.
- Automatically redirect optimized device using Generic USB redirection, set auto-redirection for storage device (for example, AutoRedirectStorage = 1) and set USB user preference settings to automatically connect USB devices; for more information, see CTX123015.

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
       Deny: VID=046D # Deny all Logitech products
```

- The following example shows an administrator-defined USB policy rule for a defined class, sub-class, and protocol:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
      Allow: Class=EF SubClass=01 # Allow Sync devices
      Allow: Class=EF # Allow all USB-Miscellaneous devices
```

Update the list of USB devices available for remoting

By default, 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 for Desktop Appliance sites or desktop hosted applications. In some instances, however, you might not want to automatically redirect all USB devices. For more information, see CTX123015.

Desktop Viewer users can redirect devices that are not automatically redirected by selecting them from the USB device list. To prevent USB devices from being listed or redirected, specify device rules on the user device and the VDA.

You can update the range of USB devices available for remoting by specifying USB device redirection rules for both Citrix Receiver and the VDA to override the default USB policy rules. Device rules are enforced for both Citrix Receiver and the VDA. Be sure to change both so that device remoting works as you intend.

- Edit the user device registry (or the .ini files in the case of the Citrix Receiver for Linux). 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.
- Edit the administrator override rules in the VDA registry on the Server OS machines. An ADM file is included on the installation media so you can change the VDA through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\vda_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. 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 http://www.usb.org/ for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating 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.

Important

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

When working with optimized devices such as mass storage, you usually redirect the device using the specialized CDM channel rather than with policy rules. However, you can override this behavior in one of the following ways:

- Manually redirect optimized device using Generic USB redirection, choose Switch to Generic from the Devices tab of the

Preferences dialog box.

- Automatically redirect optimized device using Generic USB redirection, set auto-redirection for storage device (for example, AutoRedirectStorage = 1) and set USB user preference settings to automatically connect USB devices; for more information, see CTX123015.

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
       Deny: VID=046D # Deny all Logitech products
```

- The following example shows an administrator-defined USB policy rule for a defined class, sub-class, and protocol:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
    Allow: Class=EF SubClass=01 # Allow Sync devices
    Allow: Class=EF # Allow all USB-Miscellaneous devices
```

Use and remove USB devices

Users can connect a USB device before or after starting a virtual session.

When using Citrix 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.

USB mass storage devices

For mass storage devices only, remote access is also available through client drive mapping, where the 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.

The main differences between the two types of remoting policy are:

Feature	Client drive mapping	Generic USB redirection
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, provided users follow operating system recommendations for safe removal

If both Generic USB 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 and the client drive mapping policies are enabled and a device is configured for automatic redirection (see http://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.

> **Note**
>
> USB redirection is supported over lower bandwidth connections, for example 50 Kbps, however copying large files will not work.

File access for mapped client drives

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.

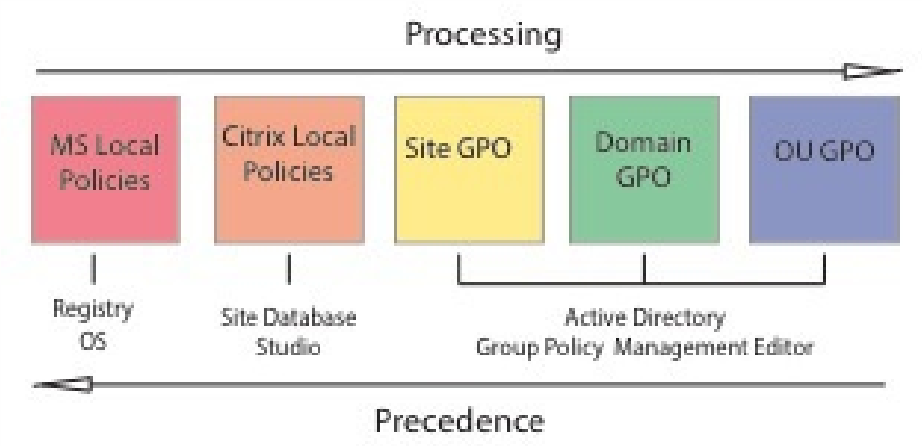
To prevent users from adding or modifying files and folders on mapped client-devices, enable the Read-only client drive access policy setting. When adding this setting to a policy, make sure the Client drive redirection setting is set to Allowed and is also added to the policy.

Policies

May 31, 2016

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, and if you do not specifically assign the policies, the settings are applied to all connections.



You can apply policies on different levels of the network. Policy settings placed at the Organizational Unit GPO level take the highest precedence on the network. Policies at the Domain GPO level override policies on the Site Group Policy Object level, which override any conflicting policies on both the Microsoft and Citrix Local Policies levels.

All Citrix Local Policies are created and managed in the Citrix Studio console and stored in the Site Database; whereas, Group Policies are created and managed with 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 generally 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.
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 and 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 may 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: Mixing Windows and Citrix policies in the same GPO is not supported.

Related content

- Work with policies
- Policy templates
- Create policies
- Compare, prioritize, model, and troubleshoot policies
- Default policy settings
- Policy settings reference

Work with policies

Sep 29, 2015

Configure Citrix policies to control user access and session environments. Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple settings.

Tools for working with Citrix policies

You can use the following tools to work with Citrix policies.

- **Studio** - If you are a Citrix administrator without permission to manage group policy, use Studio to create policies for your site. Policies created using Studio are stored in the site database and updates are pushed to the virtual desktop either when that virtual desktop registers with the broker or when a user connects to that virtual desktop.
- **Local Group Policy Editor** (Microsoft Management Console snap-in) - If your network environment uses Active Directory and you have permission to manage group policy, you can use the Local Group Policy Editor to create policies for your Site. The settings you configure affect the Group Policy Objects (GPOs) you specify in the Group Policy Management Console.
  Important: You must use the Local Group Policy Editor to configure some policy settings, including those related to registering VDAs with a Controller and those related to Microsoft App-V servers.

Policy processing order and precedence

Group policy settings are processed in the following order:

1. Local GPO
2. XenApp or XenDesktop Site GPO (stored in the Site database)
3. Site-level GPOs
4. Domain-level GPOs
5. Organizational Units

However, if a conflict occurs, policy settings that are processed last can overwrite those that are processed earlier. This means that policy settings take precedence in the following order:

1. Organizational Units
2. Domain-level GPOs
3. Site-level GPOs
4. XenApp or XenDesktop Site GPO (stored in the Site database)
5. Local GPO

For example, a Citrix administrator uses Studio to create a policy (Policy A) that enables client file redirection for the company's sales employees. Meanwhile, another administrator uses the Group Policy Editor to create a policy (Policy B) that disables client file redirection for sales employees. When the sales employees log on to the virtual desktops, Policy B is applied and Policy A is ignored because Policy B was processed at the domain level and Policy A was processed at the XenApp or XenDesktop Site GPO level.

However, when a user launches an ICA or Remote Desktop Protocol (RDP) session, Citrix session settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical RDP client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging.

When using multiple policies, you can prioritize policies that contain conflicting settings; see Compare, prioritize, model, and troubleshoot policies for details.

Workflow for Citrix policies

The process for configuring policies is as follows:

1. Create the policy.
2. Configure policy settings.
3. Assign the policy to machine and user objects.
4. Prioritize the policy.
5. Verify the effective policy by running the Citrix Group Policy Modeling wizard.

Navigate Citrix policies and settings

In the Local Group Policy Editor, policies and settings appear in two categories: Computer Configuration and User Configuration. Each category has a Citrix Policies node. See the Microsoft documentation for details about navigating and using this snap-in.

In Studio, policy settings are sorted into categories based on the functionality or feature they affect. For example, the Profile management section contains policy settings for Profile management.

- Computer settings (policy settings applying to machines) define the behavior of virtual desktops and are applied when a virtual desktop starts. These settings apply even when there are no active user sessions on the virtual desktop. User settings define the user experience when connecting using ICA. User policies are applied when a user connects or reconnects using ICA. User policies are not applied if a user connects using RDP or logs on directly to the console.
  To access policies, settings, or templates, select Policies in the Studio navigation pane.
  - The **Policies** tab lists all policies. When you select a policy, tabs to the right display: Overview (name, priority, enabled/disabled status, and description), Settings (list of configured settings), and Assigned to (user and machine objects to which the policy is currently assigned). For more information, see Create policies.
  - The **Templates** tab lists Citrix-provided and custom templates you created. When you select a template, tabs to the right display: Description (why you might want to use the template) and Settings (list of configured settings). For more information, see Policy templates.
  - The **Comparison** tab enables you to compare the settings in a policy or template with those in other policies or templates. For example, you might want to verify setting values to ensure compliance with best practices. For more information, see Compare, prioritize, model, and troubleshoot policies.
  - From the **Modelling** tab, you can simulate connection scenarios with Citrix policies. For more information, see Compare, prioritize, model, and troubleshoot policies.

  To search for a setting in a policy or template:
  1. Select the policy or template.
  2. Select Edit policy or Edit Template in the Actions pane.
  3. On the Settings page, begin to type the name of the setting.

  You can refine your search by selecting a specific product version, selecting a category (for example, Bandwidth), or by selecting the View selected only check box or selecting to search only the settings that have been added to the selected policy. For an unfiltered search, select All Settings.

- To search for a setting within a policy :
  1. Select the policy.
  2. Select the Settings tab, begin to type the name of the setting.

You can refine your search by selecting a specific product version or by selecting a category. For an unfiltered search, select

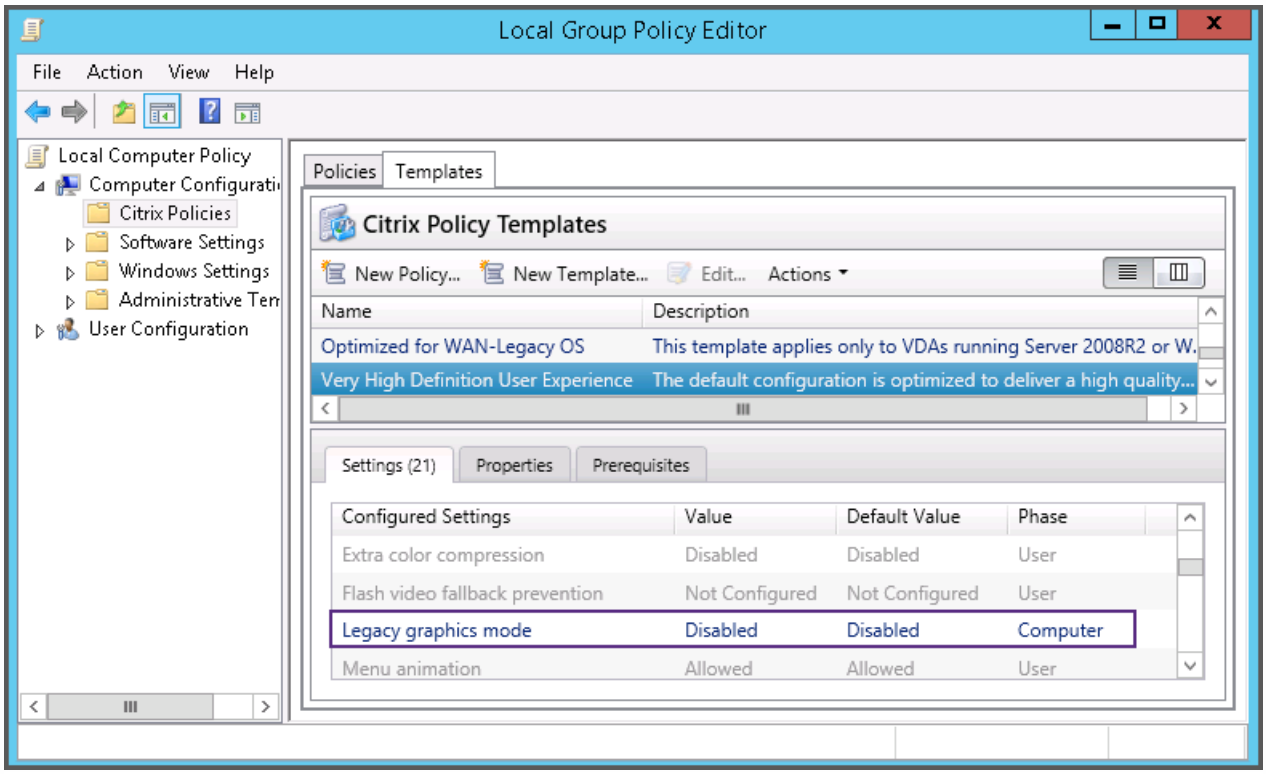
All Settings.

A policy, once created, is completely independent of the template used. You can use the Description field on a new policy to keep track of the source template used.

In Studio, policies and templates are displayed in a single list regardless of whether they contain user, computer or both types of settings and can be applied using both user and computer filters.

In Group Policy Editor, Computer and User settings must be applied separately, even if created from a template that contains both types of settings. In this example choosing to use Very High Definition User Experience in Computer Configuration:

- Legacy Graphics mode is a Computer setting that will be used in a policy created from this template.
- The User settings, grayed out, will not be used in a policy created from this template.



Policy templates

Sep 29, 2015

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.

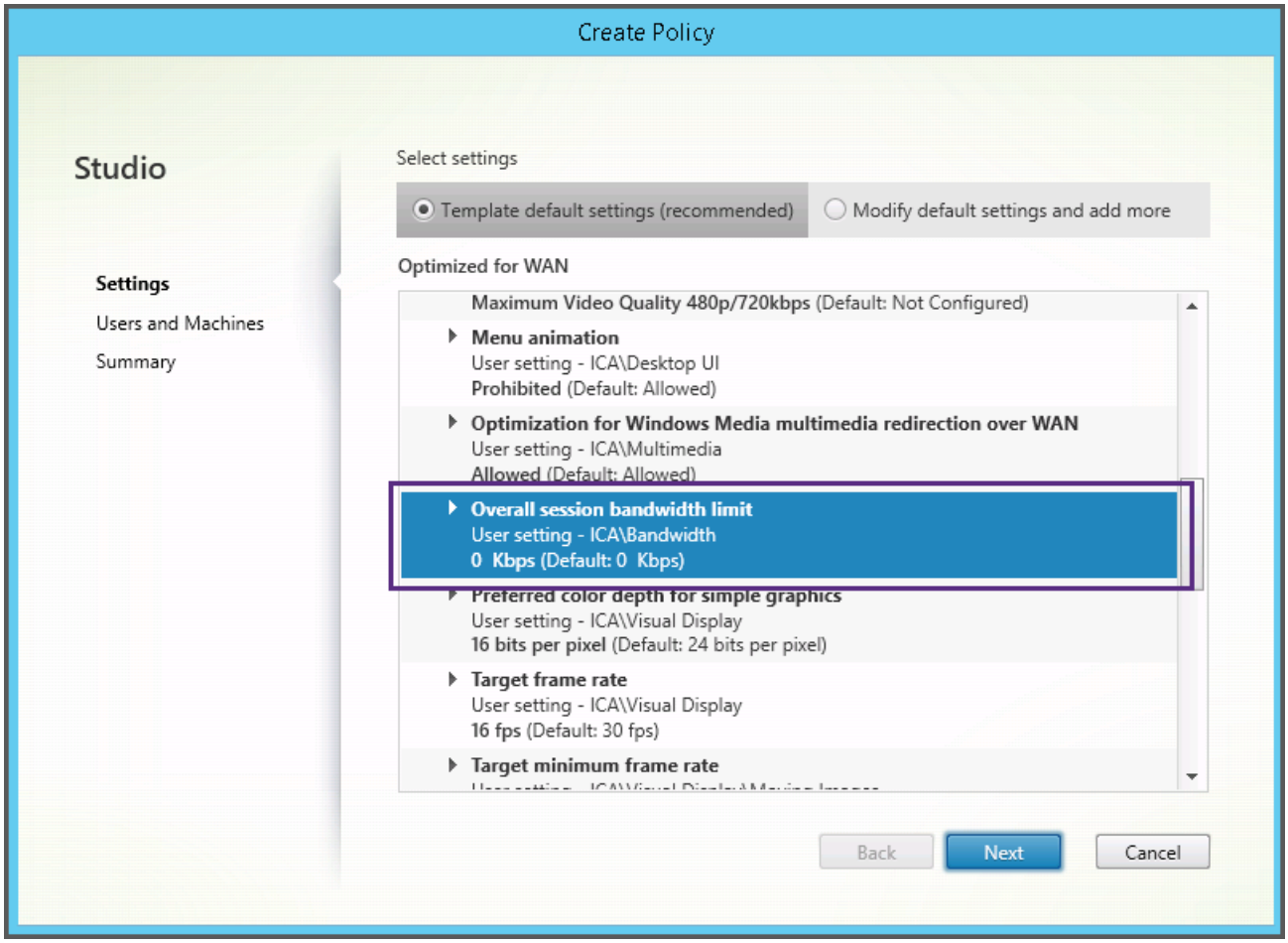
For considerations when using templates to create policies, see CTX202330.

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 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 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.

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 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.

Create policies

Sep 22, 2015

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.

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.

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.
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.

An assignment's mode determines if the policy is applied only to connections that match all the assignment criteria. If the mode is set to Allow (the default), the policy is applied only to connections that match the assignment criteria. If the mode is set to Deny, the policy is applied if the connection does not match the assignment criteria. The following examples illustrate how assignment modes affect Citrix policies when multiple assignments are present.

- **Example: Assignments of like type with differing modes** - In policies with two assignments of the same type, one set to Allow and one set to Deny, the assignment set to Deny takes precedence, provided the connection satisfies both assignments. For example:
  Policy 1 includes the following assignments:
  - Assignment A specifies the Sales group; the mode is set to Allow
  - Assignment B specifies the Sales manager's account; the mode is set to Deny

  Because the mode for Assignment B is set to Deny, the policy is not applied when the Sales manager logs on to the Site, even though the user is a member of the Sales group.

- **Example: Assignments of differing type with like modes** - In policies with two or more assignments of differing types, set to Allow, the connection must satisfy at least one assignment of each type in order for the policy to be applied. For example:
  Policy 2 includes the following assignments:
  - Assignment C is a User assignment that specifies the Sales group; the mode is set to Allow
  - Assignment D is a Client IP Address assignment that specifies 10.8.169.* (the corporate network); the mode is set to Allow

  When the Sales manager logs on to the Site from the office, the policy is applied because the connection satisfies both assignments.

  Policy 3 includes the following assignments:
  - Assignment E is a User assignment that specifies the Sales group; the mode is set to Allow
  - Assignment F is an Access Control assignment that specifies NetScaler Gateway connection conditions; the mode is set to Allow

  When the Sales manager logs on to the Site from the office, the policy is not applied because the connection does not satisfy Assignment F.

Create a new policy based on a template, using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Templates tab and select a template.
3. Select Create Policy from Template in the Actions pane.

4. By default, the new policy uses all the default settings in the template (the Use template default settings radio button is selected). If you want to change settings, select the Modify defaults and add more settings radio button, and then add or remove settings.
5. Specify how to apply the policy by selecting one of the following:
   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
   - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.
   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create a new policy using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Policies tab.
3. Select Create Policy in the Actions pane.
4. Add and configure policy settings.
5. Specify how to apply the policy by choosing one of the following:
   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
   - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.
   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create and manage policies using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the Policies node and then select Citrix Policies. Choose the appropriate action below.

Task	Instruction
Create a new policy	On the Policies tab, click New.
Edit an existing policy	On the Policies tab, select the policy and then click Edit.
Change the priority of an existing policy	On the Policies tab, select the policy and then click either Higher or Lower.
View summary information about a policy	On the Policies tab, select the policy and then click the Summary tab.
View and amend policy settings	On the Policies tab, select the policy and then click the Settings tab.

Task	Instruction
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

Sep 16, 2016

You can use multiple policies to customize your environment to meet users' needs based on their job functions, geographic locations, or connection types. For example, for security you may need to place restrictions on user groups who regularly work with sensitive data. You can create a policy that prevents users from saving sensitive files on their local client drives. However, if some people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence.

When using multiple policies, you must determine how to prioritize them, how to create exceptions, and how to view the effective policy when policies conflict.

In general, policies override similar settings configured for the entire Site, for specific Delivery Controllers, or on the user device. The exception to this principle is security. The highest encryption setting in your environment, including the operating system and the most restrictive shadowing setting, always overrides other settings and policies.

Citrix policies interact with policies you set in your operating system. In a Citrix environment, Citrix settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical Remote Desktop Protocol (RDP) client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging. For some policy settings, such as Secure ICA, the settings in policies must match the settings in the operating system. If a higher priority encryption level is set elsewhere, the Secure ICA policy settings that you specify in the policy or when you are delivering application and desktops can be overridden.

For example, the encryption settings that you specify when creating Delivery Groups should be at the same level as the encryption settings you specified throughout your environment.

Note: In the second hop of double-hop scenarios, when a 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. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy.

You prioritize policies by giving them different priority numbers in Studio. By default, new policies are given the lowest priority. If policy settings conflict, a policy with a higher priority (a priority number of 1 is the highest) overrides a policy with a

lower priority. Settings are merged according to priority and the setting's condition; for example, whether the setting is disabled or enabled. Any disabled setting overrides a lower-ranked setting that is enabled. Policy settings that are not configured are ignored and do not override the settings of lower-ranked settings.

1. Select Policies in the Studio navigation pane. Make sure the Policies tab is selected.
2. Select a policy.
3. Select Lower Priority or Higher Priority in the Actions pane.

Exceptions

When you create policies for groups of users, user devices, or machines, you may find that some members of the group require exceptions to some policy settings. You can create exceptions by:

- Creating a policy only for those group members who need the exceptions and then ranking the policy higher than the policy for the entire group
- Using the Deny mode for an assignment added to the policy

An assignment with the mode set to Deny applies a policy only to connections that do not match the assignment criteria. For example, a policy contains the following assignments:

- Assignment A is a client IP address assignment that specifies the range 208.77.88.*; the mode is set to Allow
- Assignment B is a user assignment that specifies a particular user account; the mode is set to Deny

The policy is applied to all users who log on to the Site with IP addresses in the range specified in Assignment A. However, the policy is not applied to the user logging on to the Site with the user account specified in Assignment B, even though the user's computer is assigned an IP address in the range specified in Assignment A.

Determine which policies apply to a connection

Sometimes a connection does not respond as expected because multiple policies apply. If a higher priority policy applies to a connection, it can override the settings you configure in the original policy. You can determine how final policy settings are merged for a connection by calculating the Resultant Set of Policy.

You can calculate the Resultant Set of Policy in the following ways:

- Use the Citrix Group Policy Modeling Wizard to simulate a connection scenario and discern how Citrix policies might be applied. You can specify conditions for a connection scenario such as domain controller, users, Citrix policy assignment evidence values, and simulated environment settings such as slow network connection. The report that the wizard produces lists the Citrix policies that would likely take effect in the scenario. If you are logged on to the Controller as a domain user, the wizard calculates the Resultant Set of Policy using both site policy settings and Active Directory Group Policy Objects (GPOs).
- Use Group Policy Results to produce a report describing the Citrix policies in effect for a given user and controller. The Group Policy Results tool helps you evaluate the current state of GPOs in your environment and generates a report that describes how these objects, including Citrix policies, are currently being applied to a particular user and controller.

You can launch the Citrix Group Policy Modeling Wizard from the Actions pane in Studio. You can launch either tool from the Group Policy Management Console in Windows.

If you run the Citrix Group Policy Modeling Wizard or Group Policy Results tool from the Group Policy Management Console, site policy settings created using Studio are not included in the Resultant Set of Policy.

To ensure you obtain the most comprehensive Resultant Set of Policy, Citrix recommends launching the Citrix Group Policy Modeling wizard from Studio, unless you create policies using only the Group Policy Management Console.

Use the Citrix Group Policy Modeling Wizard

Open the Citrix Group Policy Modeling Wizard using one of the following:

- Select Policies in the Studio navigation pane, select the Modeling tab, and then select Launch Modeling Wizard in the Actions pane.
- Launch the Group Policy Management Console (gpmc.msc), right-click Citrix Group Policy Modeling in the tree pane, and then select Citrix Group Policy Modeling Wizard.

Follow the wizard instructions to select the domain controller, users, computers, environment settings, and Citrix assignment criteria to use in the simulation. After you click Finish, the wizard produces a report of the modeling results. In Studio, the report appears in the middle pane under the Modeling tab.

To view the report, select View Modeling Report.

Troubleshoot policies

Users, IP addresses, and other assigned objects can have multiple policies that apply simultaneously. This can result in conflicts where a policy may not behave as expected. When you run the Citrix Group Policy Modeling Wizard or the Group Policy Results tool, you might discover that no policies are applied to user connections. When this happens, users connecting to their applications and desktops under conditions that match the policy evaluation criteria are not affected by any policy settings. This occurs when:

- No policies have assignments that match the policy evaluation criteria.
- Policies that match the assignment do not have any settings configured.
- Policies that match the assignment are disabled.

If you want to apply policy settings to the connections that meet the specified criteria, make sure:

- The policies you want to apply to those connections are enabled.
- The policies you want to apply have the appropriate settings configured.

Default policy settings

Aug 03, 2016

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
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
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

Name	Default setting	VDA
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
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

Name	Default setting	VDA
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
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

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, VDA

Name	Default setting	VDA
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
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

Name	Default setting	VDA
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
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

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
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 machines.
Remote the combo box	Prohibited	VDA 5.6 FP1, VDA for Server OS 7 through current, VDA for Desktop OS 7 through current

ICA/Multimedia

Name	Default setting	VDA
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
Video load management policy setting	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
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
Printer assignments	User's current printer is used as the default printer for the	All VDA

Name	Default setting	VDA
Printer auto-creation event log preference	Log errors and warnings	All VDA versions
Session printers	No printers are specified	All VDA versions
Wait for printers to be created (desktop)	Disabled	All VDA versions

ICA/Printing/Client Printers

Name	Default setting	VDA
Auto-create client printers	Auto-create all client printers	All VDA versions
Auto-create generic universal printer	Disabled	All VDA versions
Client printer names	Standard printer names	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
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
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

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

Name	Default setting	VDA
Use local time of client	Use server time zone	All VDA versions

ICA/TWAIN Devices

Name	Default setting	VDA
Client TWAIN device redirection	Allowed	VDA 5.5, 5.6 FP1, VDA for 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	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

Name	Default setting	VDA

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

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

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
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

Name	Default setting	VDA
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
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

Name	Default setting	VDA
Grant administrator access	Disabled	All VDA versions
Include domain name	Disabled	All VDA versions

Profile Management/Folder Redirection/AppData(Roaming)

Name	Default setting	VDA
AppData(Roaming) path	Disabled. No location is specified.	All VDA versions
Redirection settings for AppData(Roaming)	Contents are redirected to the UNC path specified in the AppData(Roaming) path policy settings	All VDA versions

Profile Management/Folder Redirection/Contacts

Name	Default setting	VDA
Contacts path	Disabled. No location is specified.	All VDA versions
Redirection settings for Contacts	Contents are redirected to the UNC path specified in the Contacts path policy settings	All VDA versions

Profile Management/Folder Redirection/Desktop

Name	Default setting	VDA
Desktop path	Disabled. No location is specified.	All VDA versions
Redirection settings for Desktop	Contents are redirected to the UNC path specified in the Desktop path policy settings	All VDA versions

Profile Management/Folder Redirection/Documents

Name	Default setting	VDA
Documents path	Disabled. No location is specified.	All VDA versions
Redirection settings for Documents	Contents are redirected to the UNC path specified in the Documents path policy settings	All VDA versions

Profile Management/Folder Redirection/Downloads

Name	Default setting	VDA

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

Profile Management/Folder Redirection/Music

Name	Default setting	VDA
Music path	Disabled. No location is specified.	All VDA versions
Redirection settings for Music	Contents are redirected to the UNC path specified in the Music path policy settings	All VDA versions

Profile Management/Folder Redirection/Pictures

Name	Default setting	VDA
Pictures path	Disabled. No location is specified.	All VDA versions
Redirection settings for Pictures	Contents are redirected to the UNC path specified in the Pictures path policy settings	All VDA versions

Profile Management/Folder Redirection/Saved Games

Name	Default setting	VDA
Saved Games path	Disabled. No location is specified.	All VDA versions
Redirection settings for Saved Games	Contents are redirected to the UNC path specified in the Saved Games path policy settings	All VDA versions

Profile Management/Folder Redirection/Searches

Name	Default setting	VDA
Searches path	Disabled. No location is specified.	All VDA versions
Redirection settings for Searches	Contents are redirected to the UNC path specified in the Searches path policy settings	All VDA versions

Profile Management/Folder Redirection/Start Menu

Name	Default setting	VDA
Start Menu path	Disabled. No location is specified.	All VDA versions
Redirection settings for Start Menu	Contents are redirected to the UNC path specified in the Start Menu path policy settings	All VDA versions

Profile Management/Folder Redirection/Video

Name	Default setting	VDA
Video path	Disabled. No location is specified.	All VDA versions
Redirection settings for Video	Contents are redirected to the UNC path specified in the Video path policy settings	All VDA versions

Profile Management/Log settings

Name	Default setting	VDA
Active Directory actions	Disabled	All VDA versions
Common information	Disabled	All VDA versions
Common warnings	Disabled	All VDA

Name	Default setting	VDA versions
Enable logging	Disabled	All VDA versions
File system actions	Disabled	All VDA versions
File system notifications	Disabled	All VDA versions
Logoff	Disabled	All VDA versions
Logon	Disabled	All VDA versions
Maximum size of the log file	1048576	All VDA versions
Path to log file	Disabled. Log files are saved in the default location; %SystemRoot%\System32\Logfiles\UserProfileManager.	All VDA versions
Personalized user information	Disabled	All VDA versions
Policy values at logon and logoff	Disabled	All VDA versions
Registry actions	Disabled	All VDA versions
Registry differences at logoff	Disabled	All VDA versions

Profile Management/Profile handling

Name	Default setting	VDA
Delay before deleting cached profiles	0	All VDA versions
Delete locally cached profiles on logoff	Disabled	All VDA versions
Local profile conflict handling	Use local profile	All VDA versions
Migration of existing profiles	Local and roaming	All VDA versions

Name	Default setting	VDA
Path to the template profile	Disabled. New user profiles are created from the default user profile on the device where a user first logs on.	All VDA versions
Template profile overrides local profile	Disabled	All VDA versions
Template profile overrides roaming profile	Disabled	All VDA versions
Template profile used as a Citrix mandatory profile for all logons	Disabled	All VDA versions

Profile Management/Registry

Name	Default setting	VDA
Exclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions
Inclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions

Profile Management/Streamed user profiles

Name	Default setting	VDA
Always cache	Disabled	All VDA versions
Always cache size	0 Mb	All VDA versions
Profile streaming	Disabled	All VDA versions
Streamed user profile groups	Disabled. All user profiles within an OU are processed normally.	All VDA versions
Timeout for pending area lock files (days)	1 day	All VDA versions

Receiver

Name	Default setting	VDA
StoreFront accounts list	No stores are specified	VDA for 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 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

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

Policy settings reference

Jun 01, 2016

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
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

To limit bandwidth used for	Use this policy setting
Client session	Overall session bandwidth limit
Printing	• Printer redirection bandwidth limit or • Printer redirection bandwidth limit percent
TWAIN devices (such as a camera or scanner)	• TWAIN device redirection bandwidth limit or • TWAIN device redirection bandwidth limit percent
USB devices	• Client USB device redirection bandwidth limit or • Client USB device redirection bandwidth limit percent

Redirection of client drives and user devices

For this task	Use this policy setting
Control whether or not drives on the user device are connected when users log on to the server	Auto connect client drives
Control cut-and-paste data transfer between the server and the local clipboard	Client clipboard redirection
Control how drives map from the user device	Client drive redirection
Control whether users' local hard drives are available in a session	• Client fixed drives and • Client drive redirection
Control whether users' local floppy drives are available in a session	• Client floppy drives and • Client drive redirection
Control whether users' network drives are available in a session	• Client network drives and • Client drive redirection
Control whether users' local CD, DVD, or Blu-ray drives are available in a session	• Client optical drives and • Client drive redirection
Control whether users' local removable drives are available in a session	• Client removable drives and • Client drive redirection
Control whether users' TWAIN devices, such as scanners and	• Client TWAIN device redirection

For this task	Use this policy setting
cameras, are available in a session and control compression of image data transfers	• TWAIN compression redirection
Control whether USB devices are available in a session	• Client USB device redirection and • Client USB device redirection rules
Improve the speed of writing and copying files to a client disk over a WAN	Use asynchronous writes

Content redirection

For this task	Use this policy setting
Control whether to use content redirection from the server to the user device	Host to client redirection

Desktop UI

For this task	Use this policy setting
Control whether or not Desktop wallpaper is used in users' sessions	Desktop wallpaper
View window contents while a window is dragged	View window contents while dragging

Graphics and multimedia

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

For this task	Use this policy setting
	• Flash video fallback prevention policy setting • Flash video fallback prevention error *.swf

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 between 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	o Auto-create client printers and o Client printer redirection
Control the location where printer properties are stored	Printer properties retention
Control whether print requests are processed by the client or the server	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's session information	Default printer
Load balance and set failover threshold for Universal Print Servers	o Universal Print Servers for load balancing o 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

Jun 01, 2016

The ICA section contains policy settings related to ICA listener connections and mapping to the clipboard.

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 but you can use this setting to allow specific data formats to be shared with the client endpoint clipboard. To use this setting, enable it and add the specific formats to be allowed.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT

- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML Format

HTML Format is disabled by default. To enable this feature:

- Make sure **Client clipboard redirection** is set to allowed.
- Make sure **Restrict client clipboard write** is set to enabled.
- Add an entry for **HTML Format** (and any other formats you want supported) in **Client clipboard write allowed formats**.

Note: Enabling HTML format clipboard copy support (HTML Format) will copy 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 will only be live 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's Direct Access Users group connecting to a session on that VDA using an ICA connections.

By default, non-administrative users cannot connect to these sessions.

This setting has no effect on non-administrative users in a VDA's Direct Access Users group who are using a 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's 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 launching initial applications through RDP on the server.

By default, launching initial applications through RDP on the server is not allowed.

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 is set to 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 is set to Prohibited.

Session clipboard write allowed formats

When the Restrict session clipboard write setting is Allowed, client clipboard data cannot be shared with session applications, but you can use this setting to allow specific data formats to be shared with the session clipboard.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML Format

HTML Format is disabled by default. To enable this feature:

- Make sure **Client clipboard redirection** is set to allowed.
- Make sure **Restrict session clipboard write** is set to enabled.
- Add an entry for **HTML Format** (and any other formats you want supported) in **Session clipboard write allowed formats**.

Note: Enabling HTML Format clipboard copy support (HTML Format) will copy 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 will only be live 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 the Client clipboard redirection setting or Restrict session clipboard write setting is set to Prohibited.

Auto Client Reconnect policy settings

Sep 29, 2015

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.

By default, automatic reconnection is allowed.

Allowing automatic reconnection 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.

However, automatic reconnection can result in a new session being launched (instead of reconnecting to an existing session) if the Citrix Receiver cookie, which contains the key to the session ID and credentials, is not used. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be reentered. Auto client reconnect is not triggered if users intentionally disconnect.

For application sessions, when automatic reconnection is allowed, Citrix Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, when automatic reconnection is allowed, 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.

Auto client reconnect authentication

This setting requires authentication for automatic client reconnections.

By default, authentication is not required.

When a user initially logs on, their credentials are encrypted, stored in memory, and a cookie is created containing the encryption key that 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.

Auto client reconnect logging

This setting enables or disables the recording of auto client reconnections in the event log.

By default, logging is disabled.

When logging is enabled, the server's 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.

Audio policy settings

Sep 30, 2014

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 and consuming low bandwidth. If VoIP quality is unsatisfactory, ensure that the Audio over UDP Real-time Transport policy setting is set to Allowed.
- 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.

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

Jun 01, 2016

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.

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.

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.

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.
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.

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.

Client sensors policy settings

Jul 24, 2014

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.
  - 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

Aug 03, 2016

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.

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

Jul 24, 2014

The End User Monitoring section contains policy settings for measuring session traffic.

ICA round trip calculation

This setting determines whether ICA round trip calculations are performed for active connections.

By default, calculations for active connections are enabled.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

ICA round trip calculation interval

This setting specifies the frequency, in seconds, at which ICA round trip calculations are performed.

By default, ICA round trip is calculated every 15 seconds.

ICA round trip calculations for idle connections

This setting determines whether ICA round trip calculations are performed for idle connections.

By default, calculations are not performed for idle connections.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

Enhanced desktop experience policy setting

Jul 24, 2014

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.

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

Jul 24, 2014

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

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.

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.

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.

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

Sep 29, 2015

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.

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: http://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).

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.

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

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 (http://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.

Graphics policy settings

Jun 01, 2016

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.

For connections requiring more color depth and higher resolution, increase the limit. Calculate the maximum memory required using the equation:

Memory depth in bytes = (color-depth-in-bits-per-pixel) / 8) * (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.

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.
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, providing fallback to the legacy graphics experience to improve scalability over a WAN or mobile connection.

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. While it is also supported on Windows 2012 and 2012 R2, it is not recommended.

Legacy graphics mode is not supported on Windows 10, 8.1 or 8.

See CTX202687 for more on optimizing graphics modes and policies in XenApp and XenDesktop 7.6 FP3 or higher.

Maximum allowed color depth

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting specifies the maximum color depth allowed for a session.

By default, the maximum allowed color depth is 32 bits per pixel.

This setting applies only to ThinWire drivers and connections. It does not apply to VDAs that have a non-ThinWire driver as

the primary display driver, such as VDAs that use a Windows Display Driver Model (WDDM) driver as the primary display driver. For 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.

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 to compress graphics when video decoding is available on the endpoint. When video decoding is not available on the endpoint, or when you specify **Do not use video codec**, a combination of still image compression and bitmap caching is used. When **Use 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 **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.

Select **Use video codec when available** to optimize for improved user experience and bandwidth, especially in cases with heavy use of server-rendered video and 3D graphics.

Select **Use video codec when preferred** to allow the system to make its best effort to choose appropriate settings for the current scenario.

The default is Use video codec when preferred.

Caching policy settings

Jul 24, 2014

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

Dec 01, 2015

The Framehawk section contains policy settings that enable and configure the Framehawk display channel on the server.

Framehawk display channel

When enabled, the server attempts to use the Framehawk display channel for the user's graphics and input remoting. That display channel will use UDP to provide a better user experience on networks with high loss and latency characteristics; however, it may also use more server resources and bandwidth than other graphics modes.

By default, the Framehawk display channel is disabled.

Framehawk display channel port range

This policy setting specifies the range of UDP port numbers (in the form *lowest port number,highest port number)* the VDA uses to exchange Framehawk display channel data with the user device. The VDA attempts to use each port, starting with the lowest port number and incrementing for each subsequent attempt. The port handles inbound and outbound traffic.

By default, the port range is 3224,3324.

Keep alive policy settings

Jul 24, 2014

The Keep Alive section contains policy settings for managing ICA keep-alive messages.

ICA keep alive timeout

This setting specifies the number of seconds between successive ICA keep-alive messages.

By default, the interval between keep-alive messages is 60 seconds.

Specify an interval between 1-3600 seconds in which to send ICA keep-alive messages. Do not configure this setting if your network monitoring software is responsible for closing inactive connections.

ICA keep alives

This setting enables or disables sending ICA keep-alive messages periodically.

By default, keep-alive messages are not sent.

Enabling this setting prevents broken connections from being disconnected. If the server detects no activity, this setting prevents Remote Desktop Services (RDS) from disconnecting the session. The server sends keep-alive messages every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

ICA keep-alive does not work if you are using session reliability. Configure ICA keep-alive only for connections that are not using Session Reliability.

Related policy settings: Session reliability connections.

Local App Access policy settings

Jul 24, 2014

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

Sep 29, 2015

The Mobile Experience section contains policy settings for handling the Citrix Mobility Pack.

Automatic keyboard display

This setting enables or disables the automatic display of the keyboard on mobile device screens.

By default, the automatic display of the keyboard is disabled.

Launch touch-optimized desktop

This setting is disabled and not available for Windows 10 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

Sep 29, 2015

The Multimedia section contains policy settings for managing streaming audio and video in user sessions.

Limit video quality

This setting specifies the maximum video quality level allowed for an HDX connection. When configured, maximum video quality is limited to the specified value, ensuring that multimedia Quality of Service (QoS) is maintained within an environment.

By default, this setting is not configured.

To limit the maximum video quality level allowed, choose one of the following options:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Note: 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 support for video conferencing applications.

By default, video conferencing support is allowed.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed.

When using multimedia conferencing, make sure the following conditions are met:

- Manufacturer-supplied drivers for the web cam used for multimedia conferencing must be installed.
- The web cam must be connected to the user device before initiating a video conferencing session. The server uses only one installed web cam at any given time. If multiple web cams are installed on the user device, the server attempts to use each web cam in succession until a video conferencing session is created successfully.

Optimization for Windows Media multimedia redirection over WAN

This setting enables real-time multimedia transcoding, allowing audio and video media streaming to mobile devices, and enhancing the user experience by improving how Windows Media content is delivered over a WAN.

By default, the delivery of Windows Media content over the WAN is optimized.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed.

When this setting is enabled, real-time multimedia transcoding is deployed automatically as needed to enable media streaming, providing a seamless user experience even in extreme network conditions.

Use GPU for optimizing Windows Media multimedia redirection over WAN

This setting enables real-time multimedia transcoding to be done in the Graphics Processing Unit (GPU) on the Virtual

Delivery Agent (VDA), to 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.

Video fallback prevention

Administrators can use the Video 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. This allows Client Side Fetching to RAVE to Server Side fallbacks.

To configure this setting, choose one of the following options:

- **Server Fetched - Server Rendered**. Allow Client Side Fetching to RAVE to Server Side fallbacks.
- **Server Fetched - Client Rendered**. Allow Client Side Fetching to RAVE fallback, however, block RAVE to Server Side Rendering fallback.
- **Client Fetched - Client Rendered**. Block Client Side Fetching to RAVE to Server Side Rendering fallbacks.

When the content does not play, the error message "Company has blocked video because of lack of resources" displays in the player window.

Windows Media client-side content fetching

This setting enables a user device to stream multimedia files directly from the source provider on the Internet or Intranet, rather than through the host server.

By default, the streaming of multimedia files to the user device direct from the source provider is allowed.

Allowing this setting improves network utilization 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 this setting is disabled, the streaming of multimedia files to the user device direct from the source provider is also disabled.

Windows Media Redirection

This setting controls and optimizes the way servers deliver streaming audio and video to users.

By default, the delivery of streaming audio and video to users is allowed.

Allowing this setting increases the quality of audio and video rendered from the server to a level that compares with audio and video played locally on a user device. The server streams multimedia to the client in the original, compressed form and allows the user device to decompress and render the media.

Windows Media redirection optimizes multimedia files that are encoded with codecs that adhere to Microsoft DirectShow, DirectX Media Objects (DMO), and Media Foundation standards. To play back a given multimedia file, a codec compatible

with the encoding format of the multimedia file must be present on the user device.

By default, audio is disabled on Citrix Receiver. To allow users to run multimedia applications in ICA sessions, turn on audio or give users permission to turn on audio in their Citrix Receiver interface.

Select Prohibited only if playing media using Windows Media redirection appears worse than when rendered using basic ICA compression and regular audio. This is rare but can happen under low bandwidth conditions, for example, with media with a very low frequency of key frames.

Windows Media Redirection buffer size

This setting 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 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 (5 seconds).

Multi-stream connections policy settings

Aug 08, 2014

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 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 Cloudbridge 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.

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

Jun 01, 2016

The Port Redirection section contains policy settings for client LPT and COM port mapping.

For Virtual Delivery Agent versions **earlier than 7.0**, use the following policy settings to configure port redirection. For VDA versions **7.0 through 7.8**, configure these settings using the registry; see Configure COM Port and LPT Port Redirection settings using the registry. For VDA version **7.9**, use the following policy settings.

Auto connect client COM ports

This setting enables or disables automatic connection of COM ports on user devices when users log on to a site.

By default, client COM ports are not automatically connected.

Auto connect client LPT ports

This setting enables or disables automatic connection of LPT ports on user devices when users log on to a site.

By default, client LPT ports are not connected automatically.

Client COM port redirection

This setting allows or prevents access to COM ports on the user device.

By default, COM port redirection is prohibited.

The following policy settings are related:

- COM port redirection bandwidth limit
- COM port redirection bandwidth limit percent

Client LPT port redirection

This setting allows or prevents access to LPT ports on the user device.

By default, LPT port redirection is prohibited.

LPT ports are used only by legacy applications that send print jobs to the LPT ports and not to the print objects on the user device. Most applications today can send print jobs to printer objects. This policy setting is necessary only for servers that host legacy applications that print to LPT ports.

Note, although Client COM port redirection is bi-directional, LPT port redirection is output only and limited to \\client\LPT1 and \\client\LPT2 within an ICA session.

The following policy settings are related:

- LPT port redirection bandwidth limit
- LPT port redirection bandwidth limit percent

Printing policy settings

Aug 26, 2014

The Printing section contains policy settings for managing client printing.

Client printer redirection

This setting controls whether client printers are mapped to a server when a user logs on to a session.

By default, client printer mapping is allowed. If this setting is disabled, the PDF printer for the session is not auto-created.

Related policy settings: auto-create client printers

Default printer

This setting specifies how the default printer on the user device is established in a session.

By default, the user's current printer is used as the default printer for the session.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do not adjust the user's default printer. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session 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.
- 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

Sep 29, 2015

The Client Printers section contains policy settings for client printers, including settings to autocreate client printers, retain printer properties, and connect to print servers.

Auto-create client printers

This setting specifies the client printers that are auto-created. This setting overrides default client printer auto-creation settings.

By default, all client printers are auto-created.

This setting takes effect only if the Client printer redirection setting is present and set to Allowed.

When adding this setting to a policy, select an option:

- Auto-create all client printers automatically creates all printers on a user device.
- Auto-create the client's default printer only automatically creates only the printer selected as the default printer on the user device.
- Auto-create local (non-network) client printers only automatically creates only printers directly connected to the user device through an LPT, COM, USB, TCP/IP, or other local port.
- Do not auto-create client printers turns off autocreation for all client printers when users log on. This causes the Remote Desktop Services (RDS) settings for autocreating client printers to override this setting in lower priority policies.

Auto-create generic universal printer

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 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.

By default, no rules are specified.

When you define driver substitution rules, you can allow or prevent printers to be created with the specified driver. Additionally, you can allow created printers to use only universal print drivers. Driver substitution overrides or maps printer driver names the user device provides, substituting an equivalent driver on the server. This gives server applications access to client printers that have the same drivers as the server, but different driver names.

You can add a driver mapping, edit an existing mapping, override custom settings for a mapping, remove a mapping, or change the order of driver entries in the list. When adding a mapping, enter the client printer driver name and then select the server driver you want to substitute.

Printer properties retention

This setting specifies whether or not to store printer properties and where to store them.

By default, the system determines if printer properties are stored on the user device, if available, or in the user profile.

When adding this setting to a policy, select an option:

- Saved on the client device only is for user devices that have a mandatory or roaming profile that is not saved. Choose this option only if all the servers in your farm are running XenApp 5 and above and your users are using Citrix online plug-in versions 9 through 12.x, or Citrix Receiver 3.x.
- Retained in user profile only is for user devices constrained by bandwidth (this option reduces network traffic) and logon speed or for users with legacy plug-ins. This option stores printer properties in the user profile on the server and prevents any properties exchange with the user device. Use this option with MetaFrame Presentation Server 3.0 or earlier and MetaFrame Presentation Server Client 8.x or earlier. Note that this is applicable only if a Remote Desktop Services (RDS) roaming profile is used.
- Held in profile only if not saved on client allows the system to determine where printer properties are stored. Printer properties are stored either on the user device, if available, or in the user profile. Although this option is the most flexible, it can also slow logon time and use extra bandwidth for system-checking.
- Do not retain printer properties prevents storing printer properties.

Retained and restored client printers

This setting enables or disables the retention and re-creation of printers on the user device. By default, client printers are auto-retained and auto-restored.

Retained printers are user-created printers that are created again, or remembered, at the start of the next session. When 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

Jul 24, 2014

The Drivers section contains policy settings related to printer drivers.

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.
- 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

Jun 01, 2016

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.

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.

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

Jul 24, 2014

The Universal Printing section contains policy settings for managing universal printing.

Universal printing EMF processing mode

This setting controls the method of processing the EMF spool file on the Windows user device.

By default, EMF records are spooled directly to the printer.

When adding this setting to a policy, select an option:

- Reprocess EMFs for printer forces the EMF spool file to be reprocessed and sent through the GDI subsystem on the user device. You can use this setting for drivers that require EMF reprocessing but that might not be selected automatically in a session.
- Spool directly to printer, when used with the Citrix Universal print driver, ensures the EMF records are spooled and delivered to the user device for processing. Typically, these EMF spool files are injected directly to the client's spool queue. For printers and drivers that are compatible with the EMF format, this is the fastest printing method.

Universal printing image compression limit

This setting specifies the maximum quality and the minimum compression level available for images printed with the Citrix Universal print driver.

By default, the image compression limit is set to Best quality (lossless compression).

If No Compression is selected, compression is disabled for EMF printing only.

When adding this setting to a policy, select an option:

- No compression
- Best quality (lossless compression)
- High quality
- Standard quality
- Reduced quality (maximum compression)

When adding this setting to a policy that includes the Universal printing optimization defaults setting, be aware of the following:

- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing optimization defaults

This setting specifies the default values for printing optimization when the universal print driver is created for a session.

- Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
- Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.

- Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached. Note that these settings apply only if the user device supports this behavior.
- Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.

Note: All of these options are supported for EMF printing. For XPS printing, only the Desired image quality option is supported.
When adding this setting to a policy that includes the Universal printing image compression limit setting, be aware of the following:
- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing preview preference

This setting specifies whether or not to use the print preview function for auto-created or generic universal printers.

By default, print preview is not used for auto-created or generic universal printers.

When adding this setting to a policy, select an option:
- Do not use print preview for auto-created or generic universal printers
- Use print preview for auto-created printers only
- Use print preview for generic universal printers only
- Use print preview for both auto-created and generic universal printers

Universal printing print quality limit

This setting specifies the maximum dots per inch (dpi) available for generating printed output in a session.

By default, No Limit is enabled, meaning users can select the maximum print quality allowed by the printer to which they connect.

If this setting is configured, it limits the maximum print quality available to users in terms of output resolution. Both the print quality itself and the print quality capabilities of the printer to which the user connects are restricted to the configured setting. For example, if configured to Medium Resolution (600 DPI), users are restricted to printing output with a maximum quality of 600 DPI and the Print Quality setting on the Advanced tab of the Universal Printer dialog box shows resolution settings only up to and including Medium Quality (600 DPI).

When adding this setting to a policy, select an option:
- Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)
- No Limit

Security policy settings

Apr 22, 2015

The Security section contains the policy setting for configuring session encryption and encryption of logon data.

SecureICA minimum encryption level

This setting specifies the minimum level at which to encrypt session data sent between the server and a user device.

Important: For the Virtual Delivery Agent 7.x, this policy setting can be used only to enable the encryption of the logon data with RC5 128-bit encryption. Other settings are provided only for backwards compatibility with legacy versions of 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.

Server limits policy settings

Sep 01, 2015

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).

> **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 is a Mircosoft dialog box that is not controlled by Citirx policy settings. For more information, see http://support.citrix.com/article/CTX118618.

Session limits policy settings

Jul 24, 2014

The Session Limits section contains policy settings that control how long sessions remain connected before they are forced to log off.

Disconnected session timer

This setting enables or disables a timer that specifies how long a disconnected, locked desktop can remain locked before the session is logged off.

By default, disconnected sessions are not logged off.

Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop can remain locked before the session is logged off.

By default, the time period is 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.

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 will be maintained if there is no input from the user.

By default, this timer is enabled.

Session idle timer interval

This setting specifies how many minutes an uninterrupted user device connection to a desktop will be maintained if there is no input from the user.

By default, idle connections are maintained for 1440 minutes (24 hours).

Session reliability policy settings

Jul 24, 2014

The Session Reliability section contains policy settings for managing session reliability connections.

Session reliability connections

This setting allows or prevents sessions to remain open during a loss of network connectivity.

By default, session reliability is allowed.

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.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity is restored. 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. If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, configure the Auto client reconnect authentication setting to require authentication. Users are then prompted 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 specified in the Session reliability timeout setting. After that, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session.

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.

Session reliability timeout

This setting specifies the length of time, in seconds, the session reliability proxy waits for a user to reconnect before allowing the session to be disconnected.

By default, this is set to 180 seconds, or three minutes.

Although you can extend the amount of time a session is kept open, this feature is designed to be convenient to the user and it 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.

Time zone control policy settings

Jul 24, 2014

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.

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

Jul 24, 2014

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 not currently supported.

Client TWAIN device redirection

This setting allows or prevents users from accessing TWAIN devices on the user device from image processing applications hosted on servers. By default, TWAIN device redirection is allowed.

The following policy settings are related:

- TWAIN compression level
- TWAIN device redirection bandwidth limit
- TWAIN device redirection bandwidth limit percent

TWAIN compression level

This setting specifies the level of compression of image transfers from client to server. Use Low for best image quality, Medium for good image quality, or High for low image quality. By default, medium compression is applied.

USB devices policy settings

Jul 24, 2014

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 handled as Interactive mode (02). Capture mode (04) is the recommended mode for signature devices. 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 http://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:

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.
PID	Product ID from the device descriptor.
REL	Release ID from the device descriptor.
Class	Class from either the device descriptor or an interface descriptor.

SubClass	Subclass from either the device descriptor or an interface descriptor.
Prot	Protocol from either the device descriptor or an interface descriptor.

Examples

Mode=00000004 VID=1230 PID=1230 class=03 #Input device operating in capture mode

Mode=00000002 VID=1230 PID=1230 class=03 #Input device operating in interactive mode (default)

Mode=00000001 VID=1230 PID=1230 class=03 #Input device operating without any optimization

Mode=00000100 VID=1230 PID=1230 # Device setup optimization disabled (default)

Mode=00000200 VID=1230 PID=1230 # Device setup optimization enabled

Disabling the optimization mode using a registry setting

The optimization mode can be disabled system-wide by a registry flag:

HKLM\System\CurrentControlSet\Services\Icausbb\Parameters

DisableInputOptimization DWORD - set value to **1**

A system restart is required for this registry change to take effect.

Disabling the screen saver for Wacom signature pad devices

For the use of Wacom signature pads and tablets, Citrix recommends that you disable the screen saver as follows:

1. Install the **Wacom-STU-Driver** after redirecting the device.
2. Install **Wacom-STU-Display MSI** to gain access to the signature pad control panel.
3. Go to **Control Panel > Wacom STU Display > STU430** or **STU530**, and select the tab for your model.
4. 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
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, remember:

- 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=1230_.
- 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=1230 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

Jun 01, 2016

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

Allows lowering of the color depth at which simple graphics are set to **16 bits per pixel**, potentially improving responsiveness over low bandwidth connections, at the cost of a slight degradation of image quality. This option is supported only when a video codec is not used to compress graphics.

By default, this is set to 24 bits per pixel.

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.

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**
- **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

Aug 03, 2016

The Moving Images section contains settings that enable you to remove or alter compression for dynamic images.

> ## Note
>
> For VDA versions 7.0 through 7.6, **Moving image compression** and **Target minimum frame rate** policy settings apply only when **Legacy graphics mode** is enabled. For VDA versions 7.6 FP1 and later, these settings apply when the Legacy graphics mode is disabled or enabled.

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.

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.

> ## Note
>
> For the Virtual Delivery Agent 7.x, the following policy settings apply only when the **Legacy graphics mode** policy setting is enabled.

Minimum image quality

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.

Progressive compression level

This setting provides a less detailed but faster initial display of images.

By default, no progressive compression is applied.

The more detailed image, defined by the normal lossy compression setting, appears when it becomes available. Use Very High or Ultra High compression for improved viewing of bandwidth-intensive graphics such as photographs.

For progressive compression to be effective, its compression level must be higher than the Lossy compression level setting.
Note: The increased level of compression associated with progressive compression also enhances the interactivity of dynamic images over client connections. The quality of a dynamic image, such as a rotating three-dimensional model, is temporarily decreased until the image stops moving, at which time the normal lossy compression setting is applied.
The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

Progressive compression threshold value

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

Still images policy settings

Aug 03, 2016

The Still Images section contains settings that enable you to remove or alter compression for static images.

> **Note**
>
> For the Virtual Delivery Agent 7.x, these policy settings apply only when the **Legacy graphics mode** policy setting is enabled.

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

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

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

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

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

Jul 24, 2014

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.

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

Jul 24, 2014

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.

CPU usage

This setting specifies the level of CPU usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and CPU usage is excluded from load calculations.

CPU usage excluded process priority

This setting specifies the priority level at which a process' CPU usage is excluded from the CPU Usage load index.

By default, this is set to Below Normal or Low.

Disk usage

This setting specifies the disk queue length at which the server reports a 75% full load. When enabled, the default value for disk queue length is 8.

By default, this setting is disabled and disk usage is excluded from load calculations.

Maximum number of sessions

This setting specifies the maximum number of sessions a server can host. When enabled, the default setting for maximum number of sessions a server can host is 250.

By default, this setting is enabled.

Memory usage

This setting specifies the level of memory usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and memory usage is excluded from load calculations.

Memory usage base load

This setting specifies an approximation of the base operating system's memory usage and defines, in MB, the memory usage below which a server is considered to have zero load.

By default, this is set to 768 MB.

Profile management policy settings

Nov 20, 2014

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

Jul 25, 2014

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.

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.

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

Jul 25, 2014

The Basic settings section contains policy settings relating to the basic configuration of Profile management.

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.

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

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

Jul 25, 2014

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.

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

Jul 25, 2014

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

Jul 25, 2014

The Exclusions section contains policy settings for configuring which files and directories in a users profile are excluded from the synchronization process.

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

Jul 25, 2014

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 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 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.

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.

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

Jul 25, 2014

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.

AppData(Roaming) policy settings

Jul 25, 2014

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

Jul 25, 2014

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.

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

Jul 25, 2014

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

Mar 25, 2015

The Documents section contains policy settings for specifying whether to redirect the contents the Documents folder to a shared network location.

Documents path

This setting specifies the network location to which files in the Documents folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

The Documents path setting must be enabled not only to redirect files to the Documents folder, but also to redirect files to the Music, Pictures, and Videos folders.

Redirection settings for Documents

This setting specifies how to redirect the contents of the Documents folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Documents folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Documents path policy setting.
- Redirect to the users home directory. Redirects content to the users home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.

If this setting is not configured here, Profile management does not redirect the specified folder.

Downloads policy settings

Jul 25, 2014

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.

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

Jul 25, 2014

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

Jul 25, 2014

The Links section contains policy settings that specify whether to redirect the contents the Links folder to a shared network location.

Links path

This setting specifies the network location to which the contents of the Links folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Links

This setting specifies how to redirect the contents of the Links folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Music policy settings

Mar 25, 2015

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.

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

Mar 25, 2015

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.

Saved Games policy settings

Jul 25, 2014

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.

Searches policy settings

Jul 25, 2014

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.

Start menu policy settings

Jul 25, 2014

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.

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.

Video policy settings

Mar 25, 2015

The Video section contains policy settings that specify whether to redirect the contents the Video folder to a shared network location.

Redirection settings for Video

This setting specifies how to redirect the contents of the Video folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Video folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Video path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

Video path

This setting specifies the network location to which the contents of the Video folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Log policy settings

Jul 25, 2014

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.

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.

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.

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\UserProfileManager is used.

Personalized user information

This setting enables or disables verbose logging of personalized user information.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Policy values at logon and logoff

This setting enables or disables verbose logging of policy values when a user logs on and off.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Registry actions

This setting enables or disables verbose logging of actions performed in the registry.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Registry differences at logoff

This setting enables or disables verbose logging of any differences in the registry when a user logs off.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Profile handling policy settings

Jul 25, 2014

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.

When enabling this setting, ensure the Delete locally cached profiles on logoff is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, profiles are deleted immediately.

Delete locally cached profiles on logoff

This setting specifies whether locally cached profiles are deleted after a user logs off.

When this setting is enabled, a user's local profile cache is deleted after they have logged off. Citrix recommends enabling this setting for terminal servers.

By default, this setting is disabled and a users local profile cache is retained after they log off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, cached profiles are not deleted.

Local profile conflict handling

This setting configures how Profile management behaves if a user profile exists both in the user store and as a local Windows user profile (not a Citrix user profile).

By default, Profile management uses the local Windows profile, but does not change it in any way.

To control how Profile management behaves, choose one of the following options:

- Use local profile. Profile management uses the local profile, but does not change it in any way.
- Delete local profile. Profile management deletes the local Windows user profile, and then imports the Citrix user profile from the user store.
- Rename local profile. Profile management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local profiles are used.

Migration of existing profiles

This setting specifies the types of profile migrated to the user store during logon if a user has no current profile in the user store.

Profile management can migrate existing profiles "on the fly" during logon if a user has no profile in the user store. After this, the user store profile is used by Profile management in both the current session and any other session configured with the path to the same user store.

By default, both local and roaming profiles are migrated to the user store during logon.

To specifies the types of profile migrated to the user store during logon, choose one of the following options:

- Local and roaming profiles
- Local
- Roaming
- None (Disabled)

If you select None, the system uses the existing Windows mechanism to create 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\ntuser.dat, 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.

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

Jul 25, 2014

The Registry section contains policy settings that specify which registry keys are included or excluded from Profile management processing.

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

Jul 25, 2014

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.

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.

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

Jul 25, 2014

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.

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.
- 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

Jul 25, 2014

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

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.

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.

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.

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.

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.

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.

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

Jul 25, 2014

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.

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.

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.

Virtual IP policy settings

Aug 06, 2014

The Virtual IP section contains policy settings that control whether sessions have their own virtual loopback address.

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.

This setting specifies the application executables that can use virtual loopback addresses. When adding programs to the list, specify only the executable name; you do not need to specify the entire path.

By default, no executables are specified.

Configure COM Port and LPT Port Redirection settings using the registry

Jun 01, 2016

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 version 7.9, 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\Defaults\Deprecated 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
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

Jun 18, 2014

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.

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).

This setting contains the editable text of the message to users notifying them of upcoming software updates or maintenance that requires them to log off.

By default, the message is: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}

This setting contains the editable text of the title bar of the advance warning message to users.

By default, the title is: Upcoming Maintenance

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.

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

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

This setting defines the period of time between notifying users to log off and the implementation of the forced logoff to process the pending maintenance.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the force logoff grace period setting is 5 minutes (00:05:00).

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}

This setting contains the editable text of the title bar of the force logoff message.

By default, the title is: Notification From IT Staff

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.

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

This setting determines how frequently the Citrix Connector agent task runs.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the regular time interval setting is 5 minutes (00:05:00).

Manage

Feb 24, 2016

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 resources

If you are using a hypervisor or cloud service to host machines that will deliver applications and desktops to users, you create your first connection to that hypervisor or cloud service when you create a Site. The storage and network details for that connection form its *resources*. Later, you can change that connection and its resources, and create new connections. You can also manage the machines that use a configured connection.

Connection leasing

Connection leasing 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. While connection leasing can improve connection resiliency and user productivity, this article covers the considerations related to the availability, operation, and performance of other features when a Controller is in leased connection mode.

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

Before a VDA can facilitate delivery of applications and desktops, it must register (establish communication) with a Controller. Controller addresses can be specified when you install the VDA, in Citrix policy settings, registry settings, and in several other ways. It is critical that VDAs get current information as Controllers are added, moved, and removed in the Site. This article describes how and when VDAs registers, methods for updating Controller information, and how to add, remove, and move Controllers

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

This release of XenApp and XenDesktop supports pure IPv4, pure IPv6,a nd 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 determine use of IPv4 or IPv6.

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.

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 the Citrix platform for instrumentation, telemetry, and business insight generation.

Licensing

Aug 31, 2016

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.

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.

> **Note**
>
> Studio and Director do not support Citrix License Server VPX. For more information about Citrix License Server VPX, see the Citrix Licensing documentation.

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

To 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:

- When configuring the Site, after you specify the license server, you are prompted to select the type of license to use. If there are no licenses on the server, the option to use the product for a 30-day trial period without a license is automatically selected.
- If there are licenses on the server, their details are displayed and you can select one of them. Or, you can add a license file to the server and then select that one.

To change the product edition and licensing model:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select **Edit Product Edition** in the Actions pane.
3. Update the appropriate options.

To access the License Administration Console, in the Actions pane, select **License Administration Console**. The console either appears immediately, or if the dashboard is configured as password-protected, you are prompted for License Administration Console credentials. For details about how to use the console, see the licensing documentation.

To add a licensing administrator:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane.
3. Select **Add licensing administrator** in the Actions pane.
4. Browse to the user you want to add as an administrator and choose permissions.

To change a licensing administrator's permissions or delete a licensing administrator:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane and then select the administrator.
3. Select either **Edit licensing administrator** or **Delete licensing administrator** in the Actions pane.

To add a licensing administrator group:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane.
3. Select **Add licensing administrator group** in the Actions pane.
4. Browse to the group you want to act as licensing administrators and choose permissions. Adding an Active Directory Group gives licensing administrator permissions to the users within that group.

To change a licensing administrator group's permissions or delete a licensing administrator group:

1. Select **Configuration > Licensing** in the Studio navigation pane.
2. Select the Licensing Administrators tab in the middle pane and then select the administrator group.
3. Select either **Edit licensing administrator group** or **Delete licensing administrator group** in the Actions pane.

Applications

Aug 31, 2016

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.

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.

This page lists all the Delivery Groups in the Site. If you have also created Application Groups, the page lists the Application Groups and Delivery Groups. You can choose from either group, but not from both groups. In other words, you cannot add applications to an Application Group and a Delivery Group at the same time. Generally, if you are using Application Groups, applications should be added to Application Groups rather than Delivery Groups.

When adding an application, you must select the check box next to at least one Delivery Group (or Application Group, if available) because every application must always be associated with at least one group

Click the **Add** dropdown to display the application sources.

Source	Description
From Start menu	Applications that are discovered on a machine in the selected Delivery Groups. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add, and then click **OK**. This source cannot be selected if you (1) selected Application Groups that have no associated Delivery Groups, (2) selected Application Groups with associated Delivery Groups that contain no machines, or (3) selected a Delivery Group containing no machines.
Manually defined	Applications located in the Site or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, click **OK**.
Existing	Applications previously added to the Site. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add and then click **OK**. This source cannot be selected If the Site has no applications.

App-V	Applications in App-V packages. When you select this source, a new page launches where you select the App-V server or the Application Library. From the resulting display, select the checkboxes of applications to add, and then click **OK**. For more information, see the App-V article. This source cannot be selected if App-V is not configured for the Site.
Application Group	Application Groups. When you select this source, a new page launches with a list of Application Groups. (Although the display also lists the applications in each group, you can select only the group, not individual applications.) All current and future applications in the selected groups will be added. Select the check boxes of Application Groups to add, and then click **OK**. This source cannot be selected if (1) there are no Application Groups, or (2) if the selected Delivery Groups do not support Application Groups (for example, Delivery Groups with statically assigned machines).

As noted in the table, some sources in the Add dropdown cannot be selected if there is no valid source of that type. Sources that are incompatible (for example, you cannot add Application Groups to Application Groups) are not included in the dropdown. Applications that have already been added to the groups you chose cannot be selected.

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.

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 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.
2. Select one or more applications in the middle pane and then select the appropriate task in the Actions pane.
3. Confirm the action, when prompted.

Remove applications from a Delivery Group

An application must be associated (belong) with at least one Delivery Group or Application Group. If you attempt to remove an application from a Delivery Group that would remove that application's association with any Delivery Group or Application Group, you are notified that the application will be deleted if you continue. When that happens, if you want to deliver that application, you must add it again from a valid source.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a Delivery Group. In the lower middle pane, select the **Applications** tab and then the application you want to remove.
3. Select **Remove Application** from the Actions pane.
4. Confirm the removal.

Remove applications from an Application Group

An application must belong to at least one Delivery Group or Application Group. If you attempt to remove an application from an Application Group that will result in that application no longer belonging to any Delivery Group or Application Group, you are notified that the application will be deleted if you continue. When that happens, if you want to deliver that application, you must add it again from a valid source.

1. Select **Applications** in the Studio navigation pane.
2. Select the Application Group in the middle pane, and then select one or more applications in the middle pane.
3. Select **Remove from Application Group** in the Actions pane.
4. Confirm the removal.

Change application properties

You can change the properties of only one application at a time.

To change the properties of an application:

1. Select **Applications** in the Studio navigation pane.
2. Select an application and then select **Edit Application Properties** in the Actions pane.
3. Select the page containing the property you want to change.
4. When you are finished, click **Apply** to apply any hanges you made and keep the window open, or click **OK** to apply changes tand close the window.

Property	**Select this page**
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.

Important: 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.
- 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.)

- 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.
- 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.)

Zones

Feb 24, 2016

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.

Throughout this article the term local refers to the zone being discussed. For example, "A VDA registers with a local Controller" means that a VDA registers with a Controller in the zone where the VDA is located.

Zones in this release are similar, but not identical to zones in XenApp version 6.5 and earlier. For example, in this implementation of zones, there are no data collectors. All Controllers in the Site communicate with one Site database in the primary zone. Also, failover and preferred zones work differently in this release.

Zone types

A Site always has one primary zone. It can also optionally have one or more satellite zones. Satellite zones can be used for disaster recovery, geographically-distant datacenters, branch offices, a cloud, or an availability zone in a cloud.

Primary zone

The primary zone has the default name "Primary," which contains the SQL Server Site database (and high availability SQL servers, if used), Studio, Director, Citrix StoreFront, Citrix License Server, and 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.

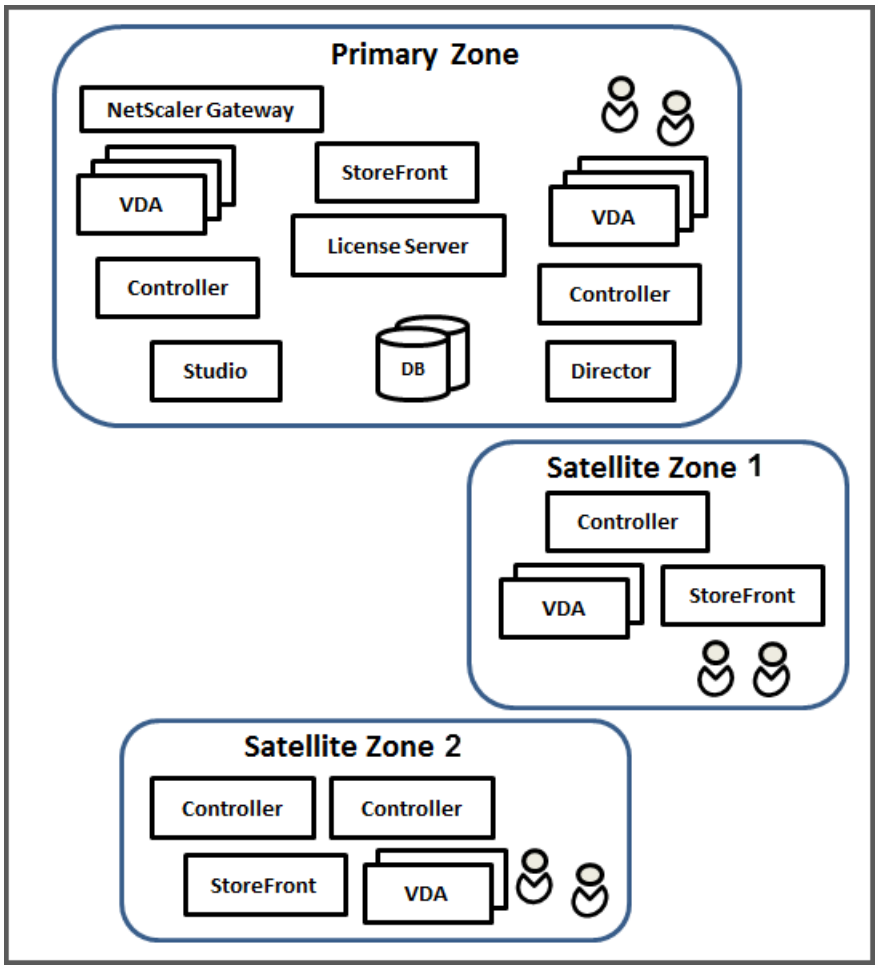
Satellite zone

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 different types of satellite zones, based on your unique needs and environment. The following figure illustrates a primary zone and examples of satellite zones.



- 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, 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.

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.)

Considerations, requirements, and best practice

- You can place the following items in a zone: Controllers, Machine Catalogs, and host connections. If a Machine Catalog uses a host connection, both the catalog and the connection should be in the same zone.
- 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, could 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.
- For optimal performance, install Studio and Director only in the primary zone. If you want another Studio instance in a satellite zone (for example, if a satellite zone containing Controllers is being used as failover in the event the primary zone becomes inaccessible), run Studio as a locally-published application. You can also access Director from a satellite zone because it is a web application.
- Ideally, 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.

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. 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.)

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.

1. Select **Configuration > Zones** in the Studio navigation pane.
2. Select a zone 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**.

1. Select **Configuration > Zones** in the Studio navigation pane.
2. Select one or more items.
3. Complete one of these actions: 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.

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.
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.

When you add a host connection or create a Machine Catalog (other than during Site creation), you can specify a zone where the item will be assigned, if you have already created at least one satellite zone.

In most cases, the primary zone is the default. When using Machine Creation Services to create a Machine Catalog, the zone that is configured for the host connection is automatically selected.

If the Site contains no satellite zones, the primary zone is assumed and the zone selection box does not appear.

Connections and resources

Jul 26, 2016

In this article:

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 form 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.

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.

VMware

- VMware virtualization environments article.
- VMware product documentation.

Microsoft Hyper-V

- Microsoft System Center Virtual Machine Manager virtualization environments article.
- Microsoft documentation.

Microsoft Azure

- Microsoft Azure virtualization environments article.
- Microsoft documentation.

Amazon Web Services (AWS)

- Citrix XenDesktop on 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.

Citrix CloudPlatform

- Citrix 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.

Host storage

When provisioning machines, data is classified by type:

- Operating system (OS) data, which includes master images.
- Temporary data, which includes all non-persistent data written to MCS-provisioned machines, Windows page files, user profile data, and any data that is synchronized with ShareFile. This data is discarded each time a machine restarts.
- Personal data stored on personal vDisks.

Providing separate storage for each data type can reduce load and improve IOPS performance on each storage device, making best use of the host's available resources. It also enables appropriate storage to be used for the different data

types – persistence and resilience is more important for some data than others.

Storage can be shared (located centrally, separate from any host, used by all hosts) or local to a hypervisor. For example, central shared storage could be one or more Windows Server 2012 clustered storage volumes (with or without attached storage), or an appliance from a storage vendor. The central storage might also provide its own optimizations such as hypervisor storage control paths and direct access through partner plugins.

Storing temporary data locally avoids having to traverse the network to access shared storage. 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.)

The storage shared by hypervisors method stores data that needs longer-term persistence centrally, providing centralized backup and management. That storage holds the OS disks and the personal vDisk disks.

When you select this method, you can choose whether to use local storage (on servers in the same hypervisor pool) for temporary machine data 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.

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

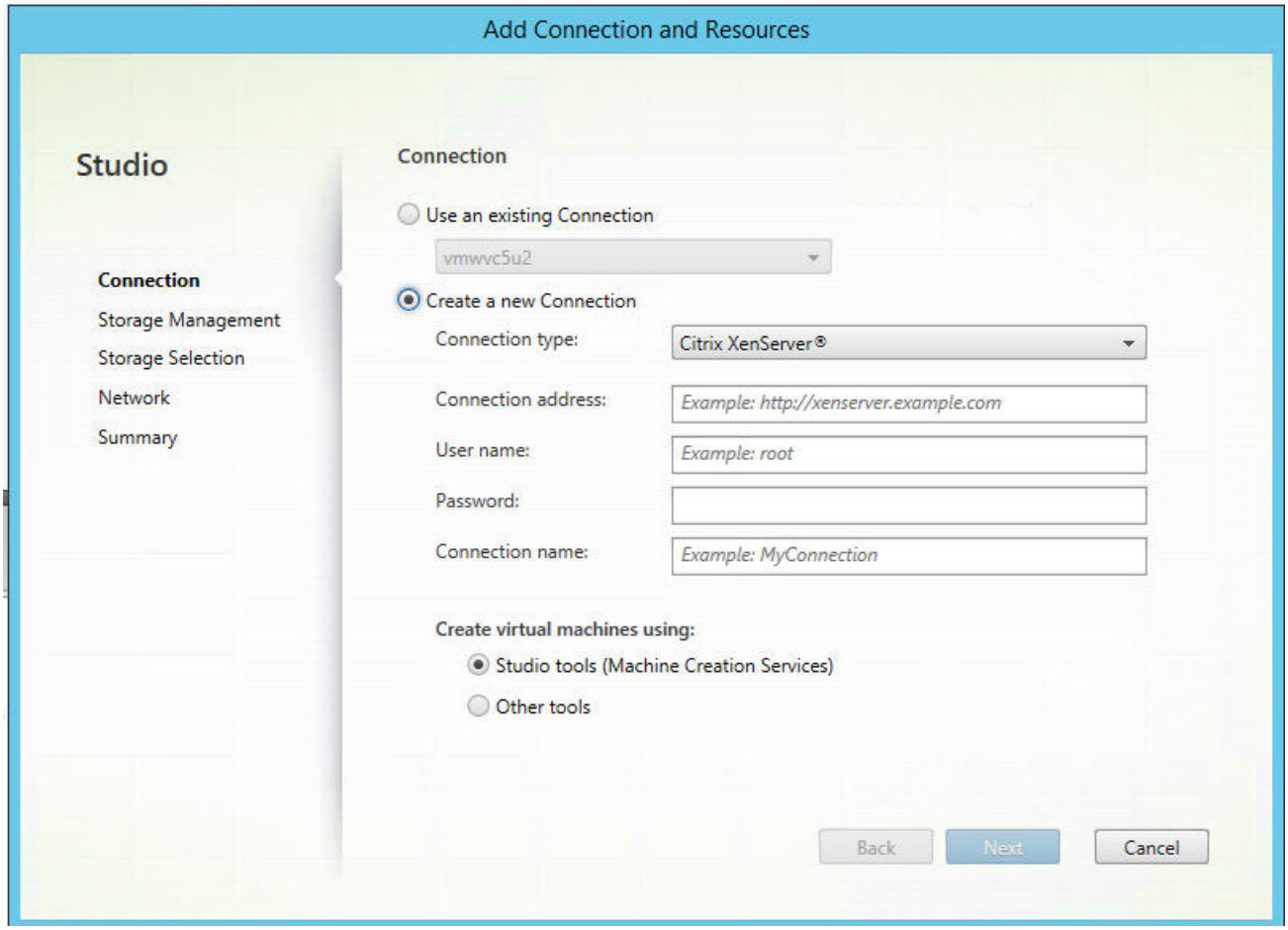
You can optionally create the first connection when you create the Site. The Site creation wizard contains the connection-related pages described below: Connection, Storage Management, Storage Selection, and Network.

If you are creating a connection after you create the Site, start with step 1 below.

If you are creating a connection based on the same host configuration as an existing connection, use this procedure.

Important: The host resources (storage and network) must be available before you create a connection.

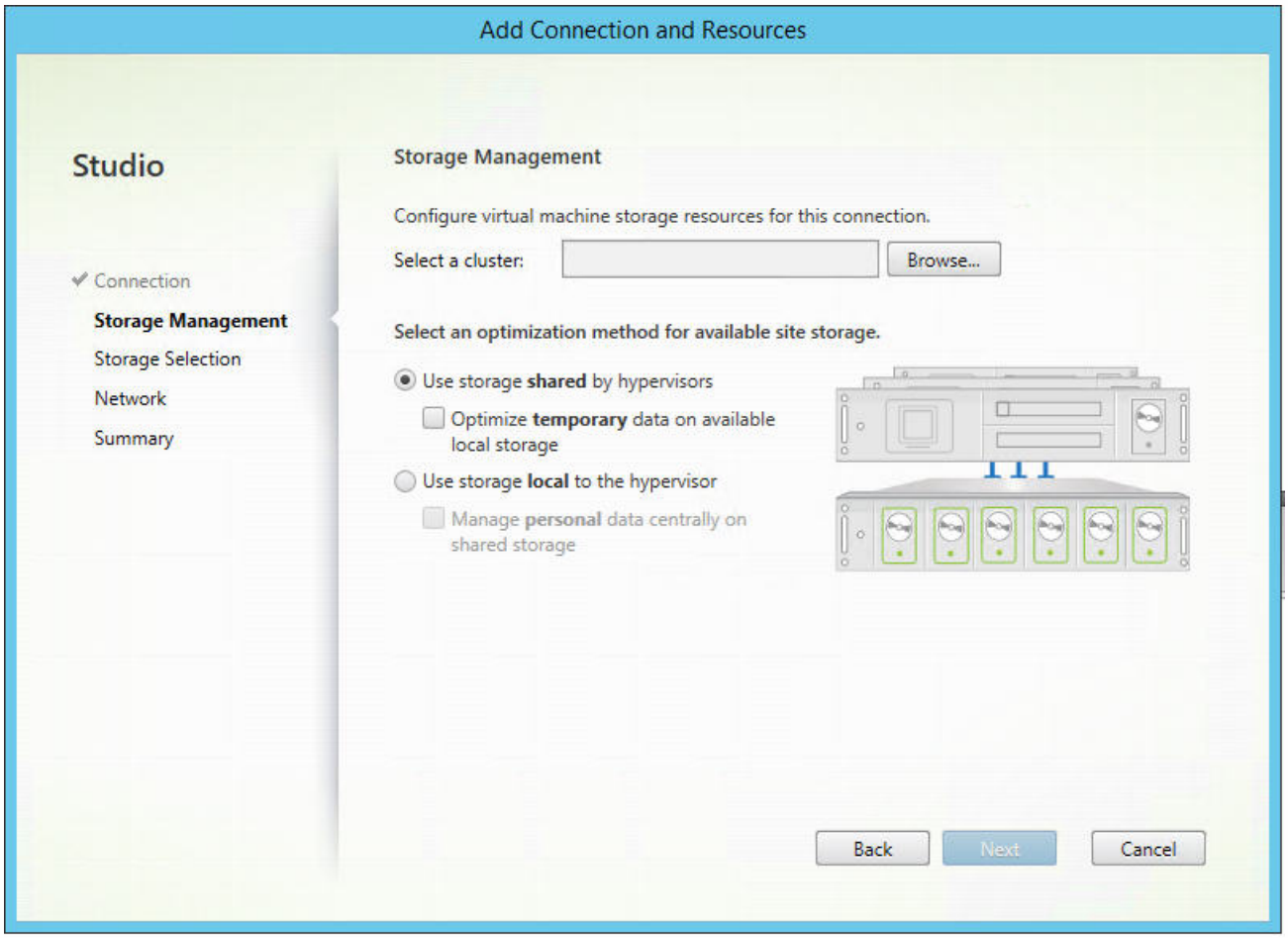
1. Select **Configuration > Hosting** in the Studio navigation pane.
2. Select **Add Connections and Resources** in the Actions pane.
3. Select **Create a new Connection**.
4. The wizard guides you through the following pages (specific page content depends on the selected connection type). After completing each page, click **Next** until you reach the Summary page.



On the **Connection** page:

- 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.

- Choose the tool you will use to create virtual machines: Studio tools (such as Machine Creation Services or Provisioning Services) or other tools.



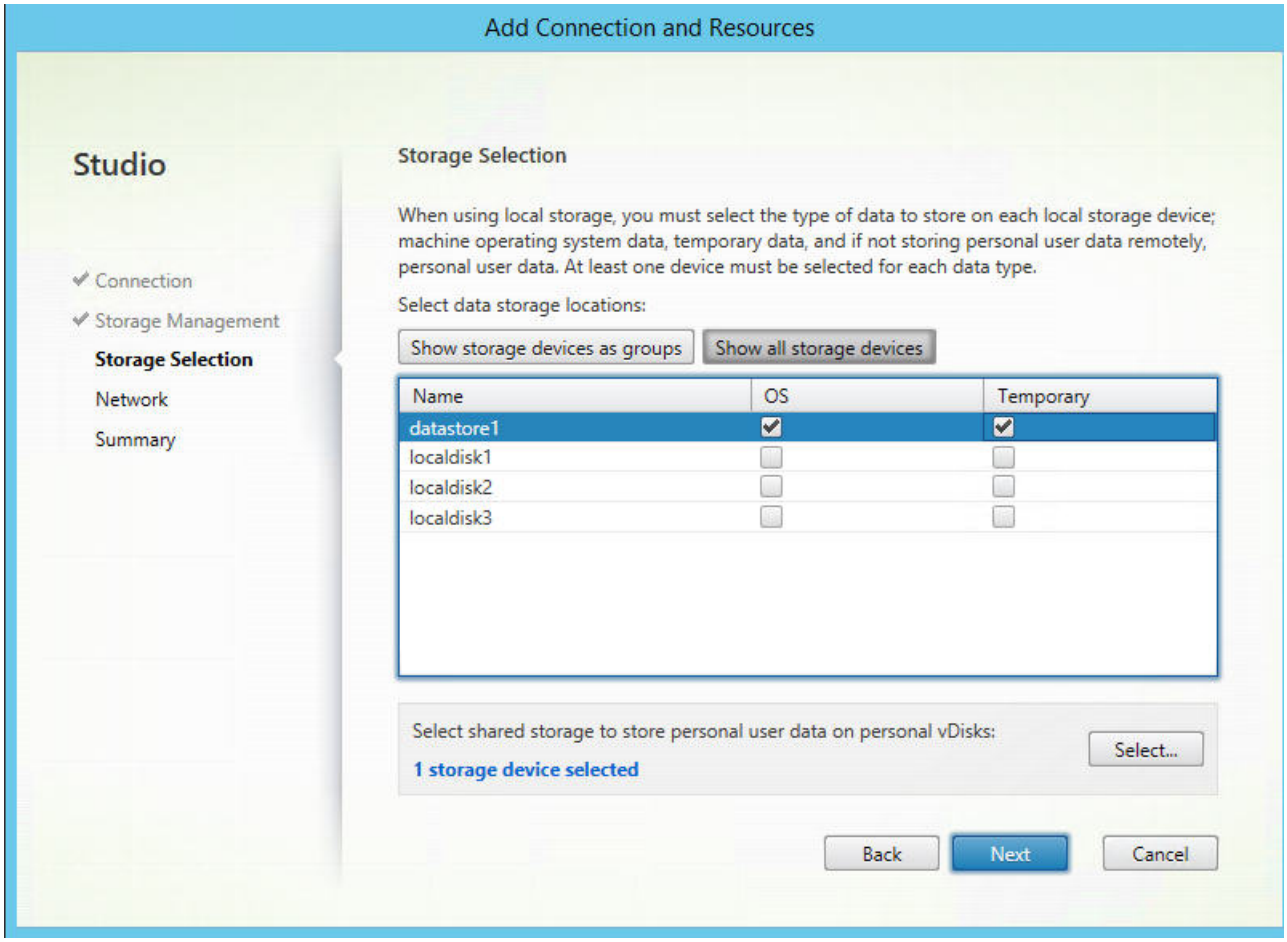
For information about storage management types and methods, see Host storage.

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.

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.



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) 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**.

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.

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.

Create a connection and resources from an existing connection

1. Select **Configuration > Hosting** in the Studio navigation pane.
2. Select **Add Connection and Resources** in the Actions pane.
3. Select **Use an existing Connection** and then choose the relevant connection.
4. The wizard guides you through the pages described in Create a connection and resources.

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:

- 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.

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.

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.
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.

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.

Connection leasing

Sep 09, 2015

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 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.

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>

  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.

For more considerations, see XenDesktop 7.6 Connection Leasing Design Considerations.

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.

Connection leasing is enabled by default.

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

Sep 29, 2015

Note: These features are valid only for Windows Server 2008 R2 and Windows Server 2012 R2 machines. They do not apply to Windows Desktop OS machines.

The Microsoft virtual IP address feature provides a published application with a unique dynamically-assigned IP address for each session. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a 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.
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

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.

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.

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 on Windows 2008 R2 only.

- 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\VIP for 32-bit machines)
- Name: PreferLoopback, Type: REG_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <list of processes>

Delivery Controllers

Aug 31, 2016

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.

Tip: Do not change the computer name or the domain membership of a Controller after the Site is configured.

How VDAs discover Controllers

Before a VDA can be used, it must register (establish communication) with a Controller on the Site. The VDA finds a Controller by checking a list of Controllers called the ListofDDCs. The ListOfDDCs comprises one or more DNS entries or IP addresses that point the VDA to Controllers on the Site. For load balancing, the VDA automatically distributes connections across all Controllers in the list.

In addition to the ListOfDDCs, the ListOfSIDs indicates which machine Security IDs (SIDs) the VDA allows to contact it as a Controller. The ListOfSIDs can be used to decrease the load on Active Directory or to avoid possible security threats from a compromised DNS server.

It is important to ensure that the ListOfDDCs and ListOfSIDs on all VDAs contain current information as Controllers are added and removed in the Site. If the lists are not updated, a VDA might reject session launches that were brokered by an unlisted Controller. Invalid entries can delay the startup of the virtual desktop system software. To keep the lists current, you can:

- Use the auto-update feature, which automatically updates the ListOfDDCs and ListOfSIDs as Controllers are added or removed. By default, auto-update is enabled.
- Self-manage – that is, manually update policy or registry settings that identify Controllers.

Information in the ListOfDDCs and ListOfSIDs can come from several places in a deployment. The VDA checks the following locations, in order, stopping at the first place it finds the lists:

1. A persistent storage location maintained for the auto-update feature. This location contains Controller information when auto-update is enabled and after the VDA successfully registers for the first time after installation. (This storage also holds machine policy information, which ensures that policy settings are retained across restarts.) For its initial registration after installation, or when auto-update is disabled, the VDA checks the following locations.

2. Policy settings (Controllers, Controller SIDs).
3. The Controller information under the Virtual Desktop Agent key in the registry. The VDA installer initially populates these values, based on Controller information you specify when installing the VDA.
4. OU-based Controller discovery. This is a legacy method maintained for backward compatibility.
5. The Personality.ini file created by Machine Creation Services.

If a ListOfDDCs specifies more than one Controller, the VDA attempts to connect to them in random order. The ListOfDDCs can also contain Controller groups, which are designated by brackets surrounding two or more Controller entries. The VDA attempts to connect to each Controller in a group before moving to other entries in the ListOfDDCs.

For XenDesktop users who have upgraded from versions earlier than 7.0, the auto-update feature replaces the CNAME function from the earlier version. You can manually re-enable the CNAME function, if desired; however, for DNS aliasing to work consistently, you cannot use both the auto-update feature and the CNAME function. See CTX137960 for information about re-enabling the CNAME functionality.

See the *Zones* article for information about where VDAs attempt to register in a Site that has more than one zone.

Considerations for choosing auto-update or self-manage

The policy setting that enables/disables auto-update is enabled by default.

The following types of deployments cannot use auto-update, and must self-manage.

- Deployments that use Controller groups.
- Deployments that use ListOfSIDs for security reasons. (Deployments that use ListOfSIDs to decrease the Active Directory load can use auto-update.)
- Deployments that use Provisioning Services without a write-back disk.
- Deployments that use the Controllers or Controller SIDs policy setting.

Auto-update

The *Enable auto update of Controllers* policy setting is located in the Virtual Delivery Agent category. To enable auto-update, enable the policy setting; this is the default. To disable auto-update, disable the policy setting.

When auto-update is enabled and you install a VDA, the VDA attempts to register with one of the Controller values you specified when you installed the VDA. The installer writes the Controller information you specify during VDA installation to the ListOfDDCs registry value.

After the VDA registers, the Controller with which it registered sends a list of the current Controller Fully Qualified Domain Names (FQDNs) and Security IDs (SIDs) to the VDA. The VDA writes this list to the auto-update persistent storage. Each Controller also checks the Site Configuration 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.

If a VDA receives a list that does not include the Controller it is registered with (in other words, that Controller was removed

from the Site), the VDA re-registers, choosing among the Controllers in the list. After a VDA registers or re-registers, it receives an updated list.

For example:

1. A deployment has three Controllers: A, B, and C. A VDA is installed and registers with Controller B (which was specified during VDA installation).
2. Two Controllers (D and E) are added to the Site. Within 90 minutes, VDAs receive updated lists and will accept connections from Controllers A, B, C, D, and E. (The load will not be spread equally to all Controllers until the VDAs are restarted.)
3. Controller B is removed from the Site. Within 90 minutes, VDAs receive updated lists because there has been a Controller change since the last check. The VDA installed in step 1 is registered with Controller B, which is no longer on the list, so that VDA re-registers, choosing among the Controllers in the current list (A, C, D, and E).

Self-manage

If you do not use auto-update, you must update the Citrix policy setting or registry values for each VDA in the Site after you add, move, or remove Delivery Controllers in the Site. Registry changes can also be updated using Group Policy Object.

To self-manage using Citrix policy settings:

1. Update the FQDN values specified in the Controllers policy setting. This policy setting is located in the Virtual Delivery Agent category.
2. If you also use ListOfSIDs in your deployment, update the SID values specified in the Controller SIDspolicy setting.

To self-manage using the registry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Update the ListOfDDCs registry key, which lists the FQDNs of all the Controllers in the Site. (This key is the equivalent of the Active Directory Site OU.) Separate multiple values with spaces. Surround Controller groups with brackets. 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 discovery; FarmGUID is present if a site OU was specified during VDA installation.

2. Optionally, update the ListOfSIDs registry key: HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

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.

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.

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.

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.

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.

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.

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.
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.

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.

Active Directory OU-based Controller discovery

This Delivery Controller discovery method is supported primarily for backward compatibility, and is valid only for Virtual Delivery Agents (VDAs) for Windows Desktop OS, not VDAs for Windows Server OS. Active Directory-based discovery requires that all computers in a Site are members of a domain, with mutual trusting relationships between the domain used by the Controller and the domain(s) used by desktops. If you use this method, you must configure the GUID of the OU in each desktop registry.

To perform an OU-based Controller discovery, run the Set-ADControllerDiscovery.ps1 PowerShell script on the Controller (each Controller contains this script in the folder $Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts). To run the script, you must have CreateChild permissions on a parent OU, plus full administration rights.

When you create a Site, a corresponding Organizational Unit (OU) must be created in Active Directory if you want desktops to discover the Controllers in the Site through Active Directory. The OU can be created in any domain in the forest that contains your computers. As best practice, the OU should also contain the Controllers in the Site, but this is not enforced or required. A domain administrator with appropriate privileges can create the OU as an empty container, then delegate administrative authority over the OU to a Citrix administrator.

The script creates several essential objects. Only standard Active Directory objects are created and used. It is not necessary to extend the schema.

- A Controllers security group. The computer account of all Controllers in the Site must be a member of this security group. Desktops in a Site accept data from Controllers only if they are members of this security group.
  Ensure that all Controllers have the 'Access this computer from the network' privilege on all virtual desktops running the VDA. You can do this by giving the Controllers security group this privilege. If Controllers do not have this privilege, VDAs will not register.

- A Service Connection Point (SCP) object that contains information about the Site, such as the Site name. If you use the Active Directory Users and Computers administrative tool to inspect a Site OU, you might need to enable Advanced Features in the View menu to see SCP objects.
- A container called RegistrationServices, which is created in the Site OU. This contains one SCP object for each Controller in the Site. Each time the Controller starts, it validates the contents of its SCP and updates it, if necessary.

If multiple administrators are likely to add and remove Controllers after the initial installation, they need permissions to create and delete children on the RegistrationServices container, and Write properties on the Controllers security group; these permissions are granted automatically to the administrator who runs the Set-ADControllerDiscovery.ps1 script. The domain administrator or the original installing administrator can grant these permissions, and Citrix recommends setting up a security group to do this.

When you are using a Site OU:

- Information is written to Active Directory only when installing or uninstalling this software, or when a Controller starts and needs to update the information in its SCP (for example, because the Controller was renamed or because the communication port was changed). By default, the Set-ADControllerDiscovery.ps1 script sets up permissions on the objects in the Site OU appropriately, giving each Controller Write access to its SCP. The contents of the objects in the Site OU are used to establish trust between desktops and Controllers. Ensure that:
  - Only authorized administrators can add or remove computers from the Controllers security group, using the security group's access control list (ACL).

    - Only authorized administrators and the respective Controller can change the information in the controller's SCP.
- If your deployment uses replication, be aware of potential delays; see the Microsoft documentation for details. This is particularly important if you create the Site OU in a domain that has domain controllers in multiple Active Directory sites. Depending on the location of desktops, Controllers, and domain controllers, changes that are made to Active Directory when you are initially creating the Site OU, installing or uninstalling Controllers, or changing Controller names or communication ports might not be visible to desktops until that information is replicated to the appropriate domain controller. The symptoms of such replication delay include desktops that cannot establish contact with Controllers and are therefore not available for user connections.
- This software uses several standard computer object attributes in Active Directory to manage desktops. Depending on your deployment, the machine object's fully qualified domain name, as stored in the desktop's Active Directory record, can be included as part of the connection settings that are returned to the user to make a connection. Ensure that this information is consistent with information in your DNS environment.

To move a Controller to another Site using OU-based Controller discovery, follow the directions above for moving a Controller. After you remove the Controller from the old Site (step 2), run the PowerShell script **Set-ADControllerDiscovery –sync**. This script synchronizes the OU with the current set of Controllers. After joining the existing Site (step 3), run the same script on any Controller in the new Site.

To create a Site, the Citrix administrator who runs the script must have rights over the Site OU to create objects (SCP, container, and security group).

> (If the Site OU is not present, the administrator must have rights to create that as well. Citrix recommends that the AD domain administrator pre-create that OU and delegate rights to it to the Citrix Site administrator identity. Optionally, the script can also create the Site OU. To allow this, the administrator needs the “create OU” right on the new OU’s parent OU. However, as noted, Citrix does not recommend this.)

Later, to add or remove a Controller from the Site, the Citrix administrator must have rights to add/remove a machine from the security group, and create/delete an SCP.

During normal operations, Controllers and VDAs need read rights to all objects in the OU and below. VDAs access the OU as their own machine identity; that machine identity needs at least read rights in the OU to be able to discover Controllers. A Controller also needs the rights to set properties on its own SCP object in the container.

Granting the Citrix administrator full rights to the child OUs will permit all these actions. However, if your deployment has stricter security requirements (such as restricting who can use the script for which action), you can use the Delegation of Control wizard to set specific rights. The following example procedure grants rights to create the Site.

1. Create an OU to contain the child objects (Service Connection Point (SCP), container, and security group).
2. Select the OU, then right-click and select **Delegate Control**.
3. In the Delegation of Control wizard, specify the domain user to delegate control to for the OU.
4. On the **Tasks to Delegate** page, select **Create a custom task to delegate**.
5. On the **Active Directory Object type** page, accept the default **This folder, existing objects in this folder, and creation of new objects in this folder**.
6. On the **Permissions** page, select **Permissions Create All Child Objects**.
7. Finish the wizard to confirm the privileges.

Sessions

Jan 07, 2016

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, and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

- Session reliability
- Auto Client Reconnect
- ICA Keep-Alive
- Workspace control
- Session roaming

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 sessions through 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 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.

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.

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.

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 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.

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.

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: This setting applies only to VMs with desktop (workstation) VDAs; Microsoft controls the logon timeout on machines with server VDAs.

Use Search in Studio

Sep 09, 2015

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

Jan 13, 2016

Tags are strings that identify items such as machines, applications, Delivery Groups, and policies. After creating a tag and then adding it to an item, you can tailor certain operations to apply only to items that have a specified tag:

- Tailor search displays in Studio.

  For example, if you want to display only applications that have been optimized for testers, add a tag named “test” to those applications. Then, filter the Studio search with the tag “test”. Similarly, if you want to display only Delivery Groups that contain test team members, add a “tester” tag to Delivery Groups that contain test team members and then filter the Studio search with the “tester” tag.

- Apply (assign) Citrix policies to applications, machines, or Delivery Groups 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.

Manage tags

Select a machine, application, or Delivery Group in Studio 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 item you selected.

- An enabled checkbox indicates that tag has already been added to the selected item.
- If you select a group, a checkbox containing a hyphen indicates that some, but not all items in that group have that tag added.

The following actions are available from the Manage Tags dialog box:

- To add or remove a tag, enable or clear the checkbox next to the tags you want to add or remove.
- To create a tag, select **Create tag**. Enter a name and description. Tag names must be unique and are not case-sensitive. Then click **OK**.
- To edit a tag, select a tag and then select **Edit tag**. Enter a new name and/or description, and then click **Save**. You can edit only one tag at a time.
- To delete one or more tags, select the tags and then select **Delete tag**. The Delete Tag dialog box lists how many items currently use the tags you selected. Click an item to display more information; for example, if two machines are affected, clicking that item displays the two machine names. After you see which items will be affected, confirm whether you want to delete the tags.

IPv4/IPv6 support

Sep 09, 2015

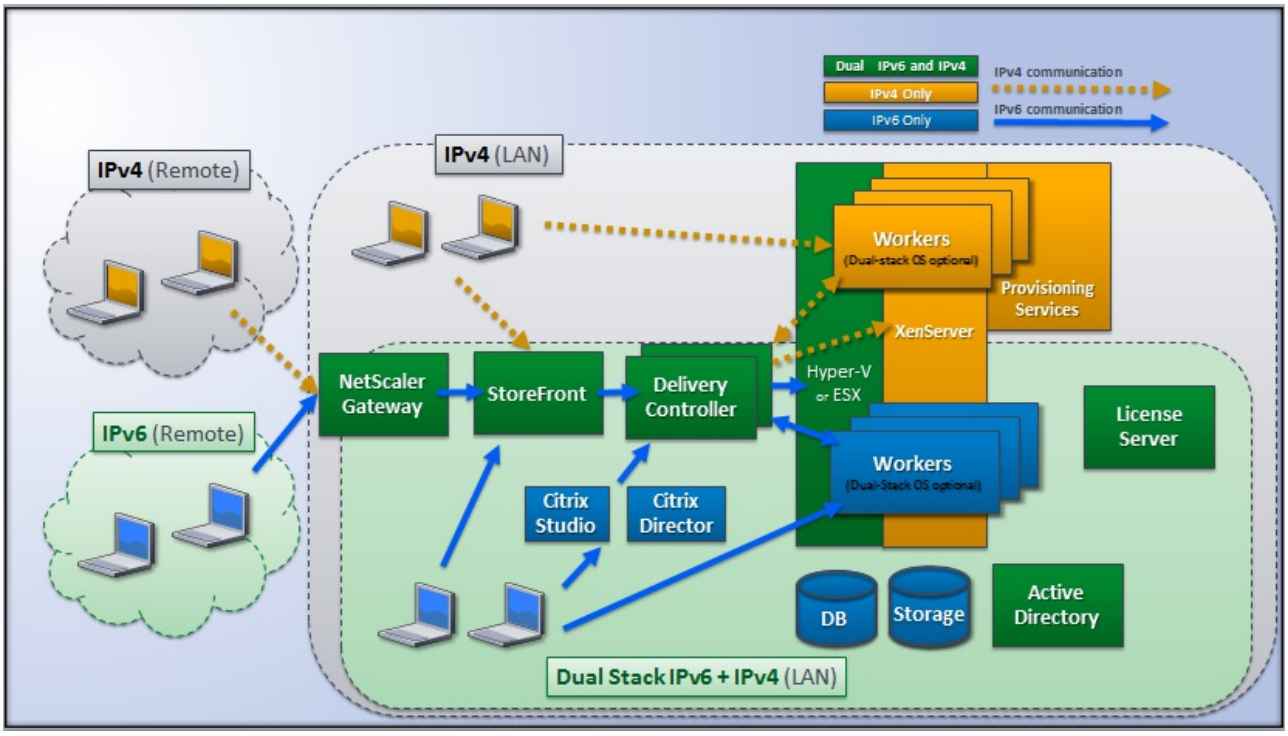
This release supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks.

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.

The following figure illustrates a dual-stack IPv4/IPv6 deployment. In this scenario, a worker is a VDA installed on a hypervisor or on a physical system, and is used primarily to enable connections for applications and desktops. Components that support dual IPv6 and IPv4 are running on operating systems that use tunneling or dual protocol software.



These Citrix products, components, and features support only IPv4:

- 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

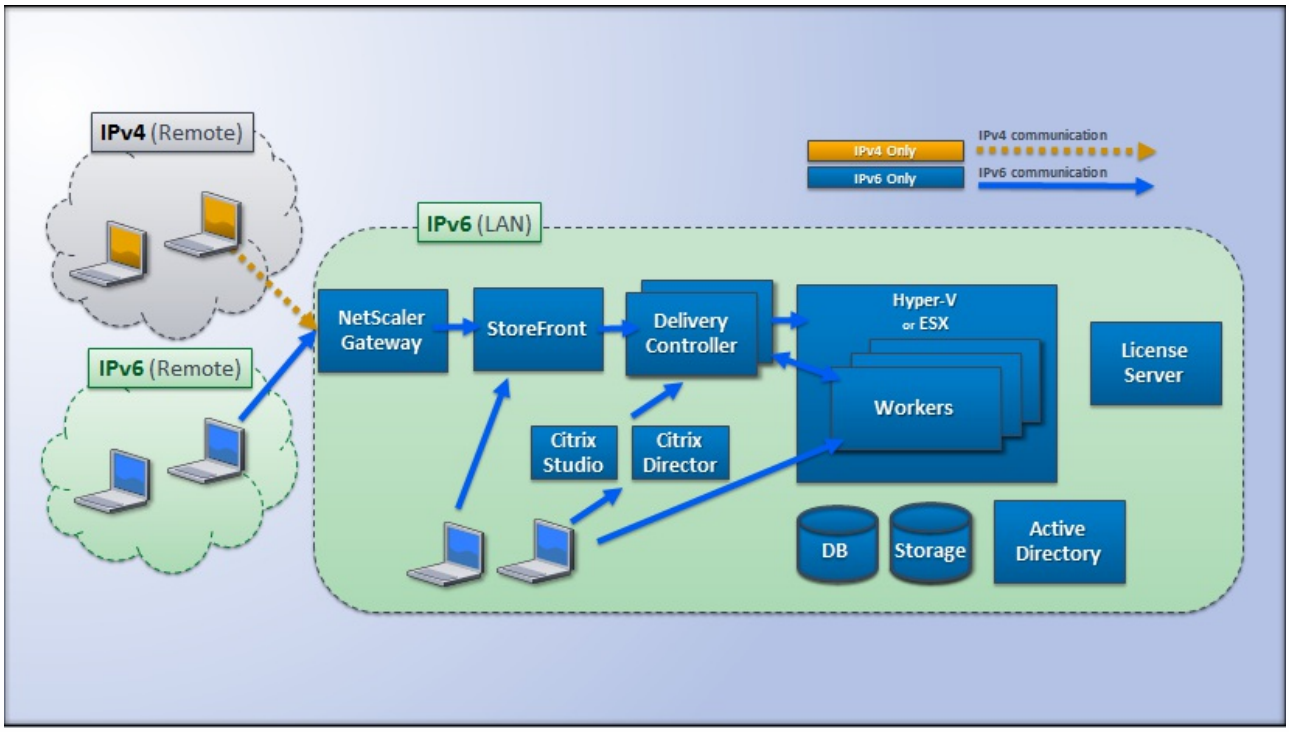
In this deployment:

- 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.

The following figure illustrates a pure IPv6 deployment. In this scenario:

- The components are running on operating systems configured to support an IPv6 network.
- The primary Citrix policy setting (Only use IPv6 Controller registration) is enabled for all VDAs; they must register with the Controller using an IPv6 address.



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

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.

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.

Client folder redirection

Sep 09, 2015

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 Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the server:
    1. Create a key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    2. Create a REG_DWORD value.
        - Name: CFROnlyModeAvailable
        - Type: REG_DWORD
        - Data: Set to 1
2. On the user device:
    1. Ensure the latest version of Citrix Receiver is installed.
    2. From the Citrix Receiver installation directory, start CtxCFRUI.exe.
    3. Select the Custom radio button and add, edit, or remove folders.
    4. Disconnect and reconnect your sessions for the setting to take effect.

User profiles

Sep 25, 2015

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.

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.

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

The following Profile management policy settings are suggested guidelines for the different machine types. They work well in most cases, but you may want to deviate from these as your deployment requires.

Important: Delete locally cached profiles on logoff, Profile streaming, and Always cache are enforced by the auto-configuration feature. Adjust the other policies manually.

Persistent machines

Policy	Both persistent and dedicated	Both persistent and shared
Delete locally cached profiles on logoff	Disabled	Enabled
Profile streaming	Disabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)
Active write back	Disabled	Disabled (note 3)
Process logons of local administrators	Enabled	Disabled (note 4)

Provisioned machines

Policy	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled (note 5)	Enabled
Profile streaming	Enabled	Enabled
Always cache	Disabled (note 6)	Disabled
Active write back	Enabled	Enabled
Process logons of local administrators	Enabled	Enabled (note 7)

1. Because Profile streaming is disabled for this machine type, the Always cache setting is always ignored.
2. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
3. Disable Active write back except to save changes in profiles of users who roam between 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 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.

In deployments with multiple operating systems (OSs), you might want some of a user's profile to be shared by each OS. The rest of the profile is not shared and is used only by one OS. To ensure a consistent user experience across the OSs, you need a different configuration for each OS. This is advanced folder redirection. For example, different versions of an application running on two OSs might need to read or edit a shared file, so you decide to redirect it to a single network location where both versions can access it. Alternatively, because the Start Menu folder contents are structured differently in two OSs, you decide to redirect only one folder, not both. This separates the Start Menu folder and its contents on each OS, ensuring a consistent experience for users.

If your deployment requires advanced folder redirection, you must understand the structure of your users' profile data and determine which parts of it can be shared between OSs. This is important because unpredictable behavior can result unless folder redirection is used correctly.

To redirect folders in advanced deployments:

- Use a separate Delivery Group for each OS.
- Understand where your virtual applications, including those on virtual desktops, store user data and settings, and understand how the data is structured.
- For shared profile data that can safely roam (because it is structured identically in each OS), redirect the containing folders in each Delivery Group.
- For non-shared profile data that cannot roam, redirect the containing folder in only one of the Desktop Groups, typically

the one with the most used OS or the one where the data is most relevant. Alternatively, for non-shared data that cannot roam between OSs, redirect the containing folders on both systems to separate network locations.

Example advanced deployment - This deployment has applications, including versions of Microsoft Outlook and Internet Explorer, running on Windows 8 desktops and applications, including other versions of Outlook and Internet Explorer, delivered by Windows Server 2008. To achieve this, you have already set up two Delivery Groups for the two OSs. Users want to access the same set of Contacts and Favorites in both versions of those two applications.
Important: The following decisions and advice are valid for the OSs and deployment described. In your organization, the folders you choose to redirect and whether your decide to share them depend on a number of factors that are unique to your specific deployment.

- Using policies applied to the Delivery Groups, you choose the following folders to redirect.

Folder	Redirected in Windows 8?	Redirected in Windows Server 2008?
My Documents	Yes	Yes
Application Data	No	No
Contacts	Yes	Yes
Desktop	Yes	No
Downloads	No	No
Favorites	Yes	Yes
Links	Yes	No
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 http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

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

Oct 31, 2016

Citrix Insight Services (CIS) is the Citrix flagship platform for diagnostics and troubleshooting. It enables technical users (customers, partners, and engineers) to self-diagnose and fix problems and optimize their environments. For details and the latest information about CIS and how it works, see https://cis.citrix.com (Citrix account credentials required).

All information uploaded to Citrix Insight Services 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 http://www.citrix.com/about/legal/privacy.html

This XenApp and XenDesktop release supports the following tools and technologies.

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. Support may ask you to upload this information, which will be used to help Citrix improve its customers' installation experiences.

The information is stored locally under %ProgramData%\Citrix\.

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 http://more.citrix.com/XD-CEIP.

You are automatically enrolled in CEIP when you create a XenApp or XenDesktop Site. 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.

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, Session Recording. See their documentation for details about installation and participation default values.

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.
- 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.

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 for analysis and troubleshooting.

Call Home runs as a background service under the name Citrix Telemetry Service.

For more information, see http://more.citrix.com/XD-CALLHOME.

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 24 hours.

- Compressing data allows Call Home to maintain a small footprint on the VDA.
- Traces are held in memory to avoid IOPs on provisioned machines.
- The trace buffer uses a circular mechanism to retain traces in memory.

You can indicate whether or not you want to participate in Call Home when you install a Delivery Controller or VDA using the graphical interface in the full-product installer.

After installing components, you can use PowerShell cmdlets to:

- Enable scheduled Call Home uploads or change your current schedule. This includes enabling scheduled uploads in a master image used in a Machine Catalog, which eliminates having to configure Call Home in each created VM.
- Manually collect data and upload it to CIS.
- Manually collect data and store it locally, and then later upload that data to CIS.

For complete PowerShell cmdlet syntax, see the cmdlet help.

When you enroll in scheduled Call Home uploads and when you manually upload diagnostic information to CIS, you must provide Citrix account credentials. CIS 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.

You can enroll in scheduled uploads to Call Home when using the full-product installation wizard or later, using PowerShell cmdlets. By default, data is collected and uploaded to CIS every Sunday at around 3:00 AM, local time. The upload time is randomized with a two hour interval form 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 bundles on a scheduled basis, you can still use PowerShell cmdlets to manually collect and upload Call Home data.

Enable scheduled uploads during component installation

When you use the graphical interface of the full-product XenApp and XenDesktop installer to install a Controller or VDA, you can indicate whether or not you want to participate in scheduled uploads to Call Home. By default, participation is selected.

- If you want to participate, sign in to CIS with your Citrix account credentials.
- If you do not want to participate (or if you want to participate, but your Citrix account credentials could not be validated), decline participation on the wizard page. You can enroll later after Site setup, using PowerShell cmdlets.

Enable scheduled uploads using PowerShell cmdlets

Enter the following cmdlets to enable scheduled uploads of Call Home diagnostic information bundles to CIS. 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.

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

You can create a custom daily or weekly schedule.

```
$timespan = New-TimeSpan –Hours <hours> -Minutes <minutes>
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek <day> -UploadFrequency {Daily|Weekly}
```

Cancel scheduled uploads

Enter the following cmdlet to cancel scheduled uploads. (You can still upload diagnostic data bundles 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
```

To confirm the schedule, enter Get-CitrixCallHomeSchedule, In the above example, it should return StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

On the machine where Call Home is enabled, in the Program Files\Citrix\Telemetry Service directory, edit the TelemetryService.exe.config file, adding the yellow highlighted portion in the following example. (The example specifies the server address and port 10.158.139.37:3128; yours will differ.)

After an upload completes, you can view the uploaded Call Home information at CIS.citrix.com.

```
<?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="0.0.0.0-7.0.0.0" newVersion="7.0.0.0" />
    </dependentAssembly>
   </assemblyBinding>
  </runtime>
<system.net>
 <defaultProxy>
  <proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.158.139.37:3128" />
 </defaultProxy>
</system.net>
</configuration>
```

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>]

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' If this parameter is omitted, data from all collectors is collected.
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.

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
```

Monitor

May 31, 2016

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 you can use to monitor, troubeleshoot, and 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.

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.

Monitor Service API using the OData protocol

Administrators can use the Site's Monitor Service API to search historical data using the OData protocol. This allows IT to analyze historical trends for planning purposes, to perform detailed troubleshooting of connection and machine failures, and extract information for feeding into other tools and processes.

The Monitor Service schema provides the following types of data:

- Data relating to connection failures
- Machines in a failure state
- Session usage
- Logon duration
- Load balancing data

For details, see the Monitor Service OData API articles.

Personal vDisk diagnostic tool

Use the PvD diagnostic tool to monitor changes made by uers to the user and application parts of their personal vDisks, such as applications they have installed and files they have modified.

For details, see the Personal vDisk monitoring article.

Session Recording

Apr 24, 2015

Session Recording allows you to record the on-screen activity of any user session hosted from a Server OS VDI machine, 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 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.

Enhanced security through logging and monitoring. Session Recording allows organizations to record on-screen user activity for applications that deal with sensitive information. This is especially critical in regulated industries such as health care 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

Feb 25, 2015

After you perform the following steps, you can begin recording and reviewing XenApp and XenDesktop sessions.

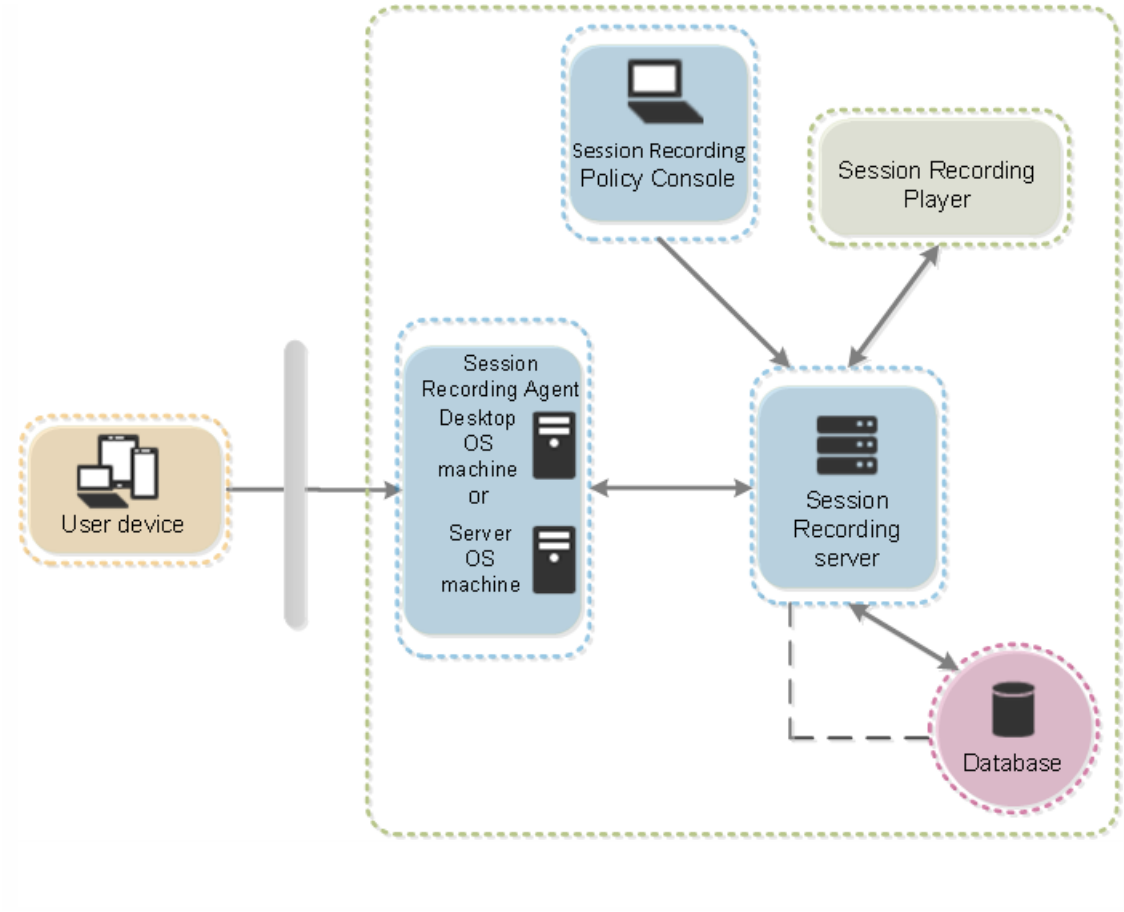
1. Become familiar with the Session Recording components.
2. Select the deployment scenario for your environment.
3. Verify the installation requirements.
4. Install the Windows roles and features prerequisites.
5. Install Session Recording.
6. Configure the Session Recording components to permit recording and viewing of sessions.

Session Recording consists of five components:

- **Session Recording Agent.** A component installed on each Server OS and VDI machine to enable recording. It is responsible for recording session data.
- **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.
- **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**. You cannot change the 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 Server OS machine. 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 Server OS machine 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

Mar 02, 2016

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.

Depending upon your environment, you can deploy the Session Recording components in different scenarios.

A Session Recording deployment does not have to be limited to a single site. With the exception of 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.

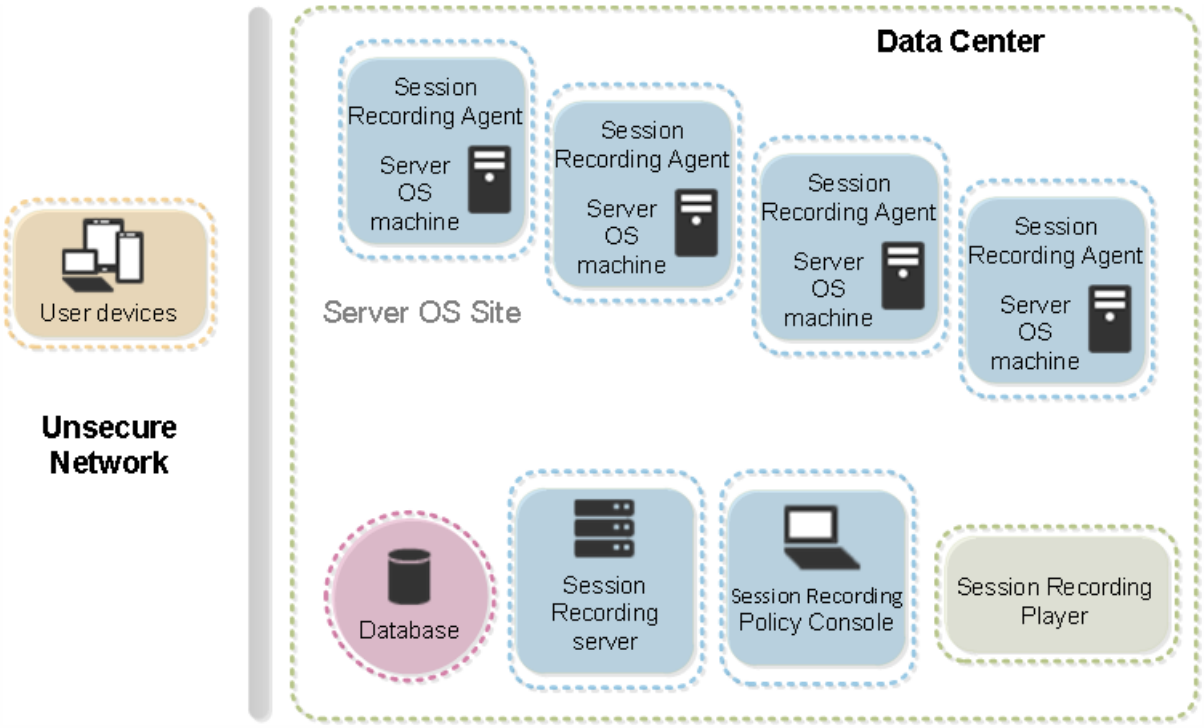
Alternatively, if you have a large site with many agents and plan to record many graphically intense applications (for example, AutoCAD applications), or you have many sessions to record, a Session Recording Server can experience a high performance demand. To alleviate performance issues, you can install multiple Session Recording Servers on different computers and point the Session Recording Agents to the different computers. Keep in mind that an agent can point to only one server at a time.

These are the two suggested configurations for a Session Recording deployment:

- Deploy the Session Recording Agent on single Server OS machine.
- Deploy the Session Recording Agent on multiple Server OS or workstation OS machines on a site.

Server site deployment

Use this type of deployment for recording sessions for one or more sites. The Session Recording Agent is installed on each Server OS machine 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, 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. Outside the firewall, in an unsecured network environment, are XenApp clients, such as a workstation, mobile devices, and a laptop computer.



- To enable Session Recording components to communicate with each other, ensure you install them in the same domain or across trusted domains that have a transitive trust relationship. The system cannot be installed into a workgroup or across domains that have an external trust relationship.
- Session Recording does not support the clustering of two or more Session Recording Servers in a deployment.
- Due to its intense graphical nature and memory usage when playing back large recordings, Citrix does 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 stand-alone server running 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. See the Microsoft documentation for information about enabling these settings.
- Consider the effects of session sharing when planning your Session Recording deployment. Session sharing for published applications can conflict with Session Recording 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 applications 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, Citrix does 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.

Security recommendations

Nov 30, 2016

Session Recording is designed to be deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is designed to be 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 each Session Recording component. MSMQ provides a reliable data transport mechanism for sending recorded session data from the Session Recording Agent to the Session Recording Server.

Consider these security recommendations when planning your deployment:

- Ensure 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 can impact the system functionality or abuse the system might occur. Citrix recommends that you assign different administrator roles to different persons or accounts that you do not allow general session users to have administrator privileges to the VDA system.
  - XenApp and XenDesktop administrators should not grant VDA local admin role to any users of published apps or desktops. If the local admin role is a requirement, protect the Session Recording Agent components with Windows mechanisms or 3rd-party solutions.
  - Separately assign the Session Recording database administrator and Session Recording policy administrator.
  - Citrix recommends 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 installed with Session Recording Player. If a user is not authorized as the Player role, do not grant that user local administrator role for any player machine. Disable anonymous access.
  - Citrix recommends 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 VDA machines unless for specific troubleshooting cases.

    To disable core memory dump:

    1. Right-click My Computer, and then click 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 https://support.microsoft.com/en-us/kb/307973.

  + Ensure log on credentials or security information does not appear in all local and Web applications published or used inside the corporation or they are recorded by Session Recording.

  + Users should close any application that might expose sensitive information before switching to a remote ICA session.

+ Session owners should notify attendees that online meetings and remote assistance software might get recorded if a desktop session is being recorded.

+ Allow only automatic authentication methods (for example, single sign on, smartcard) for accessing published desktops or applications.

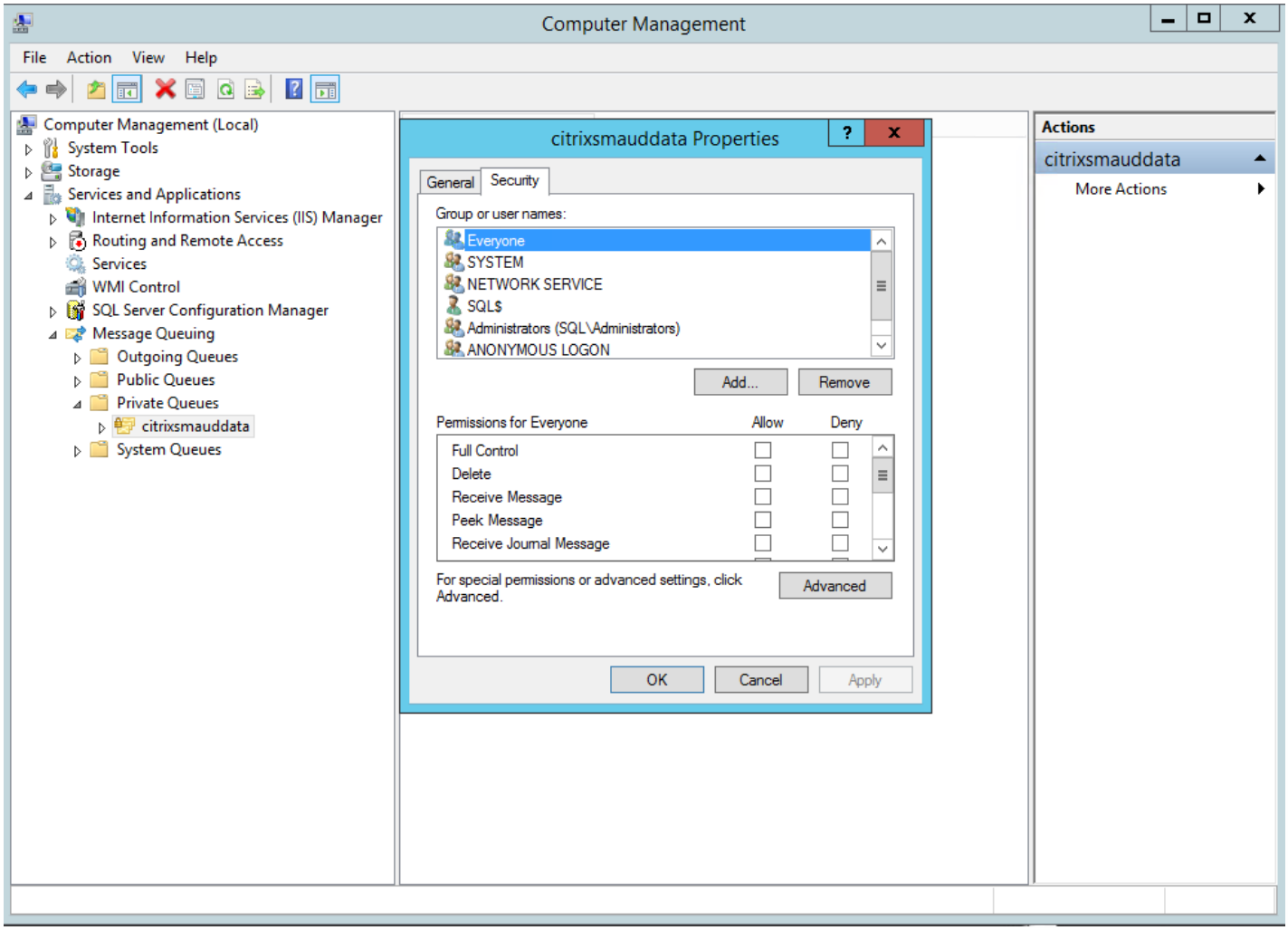
- Session Recording relies on certain hardware and hardware infrastructure (for example, corporate network devices, operation system) to function properly and to meet security needs. Take measures at the infrastructure levels to prevent damage or abuse to those infrastructures and make the Session Recording function secure and reliable.
  - Properly protect and keep network infrastructure supporting Session Recording available.
  - Citrix recommends using a 3rd-party security solution or Windows mechanism to protect Session Recording components. Session Recording components include:
    - On Session Recording Server
      - Processes: SsRecStoragemanager.exe and SsRecAnalyticsService.exe
      - Services: CitrixSsRecStorageManager and CitrixSsRecAnalyticsService
      - All files in Session Recording Server installation folder
      - Registry keys at HKLM\Software\Citrix\SmartAuditor\Server
    - On Session Recording Agent
      - Process: SsRecAgent.exe
      - Service: CitrixSmAudAgent
      - All files in Session Recording Agent installation folder
      - Registry keys at HKLM\Software\Citrix\SmartAuditor\Agent
- Set the access control list (ACL) for Message Queuing (MSMQ) at 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, and then restart the Message Queuing service.

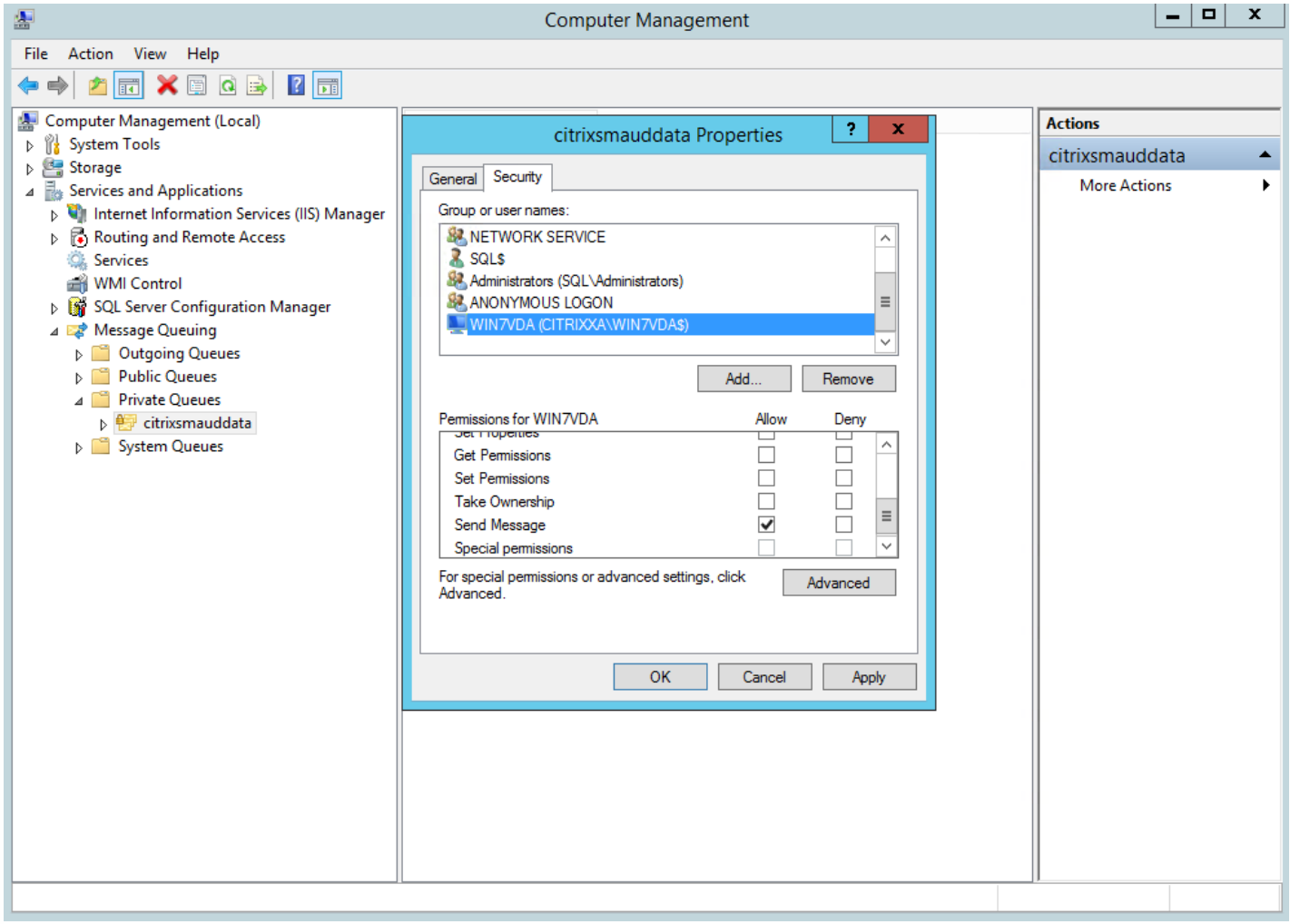
  2) From the Windows **Start** menu on each Session Recording Server, open **Administrative Tools > Computer Management**.

  3) Open **Services and Applications > Message Queuing > Private Queues**.

  4) Click on the private queue **citrixsmauddata** to open the **Properties** page and select the **Security** tab.



5) Add the computers or security groups of the VDA machines that will send MSMQ data to this server and grant them Send Message permission.



- Properly protect the event log for the Session Record Server and Session Recording Agents. Citrix recommends leveraging a Windows or 3rd-party remote logging solution to protect the event log or redirect the event log to the remote server.
- Ensure servers running 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 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 Admin Server and SQL database up to date with the latest security updates from Microsoft.
- Restrict nonadministrators 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 by setting the MSMQ protocol listed in the Session Recording Agent Properties dialog box to HTTPS. For more information, see Troubleshoot MSMQ.
- Use TLS 1.0 and disable SSLv2, SSLv3, and RC4 cipher on the Session Recording Server and Session Recording Database. For more information, see the Microsoft articles http://support.microsoft.com/default.aspx?scid=kb;en-us;187498 and http://support.microsoft.com/kb/245030/en-us.
- 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 the Session Recording Server

Properties.

- Follow NSIT guidance for cryptographic key lengths and cryptographic algorithms.

For information about configuring Session Recording features, see http://support.citrix.com/article/CTX200868.

Scalability considerations

Apr 23, 2015

Installing and running Session Recording requires few additional resources beyond what is necessary to run XenApp. However, if you plan to use Session Recording to record a large number of sessions or if the sessions you plan to record will result in large session files (for example, graphically intense applications), consider the performance of your system when planning your Session Recording deployment.

For more information about building a highly scalable Session Recording system, see http://support.citrix.com/article/CTX200869.

In this article:

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 period of time for which you are recording sessions. For example, you might record 5,000 Microsoft Outlook sessions of 20MB each over an 8-hour work day. In this case, the data input rate is approximately 3.5MBps. (5,000 sessions times 20MB divided by 8 hours, divided by 3,600 seconds per hour.)

You can improve performance by optimizing the performance of a single Session Recording Server or by installing multiple Session Recording Servers on different computers.

Disk and storage hardware are the most important factors to consider when planning a Session Recording deployment. The write performance of your storage solution is especially important. The faster data can be written to disk, the higher the performance of the system overall.

Storage solutions suitable for use with Session Recording include a set of local disks controlled as RAID arrays by a local disk controller or by an attached Storage Area Network (SAN).

Note: Session Recording should not be used with Network-Attached Storage (NAS), due to performance and security problems associated with writing recording data to a network drive.
For a local drive set up, a disk controller with built-in cache memory enhances performance. A caching disk controller must have a battery backup facility to ensure data integrity in case of a power failure.

A 100Mbps network link is suitable for connecting a Session Recording Server. A gigabit Ethernet connection may improve performance, but does not result in 10 times greater performance than a 100Mbps link.

Ensure that network switches used by Session Recording are not shared with third-party applications that may compete for available network bandwidth. Ideally, network switches are dedicated for use with the Session Recording Server.

Consider the following specification for the computer on which a Session Recording Server is installed:

- A dual CPU or dual-core CPU is recommended
- 2GB to 4GB of RAM is recommended

Exceeding these specifications does not significantly improve performance.

If a single Session Recording Server does not meet your performance needs, you can install more Session Recording Servers on different machines. In this type of deployment, each Session Recording Server has its own dedicated storage, network switches, and database. To distribute the load, point the Session Recording Agents in your deployment to different Session Recording Servers.

The Session Recording Database requires Microsoft SQL Server 2014, Microsoft SQL Server 2012, or Microsoft SQL Server 2008 R2. The volume of data sent to the database is very 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 1KB of space in the database, unless the Session Recording Event API is used to insert searchable events into the session.

The Express Editions of Microsoft SQL Server 2014, Microsoft SQL Server 2012, and Microsoft SQL Server 2008 R2 impose a database size limitation of 10GB. At 1KB per recording session, the database can catalog about four million 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 onto the session being recorded, and one when recording ends. If you used 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 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 Session Recording

Oct 21, 2016

This article contains these sections:

Before you start the installation, complete this list:

✓	Step
	Install the prequisites before starting the installation. See System Requirements and Use a script to add Windows roles and features prerequisites.
	Select the machines on which 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.
	Download the Session Recording from the Citrix download page under XenApp > https://www.citrix.com/downloads/xenapp.html or XenDesktop > https://www.citrix.com/downloads/xendesktop.html
	If you use the SSL protocol for communication between the Session Recording components, install the correct certificates in your environment.

	Install any hotfixes required for the Session Recording components. The hotfixes are available from the Citrix Support.
	Configure Director to create and activate Session Recording policies. For more information, see Configure Director to use the Session Recording Server.

Notes:

- Citrix recommends dividing the published applications into separate Delivery Groups based on the 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 with XenApp, prepare the server for a unique QMId; see the description in Known issues. Failure to do this step might result in lost recording data.
- SQL server requires that TCP/IP is enabled, the SQL Server Browser service is running, and Windows Authentication is used.
- If you want to use HTTPS, configure server certificates for TLS/HTTPS.

Session Recording installation files:

- **Session Recording Administration files**
  - Broker_PowerShellSnapIn_x64.msi
  - SessionRecordingAdministrationx64.msi
- **Session Recording Agent files**
  - SessionRecordingAgentx64.msi
- **Session Recording Player files**
  - SessionRecordingPlayer.msi

For Session Recording to work properly, you must add some Windows roles and features as prerequisites before installing the Session Recording components. Because you might have difficulty finding and installing some of the roles and features, this article contains a procedure using a Citrix-supplied script. Run the script to install the Windows roles and features prerequisites before the installation of Session Recording components.

To install Windows roles and features prerequisites

1. If you want to you use the Citrix scripts, see Scripts for Windows roles and features prerequisites.
2. Do the following on the machine on which you plan to install Session Recording Administration components:
   a) Make sure the execution policy is set to **RemoteSigned** or **Unrestricted** in PowerShell.

      Set-ExecutionPolicy RemoteSigned

   b) Start a command prompt as an administrator and run this command:

      powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1

      The script displays the features that are successfully added and then stops.

   c) After the scripts execute, ensure the execution policy is set to a proper value based on company policy.

3. Do the following on the machine on which you plan to install the Session Recording Agent component:

    a) Make sure the execution policy is set to **RemoteSigned** or **Unrestricted** in PowerShell.

    Set-ExecutionPolicy RemoteSigned

    b) Start a command prompt as an administrator and run this command:

    powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1

    The script displays the features that are successfully added and then stops.

    c) After the scripts execute, ensure the execution policy is set to a proper value based on company policy.

4. After the Windows roles and features are installed, proceed with the Session Recording installation.

The Session Recording Administration components are the Session Recording Database, Session Recording Server, and the Session Recording Policy Console. You can choose which of these components to install on a server.

Before installing the Session Recording Administration components, ensure you have all the prerequisites installed. See Session Recording system requirements.

To improve security, you can remove these permissions after installing the database.

1. Run the **Broker_PowerShellSnapIn_x64.msi** and follow the instructions to complete the installation.
2. Start the Windows command prompt as Administrator, and then run the command **msiexec /i SessionRecordingAdministrationx64.msi** or double-click the .msi file.
3. On the installation UI, select **Next** and accept the license agreement.
4. On the Session Recording Administration Setup screen, select the Session Recording Administration components you want to install.

Before installing the Session Recording Database, ensure you have all the prerequisites installed. See Session Recording system requirements.

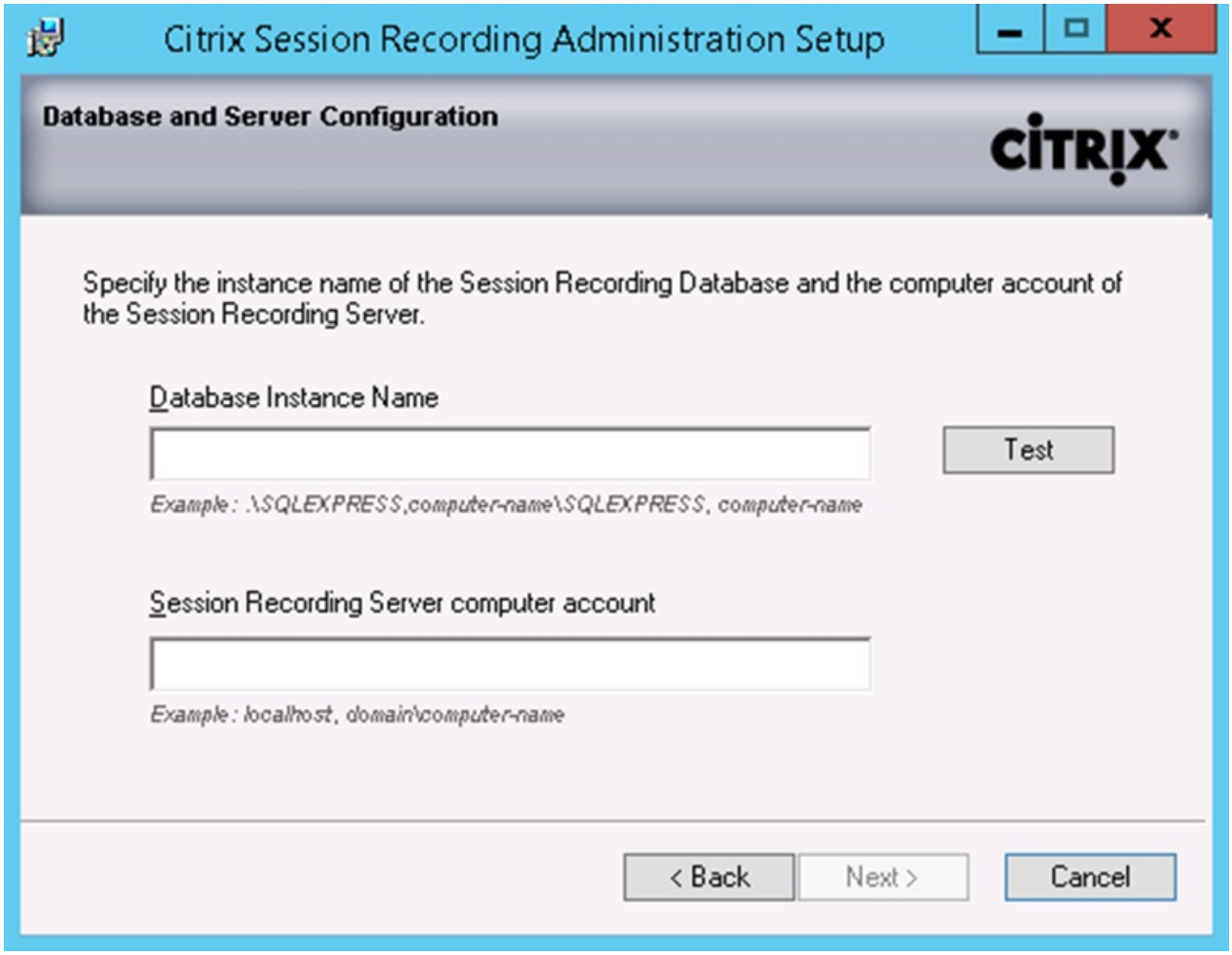
Important: The Session Recording Database is not the actual database. It is the component responsible for creating and configuring the required databases in the Microsoft SQL Server instance during installation.

There are typically these three types of Session Recording Database component and Microsoft SQL Server deployments:

- Deployment 1: Install the Session Recording Server and Session Recording Database on the same server and the Microsoft SQL Server on a remote machine. (**Recommended**)
- Deployment 2: Install the Session Recording Server, Session Recording Database, and the Microsoft SQL Server on the same machine.
- Deployment 3: Install the Session Recording Server on a server and install both the Session Recording Database and Microsoft SQL Server on the same machine but different than the Session Recording Server machine.(**Not recommended**).

1. On the Database Configuration page:
    - **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 following format: *domain**computer-name*. The Session Recording Server computer account is the user account for accessing the database.



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.

Click **Test** to test the connection to the SQL Server. Make sure the current user has the public SQL Server role permission; otherwise the test fails for permission limitation. Then click **Next** to continue the installation.

2. Follow the instructions to complete the installation. During the installation, if the current user is not the database administrator, a dialog box prompts for the credentials of a database administrator with sysadmin server role permission. 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**.

After the installation completes, the sysadmin server role permission is no longer necessary and can be safely removed for the current user.

> **Important**
>
> You cannot change the **CitrixSessionRecording** database name.

Before installing the Session Recording Server, ensure you have all the prerequisites installed. See Session Recording system requirements.

1. Enter the name of your SQL server in the Database Instance Name text box. If you are using a named instance, enter *computer-name**instance-name*; otherwise enter a computer-name only.
2. Click **Test** to test the connection to the SQL server. Make sure the current user has the public SQL Server role permission; otherwise the test fails for permission limitation. Then click **Next** to continue the installation and follow the instructions to complete the installation.
3. At the end of the installation wizard, you can choose to participate in the Citrix Customer Experience Improvement Program. When you join this program, anonymous statistics and usage information is sent to Citrix; for more information, see About the Citrix Customer Experience Improvement Program (CEIP).

You can use the Director console to create and activate Session Recording policies.

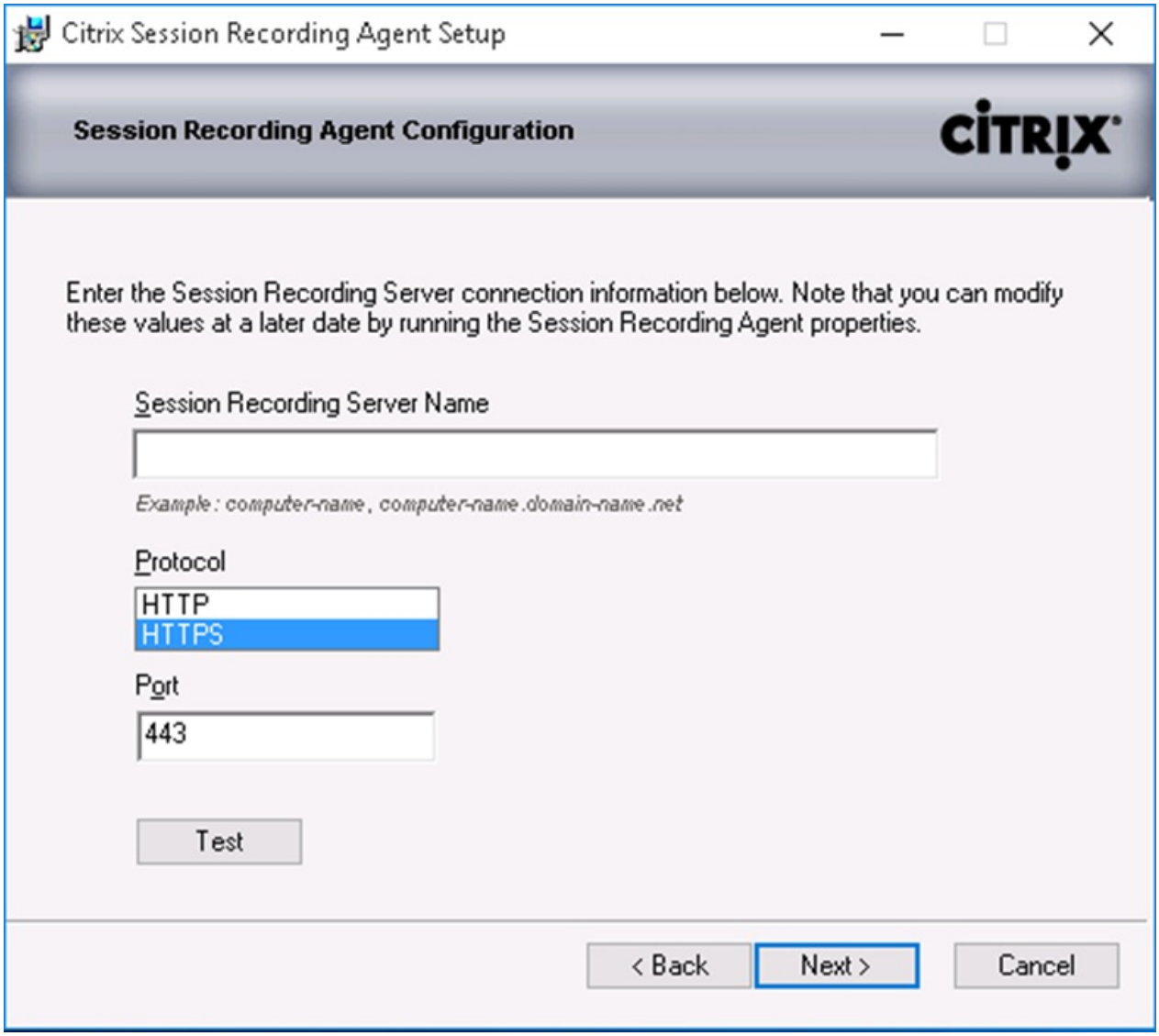
1. For an https connection, install the certificate to trust the Session Recording Server in the Trusted Root Certificates of the Director server.
2. To configure the Director server to use the Session Recording Server, run the command: **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording**
3. Enter the IP/FQDN of the Session Recording Server, the port number, and the connection type (http/https) from the Session Recording Agent to Session Recording Broker on the Director server.

The Session Recording Agent must be installed on the VDA or VDI machine on which you want to record sessions.

1. Use the Server Manager to install .NET Framework 3.5 and Microsoft Message Queuing (MSMQ) with HTTP support on the XenApp 7.8 Server OS VDA or the XenDesktop 7.8 VDI.
2. Start the Windows command prompt as Administrator, and then run the command:
   msiexec /i SessionRecordingAgentx64.msi
   or
   msiexec /i SessionRecordingAgent.msi

   or double click the .msi file.

   Use the correct .msi file based on platform type: **SessionRecordingAgent.msi** for 32 bit systems and **SessionRecordingAgentx64.msi** for 64 bit systems.
3. On the installation UI, select **Next** and accept the license agreement.
4. In the Session Recording Agent Configuration page, 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.



The Session Recording default installation uses HTTPS/TLS to secure communications. If TLS is not configured, use HTTP. To do so, deselect SSL in the IIS Management Console by navigating to the Session Recording Broker site. Open the SSL settings and uncheck the Require SSL box.

5. Follow the instructions to complete the installation.

Install the Session Recording Player on the Session Recording Server or one or more workstations in the domain for users who view session recordings.

Run the **SessionRecordingPlayer.msi** and follow the instructions to complete the installation.

To install 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 install information.

For 64 bit systems:

msiexec /i SessionRecordingAgentx64.msi
sessionrecordingservername=yourservername sessionrecordingbrokerprotocol=yourbrokerprotocol
sessionrecordingbrokerport=yourbrokerport /l*v yourinstallationlog /q

For 32 bit systems:

msiexec /i SessionRecordingAgent.msi sessionrecordingservername=yourservername
sessionrecordingbrokerprotocol=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport /l*v yourinstallationlog /q

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 either HTTP or HTTPS, and represents the protocol that Session Recording Agent uses to communicate with Session Recording Broker; this value defaults to HTTPS if not specified.

yourbrokerport is an integer representing the port 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 the selected protocol: 80 for HTTP or 443 for HTTPS.

/l*v specifies verbose mode logging

yourinstallationlog is the location of the setup log file created.

/q specifies quiet mode.

You can upgrade certain deployments to newer versions without having to first set up new machines or sites. You can upgrade from Session Recording 7.6.0 (or a later version) to the latest released (current) Session Recording version.

Note: You cannot upgrade from a Technology Preview version.

- You must use Session Recording installer's graphical or command-line interface to upgrade Session Recording components on the machine where you installed corresponding Session Recording components.
- Before beginning any upgrade activity, back up the database named CitrixSessionRecording in the SQL Server instance, so 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 Session Recording Server and Session Recording Database are not installed on the same server, you must have the database sysadmin role permission to upgrade Session Recording Database; otherwise, you are asked for sysadmin role credentials during 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 a later version) can work with the latest released (current) 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.
- If there are live recording sessions when the upgrade process starts, there is very small chance the recording cannot be completed.

- Review the upgrade sequence below so you can plan and mitigation potential outages.

1. If Session Recording Database and Session Recording Server are installed on different servers, stop the Session Recording Storage Manager service manually on Session Recording Server, and then upgrade Session Recording Database first.
2. Ensure Session Recording Broker is running with IIS service. Upgrade Session Recording Server. If Session Recording Database and Session Recording Server are installed on the same server, Session Recording Database will also be upgraded.
3. Session Recording service is back online automatically when the upgrade of Session Recording Server is completed.
4. Upgrade Session Recording Agent (on master image).
5. Upgrade Session Recording Policy Console with or after Session Recording Server.
6. Upgrade Sessoin Recording Player.

To remove Session Recording components from a server or workstation, use the uninstall or remove programs available through the Windows Control Panel. To remove the Session Recording Database, you must have the same sysadmin SQL server role permissions as when you installed it.

Scripts to add Windows roles and features prerequisites

Jan 25, 2016

You can use the following scripts to install Windows roles and features prerequisites that are required for Session Recording to work properly. For more information, see Use a script to add Windows roles and features prerequisites.

```
<p>&lt;#<br>
.Synopsis<br>
   Installs Prereqs for Session Recording Administration<br>
.Description<br>
   Supports Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.<br>
   Install below windows feature on this machine:<br>
   -Application Development - ASP.NET 4.5 on Server 2012 and Server 2012 R2, Application Development - ASP.NET on Server
   -Security - Windows Authentication<br>
   -Management Tools - IIS 6 Management Compatibility<br>
      IIS 6 Metabase Compatibility<br>
      IIS 6 WMI Compatibility<br>
      IIS 6 Scripting Tools<br>
      IIS 6 Management Console<br>
 -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.<br>
#&gt;<br>
function AddFeatures($featurename)<br>
{<br>
   try<br>
   {<br>
      $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}<br>
      Add-WindowsFeature $feature<br>
   }<br>
   catch<br>
   {<br>
      Write-Host &quot;Addition of Windows feature $featurename failed&quot;<br>
      Exit 1<br>
   }<br>
   Write-Host &quot;Addition of Windows feature $featurename succeeded&quot;<br>
}<br>
<br>
$system= gwmi win32_operatingSystem | select name<br>
<br>
if (-not (($system -Like '*Microsoft Windows Server 2012*') -or ($system -Like '*Microsoft Windows Server 2008 R2*')))<br>
{<br>
   Write-Host(&quot;This is not a supported server platform. Installation aborted.&quot;)<br>
   Exit<br>
}<br>
<br>
# Start to install Windows feature<br>
Import-Module ServerManager<br>
<br>
if ($system -Like '*Microsoft Windows Server 2012*')<br>
```

```
{<br>
   AddFeatures('Web-Asp-Net45') #ASP.NET 4.5<br>
}<br>
if($system -like '*Microsoft Windows Server 2008 R2*')<br>
{<br>
   AddFeatures('Web-Asp-Net') #ASP.NET<br>
}<br>
AddFeatures('Web-Mgmt-Console') #IIS Management Console <br>
AddFeatures('Web-Windows-Auth') # Windows Authentication<br>
AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility<br>
AddFeatures('Web-WMI') #IIS 6 WMI Compatibility<br>
AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools<br>
AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console<br>
AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support</p>
```

```
<p>&lt;#<br>
.Synopsis<br>
   Installs Prereqs for Session Recording Administration<br>
.Description<br>
   Supports Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 7, Windows 8, Windows 8.1 ar
   Install below windows feature on this machine:<br>
 -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.<br>
#&gt;<br>
function AddFeatures($featurename)<br>
{<br>
   try<br>
   {<br>
      $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}<br>
      Add-WindowsFeature $feature<br>
   }<br>
   catch<br>
   {<br>
      Write-Host &quot;Addition of Windows feature $featurename failed&quot;<br>
      Exit 1<br>
   }<br>
   Write-Host &quot;Addition of Windows feature $featurename succeeded&quot;<br>
}<br>
<br>
# Start to install Windows feature<br>
$system= gwmi win32_operatingSystem | select name<br>
<br>
if (-not (($system -Like '*Microsoft Windows Server 2012*') -or ($system -Like '*Microsoft Windows Server 2008 R2*')-or ($sys
{<br>
   Write-Host(&quot;This is not a supported platform. Installation aborted.&quot;)<br>
   Exit<br>
}<br>
<br>
if ($system -Like '*Microsoft Windows Server*')<br>
{<br>
   Import-Module ServerManager<br>
```

```
    AddFeatures('MSMQ') #Message Queuing<br>
    AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support<br>
  }<br>
  else<br>
  {<br>
    try<br>
    {<br>
      if($system -Like '*Microsoft Windows 7*')<br>
      {<br>
        dism /online /enable-feature /featurename:IIS-WebServerRole /featurename:IIS-WebServer /featurename:IIS-IIS6Manag
        dism /online /enable-feature /featurename:MSMQ-Container<br>
        dism /online /enable-feature /featurename:MSMQ-Server<br>
        dism /online /enable-feature /featurename:MSMQ-HTTP<br>
      }<br>
      else<br>
      {<br>
        dism /online /enable-feature /featurename:MSMQ-HTTP /all<br>
      }          <br>
    }<br>
    catch<br>
    {<br>
      Write-Host &quot;Addition of Windows feature MSMQ HTTP Support failed&quot;<br>
      Exit 1<br>
    }<br>
    write-Host &quot;Addition of Windows feature MSMQ HTTP Support succeeded&quot;     <br>
  }</p>
```

Configure Session Recording

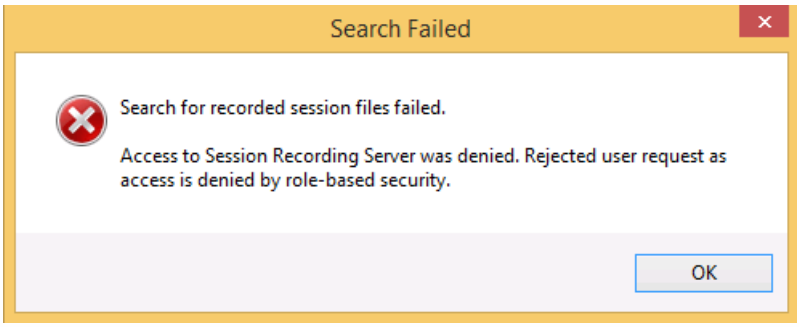
Sep 02, 2015

After you install the Session Recording components, perform these steps to configure Session Recording to record XenApp or XenDesktop sessions and allow users to view them:

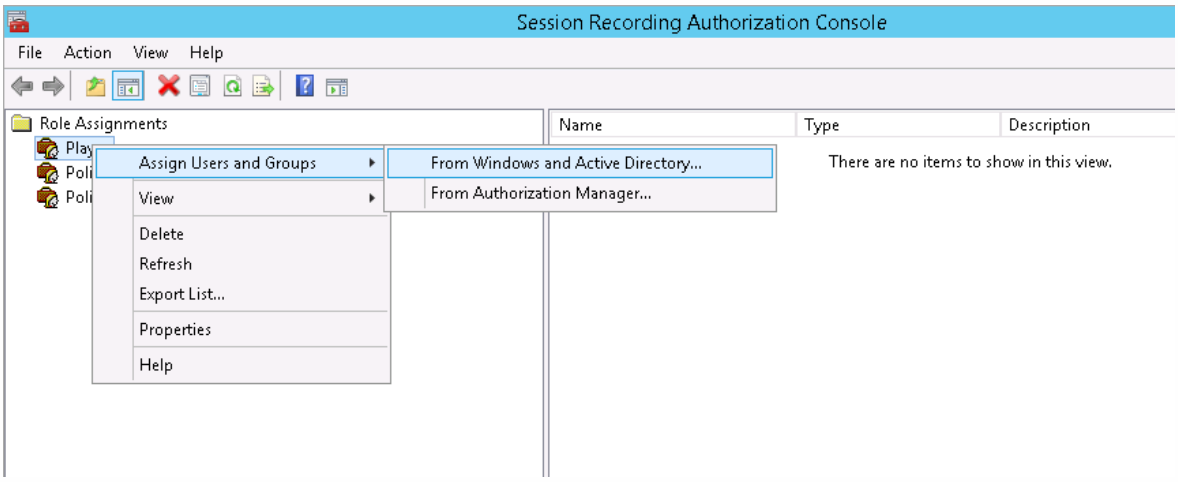
- Authorize users to play recordings
- Authorize users to administer recording policies
- Set the active recording policy to one that records sessions
- Configure custom policies
- Configure Session Recording Player to connect to the Session Recording Server

Authorize users to play recorded sessions

When you install Session Recording, no users have permission to play recorded sessions. You must assign permission to each user, including the administrator. A user without permission to play recorded sessions receives the following error message when trying to play a recorded session:



1. Log on as 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 and they will populate the right pane.



Authorize users to administer recording policies

When you install Session Recording, domain administrators grant permission to control the recordng policies by default. You can change the authorization setting.

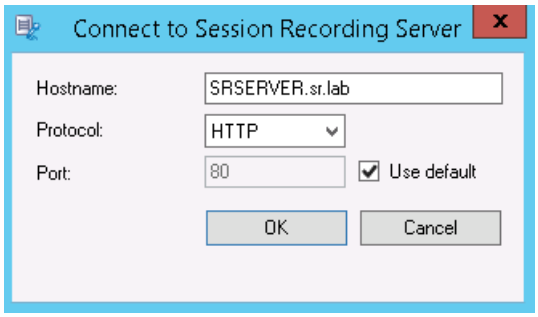
1. Log on as administrator to the machine hosting the Session Recording Server.
2. Start the Session Recording Authorization Console and select PolicyAdministrators.
3. Add the users and groups who can administer recording policies.

Set the active recording policy to record sessions

The active recording policy specifies session recording behavior on all VDAs or VDI s that have 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 there can be only one active policy 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 you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the computer hosting the Session Recording Server, protocol, and port are correct.



4. In the Session Recording Policy Console, expand Recording Policies. This displays the recording policies available when you install Session Recording, with a check mark indicating which policy is active:
   - 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 notifying the user that recording is occurring.
   - Record everyone without notification. If you choose this policy, all sessions are recorded. A pop-up window does not appear notifying the user that recording is occurring.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose Action > Activate Policy.

Note: Session Recording allows you to create your own recording policy. When you create recording policies, they appear in the Recording Policies folder within 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.

Configure 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 Session Recording Player is installed.
2. Start the Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options.
4. In the Connections tab, click Add.
5. In the Hostname field, type the name or Internet protocol (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. If you want to configure the Session Recording Player with the ability to connect to more than one Session Recording Server, repeat Steps 4 and 5 for each Session Recording Server.
7. Ensure that the check box for the Session Recording Server you want to connect to is selected.

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 Session Recording Agent is installed, use Session Recording Agent Properties.

1. Log on to the server where 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 server name or its Internet protocol (IP) address.
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.
6. In the **Message life** field, accept the default of 7200 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 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.

Grant access rights to users

Feb 25, 2015

Note: 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.

1. Log on to computer hosting the Session Recording Server, as 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

Apr 23, 2015

Use the Session Recording Policy Console to create and activate policies that determine which sessions are recorded.

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.

Session Recording provides these system policies:

- **Do not record**. If you choose this policy, no sessions are recorded. 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 notifying the user that recording is occurring.
- **Record everyone without notification**. If you choose this policy, all sessions are recorded. A pop-up window does not appear notifying the user that recording is occurring.

System policies cannot be modified or deleted.

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 make the active policy.
6. From the menu bar, choose Action > Activate Policy.

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 a 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 within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are not recorded.
- Record with notification. (Choose Enable session recording with notification within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are recorded. A pop-up window appears notifying the user that

recording is occurring.
- Record without notification. (Choose Enable session recording without notification within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are recorded. Users are unaware that they are being recorded.

For each rule, choose at least one of the following to create the rule criteria:

- Users or Groups. You create a list of users or groups to which the recording action of the rule applies.
- Published Resources. You create a list of published applications or desktops to which the recording action of the rule applies. Within the rules wizard, choose the XenApp/XenDesktop site or sites on which the applications or desktops are available
- Delivery Groups or Machines. You create a list of Delivery Groups or machines to which the recording action of the rule applies. Within the rules wizard, choose the location where the Delivery Groups or machines reside.

When you create more than one rule in a recording policy, some sessions may match the criteria for more than one rule. In these cases, the rule with the highest priority is applied to the session.

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 may 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.

Configure custom policies

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 and 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 **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 three options:
   Users or Groups
   Published resources
   Delivery Groups or Machines
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.
7. Follow the wizard to finish the configuration.

Using Active Directory Groups

Session Recording allows you to use Active Directory groups when creating policies. Using Active Directory groups instead of individual users simplifies creation and management of rules and policies. For example, if users in your company's finance department are contained in an Active Directory group named Finance, you can create a rule that applies to all members of this group by selecting the Finance group within the rules wizard when creating the rule.

White Listing Users

You can create Session Recording policies that ensure 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.

Create a new policy

Note: When using the rules wizard, you may 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.

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. 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.

When you activate a policy, the previously active policy remains in effect until the user's session ends; however, in some cases, the new policy takes effect when the file rolls over. Files roll over when they have reached the maximum size limit. For information on maximum file sizes 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 with notification	Recording continues and a notification message appears.
Record with notification	Do not record	Recording stops.
	Record without notification	Recording continues. No message appears the next time a user logs on.

Create notification messages

Feb 02, 2015

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 users type their credentials. The following message is the default notification: "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 user clicks OK to dismiss the window and continue the session.

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 of your choice; however, you can have only one notification message for each language. Your users see the notification message in the language corresponding to their user preferred locale settings.

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.

Disable or enable recording

Mar 24, 2015

You install the Session Recording Agent on each Server OS machine 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, which 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.

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.

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#. 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.

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

Feb 25, 2015

Using Session Recording Player, you can view a session after or while it is being recorded. Viewing a session that is currently recording is similar to seeing actions happening live; however, there is actually a one to two second delay as the data propagates from the XenApp or XenDesktop server.

Some functionality is not available when viewing sessions that have not completed recording:

- 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.

As a security precaution, Session Recording automatically encrypts recorded files before they are downloaded for viewing in the Session Recording Player. This playback protection prevents them 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 the cache on the workstation where the Session Recording Player is installed until they are opened by an authorized user.

Citrix recommends 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.

Enable and disable digital signing

Feb 02, 2015

If you installed 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 read permission to the Session Recording Storage Manger Service.

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.

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

Feb 03, 2015

Use Session Recording Server Properties to specify where recordings are stored and where archived recordings are restored.

Note: To archive files or restore deleted files, use the icldb command.

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 additional directories to load-balance across multiple volumes, or make use of additional space. Multiple directories in the list indicates 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.

By default, archived recordings are restored to the drive:**\SessionRecordingsRestore** directory of the computer hosting the Session Recording Server. You can change the directory where the archived recordings are restored.

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 the directory for the restored archive files.

Specify file size for recordings

Feb 02, 2015

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 limit of 1GB and activities are not recorded after that limit is reached.

You can specify two thresholds for a rollover:

- **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 rollover. 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 rollover 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.

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 1024 to specify the maximum file size in megabytes.
5. Enter an integer between 1 and 24 to specify the maximum recording duration in hours.

View recordings

Feb 25, 2015

Use Session Recording Player to view, search, and bookmark recorded XenApp or XenDesktop sessions.

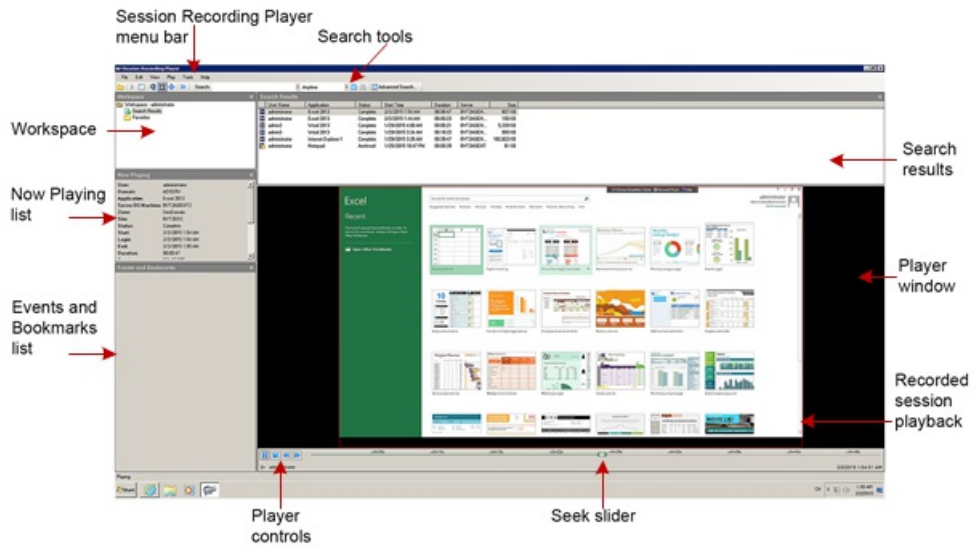
If sessions are recorded with the live playback feature enabled, you can view sessions that are in progress, with a delay of a few seconds, as well as sessions that are completed.

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 to recorded Server OS machine sessions. 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 set up information.

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 following articles.



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.

If the Session Recording administrator set up your Session Recording Player with the ability to connect to more than one Session Recording Server, 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.

Open and play recordings

Feb 04, 2015

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 share drive.
- Access recorded session files from a Favorites folder

When you open a file that was recorded without a digital signature, a warning appears telling you that the origin and integrity of the file was not verified. If you are confident of the integrity of the file, click Yes in the warning pop-up window to open the file.

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, select Play > Play

Recorded session file names begin with an i_, followed by a unique alphanumeric file ID, followed by the .icl and .icle file extension: .icl for recordings without playback protection applied, .icle for recordings with playback protection applied. Session Recording saves recorded session files in a directory structure that incorporates the date the session was 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.
3. Do any of the following:
   - From the Session Recording Player menu bar, select 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

Creating 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 Session Recording Player can download the recorded session files associated with Favorites folders. Contact your Session Recording administrator for access rights.

To create a Favorites subfolder:

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. In the Session Recording Player, 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.

Search for recorded sessions

Mar 24, 2015

Session Recording Player allows you to perform quick searches, perform advanced searches, and 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 may appear in a search, perform a search without specifying any search parameters.

To perform a quick search

1. Log on to the workstation where 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. To assist you:
   - 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.

To perform an advanced search

Tip: Advanced searches might take up to 20 seconds to return results containing more than 150K 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 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 in the tabs of the Advanced Search dialog box:
   - Common allows you to search by domain or account authority, site, group, Server OS machine, application, or file ID.
   - Date/Time allows you to search date, day of week, and time of day.
   - Events allows you to search on custom events that your Session Recording administrator 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.

   As 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.

Tip: You can save and retrieve advanced search queries. Click Save within the Advanced Search dialog box to save the current query. Click Open within the Advanced Search dialog box to retrieve a saved query. Queries are saved as files with an .isq extension.

To set search options

Session Recording Player search options allow you to limit 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 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.

Play recorded sessions

Mar 23, 2015

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

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 may 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 may 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.

Use player controls

You can click the player controls under the Player window or access them by choosing Play from the Session Recording Player menu bar. Use Player controls to:

	Play the selected session file.
	Pause playback.
	Stop playback. If you click Stop, then Play, the recording restarts at the beginning of the file.
	Halve the current playback speed down to a minimum of one-quarter normal speed.
	Double the current playback speed up to a maximum of 32 times normal speed.

Use the seek slider

Use the seek slider below 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	Seek to the beginning.

Key:	Seek action:
End	Seek to the end.
Right Arrow	Seek forward five seconds.
Left Arrow	Seek backward five seconds.
Move mouse wheel one notch down	Seek forward 15 seconds.
Move mouse wheel one notch up	Seek backward 15 seconds.
Ctrl + Right Arrow	Seek forward 30 seconds.
Ctrl + Left Arrow	Seek backward 30 seconds.
Page Down	Seek forward one minute.
Page Up	Seek backward one minute.
Ctrl + Move mouse wheel one notch down	Seek forward 90 seconds.
Ctrl + Move mouse wheel one notch up	Seek backward 90 seconds.
Ctrl + Page Down	Seek forward six minutes.
Ctrl + Page Up	Seek backward six minutes.

Note: 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 time requires more memory. The response might be slow depending on the size of of the recordings and your machine's hardware.

To 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.

To 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.

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

Feb 02, 2015

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 into the recorded sessions using the Session Recording Player. Bookmarks are associated with the recorded session until you delete them, but they are not saved as part of the session file. 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 under 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.

To 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.
3. Move the mouse pointer into the events and bookmarks list area and right-click to display the menu.
4. Choose Show Events Only, Show Bookmarks Only, or Show All.

To 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 label Bookmark or create an annotation:
   - To add a bookmark with the default label Bookmark, 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.

To 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.

To 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.

To 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 area below 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

Feb 02, 2015

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 mode, 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.

To display the Player window in full-screen format

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.

To 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.
4. To embed the Player window in the main window, choose View > Player in Separate Window, or press F10.

To 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 the image while providing a good quality image. Images are drawn quicker than when using the High Quality option but the images and text are not as sharp. Use this option if you are experiencing performance issues when using the High Quality mode.
   - Scale to Fit (High Quality) shrinks the image while providing high quality images and text. Using this option may cause the images to be drawn more slowly than the Fast Rendering option.

To 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.

To display a red border around the 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.

Cache recorded session files

Feb 02, 2015

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.

To 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.

To empty cache

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 then OK to confirm the action.

Troubleshooting Session Recording

Mar 24, 2015

This troubleshooting information contains solutions to some issues you might encounter during and after installing 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

Session Recording Agent cannot connect

When 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 the reason why the connection failed. These 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 may 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). See the Event log on the Session Recording Server for more details. 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 may be offline.

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 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 may 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, or Microsoft SQL Server 2014 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.
- Check the firewall configuration on the Session Recording Database to ensure the SQL Server connections are allowed. Refer to Microsoft article: https://msdn.microsoft.com/en-us/library/cc646023.aspx.

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 Server OS machine running the Session Recording Agent and Session Recording Server. This may 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 may 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 Server OS machines.
- **Recording is not enabled.** By default, installing the Session Recording Agent on a Server OS machine 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 the Server OS machine 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 may occur.

Unable to view live session playback

If you experience difficulties when viewing recordings using the Session Recording Player, the following error message may appear on the screen:

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 the Session Recording Server Properties dialog box, choose the Playback tab and select the Allow live session playback check box.

Recordings are corrupt or incomplete

When recordings are becoming corrupted or incomplete when viewing 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 is used to create VDAs with a configured master image and Microsoft Message Queuing (MSMQ) installed. In this condition the VDAs have the same QMIds for MSMQ.

Resolution: Create the unique QMId for each VDA. A workaround is introduced in Known Issues.

Test connection of the database instance failed when installing the Session Recording Database or Session Recording Server

When you install 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.

Resolution: Make sure the current user has the public SQL Server role permission to correct the permission limitation failure.

Verify component connections

Apr 22, 2015

During the setup of Session Recording, the components may 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 Web site certificate. If one component cannot connect to the Session Recording Server, the other components may 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.

Verify 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 Server Properties, click Connection.
4. Verify that the value for 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 Session Recording Server can be contacted by the Server OS machine.

Note: Check the application event log for errors and warnings.

Verify Session Recording Server is connected

Caution: Using Registry Editor 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.

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 the value of SmAudDatabaseInstance correctly references the Session Recording Database you installed in your SQL Server instance.

Verify 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 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 should 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 Web page 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.

To verify IIS connectivity for the Session Recording Agent

1. Log on to the server where the Session Recording Agent is installed.
2. Launch 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.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Agent is connected to the computer hosting the Session Recording Server using the configure protocol.

To verify IIS connectivity for the Session Recording Player

1. Log on to the workstation where the Session Recording Player is installed.
2. Launch 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.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Player is connected to the computer hosting the Session Recording Server using the configure protocol.

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. Launch 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.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Policy Console is connected to the computer hosting the Session Recording Server using the configure 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 Web page 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, 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 a fully qualified domain name (FQDN), then 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 if the Session Recording Player fails

Feb 04, 2015

If you experience difficulties when searching for recordings using the Session Recording Player, the following error messages may appear on the screen:

- Search for recorded session files failed. The remote server name could not be resolved: servername. where 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 for this are an incorrectly typed server name or 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 error. 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.
- 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 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 then click Modify. Change the protocol from HTTP to HTTPS.

Troubleshoot MSMQ

If your users see the notification message but the viewer cannot find the recordings after performing a search in the Session Recording Player, there could be a problem with MSMQ. Verify that the queue is connected to the Session Recording Server (Storage Manager) and 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 a number of messages in the queue, and the protocol is HTTP or HTTPS (corresponding to the protocol selected in the Connections tab in the Session Recording Agent Properties dialog box), 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 a number of messages in the queue, launch 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 the Session Recording Agent Properties dialog box to HTTPS. Otherwise, if the page reports a problem with the Web site security certificate, there may 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 a number of messages in the queue (Number of Messages Column), verify that the Session Recording StorageManager service is started. If it is not, restart the service.

Change your communication protocol

Feb 03, 2015

For security reasons, Citrix does not recommend using HTTP as a communication protocol. The Session Recording installation is configured to use HTTPS. If you want to use HTTP instead of HTTPS, you must change several settings.

To 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 each Session Recording Agent Properties dialog box:
    1. Log on to each server where the Session Recording Agent is installed.
    2. From the Start menu, choose Session Recording Agent Properties.
    3. In Session Recording Agent Properties, choose the Connections tab.
    4. In the Session Recording Broker area, select HTTP from the Protocol drop-down list and choose OK to accept the change. If you are prompted to restart the service, choose Yes.
3. Change the protocol setting from HTTPS to HTTP in the Session Recording Player settings:
    1. Log on to each 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, select the server, and choose Modify.
    4. 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:
    1. Log on to the server where the Session Recording Policy Console is installed.
    2. From the Start menu, choose Session Recording Policy Console.
    3. Choose HTTP from the Protocol drop-down list and choose OK to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording Policy Console.

To 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.
2. Change the protocol setting from HTTP to HTTPS in each Session Recording Agent Properties dialog box:
    1. Log on to each server where the Session Recording Agent is installed.
    2. From the Start menu, choose Session Recording Agent Properties.
    3. In **Session Recording Agent Properties**, choose the Connections tab.
    4. In the Session Recording Broker area, select HTTPS from the Protocol drop-down list and choose OK to accept the change. If you are prompted to restart the service, choose Yes.
3. Change the protocol setting from HTTP to HTTPS in the Session Recording Player settings:
    1. Log on to each 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, select the server, and choose Modify.
    4. 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:
    1. Log on to the server where the Session Recording Policy Console is installed.
    2. From the Start menu, choose Session Recording Policy Console.

3. Choose HTTPS from the Protocol drop-down list and choose OK to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording Policy Console.

Reference: Manage your database records

Feb 03, 2015

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] [/?]

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 verify if 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 into the Session Recording database. Use this command to rebuild the database if you lose database records. Additionally, 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.

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.

Third Party Notices

Jun 15, 2015

Session Recording may include third party software components licensed under the following terms. This list was generated using third party software as of the date listed. This list may change with specific versions of the product and may not be complete; it is provided “As-Is.” TO THE EXTENT PERMITTED BY APPLICABLE LAW, CITRIX AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, WITH REGARD TO THE LIST OR ITS ACCURACY OR COMPLETENESS, OR WITH RESPECT TO ANY RESULTS TO BE OBTAINED FROM USE OR DISTRIBUTION OF THE LIST. BY USING OR DISTRIBUTING THE LIST, YOU AGREE THAT IN NO EVENT SHALL CITRIX BE HELD LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY OTHER DAMAGES WHATSOEVER RESULTING FROM ANY USE OR DISTRIBUTION OF THIS LIST.

MMC .NET Library

Licensed under the Common Public License, Version 1.0

Configuration Logging

Feb 24, 2016

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 2.0 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). Citrix strongly recommends that you you change the location of the database used for Configuration Logging as soon as possible after creating a Site. 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.

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) could 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.

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. Selec the desired action:

   To enable Configuration Logging, select the **Enable logging** 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 logging** radio button. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.

   To enable mandatory logging, clear the **Allow changes when the database is disconnected**checkbox. 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 Configuration Logging** 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 the database is disconnected** check box.

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 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.
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.

- **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.

Monitor Personal vDisks

Jul 07, 2014

You can use a diagnostic tool to monitor the changes made by users to both parts of their Personal vDisks (the user data and the application parts). These changes include applications that users have installed and files they have modified. The changes are stored in a set of reports.

1. On the machine you want to monitor, run **C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe**.
2. Browse to a location where you want to store the reports and logs, select the reports to generate, and then click **OK.** The available reports are listed below.

Software hive report: This report generates two files: Software.Dat.Report.txt and Software.Dat.delta.txt. The Software.Dat.Report.txt file records the changes made by the user to the HKEY_LOCAL_MACHINE\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.
- 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.

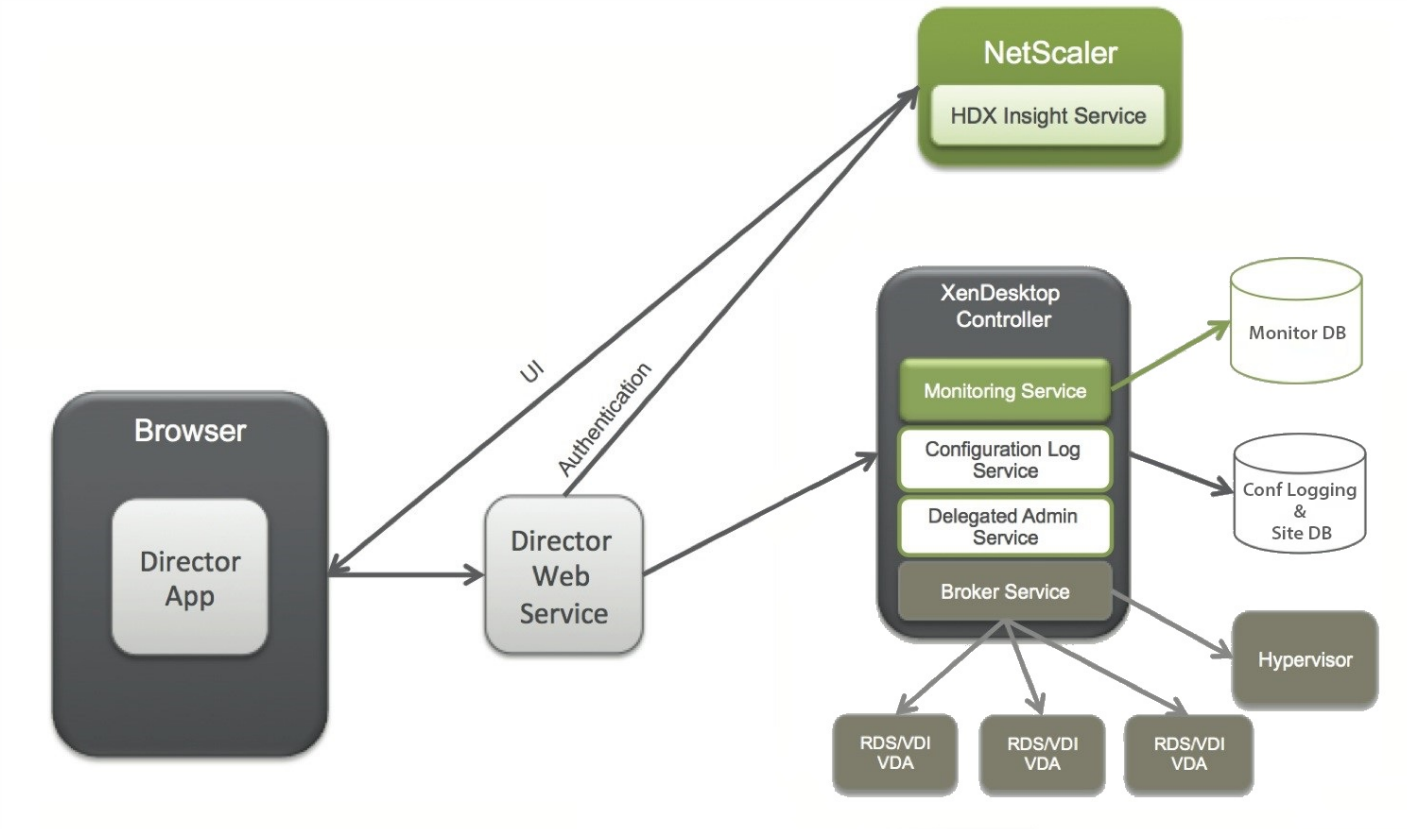
Director

Aug 26, 2016

In this article:

About Director

Director is a real-time web tool that allows administrators to monitor, troubleshoot, and perform support tasks for end users.



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 HDX Insight, 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 HDX Insight.
    - 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 IT 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 health monitoring of the XenApp or XenDesktop Site. This feature allows administrators to see failures in real time, providing a better idea of what the end user is experiencing.

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.

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 creates a 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).
- Configured Delegated Administrator roles (see Delegated Administration and Director).
- To shadow users, administrators must be configured using a Microsoft group policy for Windows Remote Assistance. In addition:
  - When installing VDAs, ensure 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 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 installer handles typical deployments. If Director was not included during installation, use the installer to add Director. To add any additional components, rerun the installer and select the components to install. For information on using the installer, see Install using the graphical interface in the installation documentation. Citrix recommends that you install using the product 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. Director communicates with that specified Controller by default. Specify only one Controller address for each Site that you will 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 between 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.

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 between 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 at **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 web site 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 will need to 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

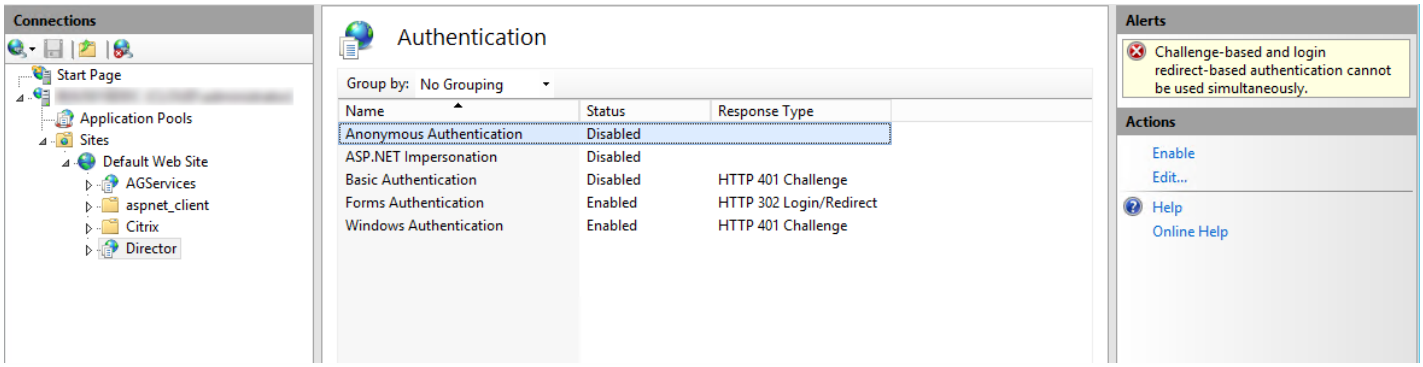
The Director website is located at https or http://<Server_FQDN>/Director.

If one of the Sites in a multi-site deployment is down, the logon for Director takes a little longer while it attempts to connect to the Site that is down.

Use Director with 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 web site which 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 should 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. Once the Active Directory Management Console is open, navigate to **Domain Name** > **Computers** > select the Director machine to assign the delegation permission to.
  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 which is used to access Director must support Integrated Windows Authentication. This may 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 higher supported version listed in the System Requirements for Director. For more information, see System Requirements.

When a user logs off Director or if the session times out, the logon page is displayed. From the logon page, the user can set the Authentication type to **Automatic logon** or **User credentials**.

Advanced configuration

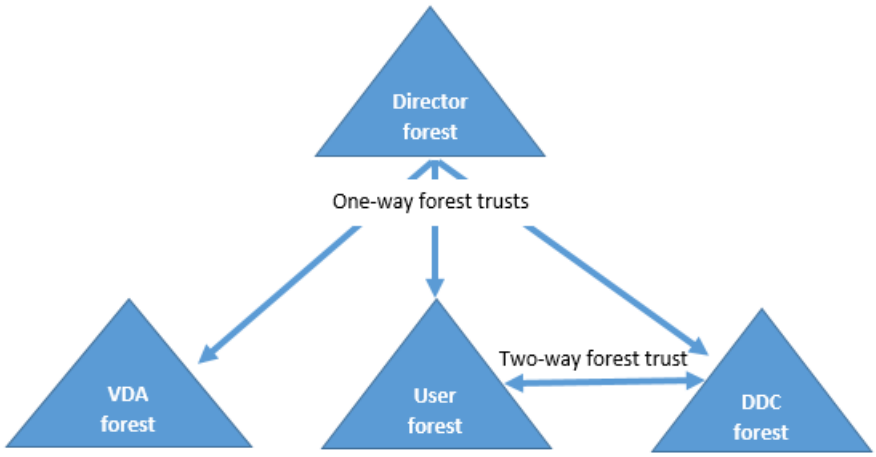
Sep 02, 2016

In this article:

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 set up 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.



The trust relationship from the Director enables the administrator 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.

Platinum licenses retain data for 90 days by default. For more information on configurations see Data granularity and retention.

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 the administrator does 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)
```

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 the administrator does 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.

To protect the privacy of users and the applications they are running, you can disable the Applications tab from listing running applications.

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.

1. On the VDA, modify the registry key located at HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information will not be displayed in the Activity Manager.
2. On the server with Director installed, modify the setting that controls the visibility of running applications. By default, the value is "true", which allows visibility of running applications in the Applications tab. Change the value to "false", which disables visibility. This option affects only the Activity Manager in Director, not the VDA.
   Modify the value of the following setting:
   `UI.TaskManager.EnableApplications = false`

Important: To disable the view of running applications, Citrix recommends making both changes to ensure the data is not displayed in Activity Manager.

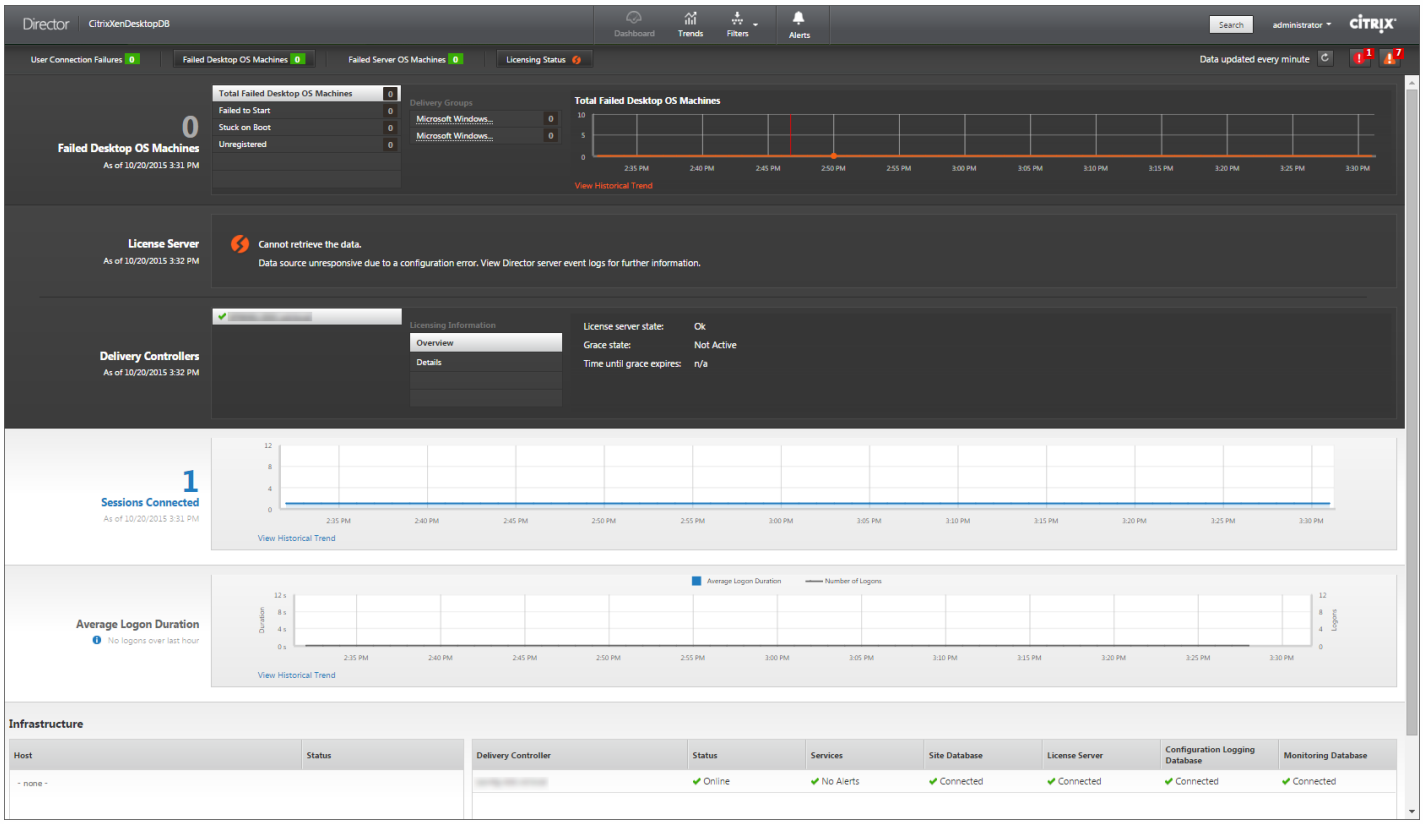
Monitor deployments

Sep 07, 2016

In this article:

Monitor sites

With full administrator permissions, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a site.



If there are currently no failures and no failures have occurred in the past 60 minutes, panels stay collapsed. When there are failures, the specific failure panel automatically appears.

Note: Depending on your organization's license and your Administrator privileges, some options or features might not be available.

Panel	Description
User Connection Failures	Connection failures over the last 60 minutes. Click the categories next to the total number to view metrics for that type of failure. In the adjacent table, that number is broken out by Delivery Groups. Connection failures includes failures caused by application limits being reached. For more information on application limits, see Applications.
Failed 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.
Licensing Status	• License Server alerts are sent by the License Server and also display the actions required to resolve the alert. • Delivery Controller alerts display the details of the licensing state as seen by the controller and are sent by the Delivery Controller. You can set the threshold for alerts in Studio. License Server and/or Delivery Controller alerts do not display if your License Server version is earlier than 11.12.1 and/or your Delivery Controller is older than XenApp 7.6 or XenDesktop 7.6.
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	Health status of your site's hosts, controllers. and infrastructure. View performance alerts. For hosts, the connection status and the health of the CPU, memory, bandwidth (network usage), and storage (disk usage) are monitored using information from XenServer or VMware. 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, in the XenServer documentation, see Configuring Performance Alerts.

Note: If no icon appears for a particular metric, this indicates that this metric is not supported by the type of host you are using. For example, no health information is available for System Center Virtual Machine Manager (SCVMM) hosts, AWS and CloudStack.
Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor sessions

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

Action	Description
View a user's currently connected machine or session	From the Activity Manager and User Details views, view the user's currently connected machine or session and a list of all machines and sessions to which this user has access. To access this list, click the session switcher icon in the user title bar. 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.
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 Agents (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.

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, and sessions across all Delivery Groups.

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 Machines view.
   - **Connections**. Filter connections by different time periods, including last 60 minutes, last 24 hours, or last 7 days.
2. For Failure 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.
   To open filter later, from the Filters menu, select the failure type (Machines, Sessions, or Connections), and then select the saved filter.

6. 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.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor historical trends across a site

The Trends view accesses historical trend information for sessions, connection failures, machine failures, logon performance, and load evaluation for each site. To locate this information, from the Dashboard or Filters view, click Trends.

The zoom-in drilldown 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.

Action	**Description**
Export graph data	Select the tab containing the data to export. Click Export and select the file format: PDF, Excel, or CSV.
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 Connection Failures tab, select the machine type, failure type, Delivery Group, and time period to view a graph containing more detailed information about the user connection failures across your site.
View trends for machine failures	From the 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, VM start time, and so on. 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. The administrator 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 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 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 specific Delivery Group. Server OS availability - displays the current state of Server OS machines by availability for the entire site or specific Delivery Group.
View network analysis data using HDX Insight	The availability of this feature depends on your organization's license and your administrator permissions. 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.

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

Note:

- HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.
- Sessions, failures and logon performance trend information is available as graphs and tables when the time period is set to Last month or shorter. When the time period is set to Last Year, the trend information is available as graphs but not as tables.
- Export of large data in Director can time out or produce an unexpected error. This can typically happen when the site monitored by Director has a large number of configured sessions and the data requested for export exceeds 500K rows.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor hotfixes

To view the hotfixes installed on a specific machine VDA (physical or VM), choose the Machine Details view.

Control user machine power states

To control the state of the machines that you select in Director, use the Power Control options. These options are available for 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 may not always shut down all running processes, and you risk losing data if you shut down a VM in this way.
Suspend	Suspends a running VM in its current state and stores that state in a file on the default storage repository. This option allows you to shut down the VM's host server and later, after rebooting it, resume the VM, returning it to its original running state.
Resume	Resumes a suspended VM and restores its original running state.
Start	Starts a VM when it is off (also called a cold start).

If power control actions fail, hover the mouse over the alert, and a pop-up message appears with details about the failure.

Prevent connections to machines

Use maintenance mode to prevent new connections temporarily while the appropriate administrator performs maintenance tasks on the image.

When you enable maintenance mode on machines, no new connections are allowed until you disable it. If users are currently logged on, maintenance mode takes effect as soon as all users are logged off. For users who do not log off, send a message informing them that machines will be shut down at a certain time, and use the power controls to force the machines to shut down.

1. Select the machine, such as from the User Details view, or a group of machines in the Filters view.
2. Select Maintenance Mode, and turn on the option.

If a user tries to connect to an assigned desktop while it is in maintenance mode, a message appears indicating that the desktop is currently unavailable. No new connections can be made until you disable maintenance mode.

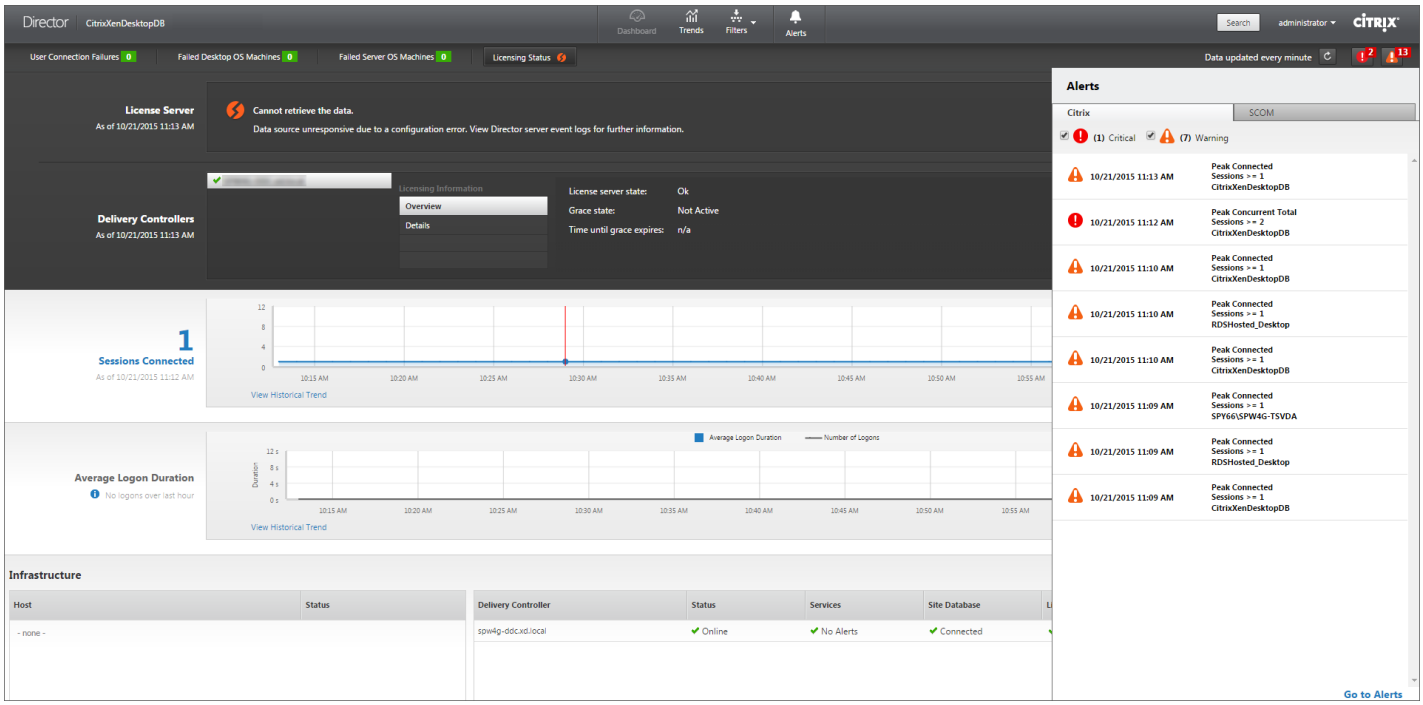
Alerts and notifications

Sep 22, 2016

In this article:

Monitor alerts

Alerts are displayed in Director on the dashboard and other high level views with warning and critical alert symbols. Alerts update automatically every minute; you can also update alerts on demand.

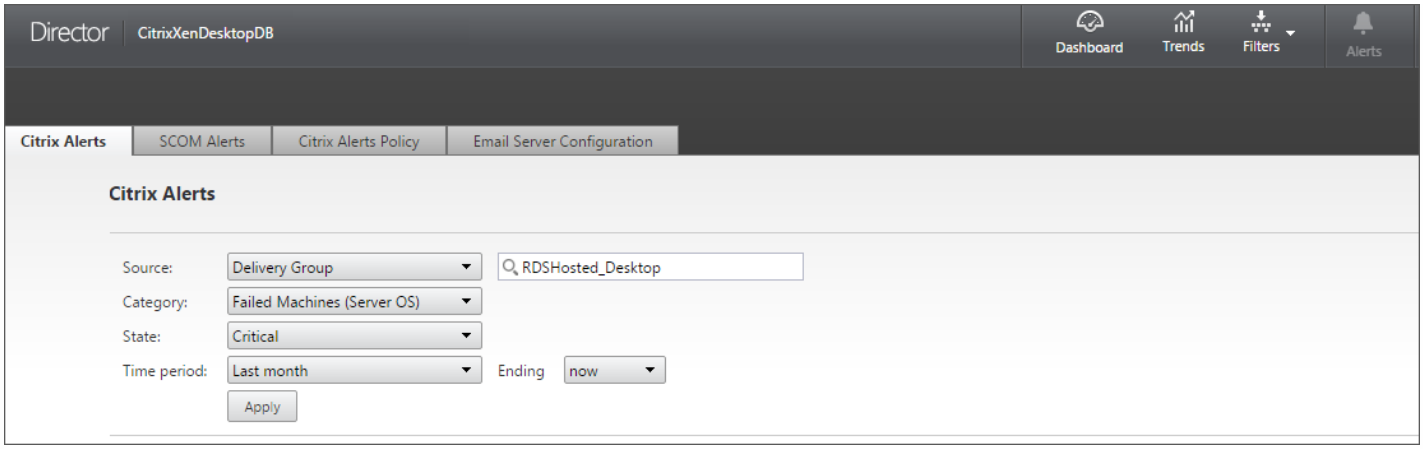


A warning alert (amber triangle) indicates that the minimum threshold of a condition has been reached.

A critical alert (red circle) shows that the maximum threshold of a condition has been 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.

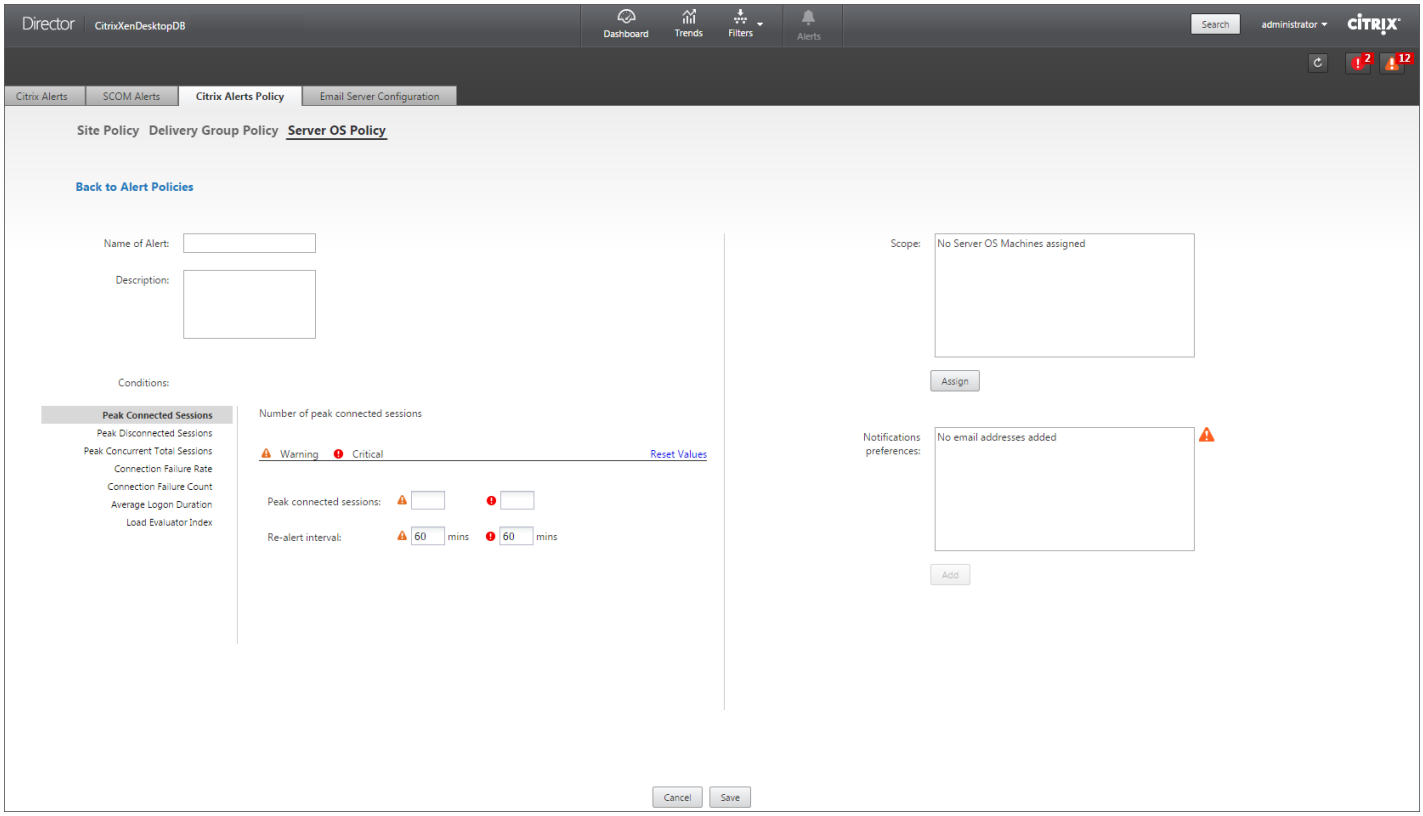


Citrix alerts. Citrix alerts are alerts monitored in Director which originate from Citrix components. You can configure Citrix alerts policies within Director in **Alerts** > **Citrix Alerts Policy**. As part of the configuration, you can set notifications to be sent by email to individuals and groups when alerts are generated as a result of an alert condition breaching the threshold. For more information on setting up Citrix Alerts, see Create alerts policies.

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 and Configure SCOM integration.

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 which 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 higher 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, then 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 will 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 SMTP server in the **Email Server Configuration** tab in order to set email Notification preferences in Alerts Policies.
7. Click **Save**.

Creating a policy with 20 or more Delivery Groups defined in the Scope may 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), may result in an increase in response time (over 5 seconds).

Alerts policies conditions

Alert policy condition	Description and recommended actions
Peak Connected Sessions	Number of peak connected sessions. Recommended actions when alert displays: • 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. Recommended actions when alert displays: • 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. • Logoff disconnected sessions if needed.
Peak Concurrent Total Sessions	Number of peak concurrent sessions. Recommended actions when alert displays: • 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. • Logoff disconnected sessions if needed.
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. Recommended actions when alert displays: • Check Director Connection Failures Trends view for events logged from the Configuration log. • Determine if applications or desktops are reachable.
Failed Machines (Desktop OS)	Number of failed Desktop OS machines. Recommended actions when alert displays: • 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. Recommended actions when alert displays: • Failures can occur for various reasons as shown in the Director Dashboard and Filters views. Run Citrix Scout diagnostics to determine root cause.
Average Logon Duration	Average logon duration for logons which occurred over the last hour. Recommended actions when alert displays: • 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. Recommended actions when alert displays: • Check Director for Server OS Machines that may have a peak load (Max load). • View both Dashboard (failures) and Trends Load Evaluator Index report.

SCOM alerts

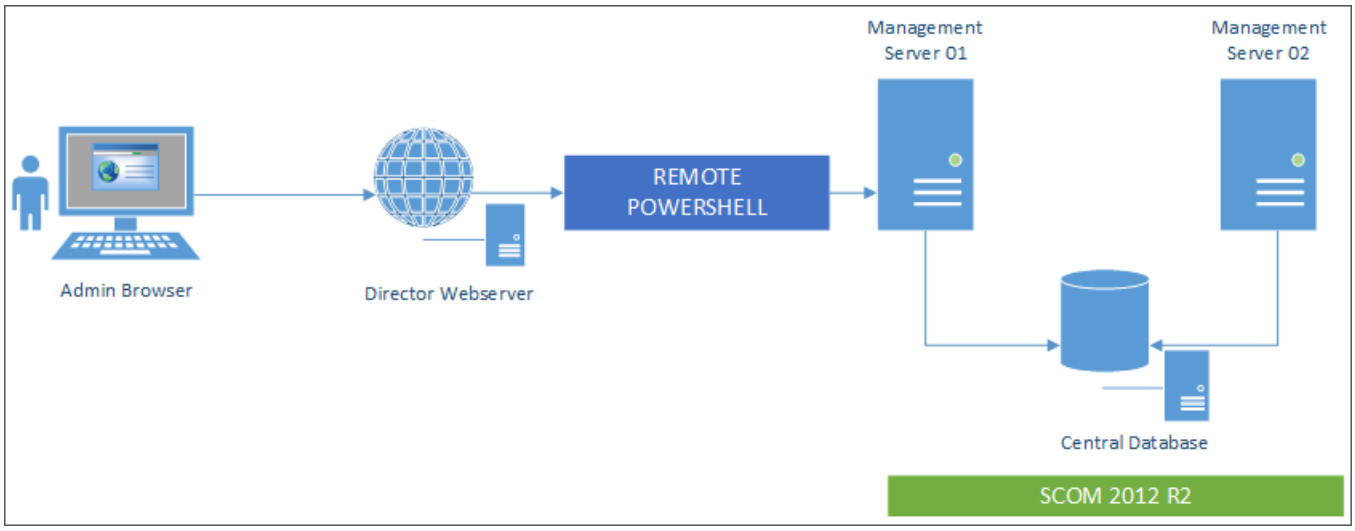
SCOM integration with Director lets you view alert information from Microsoft System Center 2012 Operations Manager (SCOM) on the Dashboard and in other high level views in Director.

SCOM alerts are displayed on-screen alongside Citrix alerts. You can access and drill down into SCOM alerts from SCOM tab in the side bar.

You can view historical alerts up to one month old, sort, filter and export the filtered information to CSV, Excel and PDF report formats.

Configure SCOM integration

SCOM integration uses remote PowerShell 3.0 or higher 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 higher (PowerShell version in Director and the SCOM server must match)
- Quad Core CPU with 16 GB RAM (recommended)
- A primary Management Server for SCOM must be configured in the Director web.config file. You can do this using the DirectorConfig tool.
- Citrix recommends that the Director administrator account is configured as a SCOM Operator role so that they can retrieve full alert information in Director. If this is not possible, a SCOM administrator account can be configured in the

web.config file using the DirectorConfig tool, however it is not recommended.

- Citrix recommends that you do not configure more than 10 Director administrators per SCOM Management Server. This is to ensure that the SCOM Management Server is moderately loaded for optimal performance.

On the Director server:

1. On the Director server, type **Enable-PSRemoting** to enable PowerShell remoting.

2. Add the SCOM Management Server to the TrustedHosts list. Open an elevated PowerShell prompt in From an elevated PowerShell command line, and execute the following command(s):

a. Get the current list of TrustedHosts

```
command
<p>Get-Item WSMAN:\localhost\Client\TrustedHosts</p>
```

b. 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.

```
command
<p>Set-Item WSMAN:\localhost\Client\TrustedHosts -Value &quot;&lt;FQDN SCOM Management Server&gt;,&lt;Old Values&
```

3. Configure SCOM using the DirectorConfig tool.

```
command
<p>C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom</p>
```

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 operators. These roles define the nature of access to SCOM data. For example, a read-only SCOM operator will not see the Administration pane and cannot discover or manage rules, machines or accounts. A SCOM Operator role is a full administrator role.

Note:

If a Director administrator is assigned to non-operator role the following operations will not be available to the Director administrator.

i. If there are multiple management servers configured and, in the event of primary management server not being available, the Director administrator will not be able to connect to secondary management server.
The primary management server is the server configured in the Director web.config file, which is the same server as the one specified in step 3. above with the DirectorConfig tool. The secondary management servers are peer management servers of the primary server.

ii. While filtering alerts, the Director administrator will not be able to 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.

3. Type **Enable-PSRemoting** to enable PowerShell remoting.

4. Set the WS-Management properties limits:

a. Modify MaxConcurrentUsers:

In CLI:

```
command
```

COPY

```
<p>winrm set winrm/config/winrs @{MaxConcurrentUsers = &quot;20&quot;} </p>
```

In PS:

```
command
```

COPY

```
<p>Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20</p>
```

b. Modify MaxShellsPerUser:

In CLI:

```
command
```

COPY

```
<p>winrm set winrm/config/winrs @{MaxShellsPerUser=&quot;20&quot;} </p>
```

In PS:

```
command
```

COPY

```
<p>Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20</p>
```

c. Modify MaxMemoryPerShellMB:

In CLI:

```
command
<p>winrm set winrm/config/winrs @{MaxMemoryPerShellMB=&quot;1024&quot;} </p>
```

In PS:

```
command
<p>Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024</p>
```

5. To ensure SCOM integration works in mixed domain environments, set the following registry entry.

Path: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Key: LocalAccountTokenFilterPolicy

Type: DWord

Value: 1

> ## 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.

Once SCOM integration is set up you may see the message "Cannot get the latest SCOM alerts. View the Director server event logs for more information". The server event logs will 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

Apr 27, 2015

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.
Delivery Group Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Read Only Administrator	Can access all views and see all objects in specified scopes as well as global information. Can download reports from HDX channels and can export Trends data using the Export option in the Trends view. Cannot perform any other commands or change anything in the views.
Help Desk Administrator	Can access only the Help Desk and User Details views and can view only objects that the administrator is delegated to manage. Can shadow a user's session and perform commands for that user. Can perform maintenance mode operations. Can use power control options for 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:

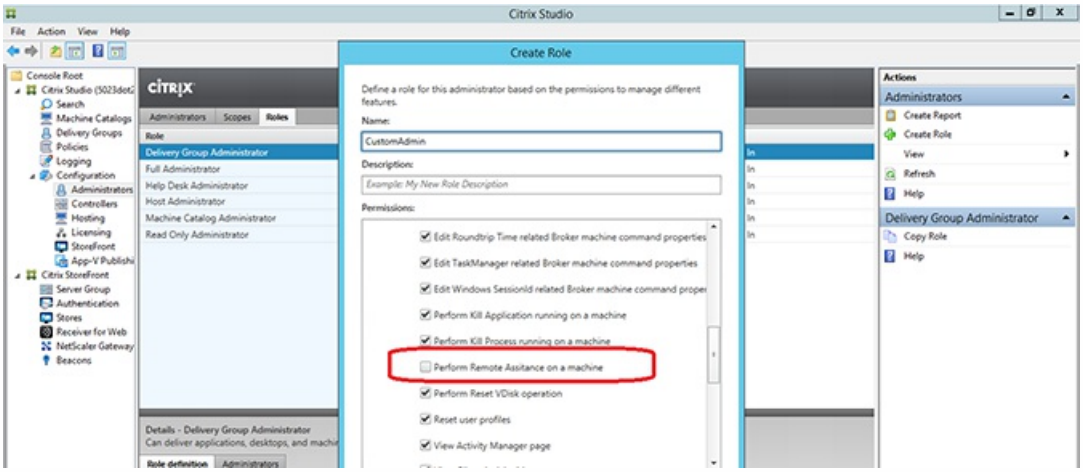
- Delivery Controller permission to log on to Director.
- Permissions to Delivery Groups to view the data related to those Delivery Groups in Director.

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.



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

Oct 24, 2016

This article highlights areas that may have an impact on system security when deploying and configuring Director.

Configure Microsoft Internet Information Services (IIS)

You can configure Director with a restricted IIS configuration. Note that this is not the default IIS configuration.

Filename extensions

You can disallow unlisted file name extensions.

Director requires these file name extensions in Request Filtering:

- .aspx
- .css
- .html
- .js
- .png
- .svc

Director requires the following HTTP verbs in Request Filtering. You can disallow unlisted verbs.

- GET
- POST
- HEAD

Director does not require:

- ISAPI filters
- ISAPI extensions
- CGI programs
- FastCGI programs

Important

- Director requires Full Trust. Do not set the global .NET trust level to High or lower.
- Director maintains a separate application pool.To modify the Director settings, select the Director Site and modify.

Configure user rights

When Director is installed, its application pools are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. This is normal installation behavior when application pools are created.

You do not need to change these user rights. These privileges are not used by Director and are automatically disabled.

Certificates in Director:

- For using HTTPS, trusted certificates can be configured and used.

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 Secure Sockets Layer (SSL) and 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.

Note: Secure communications from Director requires configuration for each connection separately.

Note: The SSL protocol is not recommended. Use TLS instead.

Note: You must secure communications with NetScaler using TLS, not IPsec.

To secure communications between Director and XenApp/XenDesktop servers (for monitoring and reports), refer to Securing endpoints using TLS.

To secure communications between Director and NetScaler (for NetScaler Insight), refer to Configure HDX Insight.

To secure communications between Director and License server, refer to Secure the License Administration Console.

Note: You cannot use TLS 1.1 or TLS 1.2 to secure communication between Director and License server.

Director security separation

If you deploy any web applications in the same web domain (domain name and port) as Director, then 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.

Configure permissions for VDAs earlier than XenDesktop 7

Apr 27, 2015

If users have VDAs earlier than XenDesktop 7 installed on their devices, 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.

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
```

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 tools folder. You must grant permissions to all Director users.

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
```

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
```

To grant the permissions to a specific computer account:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
```

For End Process, End Application, and Shadow actions:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
```

To grant the permissions to a user group:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
```

To display help for the tool:

```
ConfigRemoteMgmt.exe
```

Configure HDX Insight

Jun 01, 2016

Note: The availability of this feature depends on your organization's license and your administrator permissions.

HDX Insight is the integration of network analysis and performance management with Director:

- Network analysis leverages HDX Insight to provide an application and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in their deployment.
- Performance management provides the 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 provides Director with additional information:

- The Trends page shows latency and bandwidth effects for applications, desktops, and users across the 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 higher and the Receiver for Mac 11.8 or higher. 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 configure the network analysis feature on Director

Director provides network analysis by leveraging NetScaler HDX Insight to provide the Citrix application and desktop administrators the ability to troubleshoot and correlate issues that can be attributed to poor network performance.

NetScaler Insight Center must be installed and configured in Director to enable network analysis. Insight Center is a virtual machine (appliance) downloaded from Citrix.com. Using network analysis, Director communicates and gathers the information that is related to your deployment. This information is leveraged from HDX Insight, which provides robust analysis of the Citrix ICA protocol between the client and the back-end Citrix infrastructure.

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 in command line prompt.
2. When prompted, configure the NetScaler Insight Center machine name (FQDN or IP address), username, password, and HTTP or HTTPS connection type.
3. To verify the changes, log off and log back on.

Troubleshoot user issues

Feb 24, 2016

Use the Director's **Help Desk** view (**Activity Manager** page) to view information about the user:

- Check for details about the user's logon, connection, and applications.
- Shadow the user's machine.
- Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

Troubleshooting tips

User's issue	See these 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
Video is slow or poor quality	Run HDX channel system reports

Note: To make sure that the machine is not in maintenance mode, from the User Details view, review the Machine Details panel.

Search tips

When you type the user's name in a Search field, Director searches for users in Active Directory for users across all sites configured to support Director.

When you type a multiuser machine name in a Search field, Director displays the Machine Details for the specified machine.

When you type an endpoint name in a Search field, Director uses the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint, which enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

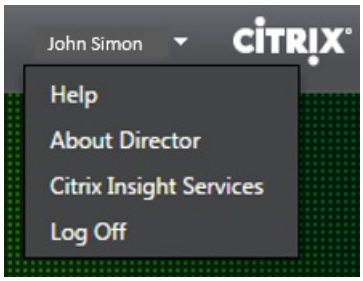
The search results also include users who are not currently using or assigned to a machine.

- Searches are not case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name (username, family name and first name, or display name), separated by a space, the results include matches for both strings. For example, if you type jo rob, the results might include strings such as “John Robertson” or Robert, Jones.

To return to the landing page, click the Director logo.

Access Citrix Insight Services

You can access Citrix Insight Services (CIS) from the User drop-down in Director to access additional diagnostic insights. The data available in CIS comes from sources including Call Home and Citrix Scout.



Upload troubleshooting information to Citrix Technical Support

Run Citrix Scout from a single Delivery Controller or VDA to capture key data points and Citrix Diagnosis Facility (CDF) traces to troubleshoot selected computers. Scout offers the ability to securely upload the data to Citrix Insight Services (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.

Shadow users

Oct 07, 2014

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.

Configure your Microsoft Internet Explorer browser to automatically open the downloaded Microsoft Remote Assistance (.msra) file with the Remote Assistance client.

To do this, you must enable the Automatic prompting for file downloads setting in the Group Policy editor:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Automatic prompting for file downloads.

By default, this option is enabled for sites in the Local intranet zone. If the Director site is not in the Local intranet zone, consider manually adding the site to this zone.

Send messages to users

Jul 07, 2014

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 log-offs and restarts, and profile resets.

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.

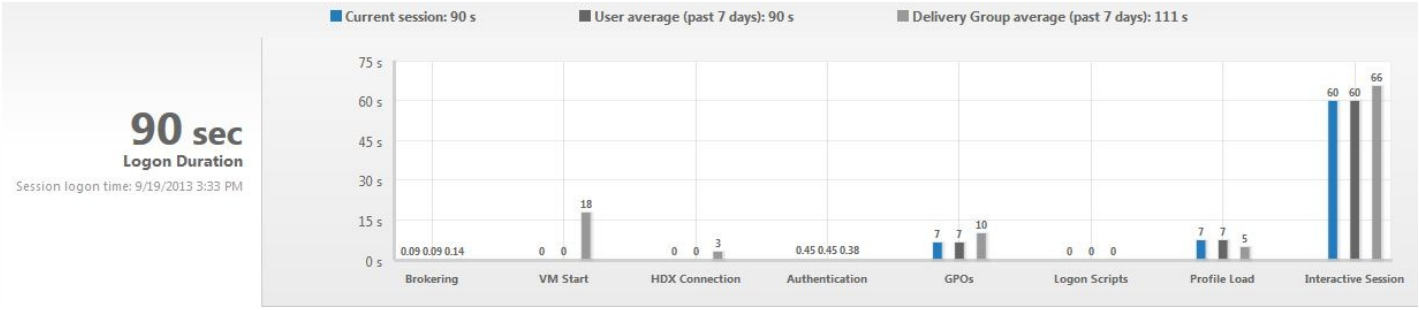
If the message is sent successfully, a confirmation message appears in Director. If the user's machine is connected, the message appears there.

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.

Diagnose user logon issues

Jul 04, 2016

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.



Logon Duration panel in the User Details view

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.
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 follows: 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 higher than 200 seconds is shown with the actual value displayed above the bar.

To identify unusual or unexpected values in the graph, compare the amount of time taken in each phase of the current session with the average duration for this user for the last seven days, and the average duration for all users in this Delivery Group for the last seven days.

Escalate as needed. For example, if the VM startup is slow, the issue 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.

Resolve application failures

Jul 07, 2014

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.
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 and escalate the issue to the appropriate administrator. Click , and from the Machine Details view, click Details and turn on the maintenance mode option. Escalate to the appropriate administrator.

Restore desktop connections

Jul 07, 2014

From Director, check the user's connection status for the current machine in the user title bar.

If the desktop connection failed, the error that caused failure is displayed and can help you decide how to troubleshoot.

Action	Description
Ensure that the machine is not in maintenance mode.	On the User Details page, make sure maintenance mode is turned off.
Restart the user's machine.	Select the machine and click Restart. Use this option if the user's machine is unresponsive or unable to connect, such as when the machine is using an unusually high amount of CPU resources, which can make the CPU unusable.

Restore sessions

Jul 07, 2014

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 Virtual Delivery Agents (VDAs) earlier than XenDesktop 7, Director cannot display complete information about the session; instead, it displays a message that the information is not available. These messages might appear in the User Details page and Activity Manager.

Run HDX channel system reports

Jul 07, 2014

In the User Details view, check the status of the HDX channels on the user's machine in the HDX panel. This panel is available only if the user machine is connected using HDX.
If a message appears indicating that the information is not currently available, wait for one minute for the page to refresh, or select the Refresh button. HDX data takes a little longer to update than other data.

Click an error or warning icon for more information.

Tip: You can view information about other channels in the same dialog box by clicking the left and right arrows in the left corner of the title bar.
HDX channel system reports are used mainly by Citrix Support to troubleshoot further.

1. In the HDX panel, click Download System Report.
2. You can view or save the .xml report file.
   - To view the .xml file, click Open. The .xml file appears in the same window as the Director application.
   - To save the .xml file, click Save. The Save As window appears, prompting you for a location on the Director machine to download the file to.

Reset a Personal vDisk

Jul 07, 2014

Caution: When you reset the disk, the settings revert back 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.

Reset a user profile

May 31, 2016

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 are 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 on again. The folders and files that were saved from the user's profile are copied to the new profile.
   Important: If the user has profiles on multiple platforms (such as Windows 8 and Windows 7), instruct the user to log back on first to the same desktop or app that the user reported as a problem. This ensures that the correct profile is reset.
   If the profile is a Citrix user profile, the profile is already reset by the time the user's desktop appears. If the profile is a Microsoft roaming profile, the folder restoration might still be in progress for a brief time. The user must stay logged on until the restoration is complete.

Note: The preceding steps assume you are using XenDesktop (desktop VDA). If you are using XenApp (server VDA) you will 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.

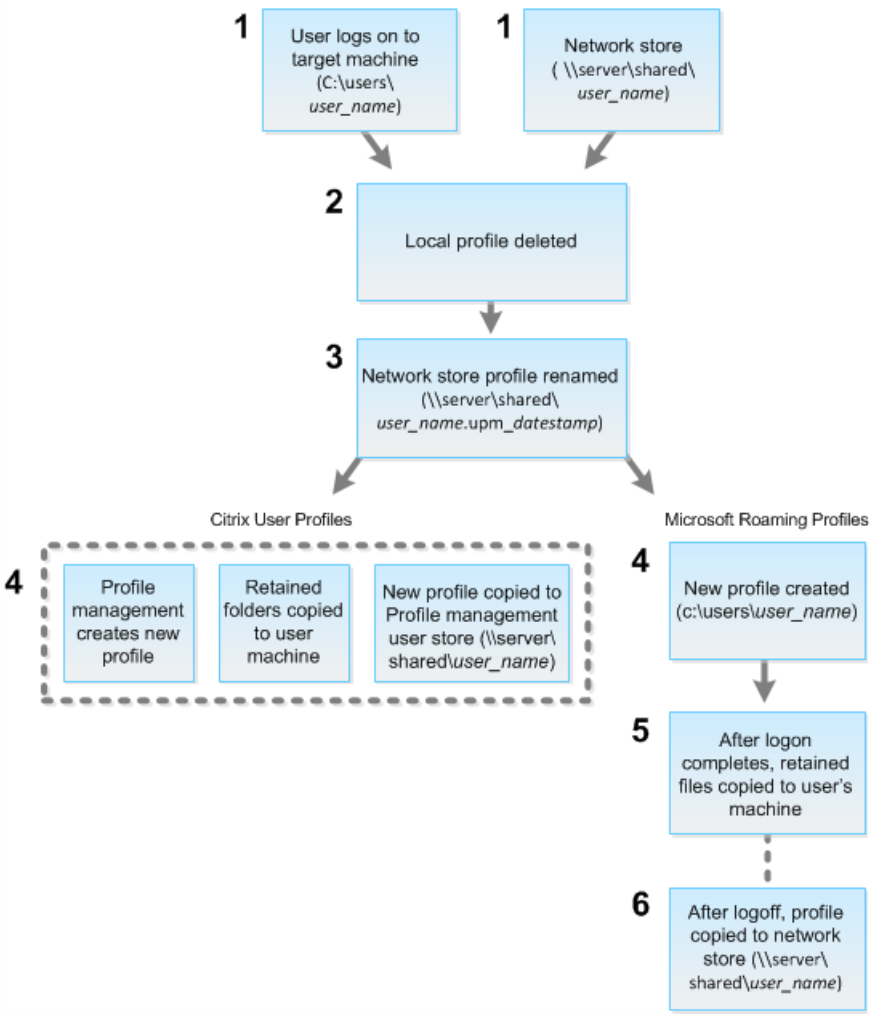
The folders (and their files) from the user's profile are saved and copied to the new profile. They are copied in the listed order:

- Desktop
- Cookies
- Favorites
- Documents
- Pictures
- Music
- Videos

Note: In Windows 8 and later, cookies are not copied when profiles are reset.

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.

The next time the user logs on, this diagram illustrates the processing that occurs.



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 rules, and the folders are copied back to the network profile, and the user can log on proceeds as normal. 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.

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.

SDKs and APIs

Jul 20, 2016

Several SDKs and APIs are available with this release.

XenApp and XenDesktop SDK: The XenApp and XenDesktop SDK is based on a number of Microsoft Windows PowerShell version 3.0 snap-ins that allow you to perform the same tasks as you would with the Citrix Studio console as well as tasks you cannot do with Studio alone.

For more information, see Citrix Developer.

Citrix Group Policy SDK: 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 the Group Policy SDK section below for more information.

Monitor Service OData API: You can use the Monitor Service OData API to:

- Analyze historical trends for future planning
- Perform detailed troubleshooting of connection and machine failures
- Extract information for feeding into other tools and processes; for example, using Microsoft Excel's PowerPivot tables to display the data in different ways
- Build a custom user interface on top of the data that the API provides

For details, see the Monitor Service OData API articles.

XenApp and XenDesktop SDK

Beginning with version 7.x, XenApp and XenDesktop share a unified architecture and management: the FlexCast Management Architecture. This means that XenApp provides many features previously only available in XenDesktop; elements of the SDK that relate to common features therefore apply equally to both XenApp and XenDesktop, even though the commands themselves refer only to XenDesktop.

If you are familiar with the XenDesktop 5 SDK, the following list summarizes the differences in 7.x versions of the XenApp and XenDesktop SDK.

- **New high-level SDK** — XenDesktop 7 provides a new high-level SDK that enables you to script and automate site creation and maintenance quickly and easily. The high-level SDK insulates you from much of the complexity of the low-level SDKs, so you can create a new Site simply by running two cmdlets.
- **New low-level SDKs** — Individual low-level SDKs are provided for the new XenDesktop 7 services, including a dedicated and enhanced SDK for the Delegated Administration Service (DAS), which was previously part of the Broker SDK in XenDesktop 5. There are also SDKs for new features including the Monitor Service, Environment Test, and Configuration Logging.
- **Windows Server OS Machine Catalogs and Delivery Groups** — You can use the XenDesktop 7 SDK to deliver cost-effective applications and desktops hosted on server operating systems.
- **Desktop OS Machine applications** — Desktop OS Machine applications have changed significantly at the SDK level.

If you have existing scripts for running applications on Desktop OSs, you will have to update these scripts for XenDesktop 7, because there is little backwards compatibility.

- **Apply settings to machines in Delivery Groups** — In XenDesktop 7, using configuration slots, you can apply settings to machines in a specific delivery group, rather than to all machines in a site. This enables you to configure, for a given delivery group, which settings apply to that group. A number of pre-defined configuration slots are provided that contain different types of settings, such as settings for StoreFront addresses for use with Receiver or App-V publishing server locations. You can use one collection of settings from a slot to affect only a particular delivery group, and a different collection of settings from the same slot to affect another delivery group. You can use names appropriate to your particular deployment; for example, "Sales Department policy."
- **Catalog types replaced** — In XenDesktop 7, catalog types have been replaced by catalogs with individual properties. However, for backwards compatibility, you can still use existing scripts that employ catalog types, such as single image (pooled) and thin clone (dedicated) etc., but internally these are converted into sets of properties.
  Caution: Backwards compatibility with XenDesktop 5 catalog types has been maintained where possible and practicable. However, when writing new scripts, do not use catalog types; instead, specify catalogs with individual properties.

- **Desktop object replaced** — In XenDesktop 5, the Desktop object is one of the main types of SDK object used in Broker SDK scripts. The Desktop object describes both the machine and the session on the machine. In XenDesktop 7, this object is replaced by the Session object and the Machine object, both of which have been expanded to do the work of the Desktop object. However, for backwards compatibility, you can still use existing scripts that employ the Desktop object.
  Caution: Backwards compatibility with XenDesktop 5 has been maintained where possible and practicable. However, when writing new scripts, do not use the Desktop object; instead, specify Session and Machine objects.

There are differences between the SDK and the Studio console in terms of policy rules. Entitlement and assignment policy rules are independent entities in the SDK; in the console, these entities are not visible as they are seamlessly merged with the Delivery Group. Also, access policy rules are less restrictive in the 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 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 3.0: 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.

Monitor Service OData API

Sep 29, 2014

In addition to using the Citrix Director console to display historical data, you can query data using the Monitor Service's API. You can use the API to:

- Analyze historical trends for future planning
- Perform detailed troubleshooting of connection and machine failures
- Extract information for feeding into other tools and processes; for example, using Microsoft Excel's PowerPivot tables to display the data in different ways
- Build a custom user interface on top of the data that the API provides

The Monitor Service API uses the Open Data (OData) protocol, which is a Web protocol for querying and updating data, built upon Web technologies such as HTTP. For more information about the OData protocol, see: http://www.odata.org.

The Monitor Service API is built on top of SQL Server databases using Windows Communication Foundation (WCF) Data Services that are populated during processing and consolidation. Two endpoints are exposed using WCF with wsHttpBinding. The base address is: http:// {dc-host}/Citrix/Monitor/OData/v2. You can also use TLS to secure endpoints; see Securing endpoints using TLS for more information.

1. The Data endpoint exposes read-only access directly to the database entities and can be accessed using the OData query language. This endpoint allows highly flexible access in terms of filtering and column selection. The Data API URI is: http://{dc-host}/Citrix/Monitor/OData/v2/Data. For more information about accessing the Monitor Service data, see Accessing data using the API.
2. The Methods endpoint exposes service operations that are used by Citrix Director to retrieve data that requires complex grouping and high performance standards, such as queries on the Dashboard and Trends pages. The Methods API URI is: http://{dc-host}/Citrix/Monitor/OData/v2/Methods. Methods are used only in Director itself so are not used by the majority of Citrix customers. They are therefore not documented here.

The version of the API included with XenApp and XenDesktop 7.6 provides the following new features:

- **Hotfix inventory.** Using the User Details view or Machine view in Director, you can see a list of all the Citrix hotfixes that have been installed on a machine. You can use the API to extract this data and create custom reports (for example, the state of installed hotfixes over an entire site) or pull it into an analytics engine. New classes have been introduced and the Machine class has been extended to support tracking Citrix hotfixes installed on the controller and VDAs.
- **Anonymous session troubleshooting.** Sessions can be run as a set of pooled local user accounts. The API has a new IsAnonymous property for the Session class (default value FALSE).
- **Hosted application usage reporting.** Director provides new capacity reports that show the usage of hosted applications over time. The API allows you to report on the details of each application instance running in a user session.

All the updates to data are fully documented in the API Reference at http://support.citrix.com/help/monitorserviceapi/7.6/.

The GetSessionSummary method has been deprecated at this release.

Accessing data using the API

Sep 29, 2014

The following types of data are available through the Monitor Service API:

- Data relating to connection failures
- Machines in a failure state
- Session usage
- Logon duration
- Load balancing data
- Hotfixes applied to a machine
- Hosted application usage

For a full description of the data objects, see http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/.

To use the Monitor Service OData API, you must be a XenApp or XenDesktop administrator. To call the API, you require read-only privileges; however, the data returned is determined by XenApp or XenDesktop administrator roles and permissions. For example, Delivery Group Administrators can call the Monitor Service API but the data they can obtain is controlled by Delivery Group access set up using Citrix Studio. For more information about XenApp or XenDesktop administrator roles and permissions, see Delegated Administration.

Querying the data

The Monitor Service API is a REST-based API that can be accessed using an OData consumer. OData consumers are applications that consume data exposed using the OData protocol. OData consumers vary in sophistication from simple web browsers to custom applications that can take advantage of all the features of the OData Protocol. For more information about OData consumers, see: http://www.odata.org/ecosystem#consumers.

Every part of the Monitor Service data model is accessible and can be filtered on the URL. OData provides a query language in the URL format you can use to retrieve entries from a service. For more information, see: http://msdn.microsoft.com/en-us/library/ff478141.aspx

The query is processed on the server side and can be filtered further using the OData protocol on the client side.

The data modeled falls into three categories: aggregate data (the summary tables), current state of objects (machines, sessions, etc), and log data, which is really historical events (connections, for example).

Note: Enums are not supported in the OData protocol; integers are used in their place. To determine the values returned by the Monitor Service OData API, see http://support.citrix.com/help/monitorserviceapi/7.6/.

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 length of time, therefore is exposed as an average over a time period.
- LogOn Count and Connection Failures are counts of occurrences over a period of time, therefore are exposed as sums over a time period.

Concurrent data evaluation

Sessions must be overlapping to be considered concurrent. However, when the time interval is 1 minute, all sessions in that minute (whether or not they overlap) are considered concurrent: the size of the interval is so small that the performance overhead involved in calculating the precision is not worth the value added. If the sessions occur in the same hour, but not in the same minute, they are not considered to overlap.

Correlation of summary tables with raw data

The data model represents metrics in two different ways.:
- The summary tables represent aggregate views of the metrics in per minute, hour, and day time granularities.
- The raw data represents individual events or current state tracked in the session, connection, application and other objects.

When attempting to correlate data across API calls or within the data model itself, it is important to understand the following concepts and limitations:

- **No summary data for partial intervals.** Metrics summaries are designed to meet the needs of historical trends over long periods of time. These metrics are aggregated into the summary table for complete intervals. There will be no summary data for a partial interval at the beginning (oldest available data) of the data collection nor at the end. When viewing aggregations of a day (Interval=1440), this means that the first and most recent incomplete days will have no data. Although raw data may exist for those partial intervals, it will never be summarized. You can determine the earliest and latest aggregate interval for a particular data granularity by pulling the min and max SummaryDate from a particular summary table. The SummaryDate column represents the start of the interval. The Granularity column represents the length of the interval for the aggregate data.
- **Correlating by time.** Metrics are aggregated into the summary table for complete intervals as described above. They can be used for historical trends, but raw events may be more current in the state than what has been summarized for trend analysis. Any time-based comparison of summary to raw data needs to take into account that there will be no summary data for partial intervals that may occur or for the beginning and ending of the time period.
- **Missed and latent events.** Metrics that are aggregated into the summary table may be slightly inaccurate if events are missed or latent to the aggregation period. Although the Monitor Service attempts to maintain an accurate current state, it does not go back in time to recompute aggregation in the summary tables for missed or latent events.
- **Connection High Availability.** During connection HA there will be gaps in the summary data counts of current connections, but the session instances will still be running in the raw data.
- **Data retention periods.** Data in the summary tables is retained on a different grooming schedule from the schedule for raw event data. Data may be missing because it has been groomed away from summary or raw tables. Retention periods may also differ for different granularities of summary data. Lower granularity data (minutes) is groomed more quickly than higher granularity data (days). If data is missing from one granularity due to grooming, it may be found in a higher granularity. Since the API calls only return the specific granularity requested, receiving no data for one granularity does not mean 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.

Data granularity and retention

The granularity of aggregated data retrieved by Director is a function of the time (T) span requested. The rules are as follows:

- 0 < T <= 1 hour uses per-minute granularity
- 0 < T <= 30 days uses per-hour granularity
- T > 31 days uses per-day granularity

Requested data that does not come from aggregated data comes from the raw Session and Connection information. This data tends to grow fast, and therefore has its own grooming setting. Grooming ensures that only relevant data is kept long term. This ensures better performance while maintaining the granularity required for reporting. For customers who are not licensed to use the Platinum edition, grooming begins at day 8 regardless of the default grooming retention. Platinum customers can change the grooming retention to their desired number of retention days, otherwise the default is used.

The following settings are used to control grooming:

Setting name	Affected grooming	Default value (days)	Accessed using
GroomSessionsRetentionDays	Session and SessionDetail records	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomSummariesRetentionDays	DesktopGroupSummary, FailureLogSummary and LoadIndexSummary records. Aggregated data - daily granularity.	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomHourlyRetentionDays	Aggregated data - hourly granularity	32 days	Monitor.Configuration Database Table. See note below.
GroomMinuteRetentionDays	Aggregated data - minute granularity	3 days	Monitor.Configuration Database Table. See note below.
GroomFailuresRetentionDays	MachineFailureLog and ConnectionFailureLog records	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomLoadIndexesRetentionDays	LoadIndex records	7 for non-	Cmdlet (set/get-monitorconfiguration)

Setting name	Affected grooming	Default value (days)	Accessed using
GroomDeletedRetentionDays	Machine, Catalog, DesktopGroup and Hypervisor entities that have a LifecycleState of 'Deleted'. This will also delete any related Session, SessionDetail, Summary, Failure or LoadIndex records.	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomMachineHotfixHistoryRetentionDays	Hotfixes applied to the VDA and Controller machines	90 for both non-Platinum and Platinum users	Cmdlet (set/get-monitorconfiguration)

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. 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.

Securing endpoints using TLS

Apr 27, 2015

This document explains how to use TLS to secure the Monitor Service OData API endpoints. If you choose to use TLS, you must configure TLS on all Delivery Controllers in the site; you cannot use a mixture of TLS and non-TLS.

To secure Monitor Service endpoints using TLS, you must perform the following configuration. Some steps need to be done only once per site, others must be run from every machine hosting the Monitor Service in the site. The steps are described below.

Part 1: Certificate registration with the system

1. Create a certificate using a trusted certificate manager. The certificate must be associated with the port on the machine that you wish to use for OData TLS.
2. Configure the Monitor Service to use this port for TLS communication. The steps depend on your environment and how this works with certificates. The following example shows how to configure port 449:

- Associate the certificate with a port:
  `netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9 appid='{00000000-0000-0000-0000-000000000000}'`
  Tip: In a PowerShell command window, ensure you put single quotes around the GUID in the appID, as shown above, or the command will not work. Note that a line break has been added to this example for readability only.

Part 2: Modify the Monitor Service configuration settings

1. From any Delivery Controller in the site, run the following PowerShell commands once. This removes the Monitor Service registration with the Configuration Service.

```
asnp citrix.*

$serviceGroup = get-configregisteredserviceinstance -servicetype Monitor | Select -First 1 ServiceGroupUid

remove-configserviceGroup -ServiceGroupUid $serviceGroup.ServiceGroupUid
```

2. Do the following on all Controllers in the site:
   - Using a cmd prompt, locate the installed Citrix Monitor directory (typically in C:\Program Files\Citrix\Monitor\Service). Within that directory run:
     `Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODataPort 449 -RequireODataSsl`
   - Run the following PowerShell commands:

```
asnp citrix.*  (if not already run within this window)

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGroupMembership
```

Examples

Sep 24, 2014

The following examples show how to export Monitor Service data using the OData API.

Example 1 - Raw XML

1. Place the URL for each data set into a web browser that is running with the appropriate administrative permissions for the XenApp or XenDesktop Site. Citrix recommends using the Chrome browser with the Advanced Rest Client add-in.
2. View the source.

Example 2 - PowerPivot with Excel

These instructions assume that you have already installed Microsoft Excel and PowerPivot.

Open Excel (running with the appropriate administrative permissions for the XenApp or XenDesktop Site).

If you are using Excel 2010:

1. Click the PowerPivot tab.
2. Click PowerPivot Window.
3. Click **From Data Feeds** in the ribbon.
4. Choose a Friendly Connection Name (for example: XenDesktop Monitoring Data) and enter the data feed url: http://{dc-host}/Citrix/Monitor/OData/v2/Data (or https: if you are using TLS).
5. Click **Next**.
6. Select the tables you want to import into Excel and click **Finish**. The data is retrieved.
7. You can now use PowerPivot to view and analyze the data with PivotTables and PivotCharts. For more information, see the Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx

If you are using Excel 2013:

1. Click the Data tab.
2. Choose From Other Sources > From OData Data Feed
3. Enter the data feed url: http://{dc-host}/Citrix/Monitor/OData/v1/Data (or https: if you are using TLS) and click **Next**.
4. Select the tables you want to import into Excel and click **Next**.
5. Accept name defaults or customize names and click **Finish**.
6. Choose **Connection Only** or **Pivot Report**. The data is retrieved.
7. You can now use PowerPivot to view and analyze the data with PivotTables and PivotCharts. For more information, see the Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx

Example 3 - LINQPad

These instructions assume that you have already installed LINQPad.

1. Run LinqPad with the appropriate administrative permissions for the XenApp or XenDesktop Site.
   Tip: the easiest way is to download, install and run on the Delivery Controller.
2. Click the Add connection link.
3. Choose WCF Data Services 5.1 (OData 3) and click **Next**.
4. Enter the data feed URL: http://{dc-host}/Citrix/Monitor/OData/v2/Data (or https: if you are using TLS). If necessary, enter the username and password to access the Delivery Controller. Click **OK**.

5. You can now run LINQ queries against the data feed and export the data as needed. For example, right-click Catalogs and choose **Catalogs.Take(100)**. This returns the first 100 Catalogs in the database. Choose Export>Export to Excel with formatting.

For further worked examples of how to use the API with LINQPad, see http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/.