

About Citrix Receiver for Windows 4.7

Mar 27, 2017

This pdf file includes the Citrix Receiver for Windows 4.7 documentation. You can save a local copy of this file and use it offline. Use the built-in Search and Bookmark features to find what you need.

Citrix Receiver for Windows provides users with secure, self-service access to virtual desktops and apps provided by XenApp and XenDesktop.

What's new in this release

Bidirectional content redirection

Bidirectional content redirection enables administrators to specify client to host and host to client URL redirection using client and host policies. Server policies are set in Citrix Studio, and client policies are set in the Citrix Receiver Group Policy Object administrative template. This feature works in both desktop sessions and application sessions.

Bidirectional content redirection is supported on domain-joined client devices only. Bidirectional content redirection functions even when there are no active sessions running on the server.

Citrix recommends that you use bidirectional content redirection for URL redirection.

Bidirectional content redirection requires XenApp or XenDesktop 7.13 and later. This feature supports only Internet Explorer 8 through 11.

For information on configuring bidirectional content redirection, see [Configuring Bidirectional Content Redirection](#).

Generic Client Input Method Editors (IME)

Starting with this release, Citrix Receiver for Windows allows you to use an Input Method Editor (IME) on both the client and on the server. This feature, generic client IME, provides a seamless mechanism to redirect the IME in a session for a better user experience. This feature enables you to input text in East Asian characters dynamically in a VDA session.

Using this feature, you can compose text at the insertion point rather than in a separate window. At the insertion point, a candidate window with the list of composing characters appears when using either a physical or a touch keyboard.

By default, generic client IME inherits and honors the existing keyboard layout synchronization settings.

For more information on configuring generic client IME, see [Configuring Generic client IME](#).

Auto client reconnect and session reliability

In XenApp and XenDesktop 7.10 and earlier, you were required to configure auto client reconnect and session reliability both using a Citrix Studio policy and by modifying the registry or the default.ica file.

Starting with XenApp and XenDesktop 7.11, you can configure auto client reconnect and session reliability using only the Citrix Studio policy. Citrix Receiver for Windows registers the auto client reconnect and session reliability settings set in the Citrix Studio policy and applies them accordingly.

Note:

1. When you set the **Enable session reliability** option to **Disabled** either in the Citrix Receiver Group Policy Object administrative template or the Citrix Studio policy on the DDC, session reliability is disabled.
2. When the **Enable session reliability** option is not configured in the Citrix Studio policy, and set to **Disabled** in the Citrix

Receiver Group Policy Object administrative template, session reliability is enabled.

For more information on this feature, see [Auto client reconnect and session reliability](#).

Validating free disk space

Starting with this release, before installing Citrix Receiver for Windows, the installer verifies whether there is enough available disk space to complete the installation. This check is performed on both the graphical user interface and the command line interface installation.

For more information on this feature, see [Validating free disk space](#).

Adaptive transport

Adaptive transport for XenApp and XenDesktop optimizes data transport by applying a new Citrix protocol called Enlightened Data Transport (EDT) in preference to TCP whenever possible. Compared to TCP and UDP, EDT delivers a superior user experience on long-haul WAN and internet connections. EDT dynamically responds to changing network conditions while maintaining high server scalability and efficient use of network capacity. EDT is built on UDP and improves data throughput for all ICA virtual channels, including Thinwire display remoting, file transfer (Client Drive Mapping), printing, multimedia redirection. If UDP is not available, adaptive transport automatically reverts to TCP.

For more information on how to configure adaptive transport, see [Configuring Adaptive Transport layer](#).

Extended cipher support

Citrix Receiver for Windows extends support for RSA keys of 3072 bit length for enhanced security. The support is applicable on the following ciphers suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

For more information on supported cipher suites, see [About TLS and Group Policies](#).

CDM Enhancement

On a local area network (LAN), the performance of file copy operation using CDM between the client and the VDA and the other way around has been improved. This enhancement requires both Citrix Receiver for Windows 4.7, and XenApp and XenDesktop 7.13 and later.

Citrix Receiver for Windows 4.7 Fixed Issues

Mar 24, 2017

Citrix Receiver for Windows 4.7

Compared to: Citrix Receiver for Windows 4.6

Local App Access

User Experience

Security Issues

User Interface

Session/Connection

Local App Access

- After disconnecting from a Local App Access (LAA) desktop and connecting to a full-screen non-LAA desktop, the client side taskbar might show up above the full-screen non-LAA desktop.

[#LC5966]

Security Issues

- The setting "RemoveICAFile" might not be honored.

[#LC5840]

Session/Connection

- USB redirection might not work for fingerprint devices using a USB 3.0 port that supports "Selective Suspend" with power state D2 before redirection. The devices might fail to wake up during redirection, which can cause the redirection to fail. To enable the fix, set the following registry keys:

- *On 32-bit Windows:*

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

Name: WakeupSelSusPid

Type: DWORD

Value: pid of the device

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

Name: WakeupSelSusDisable

Type: DWORD

Value: 0 to enable and 1 to disable this feature

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

Name: WakeupSelSusVid

Type: DWORD

Value: vid of the device

- *On 64-bit Windows:*

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Name: WakeupSelSusPid

Type: DWORD

Value: pid of the device

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Name: WakeupSelSusDisable

Type: DWORD

Value: 0 to enable and 1 to disable this feature

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Name: WakeupSelSusVid

Type: DWORD

Value: vid of the device

[#LC5132]

- File type association might not work when logging on using a roaming user profile and opening an published application.

[#LC5184]

- Communication between an ICA session and the WarpDrive application might fail.

[#LC5718]

- When you update the "Display name" or "Application name" in AppCenter or Citrix Studio, the original desktop shortcut might be orphaned or broken instead of getting modified, and a new desktop shortcut with the updated application name is created.

[#LC5757]

- If a session is recovered with Session Reliability and Local App Access is enabled, the Desktop Viewer toolbar might no longer be visible.

[#LC5883]

- With Application Prelaunch enabled, subsequent refreshes might cause a prelaunch session to get recreated while the previous prelaunch session terminates after timeout.

[#LC5924]

- The CPU usage of the wfica.exe process might be very high in a double hop-scenario and cause VDAs to become slow or unresponsive. The issue occurs when you launch desktop sessions from multiple user devices to a VDA for Server OS while you start other published applications through Citrix Receiver for Windows in desktop sessions.

To enable the fix, set the following registry keys:

- *On 32-bit Windows:*

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

Name: SlowHPCPolling

Type: REG_SZ

Value: 2-500

- *On 64-bit Windows:*

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA

```
Client\Engine\Configuration\Advanced\Modules\WFClient
Name: SlowHPCPolling
Type: REG_SZ
Value: 2-500
```

[#LC5968]

- Using the CleanUp.exe process with the silent switch on does not reload Citrix Receiver properly.

[#LC6039]

- Attempts to start a user session immediately after terminating an ICA session might fail if the following registry key is added:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
Name: VdLoadUnloadTimeOut
Type: REG_DWORD
Data: Any value in seconds (Decimal)
```

[#LC6122]

- After updating to the Windows 10 Anniversary Update (Build 14393), single mouse clicks register as double clicks within an ICA session.

[#LC6127]

- When using the desktop lock appliance, the desktop might not launch and the following error message appears: "HDX engine is not running. Contact Administrator."

[#LC6332]

- When a user is running multiple sessions with Local App Access/HDX seamless apps enabled, applications and desktops might get shuffled intermittently. With this fix, Local App Access/HDX seamless apps can be enabled in only one session and is disabled for other, concurrent sessions of the same user.

[#LC6408]

- Attempts to launch an application from StoreFront might fail after restarting the computer.

[#LC6413]

- Citrix Receiver for Windows 4.5 and 4.6 might fail to perform the scan function with the following error message:

"Your operation is canceled."

[#LC6468]

- The keyboard and mouse might intermittently disconnect when switching between a wired network LAN and WiFi.

[#LC6594]

User Experience

- When launching a published desktop session in seamless mode by connecting a remote desktop to a user device, the

keyboard shortcut dialog tip window might not appear.

[#LC6483]

User Interface

- File type association might fail to work with file names that contain non-ASCII characters such as Japanese, Simplified Chinese, and Traditional Chinese.

[#LC3105]

- After upgrading Citrix Receiver to version 4.3, certain application icons might not appear.

[#LC6371]

Additional Fixes in Version 4.7

- When you close Citrix Receiver for Windows, applications launched in a double-hop scenario might not be disconnected after restarting Citrix Receiver for Windows.

[#626970]

- After upgrading Citrix Receiver to the latest version, custom settings for Auto-client Reconnect/Session Reliability are not retained; instead, the default settings are restored.

[#659754]

Note: This version of Citrix Receiver for Windows also includes all fixes included in Versions [4.6](#), [4.5](#), [4.4](#), [4.3](#), [4.2](#), [4.1](#), and [4.0](#).

Citrix Receiver for Windows 4.7 Known Issues

Feb 23, 2017

Known issues in Citrix Receiver for Windows 4.7

The following known issues have been observed in this release:

- When you are launching a session using smart card plus, the dialog to type the smart card PIN might not appear.

[RFWIN-5674]

- When connected to several VDAs simultaneously, Citrix Receiver for Windows might not honor the auto client reconnect and session reliability settings on each VDA and behave inconsistently.

[RFWIN-3077]

- When you are using thinwire-based graphics in a session launched through the NetScaler Gateway, and the session tries to reconnect in the auto client reconnect time, then the session does not honor the UDP settings and falls back to TCP for data transport.

[RFWIN-5747]

Known issues in Citrix Receiver for Windows 4.6

The following known issues have been observed in this release:

- After upgrading Citrix Receiver to the latest version, custom settings for Auto-client Reconnect/Session Reliability are not retained; instead, the default settings are restored.

[#659754]

Known issues in Citrix Receiver for Windows 4.5

The following known issues have been observed in this release:

- The desktop viewer alert message during disconnect is not applicable for anonymous user sessions. This is by design.

[#481561]

- System tray notifications can sometimes be seen in desktop lock mode.

[#488620]

- Citrix Receiver for Windows does not install on a Windows 2012 R2 machine with a User (non-admin) account.

To resolve this issue:

1. Click Start, type regedit and press Enter.
2. Locate the following setting:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

Create: DisableMSI Type: REG_DWORD value = 0 (0 should allow you to install)

[#492508]

- The language bar does not appear on the logon screen of the desktop lock client. The workaround is to use the floating language bar.

[#502678]

- The **Shortcut** options present in the Citrix Desktop Viewer are not working when the session is opened in windowed mode.

[#510529]

- Pinch and zoom gestures are not working on applications remoted through pre-7.0 versions of XenApp and XenDesktop, or on XenApp and XenDesktop version 7.0 or later on Windows 2008 R2.

[#517877]

- The NetScaler Gateway End Point Analysis Plugin (EPA) does not provide support for native Citrix Receiver for Windows.

[#534790]

- After applying the Microsoft Windows 10 Anniversary Update (Version 1607) on Windows 10 RTM Version 1511 with Citrix Receiver for Windows installed, the Single Sign-on process (SSONSvr.exe) might fail.

[#540988]

- Volume Controls might not work for RealTimes for Real Player inside the session due to compatibility issues with RAVE.

[#573549]

- In HDX 3D Pro enabled sessions running at 50+ FPS, the Desktop Viewer (CDViewer.exe) might exit unexpectedly, causing the user session to become unresponsive.

[#597875]

- Citrix Receiver for Windows might have an issue with file type association when the filename contains odd-byte UTF-8 characters.

[#602107]

- When changing the orientation of a hosted application on Windows 10 Surface Pro devices a tool tip screen appears stating 'Exiting full screen mode'. To resolve this issue, disable tip dialog messages by setting the following registry key:

HKEY_CURRENT_USER/software\HKCU\software\citrix\ica client\keyboard mappings\tips

Use a value of 1 to disable tips, and use a value of 0 to enable tips; setting this registry key value to 1 disables all tips.

[#608346]

- Performance degrades when connected to a Windows 2008 R2 VDA in H.264 Graphics mode when hardware decoding is enabled on the client. Citrix recommends using legacy graphics mode on the VDA to avoid this issue.

[#609292, #611580]

- With the "Configure Unified Experience" option enabled from the StoreFront side, the self-service plug-in refresh operation might not work when refreshed automatically. Additionally, the enumeration of applications recently added or removed from the Desktop Delivery Controller side might no longer get updated on the user device until refreshed manually.

[#623041]

- When you right-click the Citrix Receiver for Windows icon in the notification area, the "Show Application in Start Menu" option under "Start Menu Options" might not be grayed out. The issue occurs when you log on to the XenApp Services Site.

[#639947]

- Attempts to launch a XenApp session on Microsoft Windows Vista might fail. For information about a workaround to address this issue, see Knowledge Center article [CTX216607](#).

[#653135]

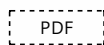
- When you add an account after upgrading from Version 4.2.100 of Citrix Receiver for Windows to 4.5, the account might no longer be visible. When attempting to add the same account, a prompt might appear, specifying that the account already exists. This occurs with non-admin users only.

[#654017]

Third party notices

Dec 06, 2016

Citrix Receiver for Windows might include third party software licensed under the terms defined in the following document:



[Citrix Receiver for Windows Third Party Notices](#)

System requirements and compatibility

Mar 07, 2017

Operating system

Citrix Receiver for Windows	Supported OS
4.7	Windows 10 [1]
	Windows Server 2016
	Windows 8.1, 32-bit and 64-bit editions (including Embedded edition)
	Windows 7, 32-bit and 64-bit editions (including Embedded edition)
	Windows Vista, 32-bit and 64-bit editions
	Windows Thin PC
	Windows Server 2012 R2, Standard and Datacenter editions
	Windows Server 2012, Standard and Datacenter editions
	Windows Server 2008 R2, 64-bit edition

[1] Windows 10 Anniversary update is also supported.

Hardware

Citrix Receiver for Windows requires a minimum of 500MB free disk space and 1GB RAM.

Touch-enabled devices

Citrix Receiver for Windows 4.7 can be used on Windows 10, 8 and 7 touch-enabled laptops, tablets, and monitors with XenApp and XenDesktop 7 or later, and with Windows 10, 8 and 7 and 2012 Virtual Desktop Agents.

Compatible Citrix Products

Citrix Receiver for Windows Version 4.7 is compatible with all currently supported versions of the following Citrix products. For information about the Citrix product lifecycle, and to find out when Citrix stops supporting specific versions of products, see the [Citrix Product Lifecycle Matrix](#).

Compatible Citrix Products:

- StoreFront
- XenApp
- XenDesktop
- Web Interface

Browser

- Internet Explorer
Connections to Citrix Receiver for Web or to Web Interface support the 32-bit mode of Internet Explorer. For the Internet Explorer versions supported, see [StoreFront system requirements](#) and [Web Interface system requirements](#).
- Latest Google Chrome (requires StoreFront)
- Latest Mozilla Firefox

Connectivity

Citrix Receiver for Windows supports HTTPS and ICA-over-TLS connections using one of the following configurations:

- For LAN connections:
 - StoreFront using StoreFront services or Citrix Receiver for Web sites
 - Web Interface 5.4 for Windows, using Web Interface or XenApp Services sitesFor information about domain-joined and non-domain-joined devices, see the [XenDesktop 7 documentation](#).
- For secure remote or local connections:
 - Citrix NetScaler Gateway 10.5 and later

Citrix Receiver for Windows supports: Windows domain-joined, managed devices (local and remote, with or without VPN) and non-domain joined devices.

For information on the supported NetScaler Gateway versions by StoreFront, see [StoreFront system requirements](#).

Private (self-signed) certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the user device to successfully access Citrix resources using Citrix Receiver for Windows.

Note

If the remote gateway's certificate cannot be verified upon connection (because the root certificate is not included in the local keystore), an untrusted certificate warning appears. If a user chooses to continue through the warning, a list of apps is displayed but the apps will not start.

Installing root certificates on user devices

For information about installing root certificates on user devices as well as configuring Web Interface for certificate use, see [Secure Receiver communication](#).

Wildcard certificates

Wildcard certificates are used instead of individual server certificates on a server within the same domain.

Citrix Receiver for Windows supports wildcard certificates, however they should only be used in accordance with your organization's security policy. In practice, alternative to wildcard certificates, a certificate containing the list of server names within the Subject Alternative Name (SAN) extension, might be considered. Such certificates can be issued by both private and public certificate authorities.

Intermediate certificates and the NetScaler Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the NetScaler Gateway server certificate. For information, see [Configuring Intermediate Certificates](#).

Authentication

For connections to StoreFront, Citrix Receiver for Windows supports the following authentication methods:

	Receiver for Web using browsers	StoreFront Services site (native)	StoreFront XenApp Services site (native)	NetScaler to Receiver for Web (browser)	NetScaler to StoreFront Services site (native)
Anonymous	Yes	Yes			
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*
Two-factor (domain with security token)				Yes*	Yes*
SMS				Yes*	Yes*
Smart card	Yes	Yes	No	Yes	Yes
User certificate				Yes (NetScaler plug-in)	Yes (NetScaler plug-in)

* With or without the NetScaler plug-in installed on the device.

Note

Citrix Receiver for Windows 4.7 supports 2FA (domain plus security token) through NetScaler Gateway to the StoreFront native service.

For connections to Web Interface 5.4, Citrix Receiver for Windows supports the following authentication methods (Web Interface uses the term "Explicit" for domain and security token authentication):

	Web Interface (browsers)	Web Interface XenApp Services site	NetScaler to Web Interface (browser)	NetScaler to Web Interface XenApp Services site
Anonymous	Yes			
Domain	Yes	Yes	Yes*	
Domain pass-through	Yes	Yes		
Security token			Yes*	
Two-factor (domain with security token)			Yes*	
SMS			Yes*	
Smart card	Yes	Yes		
User certificate			Yes (NetScaler plug-in)	

* Available only in deployments that include NetScaler Gateway, with or without the associated plug-in installed on the device.

For information about authentication, see [Configuring Authentication and Authorization](#) in the NetScaler Gateway documentation and [Manage](#) topics in the StoreFront documentation. For information about authentication methods supported by Web Interface, see [Configuring Authentication for the Web Interface](#).

Upgrading Citrix Receiver for Windows

For details on performing an upgrade of Citrix Receiver for Windows, see Knowledge Center article [CTX135933](#).

Other

- **.NET Framework minimum requirements**
 - .NET 3.5 Service Pack 1 is required by the Self-Service Plug-in, which allows users to subscribe to and launch desktops

and applications from the Receiver window or from a command line. For more information, see [Configure and install Receiver for Windows using command-line parameters](#).

- The .NET 2.0 Service Pack 1 and Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package are required to ensure that the Receiver icon displays correctly. The Microsoft Visual C++ 2005 Service Pack 1 package is included with .NET 2.0 Service Pack 1, .NET 3.5, and .NET 3.5 Service Pack 1; it is also available separately.
- For XenDesktop connections: To use the Desktop Viewer, .NET 2.0 Service Pack 1 or later is required. This version is required because, if Internet access is not available, certificate revocation checks slow down connection startup times. The checks can be turned off and startup times improved with this version of the Framework but not with .NET 2.0.
- For information about using Receiver with Microsoft Lync Server 2013 and the Microsoft Lync 2013 VDI Plug-in for Windows, see [XenDesktop, XenApp and Citrix Receiver Support for Microsoft Lync 2013 VDI Plug-in](#).
- **Supported connection methods and network transports:**
 - TCP/IP+HTTP
See [CTX 134341](#) for additional values that might be required.
 - TLS+HTTPS

Install

Feb 23, 2017

The CitrixReceiver.exe installation package can be installed in the following methods:

- By a user from Citrix.com or your own download site
 - A first-time user who obtains Citrix Receiver for Windows from Citrix.com or your own download site can set up an account by entering an email address instead of a server URL. Citrix Receiver for Windows determines the NetScaler Gateway or StoreFront Server associated with the email address and prompts the user to log on and continue the installation. This feature is referred to as "email-based account discovery."
Note: A first-time user is one who does not have Citrix Receiver for Windows installed on the device.
 - Email-based account discovery for a first-time user does not apply if Citrix Receiver for Windows is downloaded from a location other than Citrix.com (such as a Receiver for Web site).
 - If your site requires configuration of Citrix Receiver for Windows, use an alternate deployment method.
- Automatically from [Receiver for Web](#) or from a [Web Interface logon screen](#).
 - A first-time user can set up an account by entering a server URL or downloading a provisioning (CR) file.
- Using an Electronic Software Distribution (ESD) tool
 - A first-time user must enter a server URL or open a provisioning file to set up an account.

Citrix Receiver for Windows does not require administrator rights to install unless you are using pass-through authentication.

HDX RealTime Media Engine (RTME)

A single installer now combines the latest Citrix Receiver for Windows with the HDX RTME installer. When installing Citrix Receiver by using the executable file (.exe), the HDX RTME is installed as well.

If you have installed the HDX RealTime Media Engine, when you uninstall and then reinstall Citrix Receiver for Windows, ensure that you use the same mode that you used to install the HDX RTME.

Note

Installing the latest version of Citrix Receiver with integrated RTME support requires administrative privileges on the host machine.

Consider the following HDX RTME issues when installing or upgrading Citrix Receiver for Windows:

- The latest version of Citrix ReceiverPlusRTME contains HDX RTME; no further installation is required to install RTME.
- Upgrading from a previous Citrix Receiver for Windows version to the latest bundled version (Citrix Receiver with RTME) is supported. Previously installed versions of RTME are overwritten with the latest version; upgrading from the same Citrix Receiver for Windows version to the latest bundled version (for example, Receiver 4.7 to the bundled Receiver 4.7 plus RTME) is not supported.
- If you have an earlier version of RTME, installing the latest Citrix Receiver for Windows version automatically updates the RTME on the client device.
- If a more recent version of RTME is present, the installer retains the latest version.

Important

The HDX RealTime Connector on your XenApp/XenDesktop servers must be at least version 2.0.0.417 for compatibility with the new RTME package; that is, you cannot use RTME 2.0 with the 1.8 RTME Connector.

Manual Upgrade to Citrix Receiver for Windows

For deployments with StoreFront:

- Best practice for BYOD (Bring Your Own Device) users is to configure the latest versions of NetScaler Gateway and StoreFront as described in the documentation for those products on the [Product Documentation site](#). Attach the provisioning file created by StoreFront to an email and inform users how to upgrade and to open the provisioning file after installing Citrix Receiver for Windows.
- As an alternative to providing a provisioning file, inform users to enter the NetScaler Gateway URL. Or, if you configured email-based account discovery as described in the StoreFront documentation, inform users to enter their email address.
- Another method is to configure a Citrix Receiver for Web site as described in the StoreFront documentation and complete the configuration described in [Deploy Citrix Receiver for Windows from Citrix Receiver for Web](#). Inform users how to upgrade Citrix Receiver for Windows, access the Citrix Receiver for Web site, and download the provisioning file from Citrix Receiver for Web (click the user name and click Activate).

For deployments with Web Interface

- Upgrade your Web Interface site with Citrix Receiver for Windows and complete the configuration described in [Deploy Citrix Receiver for Windows from a Web Interface logon screen](#). Let your users know how to upgrade Citrix Receiver for Windows. You can, for example, create a download site where users can obtain the renamed Citrix Receiver installer.

Considerations when upgrading

Citrix Receiver for Windows 4.x can be used to upgrade Citrix Receiver for Windows 3.x as well as Citrix online plug-in 12.x.

If Citrix Receiver for Windows 3.x was installed per machine, a per-user upgrade (by a user without administrative privileges) is not supported.

If Citrix Receiver for Windows 3.x was installed per user, a per-machine upgrade is not supported.

Install and Uninstall Citrix Receiver for Windows manually

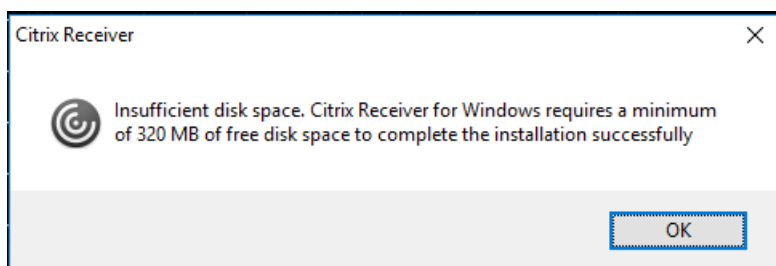
Mar 07, 2017

You can install Citrix Receiver for Windows from the installation media, a network share, Windows Explorer, or a command line by manually running the CitrixReceiver.exe installer package. For command line installation parameters and space requirements, see [Configure and install Receiver for Windows using command-line parameters](#).

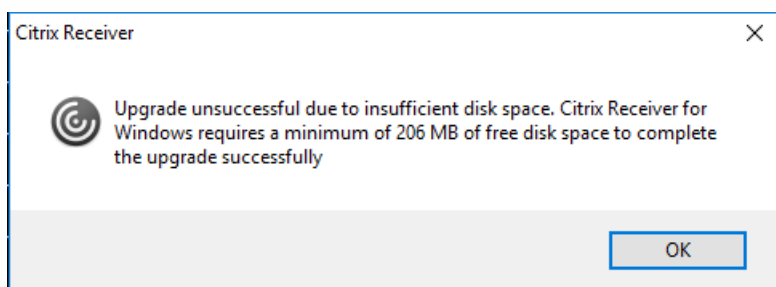
Validating free disk space

Citrix Receiver for Windows performs a check to verify whether there is enough available disk space to complete the installation. The verification is performed both during a fresh installation and an upgrade.

During a fresh installation, the installation ends when there is insufficient disk space and the following dialog appears.



When you are upgrading Citrix Receiver for Windows, the installation ends when there is insufficient disk space and the following dialog appears.



The following table provides details on the minimum required disk space to install Citrix Receiver for Windows.

Installation type	Required disk space
Fresh installation	320 MB
Upgrade of Citrix Receiver	206 MB

Note

- The installer performs the check on the disk space only after extracting the installation package.
- When the system is low on disk space during silent installation, the dialog does not appear but the error message is recorded in the **CTXInstall_TrolleyExpress-*.log**.

Uninstalling Citrix Receiver for Windows

You can uninstall Citrix Receiver for Windows with the Windows Programs and Features utility (Add/Remove Programs).

To uninstall Citrix Receiver for Windows

You can also uninstall Citrix Receiver for Windows from a command line by typing the following command:

```
CitrixReceiver.exe /uninstall
```

After uninstalling Citrix Receiver for Windows, the custom Citrix Receiver for Windows registry keys created by receiver.adm/receiver.adml or receiver.admx remain in the Software\Policies\Citrix\ICA Client directory under HKEY_LOCAL_MACHINE and HKEY_LOCAL_USER.

If you reinstall Citrix Receiver for Window, these policies might be enforced, possibly causing unexpected behavior. To remove the customizations, delete them manually.

Configure and install using command-line parameters

Mar 07, 2017

Customize Citrix Receiver for Windows installer by specifying command line options. The installer package self-extracts to the user's temp directory before launching the setup program and requires approximately 57.8 MB of free space in the %temp% directory. The space requirement includes program files, user data, and temp directories after launching several applications.

To install Citrix Receiver for Windows from a command prompt, use the syntax:

CitrixReceiver.exe [Options]

Enable bidirectional content redirection

Note

By default, Citrix Receiver for Windows does not install the bidirectional content redirection components if they're already installed on the server. If you are using XenDesktop as a client machine, you must install Citrix Receiver for Windows by using the /FORCE_LAA switch to install the bidirectional content redirection components. The feature, however, must be configured both on the server and the client.

Option	ALLOW_BIDIRCONTENTREDIRECTION=1
Description	Enables bidirectional content redirection between client to host and host to client.
Sample usage	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

Enable Local App Access

Option	FORCE_LAA=1
Description	By default, Citrix Receiver for Windows does not install the client side Local App Access components if the components are already installed on the server. To force the client side Local App Access components on the Citrix Receiver, use FORCE_LAA command line switch. Requires administrator rights. For more information on Local App Access, see Local App Access in XenApp and XenDesktop documentation.
Sample usage	CitrixReceiver.exe /FORCE_LAA =1

Display usage information

Option	/? or /help
---------------	-------------

Description	This switch displays usage information
Sample usage	CitrixReceiver.exe /? CitrixReceiver.exe /help

Suppress reboot during UI installation

Option	/noreboot
Description	Suppresses reboot during UI installations. This option is not necessary for silent installs. If you suppress reboot prompts, any USB devices which are in a suspended state when Citrix Receiver for Windows installs will not be recognized by Citrix Receiver for Windows until after the user device is restarted.
Sample usage	CitrixReceiver.exe /noreboot

Silent installation

Option	/silent
Description	Disables the error and progress dialogs to run a completely silent installation.
Sample usage	CitrixReceiver.exe /silent

Enable single sign on authentication

Option	/includeSSON
Description	<p>Installs single sign-on (pass-through) authentication. This option is required for smart card single sign on.</p> <p>The related option, ENABLE_SSON, is enabled when /includeSSON is on the command line. If you use ADDLOCAL= to specify features and you want to install single sign on, you must also specify the value SSON.</p> <p>To enable pass-through authentication for a user device, you must install Citrix Receiver for Windows with local administrator rights from a command line that has the option /includeSSON. On the user device, you must also enable these policies located in Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication:</p> <ul style="list-style-type: none"> • Local user name and password • Enable pass-through authentication • Allow pass-through authentication for all ICA (might be needed, depending on the Web Interface configuration and security settings)

	<p>After the changes are completed, restart the user device. For more information, see the article How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication.</p> <p>Note: Smart card, Kerberos and Local user name and password policies are inter-dependent. The order of configuration is important. We recommend to first disable unwanted policies, and then enable the policies you require. Carefully validate the result.</p>
Sample usage	CitrixReceiver.exe /includeSSON

Enable single sign on when /includeSSON is specified

Option	ENABLE_SSON={Yes No}
Description	<p>Enable Single Sign-on when /includeSSON is specified. The default value is Yes. Enables Single Sign-on when /includeSSON is also specified. This property is required for smart card Single Sign-on.</p> <p>Note that users must log off and log back on to their devices after an installation with Single Sign-on authentication enabled. Requires administrator rights.</p>
Sample usage	CitrixReceiver.exe /ENABLE_SSON=Yes

Always-on tracing

Option	/EnableTracing={true false}
Description	<p>This feature is enabled by default. Use this property to explicitly enable or disable the always-on tracing feature. Always-on tracing helps collect critical logs around connection time. These logs can prove useful when troubleshooting intermittent connectivity issues. The Always-on tracing policy overrides this setting.</p>
Sample usage	CitrixReceiver.exe /EnableTracing=true

Using the Citrix Customer Experience Improvement Program (CEIP)

Option	/EnableCEIP={true false}
Description	<p>When you enable participation 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 its products.</p>
Sample usage	CitrixReceiver.exe /EnableCEIP=true

Specify the installation directory

Option	INSTALLDIR=<Installation Directory>
Description	<p>Specifies the installation path, where Installation Directory is the location where most of the Citrix Receiver software will be installed. The default value is C:\Program Files\Citrix\Receiver. The following Receiver components are installed in the C:\Program Files\Citrix path: Authentication Manager, Citrix Receiver, and the Self-Service plug-in.</p> <p>If you use this option and specify an Installation directory, you must install RIInstaller.msi in the installation directory\Receiver directory and the other .msi files in the installation directory.</p>
Sample usage	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

Identify a user device to a server farm

Option	CLIENT_NAME=<ClientName>
Description	Specifies the client name, where ClientName is the name used to identify the user device to the server farm. The default value is %COMPUTERNAME%
Sample usage	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

Dynamic client name

Option	ENABLE_CLIENT_NAME=Yes No
Description	The dynamic client name feature allows the client name to be the same as the computer name. When users change their computer name, the client name changes to match. Defaults to Yes. To disable dynamic client name support, set this property to No and specify a value for the CLIENT_NAME property.
Sample usage	CitrixReceiver.exe DYNAMIC_NAME=Yes

Install specified components

Option	ADDLOCAL=<feature...,>
	<p>Installs one or more of the specified components. When specifying multiple parameters, separate each parameter with a comma and without spaces. The names are case sensitive. If you do not specify this parameter, all components are installed by default.</p> <p>Citrix recommends that you use the ADDLOCAL Sample Usage given below. If the Sample Usage is not</p>

Description	<p>used as described, it might possibly cause unexpected behavior.</p> <p>Components include:</p> <ul style="list-style-type: none"> • ReceiverInside – Installs the Citrix Receiver experience (required component for Receiver operation). • ICA_Client – Installs the standard Citrix Receiver (required component for Receiver operation). • WebHelper – Installs the WebHelper component. This component retrieves the ICA file from Storefront and passes it to the HDX Engine. In addition, it verifies environment parameters and shares them with Storefront (similar to ICA client detection). • [Optional] SSON – Installs single sign on. Requires administrator rights. • AM – Installs the Authentication Manager. • SELFSERVICE – Installs the Self-Service Plug-in. The AM value must be specified on the command line and .NET 3.5 Service Pack 1 must be installed on the user device. The Self-Service Plug-in is not available for Windows Thin PC devices, which do not support .NET 3.5. • For information on scripting the Self-Service Plug-in (SSP), and a list of parameters available in Receiver for Windows 4.2 and later, see Knowledge Center article CTX200337 • The Self-Service Plug-in allows users to access virtual desktops and applications from the Receiver window or from a command line, as described later in this section. To launch a virtual desktop or application from a command line. • USB – Installs USB support. Requires administrator rights. • DesktopViewer – Installs the Desktop Viewer. • Flash – Installs HDX media stream for Flash. • Vd3d – Enables the Windows Aero experience (for operating systems that support it).
Sample usage	<p>CitrixReceiver.exe</p> <p>ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d,usb,WebHelper</p>

Configure Citrix Receiver for Windows to manually add Stores

Option	ALLOWADDSTORE={N S A}
Description	<p>Specifies whether users can add and remove stores not configured through Merchandising Server deliveries; users can enable or disable stores configured through Merchandising Server deliveries, but they cannot remove these stores or change the names or the URLs.) Defaults to S. Options include:</p> <ul style="list-style-type: none"> • N – Never allow users to add or remove their own store. • S – Allow users to add or remove secure stores only (configured with HTTPS). • A – Allow users to add or remove both secure stores (HTTPS) and non-secure stores (HTTP). Not applicable if Citrix Receiver is installed per user. <p>You can also control this feature by updating the registry key HKLM\Software\Wow6432Node\Citrix\Dazzle\AllowAddStore.</p> <p>Note: Only secure (HTTPS) stores are allowed by default and are recommended for production environments. For test environments, you can use HTTP store connections through the following configuration:</p> <ol style="list-style-type: none"> 1. Set HKLM\Software\Wow6432Node\Citrix\Dazzle\AllowAddStore to A to allow users to add non-

	<p>secure stores.</p> <ol style="list-style-type: none"> Set HKLM\Software\[Wow6432Node]\Citrix\Dazzle\AllowSavePwd to A to allow users to save their passwords for non-secure stores. To enable the addition of a store that is configured in StoreFront with a TransportType of HTTP, add to HKLM\Software\[Wow6432Node]\Citrix\AuthManager the value ConnectionSecurityMode (REG_SZ type) and set it to Any. Exit and restart Citrix Receiver.
Sample usage	CitrixReceiver.exe ALLOWADDSTORE=N

Save credentials for stores locally using PNAgent protocol

Option	ALLOWSAVEPWD={N S A}
Description	<p>Specifies whether users can add and remove stores not configured through Merchandising Server deliveries; users can enable or disable stores configured through Merchandising Server deliveries, but they cannot remove these stores or change the names or the URLs.) Defaults to S. Options include:</p> <ul style="list-style-type: none"> N – Never allow users to save their passwords. S – Allow users to save passwords for secure stores only (configured with HTTPS). A – Allow users to save passwords for both secure stores (HTTPS) and non-secure stores (HTTPS) and non-secure stores (HTTP). <p>You can also control this feature by updating the registry key HKLM\Software\[Wow6432Node]\Citrix\Dazzle\AllowSavePwd.</p> <p>Note: The following registry key must be added manually if AllowSavePwd does not work:</p> <ul style="list-style-type: none"> Key for 32bit OS client: HKLM\Software\Citrix\AuthManager Key for 64bit OS client: HKLM\Software\wow6432node\Citrix\AuthManager Type: REG_SZ Value: never - never allow users to save their passwords. secureonly - allow users to save passwords for secure stores only (configured with HTTPS). always - allow users to save passwords for both secure stores (HTTPS) and non-secure stores (HTTP).
Sample usage	CitrixReceiver.exe ALLOWSAVEPWD=N

Select certificate

Option	AM_CERTIFICATESELECTIONMODE={Prompt SmartCardDefault LatestExpiry}
	<p>Use this option to select a certificate. The default value is Prompt, which prompts the user to choose a certificate from a list. Change this property to choose the default certificate (per the smart card provider) or the certificate with the latest expiry date. If there are no valid logon certificates, the user is</p>

Description	<p>notified, and given the option to use an alternate logon method if available.</p> <p>You can also control this feature by updating the registry key HKCU or HKLM\Software\Wow6432Node\Citrix\AuthManager\CertificateSelectionMode={ Prompt SmartCardDefault LatestExpiry }. Values defined in HKCU take precedence over values in HKLM to best assist the user in selecting a certificate.</p>
Sample usage	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

Use CSP components to manage Smart Card PIN entry

Option	AM_SMARTCARDPINENTRY=CSP
Description	Use CSP components to manage Smart Card PIN entry. By default, the PIN prompts presented to users are provided by Citrix Receiver rather than the smart card Cryptographic Service Provider (CSP). Receiver prompts users to enter a PIN when required and then passes the PIN to the smart card CSP. Specify this property to use the CSP components to manage the PIN entry, including the prompt for a PIN.
Sample usage	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Using Kerberos

Option	ENABLE_KERBEROS={Yes No}
Description	The default value is No. Specifies whether the HDX engine should use Kerberos authentication and applies only when single sign-on (pass-through) authentication is enabled. For more information, see Configure domain pass-through authentication with Kerberos .
Sample usage	CitrixReceiver.exe ENABLE_KERBEROS=No

Displaying legacy FTA icons

Option	LEGACYFTAICONS={False True}
Description	Use this option to display Legacy FTA icons. The default value is False. Specifies whether or not application icons are displayed for documents that have file type associations with subscribed applications. When the argument is set to false, Windows generates icons for documents that do not have a specific icon assigned to them. The icons generated by Windows consist of a generic document icon overlaid with a smaller version of the application icon. Citrix recommends enabling this option if you plan to deliver Microsoft Office applications to users running Windows 7.

Sample usage	CitrixReceiver.exe LEGACYFTAICONS=False
---------------------	---

Enabling pre-launch

Option	ENABLEPRELAUNCH={False True}
Description	The default value is False. For information about session pre-launch, see Reduce application launch time .
Sample usage	CitrixReceiver.exe ENABLEPRELAUNCH=False

Specifying the directory for Start Menu shortcuts

Option	STARTMENUDIR={Directory Name}
Description	<p>By default, applications appear under Start > All Programs. You can specify the relative path under the programs folder to contain the shortcuts to subscribed applications. For example, to place shortcuts under Start > All Programs > Receiver, specify STARTMENUDIR=\Receiver\. Users can change the folder name or move the folder at any time.</p> <p>You can also control this feature through a registry key: Create the entry REG_SZ for StartMenuDir and give it the value "\RelativePath". Location:</p> <p>HKLM\Software\[Wow6432Node\]Citrix\Dazzle</p> <p>HKCU\Software\Citrix\Dazzle</p> <p>For applications published through XenApp with a Client applications folder (also referred to as a Program Neighborhood folder) specified, you can specify that the client applications folder is to be appended to the shortcuts path as follows: Create the entry REG_SZ for UseCategoryAsStartMenuPath and give it the value "true". Use the same registry locations as noted above.</p> <p>Note: Windows 8/8.1 does not allow the creation of nested folders within the Start Menu. Applications will be displayed individually or under the root folder but not within Category sub folders defined with XenApp.</p> <p>Examples</p> <ul style="list-style-type: none"> • If client application folder is \office, UseCategoryAsStartMenuPath is true, and no StartMenuDir is specified, shortcuts are placed under Start > All Programs > Office. • If Client applications folder is \Office, UseCategoryAsStartMenuPath is true, and StartMenuDir is \Receiver, shortcuts are placed under Start > All Programs > Receiver > Office. <p>Changes made to these settings have no impact on shortcuts that are already created. To move shortcuts, you must uninstall and re-install the applications.</p>

Sample usage	CitrixReceiver.exe STARTMENUDIR=\Office
---------------------	---

Specifying the Store Name

Option	STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On Off]; [storedescription]" [STOREy="..."]
Description	<p>Use this option to specify the Store name. Specifies up to 10 stores to use with Citrix Receiver. Values:</p> <ul style="list-style-type: none"> • x and y – Integers 0 through 9. • storename – Defaults to store. This must match the name configured on the StoreFront Server. • servername.domain – The fully qualified domain name of the server hosting the store. • IISLocation – the path to the store within IIS. The store URL must match the URL in StoreFront provisioning files. The store URLs are of the form "/Citrix/store/discovery". To obtain the URL, export a provisioning file from StoreFront, open it in notepad and copy the URL from the <Address> element. • On Off – The optional Off configuration setting enables you to deliver disabled stores, giving users the choice of whether or not they access them. When the store status is not specified, the default setting is On. • storedescription – An optional description of the store, such as HR App Store. <p>Note: In this release, it is important to include "/discovery" in the store URL for successful pass-through authentication.</p>
Sample usage	CitrixReceiver.exe STORE0="Store;https://test.xx.com/Citrix/Store/Discovery"

Enabling URL Redirection on user devices

Option	ALLOW_CLIENTHOSTEDAPPSURL=1
Description	Enables the URL redirection feature on user devices. Requires administrator rights. Requires that Citrix Receiver is installed for All Users. For information about URL redirection, see Local App Access and its sub-topics in the XenDesktop 7 documentation.
Sample usage	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

Enabling self-service mode

Option	SELFSEVICEMODE={False True}
Description	The default value is True. When the administrator sets the SelfServiceMode flag to false, the user no longer has access to the self-service Citrix Receiver user interface. Instead, they can access subscribed apps from the Start menu and via desktop shortcuts - known as "shortcut-only mode".

Sample usage	CitrixReceiver.exe SELFSERVICEMODE=False

Specifying the directory for Desktop Shortcuts

Option	DESKTOPDIR=<Directory Name>
Description	Brings all shortcuts into a single folder. CategoryPath is supported for desktop shortcuts. Note: When using the DESKTOPDIR option, set the PutShortcutsOnDesktop key to True.
Sample usage	CitrixReceiver.exe DESKTOPDIR=\Office

Upgrading from an unsupported Citrix Receiver version

Option	/rcu
Description	Allows you to upgrade from an unsupported version to the latest version of Citrix Receiver.
Sample usage	CitrixReceiver.exe /rcu

Troubleshooting the installation

If there is a problem with the installation, search in the user's %TEMP%/CTXReceiverInstallLogs directory for the logs with the prefix CtxInstall- or TrolleyExpress- . For example:

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

Examples of a command line installation

To install all components silently and specify two application stores:

```
CitrixReceiver.exe /silent STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App Store" STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Backup HR App Store"
```

To specify single sign-on (pass-through authentication) and add a store that points to a [XenApp Services URL](#):

```
CitrixReceiver.exe /INCLUDESSON  
/STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"
```

To launch a virtual desktop or application from a command line

Citrix Receiver for Windows creates a stub application for each subscribed desktop or application. You can use a stub application to launch a virtual desktop or application from the command line. Stub applications are located in %appdata%\Citrix\SelfService. The file name for a stub application is the Display Name of the application, with the spaces removed. For example, the stub application file name for Internet Explorer is InternetExplorer.exe.

Deploy using Active Directory and sample startup scripts

Mar 07, 2017

You can use Active Directory Group Policy scripts to pre-deploy Citrix Receiver for Windows on systems based on your Active Directory organizational structure. Citrix recommends using the scripts rather than extracting the .msi files because the scripts allow for a single point for installation, upgrade, and uninstall; they consolidate the Citrix entries in Programs and Features, and make it easier to detect the version of Citrix Receiver that is deployed. Use the Scripts setting in the Group Policy Management Console (GPMC) under Computer Configuration or User Configuration. For general information about startup scripts, see Microsoft documentation.

Citrix includes sample per-computer startup scripts to install and uninstall CitrixReceiver.exe. The scripts are located on the Citrix Receiver for Windows [Download](#) page.

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

When the scripts are executed during Startup or Shutdown of an Active Directory Group Policy, custom configuration files might be created in the Default User profile of a system. If not removed, these configuration files can prevent some users from accessing the Receiver logs directory. The Citrix sample scripts include functionality to properly remove these configuration files.

To use the startup scripts to deploy Receiver with Active Directory

1. Create the Organizational Unit (OU) for each script.
2. Create a Group Policy Object (GPO) for the newly created OU.

Modify sample scripts

Modify the scripts by editing these parameters in the header section of each file:

- **Current Version of package.** The specified version number is validated and if it is not present, the deployment proceeds. For example, set `DesiredVersion= 3.3.0.XXXX` to exactly match the version specified. If you specify a partial version, for example 3.3.0, it matches any version with that prefix (3.3.0.1111, 3.3.0.7777, and so forth).
- **Package Location/Deployment directory.** This specifies the network share containing the packages and is not authenticated by the script. The shared folder must have Read permission for EVERYONE.
- **Script Logging Directory.** This specifies the network share where the install logs are copied and is not authenticated by the script. The shared folder must have Read and Write permissions for EVERYONE.
- **Package Installer Command Line Options.** These command line options are passed to the installer. For the command line syntax, see [Configure and install Receiver for Windows using command-line parameters](#).

To add the per-computer startup scripts

1. Open the Group Policy Management Console.
2. Select Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown).
3. In the right-hand pane of the Group Policy Management Console, select Startup.
4. In the Properties menu, click Show Files, copy the appropriate script to the folder displayed, and then close the window.
5. In the Properties menu, click Add and use Browse to find and add the newly created script.

To deploy Citrix Receiver for Windows per-computer

1. Move the user devices designated to receive this deployment to the OU you created.
2. Reboot the user device and log on as any user.
3. Verify that Program and Features (Add or Remove Programs in previous OS versions) contains the newly installed package.

To remove Citrix Receiver for Windows per-computer

1. Move the user devices designated for the removal to the OU you created.
2. Reboot the user device and log on as any user.
3. Verify that Program and Features (Add or Remove Programs in previous OS versions) removed the previously installed package.

Use the per-user sample startup scripts

Citrix recommends using per-computer startup scripts. However, for situations where you require Citrix Receiver for Windows per-user deployments, two Citrix Receiver for Windows per-user scripts are included on the XenDesktop and XenApp media in the Citrix Receiver for Windows and Plug-ins\Windows\Receiver\Startup_Logon_Scripts folder.

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

To set up the per-user startup scripts

1. Open the Group Policy Management Console.
2. Select User Configuration > Policies > Windows Settings > Scripts.
3. In the right-hand pane of the Group Policy Management Console, select Logon
4. In the Logon Properties menu, click Show Files, copy the appropriate script to the folder displayed, and then close the window.
5. In the Logon Properties menu, click Add and use Browse to find and add the newly created script.

To deploy Citrix Receiver for Windows per-user

1. Move the users designated to receive this deployment to the OU you created.
2. Reboot the user device and log on as the specified user.
3. Verify that Program and Features (Add or Remove Programs in previous OS versions) contains the newly installed package.

To remove Citrix Receiver for Windows per-user

1. Move the users designated for the removal to the OU you created.
2. Reboot the user device and log on as the specified user.
3. Verify that Program and Features (Add or Remove Programs in previous OS versions) removed the previously installed package.

Deploy Citrix Receiver for Windows from Receiver for Web

Mar 07, 2017

You can deploy Citrix Receiver for Windows from Citrix Receiver for Web to ensure that you have installed the Receiver before connecting to an application from a browser. Citrix Receiver for Web site enable you to access StoreFront stores through a web page. If the Citrix Receiver for Web site detects that a user does not have a compatible version of Citrix Receiver for Windows, you are prompted to download and install Citrix Receiver for Windows.

For more information, see [Citrix Receiver for Web sites](#) in the StoreFront documentation.

Email-based account discovery is not supported when Citrix Receiver for Windows is deployed from Citrix Receiver for Web. If email-based account discovery is configured and a first-time user installs Citrix Receiver for Windows from Citrix.com, Citrix Receiver for Windows prompts the user for an email or server address. Entering an email address results in the error message "Your email cannot be used to add an account."

Use the following configuration to prompt for the server address only.

1. Download CitrixReceiver.exe to your local computer.
2. Rename CitrixReceiver.exe to CitrixReceiverWeb.exe.
3. Deploy the renamed executable using your regular deployment method. If you use StoreFront, refer to [Configure Receiver for Web sites using the configuration files](#) in the StoreFront documentation.

Deploy Citrix Receiver for Windows from a Web Interface logon screen

Mar 07, 2017

This feature is available only for XenDesktop and XenApp releases that support Web Interface.

You can deploy Citrix Receiver for Windows from a web page to ensure that users have it installed before they try to use the Web Interface. The Web Interface provides a client detection and deployment process that detects which Citrix clients can be deployed within the user's environment and then guides them through the deployment procedure.

You can configure the client detection and deployment process to run automatically when users access a XenApp website. If the Web Interface detects that a user does not have compatible version of Citrix Receiver for Windows, the user is prompted to download and install Citrix Receiver for Windows.

For more information, see [Configuring Client Deployment](#) in the Web Interface documentation.

Email-based account discovery does not apply when Citrix Receiver for Windows is deployed from Web Interface. If email-based account discovery is configured and a first-time user installs Citrix Receiver for Windows from Citrix.com, Citrix Receiver for Windows prompts the user for an email or server address. Entering an email address results in the error message "Your email cannot be used to add an account." Use the following configuration to prompt for the server address only.

1. Download CitrixReceiver.exe to your local computer.
2. Rename CitrixReceiver.exe to CitrixReceiverWeb.exe.
3. Specify the changed filename in the ClientIcaWin32 parameter in the configuration files for your XenApp websites.
To use the client detection and deployment process, the Citrix Receiver for Windows installation files must be available on the Web Interface server. By default, the Web Interface assumes that the file names of the Citrix Receiver for Windows installation files are the same as the files supplied on the XenApp or XenDesktop installation media.
4. Add the sites from which the CitrixReceiverWeb.exe file is downloaded to the Trusted Sites zone.
5. Deploy the renamed executable using your regular deployment method.

Deploy using System Center Configuration Manager 2012 R2

Apr 04, 2017

You can use Microsoft System Center Configuration Manager (SCCM) to deploy Citrix Receiver for Windows.

Note: Only Citrix Receiver for Windows Version 4.5 and later supports SCCM deployment.

There are four parts to completing the deployment of Citrix Receiver for Windows using SCCM:

1. [Adding Citrix Receiver for Windows to the SCCM deployment](#)
2. [Adding distribution points](#)
3. [Deploying the Receiver software to the software center](#)
4. [Creating Device Collections](#)

Adding Citrix Receiver for Windows to the SCCM deployment

1. Copy the downloaded Citrix Receiver to a folder on the Configuration Manager server and launch the Configuration Manager console.
2. Select **Software Library > Application Management**. Right-click **Application** and click **Create Application**. The Create Application wizard appears.

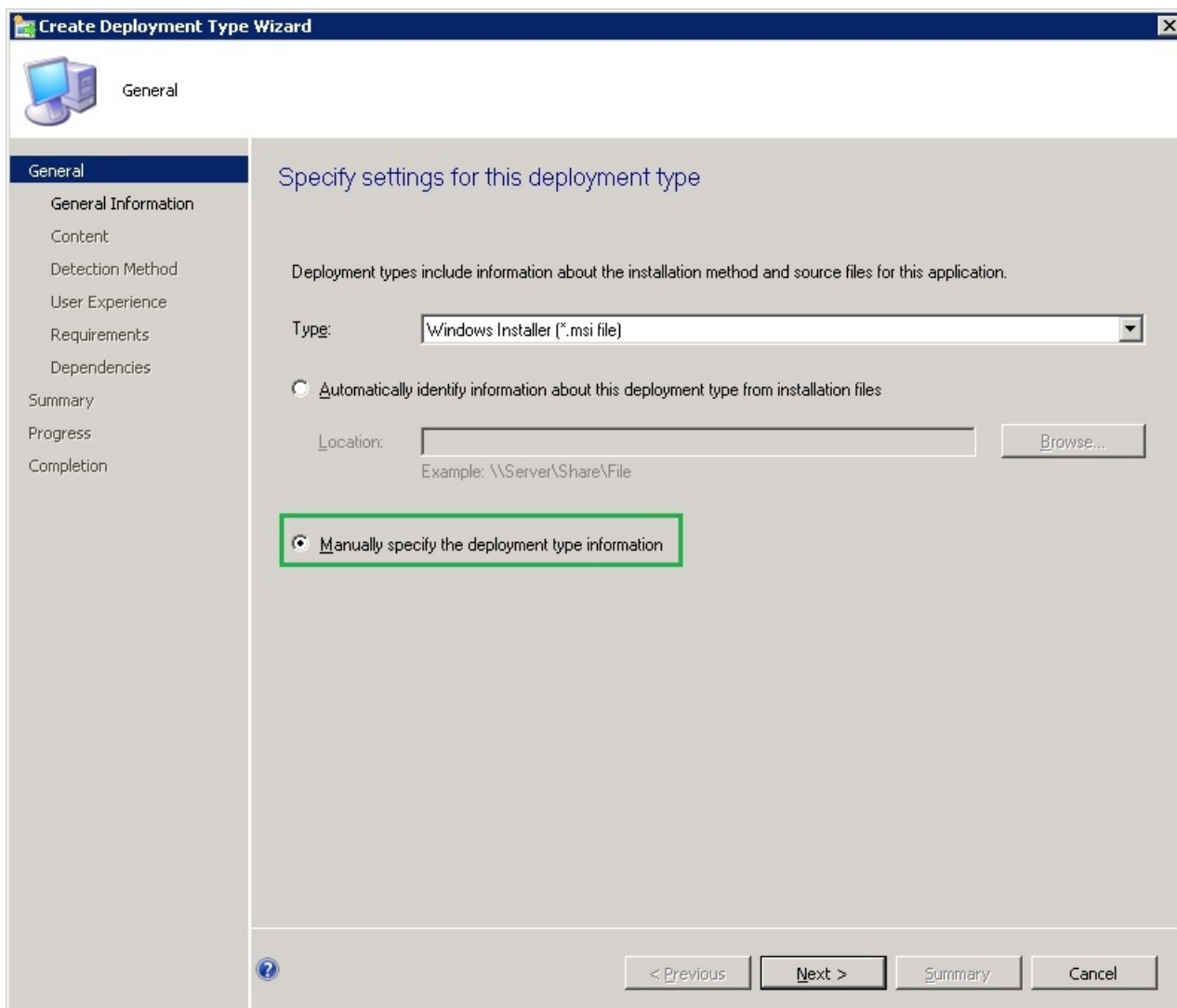
3. In the **General** pane, select **Manually specify the application information** and click **Next**.

4. In the **General Information** pane, specify information about the application such as Name, Manufacturer, Software version, and so on.

5. In the Application Catalog wizard, specify additional information such as Language, Application name, User category and so on and click **Next**.


Note: Users can see the information you specify here.

6. In the **Deployment Type** pane, click **Add** to configure the deployment type for Citrix Receiver setup. The Create Deployment Type wizard appears.



- In the **General** pane: Set the deployment type to Windows Installer (*.msi file), select **Manually specify the deployment type information** and click **Next**.
- In the **General Information** pane: Specify deployment type details (For example: Receiver Deployment) and click **Next**.
- In the **Content** pane:
 1. Provide the path where the Citrix Receiver setup file is present. For example: Tools on SCCM server.
 2. Specify **Installation program** as one of the following:
 - CitrixReceiver.exe /silent for default silent installation.
 - CitrixReceiver.exe /silent /includeSSON to enable domain pass-through.
 - CitrixReceiver.exe /silent SELFSERVICEMODE=false to install receiver in Non-Self Service Mode.
 3. Specify **Uninstall program** as CitrixReceiver.exe /uninstall (to enable uninstallation through SCCM).

Create Deployment Type Wizard

 Content

General

General Information

Content

Detection Method

User Experience

Requirements

Dependencies

Summary

Progress

Completion

Specify information about the content to be delivered to target devices

Specify the location of the deployment type's content and other settings that control how content is delivered to target devices. All the contents in the path specified will be delivered.

Content location:

☐ Persist content in the client cache

☒ Allow clients to share content with other clients on the same subnet

This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache.

Specify the command used to install this content.

Installation program:


Installation start in:

Configuration Manager can remove installations of this content if an uninstall program is specified below.

Uninstall program:

Uninstall start in:

☐ Run installation and uninstall program as 32-bit process on 64-bit clients.



- In the **Detection Method** pane: Select **Configure rules to detect the presence of this deployment type** and click **Add Clause**.

The Detection Rule dialog appears.

Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: File System

Specify the file or folder to detect this application.

Type: File

Path: %ProgramFiles(x86)%\Citrix\ICA Client\Receiver Browse...

File or folder name: Receiver.exe

☒ This file or folder is associated with a 32-bit application on 64-bit systems.

☐ The file system setting must exist on the target system to indicate presence of this application

☒ The file system setting must satisfy the following rule to indicate the presence of this application

Property: Version

Operator: Greater than or equal to

Value: 4.3.0.65534

OK Cancel

- Set **Setting Type** to File System.
- Under **Specify the file or folder to detect the application**, set the following:
 - **Type** – From the drop-down menu, select File.
 - **Path** – %ProgramFiles (x86)%\Citrix\ICA Client\Receiver
 - **File or folder name** – Receiver.exe
- **Property** – From the drop-down menu, select **Version**
- **Operator** – From the drop-down menu, select **Greater than or equal to**
- **Value** – Type **4.3.0.65534**

Note: This rule combination applies to Citrix Receiver for Windows upgrades as well.

- In the **User Experience** pane, set:

- **Installation behavior** - Install for system
 - **Logon requirement** - Whether or not a user is logged on
 - **Installation program visibility** - Normal.
- Click Next.

Note: Do not specify any requirements and dependencies for this deployment type.

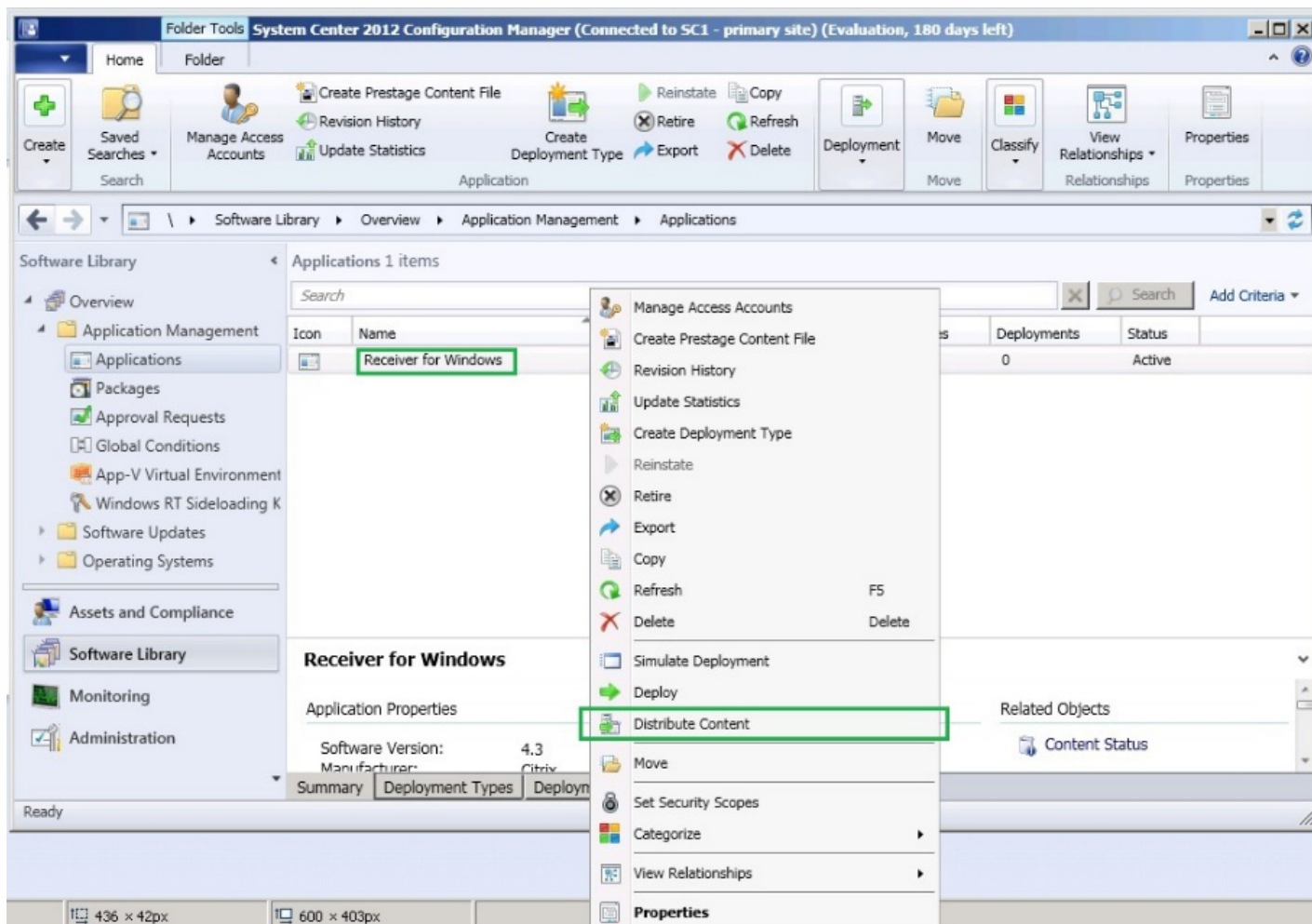
7. In the **Summary pane**, verify the settings for this deployment type. Click **Next**.

A success message appears.

8. In the **Completion** pane, a new deployment type (Receiver Deployment) is listed under the Deployment types. Click **Next** and click **Close**.

Add distribution points

1. Right-click Receiver for Windows in the Configuration Manager console and select **Distribute Content**.
The Distribute Content wizard appears.



2. In the Content Distribution pane, click **Add > Distribution Points**.

The Add Distribution Points dialog appears.

3. Browse to the SCCM server where the content is available and click **OK**.

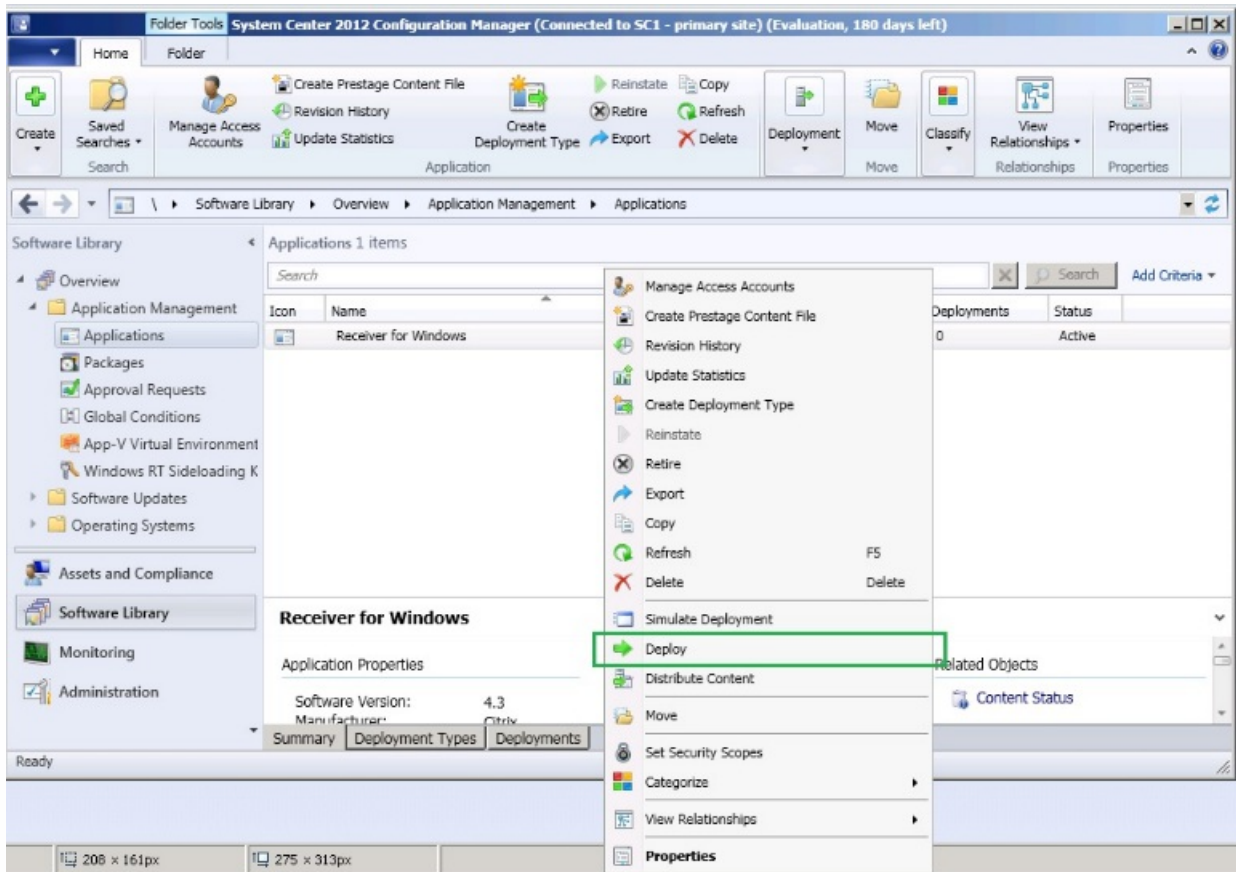
In the Completion pane, a success message appears

4. Click **Close**

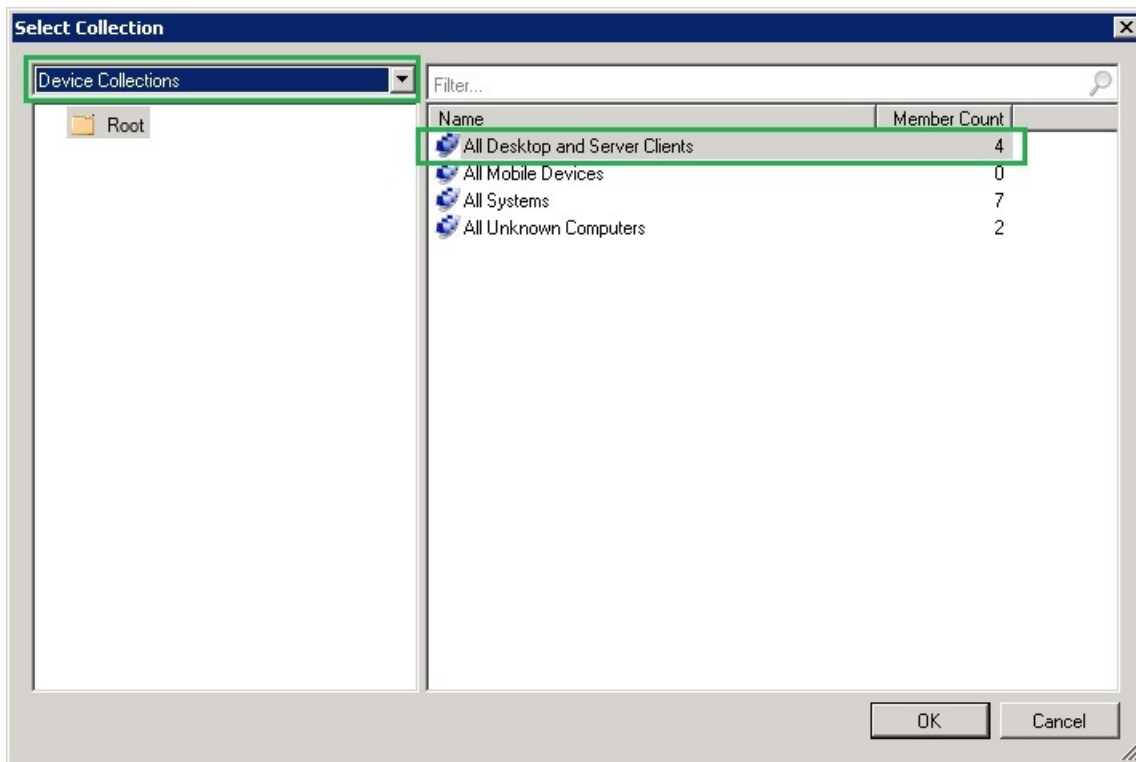
Deploy the Receiver software to the software center

1. Right-click Receiver for Windows in the Configuration Manager console select **Deploy**.

The Deploy Software wizard appears.



2. Select **Browse** against Collection (can be Device Collection or User Collection) where the application is to be deployed and click **Next**.



3. In the **Deployment Settings** pane, set **Action** to Install and **Purpose** to Required (enables unattended installation). Click **Next**.

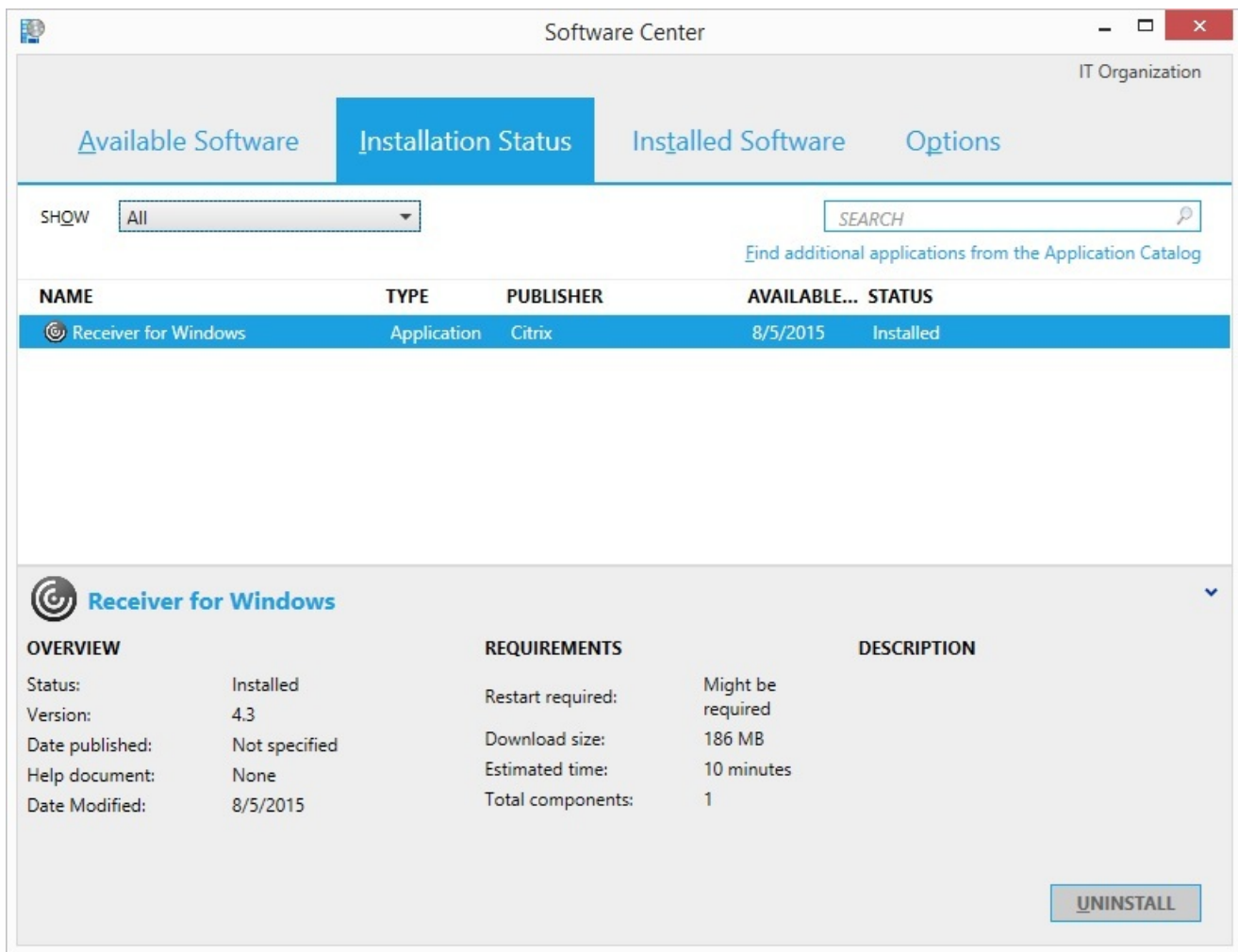
4. In the **Scheduling** pane, specify the schedule to deploy the software on target devices.

5. In the **User Experience** pane, set the **User notifications** behavior; select **Commit changes at deadline or during a maintenance window (requires restart)** and click **Next** to complete the Deploy Software wizard.

In the Completion pane, a success message appears.

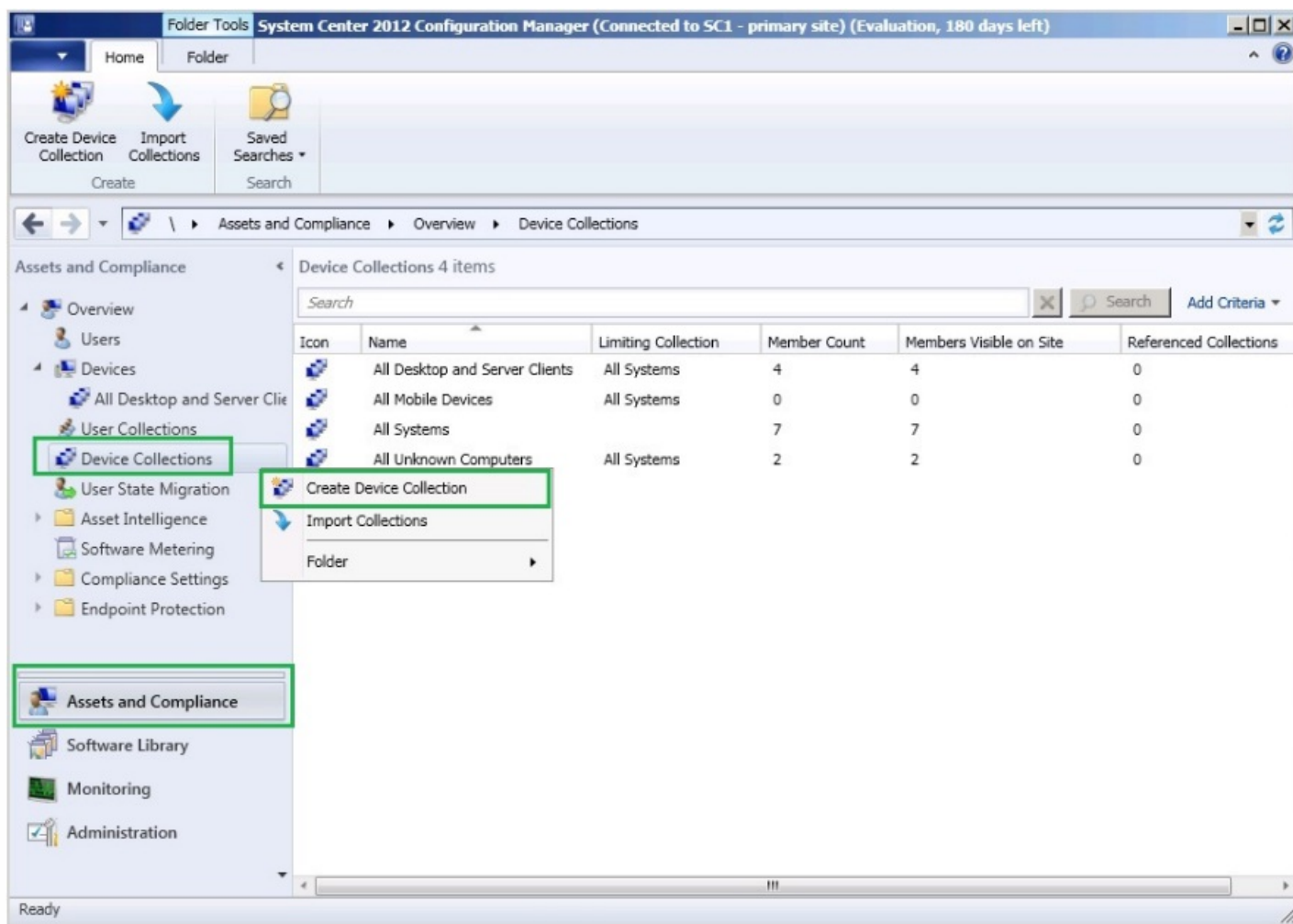
Reboot the target endpoint devices (required only to start installation immediately).

On endpoint devices, Citrix Receiver for Windows is visible in the Software Center under **Available Software**. Installation is triggered automatically based on the schedule you configure. Alternatively, you can also schedule or install on demand. The installation status is displayed in the Software Center after the installation starts.



Creating device collections

1. Launch the Configuration Manager console, click **Assets and Compliance > Overview > Devices**.



2. Right-click **Device Collections** and select **Create Device Collection**.

The Create Device Collection wizard appears.

3. In the General pane, type the **Name** for the device and click **Browse** for Limiting collection. This determines the scope of devices, which can be one the default Device Collections created by SCCM. Click **Next**.

4. In the Membership Rules pane, click **Add Rule** for filtering the devices. The Create Direct Membership Rule wizard appears.

- In the Search for Resources pane, select the **Attribute name** based on the devices you want to filter and provide the Value for Attribute name to select the devices.

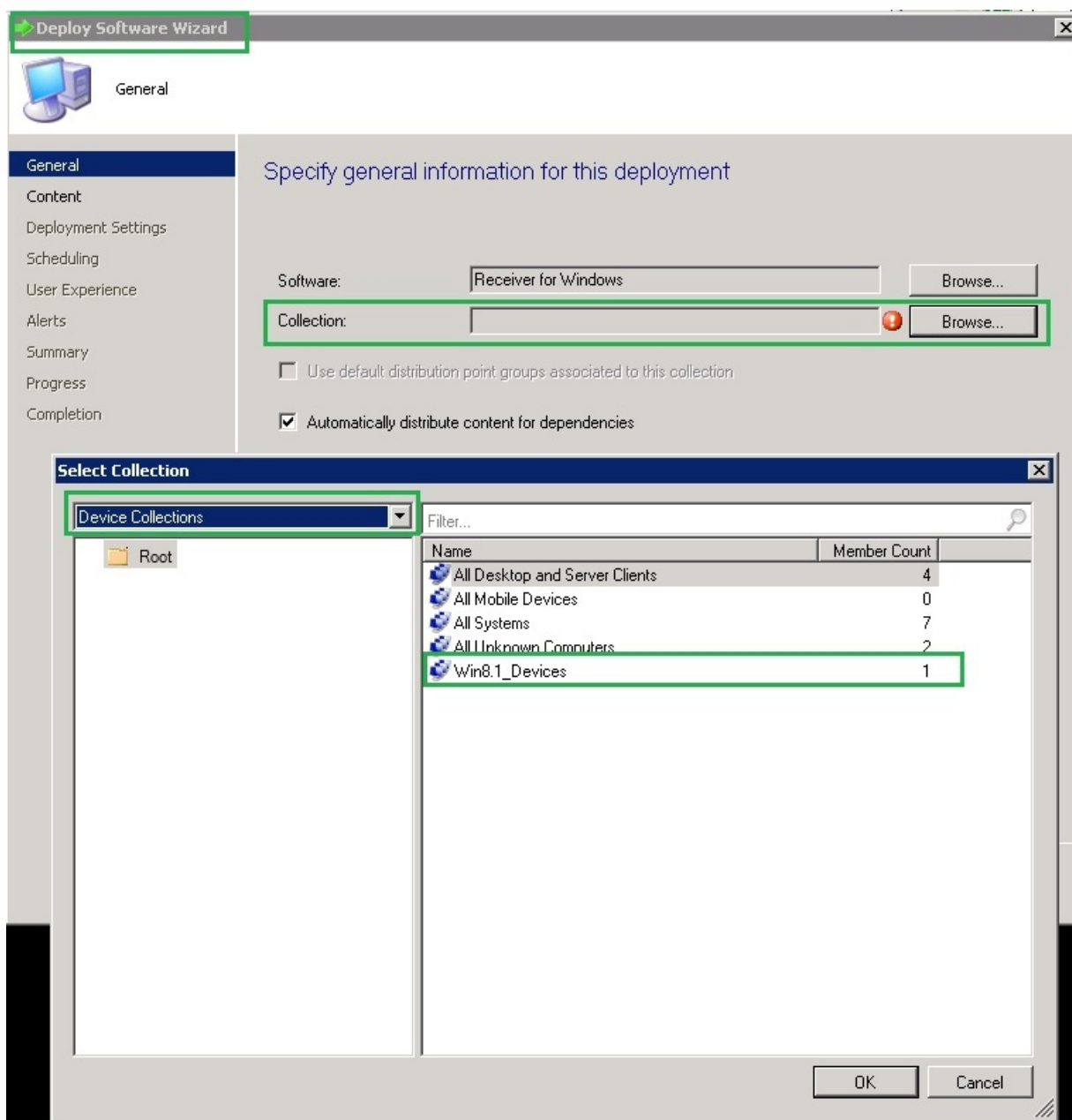
5. Click **Next**. In the Select Resources pane, select the devices that are required to be part of device collection. In the Completion pane a success message appears.

6. Click **Close**.

7. In the Membership rules pane, a new rule is listed under Click Next.

8. In the Completion pane, a success message appears. Click **Close** to complete the Create Device Collection wizard.

The new device collection is listed in **Device Collections**. The new device collection is a part of Device Collections while browsing in Deploy Software wizard.



Note

When you set the **MSIRESTARTMANAGERCONTROL** attribute to **False**, deploying Citrix Receiver for Windows using SCCM might not be successful.

As per our analysis, Citrix Receiver for Windows is NOT the cause of this failure. Also, retrying might yield successful deployment.

Configure Receiver for Windows

Mar 07, 2017

When using Citrix Receiver for Windows software, the following configuration steps allow users to access their hosted applications and desktops:

- [Configure your application delivery](#) and [Configure your XenDesktop environment](#). Ensure your XenApp environment is configured correctly. Understand your options and provide meaningful application descriptions for your users.
- [Configure self-service mode](#) by adding a StoreFront account to Citrix Receiver for Windows. This mode allows your users to subscribe to applications from the Citrix Receiver for Windows user interface.
- [Configure shortcut only mode](#), which includes:
 - [using a Group Policy Object template file to customize shortcuts](#).
 - [using registry keys for shortcut customization](#).
 - [configuring shortcuts based on StoreFront account settings](#)
- [Provide users with account information](#). Provide users with the information they need to set up access to accounts hosting their virtual desktops and applications. In some environments, users must manually set up access to those accounts.

If you have users who connect from outside the internal network (for example, users who connect from the Internet or from remote locations), configure authentication through NetScaler Gateway. For more information, see [NetScaler Gateway](#).

Configure application delivery

Mar 07, 2017

When delivering applications with XenDesktop or XenApp, consider the following options to enhance the user experience:

- Web Access Mode - Without any configuration, Citrix Receiver for Windows provides browser-based access to applications and desktops. You can open a browser to a Receiver for Web or Web Interface site to select and use the applications you want. In this mode, no shortcuts are placed on the user's desktop.
- Self Service Mode - By adding a StoreFront account to Citrix Receiver for Windows or configuring Citrix Receiver for Windows to point to a StoreFront site, you can configure *self-service mode*, which allows you to subscribe to applications from the Citrix Receiver for Windows user interface. This enhanced user experience is similar to that of a mobile app store. In self-service mode you can configure mandatory, auto-provisioned and featured app keyword settings as required.

Note: By default, Citrix Receiver for Windows allows you to select the applications to display in the Start menu.

- App shortcut-only mode - As a Citrix Receiver for Windows administrator, you can configure Citrix Receiver for Windows to automatically place application and desktop shortcuts directly in the Start menu or on the desktop in a similar way that Citrix Receiver for Windows Enterprise places them. The new *shortcut only* mode allows you to find all the published apps within the familiar Windows navigation schema where you would expect to find them.

For information on delivering applications using XenApp and XenDesktop 7, see [Create a Delivery Group application](#).

Note: Include meaningful descriptions for applications in a Delivery Group. Descriptions are visible to Citrix Receiver for Windows users when using Web access or self-service mode.

For more information on how to configure shortcuts in the Start menu or on the desktop, see [Configure Shortcut Only Mode](#).

Configuring NetScaler Gateway Store via Citrix Receiver Group Policy Object administrative template

Citrix recommends using the Group Policy Object administrative template to configure rules for network routing, proxy servers, trusted server configuration, user routing, remote user devices, and user experience.

You can use the receiver.admx / receiver.adml template files with domain policies and local computer policies. For domain policies, import the template file using the Group Policy management console. This is especially useful for applying Citrix Receiver for Windows settings to a number of different user devices throughout the enterprise. To affect a single user device, import the template file using the local Group Policy Editor on the device.

To add or specify a NetScaler Gateway via GPO:

1. As an administrator, open the Citrix Receiver Group Policy Object administrative template by running gpedit.msc.
 - If applying the policy on a single computer, launch it from the Start menu.
 - If applying on domain policies, launch it by using the Group Policy management console
 -
2. Under the Computer Configuration node, go to Administrative Templates > Classic Administrative

Templates (ADM) > Citrix Components > Citrix Receiver > StoreFront, and select NetScaler Gateway URL/StoreFront Accounts List.

3. Edit the settings.

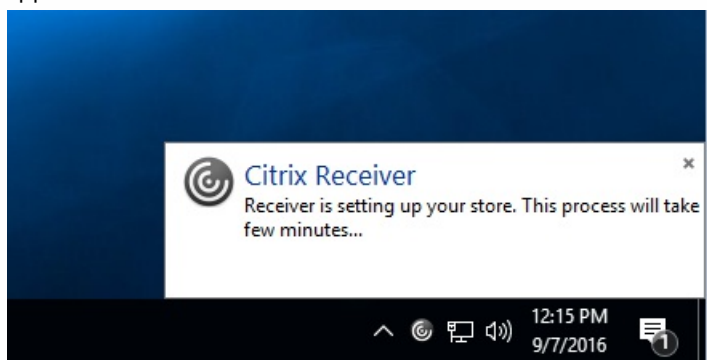
- Store name – Indicates the displayed store name
- Store URL – Indicates the URL of the store
- #Store name – Indicates the name of the store behind NetScaler Gateway
- Store enabled state – Indicates the state of the store, On/Off
- Store description – Provides description of the store

4. Add or specify the NetScaler URL. Enter the name of the URL, delimited by a semi-colon:

Example: *HRStore;https://dtls.blrwinrx.com#Store name;On;Store for HR staff*

Where, #Store name is the name of store behind NetScaler Gateway; dtls.blrwinrx.com is the NetScaler URL

When Citrix Receiver for Windows is launched after adding the Netscaler Gateway using GPO, the following message appears in the notification area.



Limitations

1. NetScaler URL should be listed as first followed by StoreFront URL(s).
2. Multiple NetScaler URLs are not supported.
3. Any change in NetScaler URL requires the Citrix Receiver for Windows to be reset for the changes to take effect.
4. NetScaler Gateway URL configured using this method does not support PNA Services site behind NetScaler Gateway.

Configure self-service mode

By simply adding a StoreFront account to Citrix Receiver or configuring Citrix Receiver to point to a StoreFront site, you can configure *self-service mode*, which allows users to subscribe to applications from the Receiver user interface. This enhanced user experience is similar to that of a mobile app store.

Note: By default, Citrix Receiver for Windows allows users to select the applications they want to display in their Start menu.

In self-service mode, you can configure mandatory, auto-provisioned and featured app keyword settings as needed.

Append keywords to the descriptions you provide for delivery group applications:

- To make an individual app mandatory, so that it cannot be removed from Citrix Receiver for Windows, append the string KEYWORDS:Mandatory to the application description. There is no Remove option for users to unsubscribe to mandatory

apps.

- To automatically subscribe all users of a store to an application, append the string KEYWORDS:Auto to the description. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
- To advertise applications to users or to make commonly used applications easier to find by listing them in the Citrix Receiver Featured list, append the string KEYWORDS:Featured to the application description.

Customize the app shortcut location using the Group Policy Object template

Note

You should make changes to group policy before configuring a store. If at any time you want to customize the group policies, reset Citrix Receiver, configure the group policy, and then reconfigure the store.

As an administrator, you can configure shortcuts using group policy.

1. Open the Local Group Policy Editor by running the command `gpedit.msc` locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add, browse to the Receiver Configuration folder and then select `receiver.admx` (or `receiver.adml`).
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Self Service.
7. Select Manage SelfServiceMode to enable or disable the self-service Receiver user interface.
8. Choose Manage App Shortcut to enable or disable:

- Shortcuts on Desktop
- Shortcuts in Start menu
- Desktop Directory
- Start menu Directory
- Category path for Shortcuts
- Remove apps on logoff
- Remove apps on exit

9. Choose Allow users to Add/Remove account to give users privileges to add or remove more than one account.
- Using StoreFront account settings to customize app shortcut locations

You can set up shortcuts in the Start menu and on the desktop from the StoreFront site. The following settings can be added in the web.config file in `C:\inetpub\wwwroot\Citrix\Roaming` in the **<annotatedServices>** section:

- To put shortcuts on the desktop, use `PutShortcutsOnDesktop`. Settings: "true" or "false" (default is false).
- To put shortcuts in the Start menu, use `PutShortcutsInStartMenu`. Settings: "true" or "false" (default is true).
- To use the category path in the Start menu, use `UseCategoryAsStartMenuPath`. Settings: "true" or "false" (default is true).

NOTE: Windows 8/8.1 does not allow the creation of nested folders within the Start Menu. Applications will be displayed individually or under the root folder but not within Category sub folders defined with XenApp.

- To set a single directory for all shortcuts in the Start menu, use StartMenuDir. Setting: String value, being the name of the folder into which shortcuts are written.
- To reinstall modified apps, use AutoReinstallModifiedApps. Settings: "true" or "false" (default is true).
- To show a single directory for all shortcuts on the desktop, use DesktopDir. Setting: String value, being the name of the folder into which shortcuts are written.
- To not create an entry on the clients 'add/remove programs', use DontCreateAddRemoveEntry. Settings: "true" or "false" (default is false).
- To remove shortcuts and Receiver icon for an application that was previously available from the Store but now is not available, use SilentlyUninstallRemovedResources. Settings: "true" or "false" (default is false).

In the web.config file, the changes should be added in the XML section for the account. Find this section by locating the opening tab:

```
<account id=... name="Store"
```

The section ends with the </account> tag.

Before the end of the account section, in the first properties section:

```
<properties> <clear /> </properties>
```

Properties can be added into this section after the <clear /> tag, one per line, giving the name and value. For example:

```
<property name="PutShortcutsOnDesktop" value="True" />
```

Note: Property elements added before the <clear /> tag may invalidate them. Removing the <clear /> tag when adding a property name and value is optional.

An extended example for this section is:

```
<properties> <property name="PutShortcutsOnDesktop" value="True" /> <property name="DesktopDir" value="Citrix Applications" />
```

Important

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#), so that the other servers in the deployment are updated.

Using per app settings in XenApp and XenDesktop 7.x to customize app shortcut locations

Citrix Receiver can be configured to automatically place application and desktop shortcuts directly in the Start Menu or on the desktop. This functionality was similar to previously released versions of Citrix Receiver, however, release 4.2.100 introduced the ability to control app shortcut placement using XenApp per app settings. This functionality is useful in environments with a handful of applications that need to be displayed in consistent locations.

If you want to set the location of shortcuts so every user finds them in the same place use XenApp per App Settings:

If you want per-app settings to determine where applications are placed independently of whether in self-service mode or Start Menu mode..

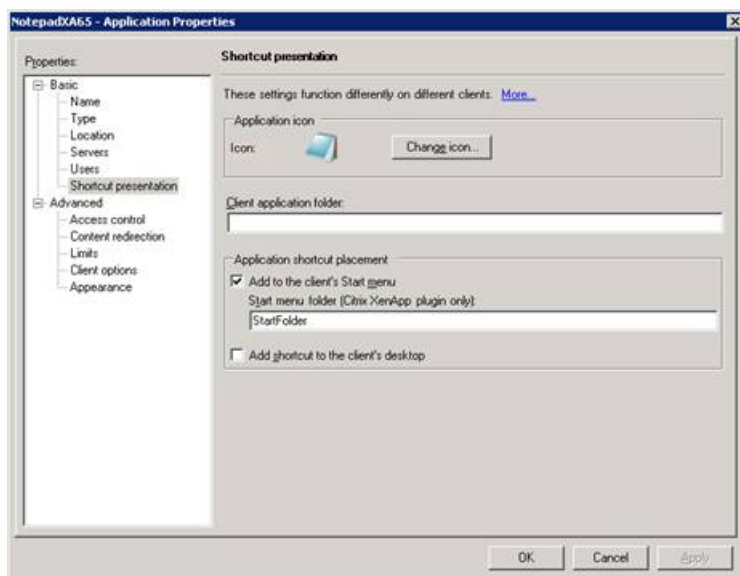
configure Receiver with **PutShortcutsInStartMenu=false** and enable per app settings.
Note: This setting applies to the Web interface site only.

Note: The **PutShortcutsInStartMenu=false** setting applies to both XenApp 6.5 and XenDesktop 7.x.

Configure per app settings in XenApp 6.5

To configure a per app publishing shortcut in XenApp 6.5:

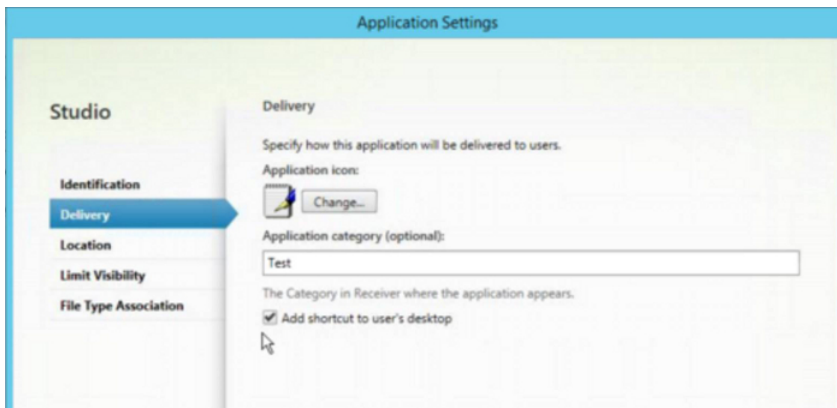
1. In the XenApp Application Properties screen, expand Basic properties.
2. Select the Shortcut presentation option.
3. In the Application shortcut placement portion of the Shortcut presentation screen, select the Add to the client's Start menu check box. After selecting the check box, enter the name of the folder where you want to place the shortcut. If you do not specify a folder name, XenApp places the shortcut in the Start Menu without placing it in a folder.
4. Select the Add shortcut to the client's desktop to include the shortcut on a client machine's desktop.
5. Click Apply.
6. Click OK.



Using per app settings in XenApp 7.6 to customize app shortcut locations

To configure a per app publishing shortcut in XenApp 7.6:

1. In Citrix Studio, locate the Application Settings screen.
2. In the Application Settings screen, select Delivery. Using this screen, you can specify how applications are delivered to users.
3. Select the appropriate icon for the application. Click Change to browse to the location of the desired icon.
4. In the Application category field, optionally specify the category in Receiver where the application appears. For example, if you are adding shortcuts to Microsoft Office applications, enter Microsoft Office.
5. Select the Add shortcut to user's desktop checkbox.
6. Click OK.



Reducing enumeration delays or digitally signing application stubs

If users experience delays in app enumeration at each logon, or if there is a need to digitally sign application stubs, Receiver provides functionality to copy the .EXE stubs from a network share.

This functionality involves a number of steps:

1. Create the application stubs on the client machine.
2. Copy the application stubs to a common location accessible from a network share.
3. If necessary, prepare a white list (or, sign the stubs with an Enterprise certificate).
4. Add a registry key to enable Receiver to create the stubs by copying them from the network share.

If RemoveappsOnLogoff and RemoveAppsonExit are enabled, and users are experiencing delays in app enumeration at every logon, use the following workaround to reduce the delays:

1. Use regedit to add HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true".
2. Use regedit to add HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true". HKCU has preference over HKLM.

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.

Enable a machine to use pre-created stub executables that are stored on a network share:

1. On a client machine, create stub executables for all of the apps. To accomplish this, add all the applications to the machine using Receiver; Receiver generates the executables.
2. Harvest the stub executables from %APPDATA%\Citrix\SelfService. You only need the .exe files.
3. Copy the executables to a network share.
4. For each client machine that will be locked down, set the following registry keys:
 1. Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs"
 2. Reg add HKLM\Software\Citrix\Dazzle /v
 3. CopyStubsFromCommonStubDirectory /t REG_SZ /d "true". It's also possible to configure these settings on HKCU if you prefer. HKCU has preference over HKLM.
 4. Exit and restart Receiver to test the settings.

Example use cases

This topic provides use cases for app shortcuts.

Allowing users to choose what they want in the Start Menu (Self-Service)

If you have dozens (or even hundreds) of apps, it's best to allow users to select which applications they want to favorite and add to the Start Menu:

If you want the user to choose the applications they want in their Start Menu..	configure Citrix Receiver in self-service mode. In this mode you also configure <i>auto-provisioned</i> and <i>mandatory</i> app keyword settings as needed.
If you want the user to choose the applications they want in their Start Menu but also want specific app shortcuts on the desktop..	configure Citrix Receiver without any options and then use per app settings for the few apps that you want on the desktop. Use <i>auto provisioned</i> and <i>mandatory</i> apps as needed.

No app shortcuts in the Start Menu

If a user has a family computer, you might not need or want app shortcuts at all. In such scenarios, the simplest approach is browser access; install Citrix Receiver without any configuration and browse to Citrix Receiver for Web and Web interface. You can also configure Citrix Receiver for self-service access without putting shortcuts anywhere.

If you want to prevent Citrix Receiver from putting application shortcuts in the Start Menu automatically..	configure Citrix Receiver with PutShortcutsInStartMenu=False. Citrix Receiver will not put apps in the Start Menu even in self-service mode unless you put them there using per app settings.
---	---

All app shortcuts in the Start Menu or on the Desktop

If the user has only a few apps, you can put them all in the Start Menu or all on the desktop, or in a folder on the desktop.

If you want Citrix Receiver to put all application shortcuts in the start menu automatically..	configure Citrix Receiver with SelfServiceMode =False. All available apps will appear in the Start Menu.
If you want all application shortcuts to put on desktop..	configure Citrix Receiver with PutShortcutsOnDesktop = true. All available apps will appear in the desktop.
If you want all shortcuts to be put on the desktop in a folder...	configure Citrix Receiver with DesktopDir=Name of the desktop folder where you want applications.

Per app settings in XenApp 6.5 or 7.x

If you want to set the location of shortcuts so every user finds them in the same place use XenApp per App Settings:

If you want per-app settings to determine where applications are placed independently of whether in self-service mode or Start Menu mode..	configure Citrix Receiver with PutShortcutsInStartMenu=false and enable per app settings. Note: This setting applies to the Web Interface site only.
--	--

Apps in category folders or in specific folders

If you want applications displayed in specific folders use the following options:

--	--

If you want the application shortcuts Citrix Receiver places in the start menu to be shown in their associated category (folder)..	configure Citrix Receiver with UseCategoryAsStartMenuPath=True. Note: Windows 8/8.1 does not allow the creation of nested folders within the Start Menu. Applications will be displayed individually or under the root folder but not within Category sub folders defined with XenApp.
If you want the applications that Citrix Receiver puts in the Start menu to be in a specific folder..	configure Citrix Receiver with StartMenuDir=the name of the Start Menu folder name.

Remove apps on logoff or exit

If you don't want users to see apps if another user is going to share the end point, you can ensure that apps are removed when the user logs off and exits

If you want Citrix Receiver to remove all apps on logoff..	configure Citrix Receiver with RemoveAppsOnLogoff=True.
If you want Citrix Receiver to remove apps on exit..	configure Citrix Receiver with RemoveAppsOnExit=True.

Configuring local app access applications

When configuring local app access applications:

- To specify that a locally installed application should be used instead of an application available in Citrix Receiver, append the string KEYWORDS:prefer="pattern". This feature is referred to as Local App Access.

Before installing an application on a user's computer, Citrix Receiver searches for the specified patterns to determine if the application is installed locally. If it is, Citrix Receiver subscribes the application and does not create a shortcut. When the user starts the application from the Citrix Receiver window, Citrix Receiver starts the locally installed (preferred) application.

If a user uninstalls a preferred application outside of Citrix Receiver, the application is unsubscribed during the next Citrix Receiver refresh. If a user uninstalls a preferred application from the Citrix Receiver window, Citrix Receiver unsubscribes the application but does not uninstall it.

Note: The keyword prefer is applied when Citrix Receiver subscribes an application. Adding the keyword after the application is subscribed has no effect.

You can specify the prefer keyword multiple times for an application. Only one match is needed to apply the keyword to an application. The following patterns can be used in any combination:

- • To specify that a locally installed application should be used instead of an application available in Citrix Receiver, append the string KEYWORDS:prefer="pattern". This feature is referred to as Local App Access.
Before installing an application on a user's computer, Citrix Receiver searches for the specified patterns to determine if the application is installed locally. If it is, Citrix Receiver subscribes the application and does not create a shortcut. When the user starts the application from the Citrix Receiver window, Citrix Receiver starts the locally installed (preferred) application.

If a user uninstalls a preferred application outside of Citrix Receiver, the application is unsubscribed during the next Citrix Receiver refresh. If a user uninstalls a preferred application from the Citrix Receiver window, Citrix Receiver unsubscribes the application but does not uninstall it.

Note: The keyword `prefer` is applied when Citrix Receiver subscribes an application. Adding the keyword after the application is subscribed has no effect.

You can specify the `prefer` keyword multiple times for an application. Only one match is needed to apply the keyword to an application. The following patterns can be used in any combination:

- `prefer="ApplicationName"`

The application name pattern matches any application with the specified application name in the shortcut file name. The application name can be a word or a phrase. Quotation marks are required for phrases. Matching is not allowed on partial words or file paths and is case-insensitive. The application name matching pattern is useful for overrides performed manually by an administrator.

KEYWORDS:prefer=	Shortcut under Programs	Matches?
Word	\Microsoft Office\Microsoft Word 2010	Yes
"Microsoft Word"	\Microsoft Office\ Microsoft Word 2010	Yes
Console	\McAfee\VirusScan Console	Yes
Virus	\McAfee\VirusScan Console	No
McAfee	\McAfee\VirusScan Console	No

- `prefer="\\Folder1\Folder2\...\ApplicationName"`

The absolute path pattern matches the entire shortcut file path plus the entire application name under the Start menu. The Programs folder is a sub folder of the Start menu directory, so you must include it in the absolute path to target an application in that folder. Quotation marks are required if the path contains spaces. The matching is case-sensitive. The absolute path matching pattern is useful for overrides implemented programmatically in XenDesktop.

KEYWORDS:prefer=	Shortcut under Programs	Matches?
"\\Programs\Microsoft Office\Microsoft Word 2010"	\Programs\Microsoft Office\Microsoft Word 2010	Yes
"\\Microsoft Office\"	\Programs\Microsoft Office\Microsoft Word 2010	No
"\\Microsoft Word 2010"	\Programs\Microsoft Office\Microsoft Word 2010	No
"\\Programs\Microsoft Word 2010"	\Programs\Microsoft Word 2010	Yes

- `prefer="Folder1\Folder2\...\ApplicationName"`

The relative path pattern matches the relative shortcut file path under the Start menu. The relative path

provided must contain the application name and can optionally include the folders where the shortcut resides. Matching is successful if the short cut file path ends with the relative path provided. Quotation marks are required if the path contains spaces. The matching is case-sensitive. The relative path matching pattern is useful for overrides implemented programmatically.

KEYWORDS:prefer=	Shortcut under Programs	Matches?
"\Microsoft Office\Microsoft Word 2010"	\Microsoft Office\Microsoft Word 2010	Yes
"\Microsoft Office\"	\Microsoft Office\Microsoft Word 2010	No
"\Microsoft Word 2010"	\Microsoft Office\Microsoft Word 2010	Yes
"\Microsoft Word"	\Microsoft Word 2010	No

For information about other keywords, see "Additional recommendations" in [Optimize the user experience](#) in the StoreFront documentation.

Configuring your XenDesktop environment

Feb 23, 2017

The topics in this article describe how to configure USB support, prevent the Desktop Viewer window from dimming, and configure settings for multiple users and devices.

Configuring Bidirectional content redirection

You can enable bidirectional content redirection by using one of the following:

1. Group Policy Object administrative template
2. Registry

Note

- Bidirectional content redirection does not work on session where **Local App Access** is enabled.
- Bidirectional content redirection must be enabled both on the server and the client. When it is disabled either on the server or the client, the functionality is disabled.

To enable bidirectional content redirection using the Group Policy Object administrative template

Use Group Policy Object administrative template configuration for a first-time installation of Citrix Receiver for Windows.

1. As an administrator, open the Citrix Receiver Group Policy Object administrative template by running gpedit.msc.
 - If you are applying the policy on a single computer, launch it from the Start menu.
 - If you are applying the policy on a domain, launch it by using the Group Policy management console.
2. Under the User Configuration node, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User experience.
3. Select the **Bidirectional Content Redirection** policy.
4. Edit the settings.

Note

When you include URLs, you can specify a single URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

Bidirectional Content Redirection

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on: All Citrix Receiver supported platforms

Options:

Published Application/Desktop Name: Iexplore

Above Name is for Published Type: Application

Allowed URLs to be redirected to VDA: https://www.citrix.com

Allowed URLs to be redirected to Client: https://twitter.com

Help:

Bidirectional Content Redirection is the feature that allows URLs to be redirected from client to server and vice versa based on configuration.

-Published Application/Desktop Name : This indicates the Published Application/Desktop that will be used to launch the URL. Whether its Desktop or Application is decided based on the Type specified below.

-Above Name is for Published Type : This indicates the above Name is whether Application or Desktop.

-Allowed URLs to be redirected to VDA : This indicates the list of URLs that will be opened on VDA. Semi Colon ";" acts as a delimiter. "*" can be used as wild card. For example *.xyz.com.

-Allowed URLs to be redirected to Client : This indicates the list of URLs that will be opened on Client. Semi Colon ";" acts as a delimiter. "*" can be used as wild card. For example *.xyz.com.

Note:

1) If there is a URL that is put in both the places, then it will be launched from wherever it originated.

OK Cancel Apply

5. Click **Apply** and **OK**.

6. From a command line, run the `gpupdate /force` command.

Note: Relaunch running XenApp and XenDesktop sessions for the changes to take effect.

To enable bidirectional content redirection using the registry

To enable bidirectional content redirection, run the **redirector.exe /RegIE** command from the Citrix Receiver for Windows installation folder (C:\Program Files (x86)\Citrix\ICA Client).

Limitations

- No fallback mechanism is present if redirection fails due to session launch issues.

Important

- Ensure that redirection rules do not result in a looping configuration. A looping configuration, for example results if VDA rules are set so that a URL, `https://www.my_company.com`, is configured to be redirected to the client, and the same URL is configured to be redirected to the VDA.
- URL redirection supports only explicit URLs (those appearing in the address bar of the browser or found using the in-browser

navigation, depending on the browser).

- If two applications with same display name are configured to use multiple StoreFront accounts, the display name in the primary StoreFront account is used for launching the application or a desktop session.
- New browser window opens only when URL is redirected to the client. When URL is redirected to VDA, if the browser is already open, then the redirected URL opens in the new tab.
- Embedded links in files like documents, emails, pdfs is supported.

Configuring Adaptive transport

Requirements

- XenApp and XenDesktop 7.12 or later (required to enable the feature using Citrix Studio).
- StoreFront 3.8.
- IPv4 VDAs only. IPv6 and mixed IPv6 and IPv4 configurations are not supported.
- Add firewall rules to allow inbound traffic on UDP ports 1494 and 2598 of the VDA.

Note: TCP ports 1494 and 2598 are also required and opened automatically when you install the VDA. However, UDP ports 1494 and 2598 are not automatically opened. You must enable them.

Adaptive transport must be configured on the VDA by applying the policy before it is available for communication between the VDA and Citrix Receiver.

By default, the adaptive transport is allowed in Citrix Receiver for Windows. However, also by default, the client attempts to use adaptive transport only if the VDA is configured to **Preferred** in the Citrix Studio policy and if the setting has been applied on the VDA.

You can enable adaptive transport using the **HDX Adaptive Transport policy** setting. Set the new policy to **Preferred** to use adaptive transport when possible, with fallback to TCP.

To disable adaptive transport on a specific client, set the EDT options appropriately using the Citrix Receiver Group Policy Object administrative template.

To configure adaptive transport using the Citrix Receiver Group Policy Object administrative template (optional)

The following are optional configuration steps to customize your environment. For example, you may choose to disable the feature for a particular client for security reasons.

Note

By default, adaptive transport is disabled (Off) and TCP is always used.

1. As an administrator, open the Citrix Receiver Group Policy Object administrative template by running `gpedit.msc`.

- If you are applying the policy on a single computer, launch it from the Start menu.
- If you are applying the policy on a domain, launch it by using the Group Policy management console.

For information on how to import the Citrix Receiver for Windows administrative template files into the Group Policy Editor, see [Configuring Citrix Receiver for Windows with the Group Policy Object template](#).

2. Under the Computer Configuration node, go to **Administrative Templates > Citrix Receiver > Network routing**.

3. Set the **Transport protocol for Receiver** policy to **Enabled**.

4. Select **Communication Protocol for Citrix Receiver** as required.

- **Off**: Indicates that TCP is used for data transfer.
- **Preferred**: Indicates that the Citrix Receiver tries to connect to the server using UDP at first and then switches to TCP as a fallback.
- **On**: Indicates that the Citrix Receiver connects to the server using UDP only. There is no fallback to TCP with this option.

5. Click **Apply** and **OK**.

6. From a command line, run the `gpupdate /force` command.

Additionally, for the adaptive transport configuration to take effect, the user is required to add the Citrix Receiver Windows template files to the Policy Definitions folder. For more information on adding admx/adml template files to the local GPO, see [Configuring Citrix Receiver for Windows with the Group Policy Object template](#).

To confirm that the policy setting has taken effect:

Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT and verify that the key **HDXOverUDP** is included.

Configuring USB support for XenApp and XenDesktop connections

USB support enables you to interact with a wide range of USB devices when connected to a virtual desktop. You can plug USB devices into their computers and the devices are remoted to their virtual desktop. USB devices available for remoting include flash drives, smartphones, PDAs, printers, scanners, MP3 players, security devices, and tablets. Desktop Viewer users can control whether USB devices are available on the virtual desktop using a preference in the toolbar.

Isochronous features in USB devices, such as webcams, microphones, speakers, and headsets are supported in typical low latency/high speed LAN environments. This allows these devices to interact with packages, such as Microsoft Office Communicator and Skype.

The following types of device are supported directly in a XenApp and XenDesktop session, and so does not use USB support:

- Keyboards
- Mice
- Smart cards

Note: Specialist USB devices (for example, Bloomberg keyboards and 3-D mice) can be configured to use USB support. For information on configuring Bloomberg keyboards, see [Configure Bloomberg keyboards](#). For information on configuring policy rules for other specialist USB devices, see Knowledge Center article [CTX119722](#).

By default, certain types of USB devices are not supported for remoting through XenDesktop and XenApp. For example, a user may have a network interface card attached to the system board by internal USB. Remoting this device would not be appropriate. The following types of USB device are not supported by default for use in a XenDesktop session:

- Bluetooth dongles
- Integrated network interface cards
- USB hubs
- USB graphics adaptors

USB devices connected to a hub can be remoted, but the hub itself cannot be remoted.

The following types of USB device are not supported by default for use in a XenApp session:

- Bluetooth dongles
- Integrated network interface cards
- USB hubs
- USB graphics adapters
- Audio devices
- Mass storage devices

For instructions on modifying the range of USB devices that are available to users, see [Update the list of USB devices available for remoting](#).

For instructions on automatically redirecting specific USB devices, see Knowledge Center article [CTX123015](#).

How USB support works

When a user plugs in a USB device, it is checked against the USB policy, and, if allowed, remoted to the virtual desktop. If the device is denied by the default policy, it is available only to the local desktop.

When a user plugs in a USB device, a notification appears to inform the user about a new device. The user can decide which USB devices are remoted to the virtual desktop by selecting devices from the list each time they connect. Alternatively, the user can configure USB support so that all USB devices plugged in both before and/or during a session are automatically remoted to the virtual desktop that is in focus.

Mass storage devices

For mass storage devices only, in addition to USB support, remote access is available through client drive mapping, which you configure through the Citrix Receiver policy Remoting client devices > Client drive mapping. When this policy is applied, 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.

The main differences between the two types of remoting policy are:

Feature	Client drive mapping	USB support
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, if the user clicks Safely Remove Hardware in the notification area

If both Generic USB and the Client drive mapping policies are enabled and a mass storage device is inserted before a session starts, it will be redirected using client drive mapping first, before being considered for redirection through USB support. If it is inserted after a session has started, it will be considered for redirection using USB support before client drive mapping.

USB device classes allowed by default

Different classes of USB device are allowed by the default USB policy rules.

Although they are on this list, some classes are only available for remoting in XenDesktop and XenApp sessions after additional configuration. These are noted below.

- **Audio (Class 01).** Includes audio input devices (microphones), audio output devices, and MIDI controllers. Modern audio devices generally use isochronous transfers, which is supported by XenDesktop 4 or later. Audio (Class01) is not applicable to XenApp because these devices are not available for remoting in XenApp using USB support.
Note: Some specialty devices (for example, VOIP phones) require additional configuration. For more information, see Knowledge Center article [CTX123015](#).
- **Physical Interface Devices (Class 05).** These devices are similar to Human Interface Devices (HIDs), but generally

provide "real-time" input or feedback and include force feedback joysticks, motion platforms, and force feedback exoskeletons.

- **Still Imaging (Class 06).** Includes digital cameras and scanners. Digital cameras often support the still imaging class which uses the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP) to transfer images to a computer or other peripheral. Cameras may also appear as mass storage devices and it may be possible to configure a camera to use either class, through setup menus provided by the camera itself.

Note: If a camera appears as a mass storage device, client drive mapping is used and USB support is not required.

- **Printers (Class 07).** In general most printers are included in this class, although some use vendor-specific protocols (class ff). Multi-function printers may have an internal hub or be composite devices. In both cases the printing element generally uses the Printers class and the scanning or fax element uses another class; for example, Still Imaging. Printers normally work appropriately without USB support.

Note: This class of device (in particular printers with scanning functions) requires additional configuration. For instructions on this, see Knowledge Center article [CTX123015](#).

- **Mass Storage (Class 08).** The most common mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There are a wide variety of devices with internal storage that also present a mass storage interface; these include media players, digital cameras, and mobile phones. Mass Storage (Class 08) is not applicable to XenApp because these devices are not available for remoting in XenApp using USB support.

Known subclasses include:

- 01 Limited flash devices
- 02 Typically CD/DVD devices (ATAPI/MMC-2)
- 03 Typically tape devices (QIC-157)
- 04 Typically floppy disk drives (UFI)
- 05 Typically floppy disk drives (SFF-8070i)
- 06 Most mass storage devices use this variant of SCSI

Mass storage devices can often be accessed through client drive mapping, and so USB support is not required.

Important: Some viruses are known to propagate actively using all types of mass storage. Carefully consider whether or not there is a business need to permit the use of mass storage devices, either through client drive mapping or USB support.

- **Content Security (Class 0d).** Content security devices enforce content protection, typically for licensing or digital rights management. This class includes dongles.
- **Video (Class 0e).** The video class covers devices that are used to manipulate video or video-related material, such as webcams, digital camcorders, analog video converters, some television tuners, and some digital cameras that support video streaming.

Note: Most video streaming devices use isochronous transfers, which is supported by XenDesktop 4 or later. Some video devices (for example webcams with motion detection) require additional configuration. For instructions on this, see Knowledge Center article [CTX123015](#).

- **Personal Healthcare (Class 0f).** These devices include personal healthcare devices such as blood pressure sensors, heart rate monitors, pedometers, pill monitors, and spirometers.
- **Application and Vendor Specific (Classes fe and ff).** Many devices use vendor specific protocols or protocols not standardized by the USB consortium, and these usually appear as vendor-specific (class ff).

USB devices classes denied by default

The following different classes of USB device are denied by the default USB policy rules.

- Communications and CDC Control (Classes 02 and 0a). The default USB policy does not allow these devices, because one of the devices may be providing the connection to the virtual desktop itself.
- Human Interface Devices (Class 03). Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are keyboards, mice, pointing devices, graphic tablets, sensors, game controllers, buttons, and control functions.

Subclass 01 is known as the "boot interface" class and is used for keyboards and mice.

The default USB policy does not allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). This is because most keyboards and mice are handled appropriately without USB support and it is normally necessary to use these devices locally as well remotely when connecting to a virtual desktop.

- USB Hubs (Class 09). USB hubs allow extra devices to be connected to the local computer. It is not necessary to access these devices remotely.
- Smart Card (Class 0b). Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card-equivalent chip.

Smart card readers are accessed using smart card remoting and do not require USB support.

- Wireless Controller (Class e0). Some of these devices may be providing critical network access, or connecting critical peripherals, such as Bluetooth keyboards or mice.

The default USB policy does not allow these devices. However, there may be particular devices to which it is appropriate to provide access using USB support.

- **Miscellaneous network devices (Class ef, subclass 04)**. Some of these devices may be providing critical network access. The default USB policy does not allow these devices. However, there may be particular devices to which it is appropriate to provide access using USB support.

Update the list of USB devices available for remoting

You can update the range of USB devices available for remoting to desktops by editing the Citrix Receiver for Windows template file. This allows you to make changes to the Citrix Receiver for Windows using Group Policy. The file is located in the following installed folder:

<root drive>\Program Files\Citrix\ICA Client\Configuration\en

Alternatively, you can edit the registry on each user device, adding the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules" Value=

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.

The product default rules are stored in:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules" Value=

Do not edit the product default rules.

For details of the rules and their syntax, see the Knowledge Center article [CTX119722](#).

Configuring USB audio per user

Citrix recommends using the Group Policy Object receiver.admx/receiver.adml template file to configure rules for network routing, proxy servers, trusted server configuration, user routing, remote user devices, and the user experience.

You can use the receiver.admx template file with domain policies and local computer policies. For domain policies, import the template file using the Group Policy Management Console. This is especially useful for applying Citrix Receiver for Windows settings to a number of different user devices throughout the enterprise. To affect a single user device, import the template file using the local Group Policy Editor on the device.

Note: This feature is available only on XenApp server.

To configure USB audio devices per user

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer, or by using the Group Policy Management Console when applying domain policies.
Note: If you already imported the receiver template into the Group Policy Editor, you can leave out steps 2 to 5.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the **Action** menu, choose **Add/Remove Templates**.
4. Choose **Add** and browse to the Configuration folder for Receiver (for 32-bit machines, usually C:\Program Files\Citrix\ICA Client\Configuration, for 64-bit machines usually C:\Program Files (x86)\Citrix\ICA Client\Configuration) and select receiver.admx.
5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.
6. Under the Computer Configuration node, go to **Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User experience**, and select **Audio through Generic USB Redirection**.
7. Edit the settings.
8. Click **Apply** and **OK**.
9. Open cmd prompt in administrator mode.
10. Run the below command
gpupdate /force

Note: Any change in the policy requires the XenApp server to be restarted for the changes to take effect.
Configure Bloomberg keyboards

Bloomberg keyboards are supported by XenDesktop and XenApp sessions (but not other USB keyboards). The required components are installed automatically when the plug-in is installed, but you must enable this feature either during the installation or later by changing a registry key.

On any one user device, multiple sessions to Bloomberg keyboards are not recommended. The keyboard only operates correctly in single-session environments.

To turn Bloomberg keyboard support on or off

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. Locate the following key in the registry:
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Do one of the following:

- To turn on this feature, for the entry with Type DWORD and Name EnableBloombergHID, set Value to 1.
- To turn off this feature, set the Value to 0.

To prevent the Desktop Viewer window from dimming

If users have multiple Desktop Viewer windows, by default the desktops that are not active are dimmed. If users need to view multiple desktops simultaneously, this can make the information on them unreadable. You can disable the default behavior and prevent the Desktop Viewer window from dimming by editing 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. On the user device, create a REG_DWORD entry called DisableDimming in one of the following keys, depending on whether you want to prevent dimming for the current user of the device or the device itself. An entry already exists if the Desktop Viewer has been used on the device:

- HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

Optionally, instead of controlling dimming with the above user or device settings, you can define a local policy by creating the same REG_WORD entry in one of the following keys:

- HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

The use of these keys is optional because XenDesktop administrators, rather than plug-in administrators or users, typically control policy settings using Group Policy. So, before using these keys, check whether your XenDesktop administrator has set a policy for this feature.

2. Set the entry to any non-zero value such as 1 or true.

If no entries are specified or the entry is set to 0, the Desktop Viewer window is dimmed. If multiple entries are specified, the following precedence is used. The first entry that is located in this list, and its value, determine whether the window is dimmed:

1. HKEY_CURRENT_USER\Software\Policies\Citrix\...
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\...
3. HKEY_CURRENT_USER\Software\Citrix\...
4. HKEY_LOCAL_MACHINE\Software\Citrix\...

Configuring StoreFront

Dec 06, 2016

Citrix StoreFront authenticates users to XenDesktop, XenApp, and VDI-in-a-Box, enumerating and aggregating available desktops and applications into stores that users access through Citrix Receiver for Windows.

In addition to the configuration summarized in this section, you must also configure NetScaler Gateway to enable users to connect from outside the internal network (for example, users who connect from the Internet or from remote locations).

Tip

Citrix Receiver for Windows occasionally shows the older StoreFront UI instead of the updated StoreFront UI after you select the option to show all stores.

To configure StoreFront

1. Install and configure StoreFront as described in the [StoreFront](#) documentation. Citrix Receiver for Windows requires an HTTPS connection. If the StoreFront server is configured for HTTP, a registry key must be set on the user device as described in [Configure and install Receiver for Windows using command-line parameters](#) under the ALLOWADDSTORE property description.

Note: For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Receiver for Windows.

Manage workspace control reconnect

Workspace control lets applications follow users as they move between devices. This enables, for example, clinicians in hospitals to move from workstation to workstation without having to restart their applications on each device. For Citrix Receiver for Windows, you manage workspace control on client devices by modifying the registry. This can also be done for domain-joined client devices using Group Policy.

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 the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Create WSCReconnectModeUser and modify the existing registry key WSCReconnectMode in the Master Desktop Image or in XenApp server hosting. The published desktop can change the behavior of the Citrix Receiver for Windows.

WSCReconnectMode key settings for Citrix Receiver for Windows:

- 0 = do not reconnect to any existing sessions
- 1 = reconnect on application launch
- 2 = reconnect on application refresh
- 3 = reconnect on application launch or refresh
- 4 = reconnect when Receiver interface opens
- 8 = reconnect on Windows log on
- 11 = combination of both 3 and 8

Disable workspace control for Citrix Receiver for Windows

To disable workspace control for Citrix Receiver for Windows, create the following key:

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64-bit)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle for (32-bit)

Name: **WSCReconnectModeUser**

Type: REG_SZ

Value data: 0

Modify the following key from the default value of 3 to zero

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64-bit)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32-bit)

Name: **WSCReconnectMode**

Type: REG_SZ

Value data: 0

Note: Alternatively, you can set the REG_SZ value WSCReconnectAll to false if you do not want to create a new key.

Changing the status indicator timeout

You can change the amount of time the status indicator displays when a user is launching a session. To alter the time out period, create a REG_DWORD value SI_INACTIVE_MS in HKLM\SOFTWARE\Citrix\ICA_CLIENT\Engine\.. The REG_DWORD value can be set to 4 if you want the status indicator to disappear sooner.

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.

Customizing location for application shortcut via CLI

Start menu integration and desktop shortcut only mode lets you bring published application shortcuts into the Windows Start menu and onto the desktop. Users do not have to subscribe to applications from the Citrix Receiver user interface. Start menu integration and desktop shortcut management provides a seamless desktop experience for groups of users, who need access to a core set of applications in a consistent way.

As a Citrix Receiver administrator, you use a command-line install flags, GPOs, account services, or registry settings to disable the usual "self-service" Citrix Receiver interface and replace it with a pre-configured Start menu. The flag is called SelfServiceMode and is set to true by default. When the administrator sets the SelfServiceMode flag to false, the user no longer has access to the self-service Citrix Receiver user interface. Instead, they can access subscribed apps from the Start menu and via desktop shortcuts - referred to here as shortcut-only mode.

Users and administrators can use a number of registry settings to customize the way shortcuts are set up. See [Using registry keys to customize app shortcut locations](#).

Working with shortcuts

- Users cannot remove apps. All apps are mandatory when working with the SelfServiceMode flag set to false (shortcut-only mode). If the user removes a shortcut icon from the desktop, the icon comes back when the user selects Refresh from the Citrix Receiver for Windows system tray icon.
- Users can configure only one store. The Account and Preferences options are not available. This is to prevent the user from configuring additional stores. The administrator can give a user special privileges to add more than one account using the Group Policy Object template, or by manually adding a registry key (HideEditStoresDialog) on the client machine. When the administrator gives a user this privilege, the user has a Preferences option in the system tray icon, where they can add and remove accounts.
- Users cannot remove apps via the Windows Control Panel.
- You can add desktop shortcuts via a customizable registry setting. Desktop shortcuts are not added by default. After you make any changes to the registry settings, Citrix Receiver for Windows must be restarted.
- Shortcuts are created in the Start menu with a category path as the default, UseCategoryAsStartMenuPath.

Note: Windows 8/8.1 does not allow the creation of nested folders within the Start Menu. Applications will be displayed individually or under the root folder but not within Category sub folders defined with XenApp.

- You can add a flag [/DESKTOPDIR="Dir_name"] during installation to bring all shortcuts into a single folder. CategoryPath is supported for desktop shortcuts.
- Auto Re-install Modified Apps is a feature which can be enabled via the registry key AutoReInstallModifiedApps. When AutoReInstallModifiedApps is enabled, any changes to attributes of published apps and desktops on the server are reflected on the client machine. When AutoReInstallModifiedApps is disabled, apps and desktop attributes are not updated and shortcuts are not re-stored on refresh if deleted on the client. By default, this AutoReInstallModifiedApps is enabled. See Using registry keys to customize app shortcut locations.

Customizing location for application shortcut via Registry

Note

By default, registry keys use String format

You can use registry key settings to customize shortcuts. You can set the registry keys at the following locations. Where they apply, they are acted on in the order of preference listed.

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.

Note: You should make changes to registry keys before configuring a store. If at any time you or a user wants to customize the registry keys, you or the user must reset Receiver, configure the registry keys, and then reconfigure the store.

Registry keys for 32-bit machines

Registry name	Default value	Locations in order of preference
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\" + StoreID + \Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle

		HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
StartMenuDir	"" (empty)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	"" (empty)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID

		+ \Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	True inSelfServiceMode, and False inNonSelfServiceMode	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle

Registry keys for 64-bit machines

Registry name	Default value	Locations in order of preference
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\" + StoreID + \Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\" + StoreID + \Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\" + StoreID + \Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties

		HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	"" (empty)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
DesktopDir	"" (empty)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
HideEditStoresDialog	True inSelfServiceMode, and False inNonSelfServiceMode	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties

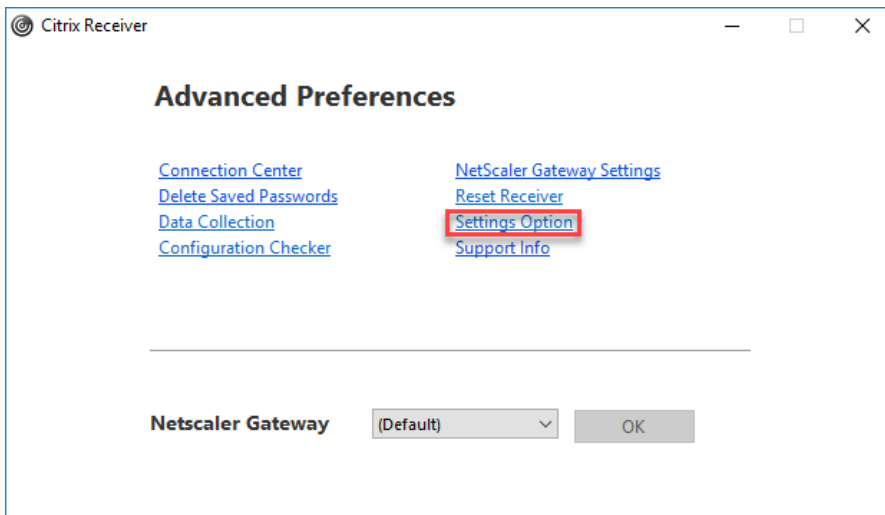
		HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

Configuring Application Display via Graphical User Interface

Note

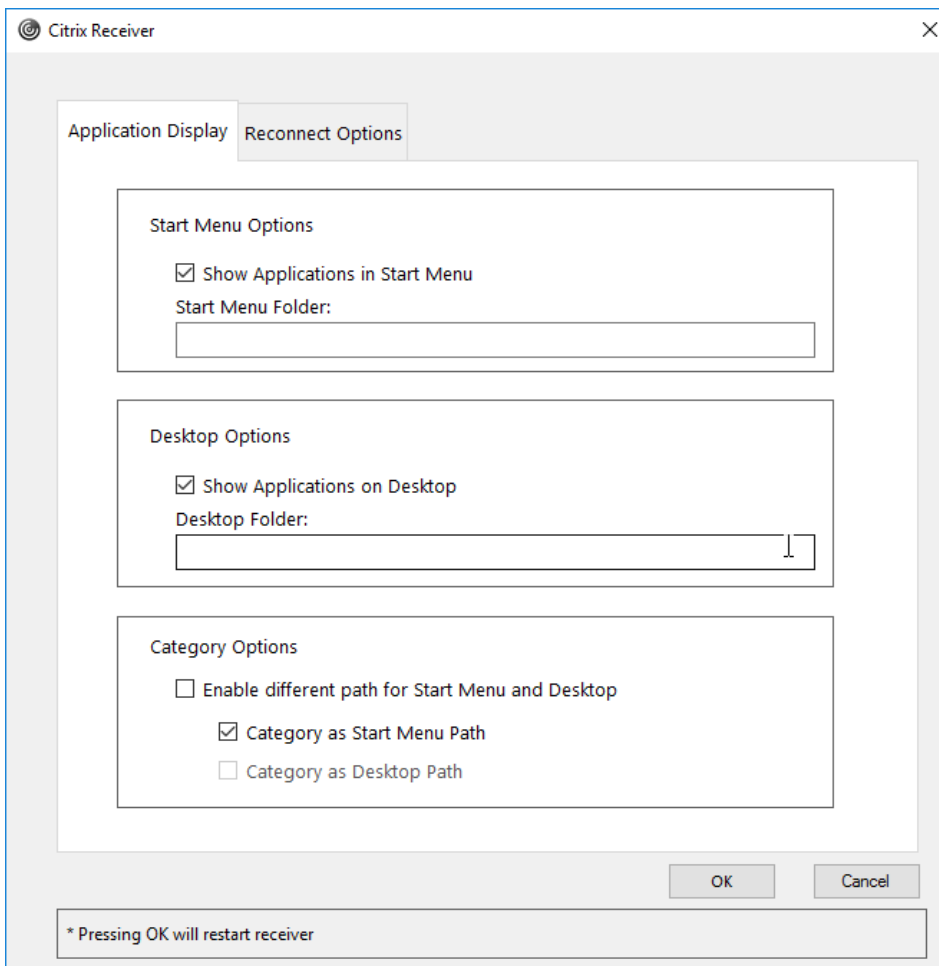
Shortcuts can be set only for the subscribed applications and desktops.

1. Logon to Citrix Receiver for Windows
2. Right click on the Citrix Receiver for Windows icon in the notification area and click **Advanced Preferences**.
The Advanced Preferences window appears.



3. Click **Settings Option**

Note: By default, Show Applications in Start Menu option is selected.



4. Specify the folder name. This moves all the subscribed apps to the specified folder in the Start menu. Applications can be added both to a new or existing folder in the Start menu.
On enabling this feature, both existing and newly added applications get added to the specified folder.

5. Select the checkbox **Show Applications on Desktop** under **Desktop Options** pane.
6. Specify the folder name. This moves all the subscribed apps to the specified folder on your local desktop.
7. Select the checkbox **Enable different path for Start Menu and Desktop** under **Category** Options.
This creates the shortcuts and category folder for applications as defined in the application properties server. For ex, IT Apps, Finance Apps

Note: By default, Category as Start Menu Path option is selected.

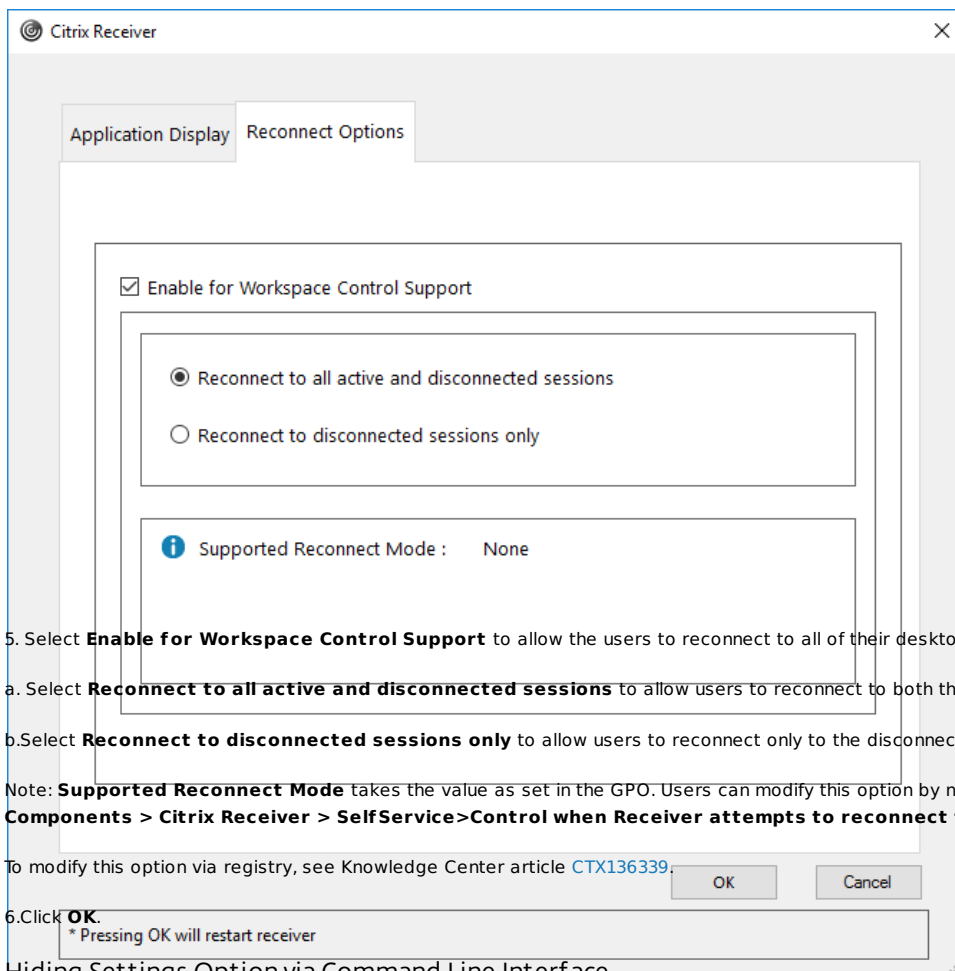
- a. Select **Category as Start Menu Path** to display the subscribed apps and their category folder as defined in the application properties server in the Windows Start menu.
- b. Select **Category as Desktop Path** to display the subscribed apps and their category folder as defined in the application properties server on your local desktop.

5. Click OK.

Configuring Reconnect Options via Graphical User Interface

After logging on to the server, users can reconnect to all of their desktops or applications at any time. By default, Reconnect Options opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect Options to reconnect only those desktops or applications that the user disconnected from previously.

1. Logon to Citrix Receiver for Windows
2. Right click on the Citrix Receiver for Windows icon in the system tray and click **Advanced Preferences**.
The Advanced Preferences window appears.
3. Click **Settings Option**
4. Click **Reconnect Options**



5. Select **Enable for Workspace Control Support** to allow the users to reconnect to all of their desktops or applications at any time.

a. Select **Reconnect to all active and disconnected sessions** to allow users to reconnect to both the active and disconnected sessions.

b. Select **Reconnect to disconnected sessions only** to allow users to reconnect only to the disconnected sessions.

Note: **Supported Reconnect Mode** takes the value as set in the GPO. Users can modify this option by navigating to **Administrative Templates > Citrix Components > Citrix Receiver > SelfService>Control when Receiver attempts to reconnect to existing sessions**.

To modify this option via registry, see Knowledge Center article [CTX136339](https://docs.citrix.com/en-us/knowledge-center/CTX136339).

6. Click **OK**.

* Pressing OK will restart receiver

Hiding Settings Option via Command Line Interface

Option	/DisableSetting
Description	Suppresses Settings Option to be displayed in the Advanced Preferences dialog.
Sample usage	CitrixReceiver.exe /DisableSetting=3

If you want both Application Display and Reconnect Options to be displayed in the Settings Option.. Enter CitrixReceiver.exe /DisableSetting=0

If you want Settings Option to be hidden in the Advanced Preferences dialog Enter CitrixReceiver.exe /DisableSetting=3

If you want Settings Option to display only Application Display Enter CitrixReceiver.exe /DisableSetting=2

If you want Settings Option to display only Reconnect Options Enter CitrixReceiver.exe /DisableSetting=1

Configure with the Group Policy Object administrative template

Apr 06, 2017

Citrix recommends using the Windows Group Policy Object Editor to configure Citrix Receiver for Windows. Citrix Receiver for Windows includes administrative template files (receiver.adm or receiver.admx\receiver.adml -depending on the Operating System) in the installation directory.

Note

- Starting with Citrix Receiver for Windows Version 4.6, the installation directory includes CitrixBase.admx and CitrixBase.adml files. Citrix recommends that you use the CitrixBase.admx and CitrixBase.adml files to ensure that the options are correctly organized and displayed within the Group Policy Object Editor.
- The .adm file is for use with Windows XP Embedded platforms only. The .adm/.adml files are for use with Windows Vista/Windows Server 2008 and all later versions of Windows.
- If Citrix Receiver for Windows is installed with VDA, admx/adml files are found in the Citrix Receiver for Windows installation directory. For example: <installation directory>\Online Plugin\Configuration.
- If Citrix Receiver for Windows is installed without VDA, the admx/adml files are typically found in the C:\Program Files\Citrix\ICA Client\Configuration directory.

See the table below for information on Citrix Receiver for Windows templates files and their respective location.

Note: Citrix recommends that you use the GPO template files provided with latest Citrix Receiver for Windows.

File Type	File Location
receiver.adm	<Installation Directory>\ICA Client\Configuration
receiver.admx	<Installation Directory>\ICA Client\Configuration
receiver.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	<Installation Directory>\ICA Client\Configuration
CitrixBase.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]

Note

- If the CitrixBase.admx\adml is not added to the local GPO, the Enable ICA File Signing policy might be lost.
- When upgrading Citrix Receiver for Windows, you must add the latest template files to local GPO as explained in the procedure below. While importing the latest files, previous settings are retained.

To add the receiver.adm template file to the local GPO (Windows XP Embedded Operating system only)

Note: You can use .adm template files to configure Local GPO and/or Domain-Based GPO.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer, or by using the Group Policy Management Console when applying domain policies.

Note: If you already imported the Citrix Receiver for Windows template into the Group Policy Editor, you can leave out steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the **Administrative Templates** folder.

3. From the Action menu, choose **Add/Remove Templates**.

4. Select Add and browse to the template file location <Installation Directory>\ICA Client\Configuration\receiver.adm

5. Select Open to add the template and then Close to return to the Group Policy Editor.

Citrix Receiver for window template file will be available on local GPO in path **Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver**.

After the .adm template files are added to the local GPO, the following message is displayed:

"The following entry in the [strings] section is too long and has been truncated:

Click **OK** to ignore the message.

To add the receiver.admx/adml template files to the local GPO (later versions of Windows Operating System)

NOTE: You can use admx/adml template files to configure Local GPO and/or Domain-Based GPO. Refer Microsoft MSDN article on managing ADMX files [here](#).

1. After installing Citrix Receiver for Windows, copy the template files.

admx:

From: <Installation Directory>\ICA Client\Configuration\receiver.admx

To: %systemroot%\policyDefinitions

From: <Installation Directory>\ICA Client\Configuration\CitrixBase.admx

To: %systemroot%\policyDefinitions

adml:

From: <Installation Directory>\ICA Client\Configuration\[MUIculture]receiver.adml

To: %systemroot%\policyDefinitions\[MUIculture]

From: <Installation Directory>\ICA Client\Configuration\[MUIculture]\CitrixBase.adml

To: %systemroot%\policyDefinitions\[MUIculture]

Note

Citrix Receiver for Window template files are available on local GPO in Administrative Templates > Citrix Components > Citrix Receiver folder only when the user adds the CitrixBase.admx/CitrixBase.adml to the \ policyDefinitions folder.

About TLS and Group Policies

Use this policy to configure the TLS options that ensure Citrix Receiver for Windows securely identifies the server that it is connecting to, and encrypts all communication with the server.

You can use these options to:

- enforce use of TLS. Citrix recommends that all connections over untrusted networks, including the Internet, use TLS.
- enforce use of FIPS (Federal Information Processing Standards) Approved cryptography and help comply with the recommendations in NIST SP 800-52. These options are disabled by default.
- enforce use of a specific version of TLS, and specific TLS cipher suites, Citrix supports TLS 1.0, TLS 1.1 and TLS 1.2 protocols between Citrix Receiver for Windows, and XenApp or XenDesktop.
- connect only to specific servers.
- check for revocation of the server certificate.
- check for a specific server certificate issuance policy.
- select a particular client certificate, if the server if is configured to request one.

When this policy is enabled, you can force Citrix Receiver for Windows to use TLS for all connections to published applications and desktops by checking the **Require TLS for all connections** checkbox.

To enforce use of FIPS Approved cryptography, select **Enable FIPS**.

Important

If you select Enable FIPS, you must also enable the Windows security option **System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**, or Citrix Receiver for Windows may fail to connect to published applications and desktops.

For compliance with NIST SP 800-52 recommendations, select Security Compliance Mode SP800-52. Only do this if all servers or gateways also comply with NIST SP 800-52 recommendations.

Important

If you select Security Compliance Mode SP800-52, FIPS Approved cryptography is automatically used, even if Enable FIPS is not selected. You must also enable the Windows security option **System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**, or Citrix Receiver for Windows may fail to connect to published applications and desktops.

If you select Security Compliance Mode SP800-52, you must also select either select the Certificate Revocation Check Policy setting with Full Access Check, or Full access check and CRL required.

If you select Security Compliance Mode SP800-52, Citrix Receiver for Windows will verify that the server certificate complies with the recommendations in NIST SP 800-52. If the server certificate does not, Citrix Receiver for Windows will fail to connect.

Citrix Receiver for Windows supports RSA keys of 1024, 2048, and 3072 bit lengths. Additionally, root certificates with RSA keys of 4096 bit length are supported.

Note

Citrix does not recommend using RSA keys of 1024 bit length.

To enforce use of a specific version of TLS, select the TLS version setting:

Some regulations do not permit the use of TLS 1.0, and prefer the use of TLS 1.2. Citrix Receiver will use the highest version of TLS that is also available at the server or gateway.

You can choose:

- TLS 1.0 or TLS 1.1 or TLS 1.2- This is the default setting. This option is recommended only if there is a business requirement for TLS 1.0 for compatibility.
- TLS 1.1 or TLS 1.2.
- TLS 1.2 only- This option is recommended if TLS 1.2 is a business requirement.

To enforce use of specific TLS cipher suites, select either Government (GOV), Commercial (COM) or All (ALL). For certain NetScaler Gateway configurations, you might need to select COM.

The available cipher suites depend also on the Enable FIPS and Security Compliance Mode settings.

The following table lists the cipher suites in each set:

TLS cipher suite	GOV	COM	ALL	GOV	COM	ALL	GOV	COM	ALL
Enable FIPS	Off	Off	Off	On	On	On	On	On	On
Security Compliance Mode SP800-52	Off	Off	Off	Off	Off	Off	On	On	On
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X			
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X			
TLS_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X	X		X
TLS_RSA_WITH_AES_128_GCM_SHA256	X	X	X	X	X	X	X	X	X

TLS_RSA_WITH_AES_256_CBC_SHA256	X		X	X		X		
TLS_RSA_WITH_AES_256_CBC_SHA	X		X	X		X	X	X
TLS_RSA_WITH_AES_128_CBC_SHA		X	X		X	X		X
TLS_RSA_WITH_RC4_128_SHA		X	X					
TLS_RSA_WITH_RC4_128_MD5		X	X					
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X		X	X		X	X	X

You can restrict Citrix Receiver for Windows to connect only to particular servers. Citrix Receiver for Windows identifies the server by the name in the security certificate that the server presents. This has the form of a DNS name (for example, www.citrix.com). Specify the list of names, separated by commas, in the **Allowed TLS servers** setting. Wildcards and port numbers can be specified here; for example, *.citrix.com:4433 allows connection to any server whose common name ends with.citrix.com on port 4433. The accuracy of the information in a security certificate is asserted by the certificate's issuer. If Citrix Receiver for Windows does not recognize and trust a certificate's issuer, the connection is rejected.

Citrix Receiver for Windows checks whether a server certificate has been revoked, using a Certificate Revocation List (CRL). If the certificate has been revoked, the connection is rejected. The certificate's issuer can revoke a certificate if the server has been compromised.

Select the Certificate Revocation Check Policy setting as follows:

- **No Check**- Select this option if you wish the connection to proceed with no CRL check.
- **Check with no network access**- Select this option if you want the CRL to be checked, without retrieving an up-to-date CRL.
- **Full Access Check**- Select this option if you want the CRL to be checked, first retrieving an up-to-date CRL if possible.
- **Full access check and CRL required**- Select this option if you want the CRL to be checked. The connection will be rejected if an up-to-date CRL is not available.

You can restrict Citrix Receiver for Windows to connect only to servers with a specific certificate issuance policy. This is identified by the Policy Extension OID. If selected, Citrix Receiver for Windows accepts only server certificates containing that Policy Extension OID.

When connecting using TLS, the server may be configured to request Citrix Receiver for Windows to provide a client certificate. Select **Client Authentication** setting as follows:

- **Disabled**- Select this option if the server is not configured to request a client certificate. This protects the information in the client certificate from being disclosed incorrectly.
- **Select automatically if possible**- This is usually the best option if the server is configured to request a client certificate.
- **Display certificate selector**- Select this option if **Select automatically if possible** does not select the correct certificate. The user will be prompted.
- **Use specified certificate** - Select this option if **Select automatically if possible** does not select the correct certificate, and you do not want the user to be prompted. You must then specify the certificate's thumbprint.

Session reliability group policy

When configuring session reliability group policy, set the transparency level. Using this option, you can control the transparency level applied to a published app (or desktop) during the session reliability reconnection period.

To configure the transparency level, select **Computer Configuration - > Administrative Templates-> Citrix Components - > Network Routing -> Session reliability and automatic reconnection - > Transparency Level**.

Note

By default, Transparency Level is set to 80.

Session reliability and automatic reconnection

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: ADMX Migrator encountered a policy that does not have a supportedOn value.

Options:

☒ Enable automatic reconnection

☒ Enable session reliability (has precedence if both are selected)

Transparency Level 80

Help:

Use this policy to control how the client behaves when a network failure causes a dropped connection.

If you select "Enable" and then choose a check box for "Enable session reliability" and/or "Enable automatic reconnection," the client attempts to reconnect to a server.

The "Enable session reliability" selection enables reconnection to an SSL/TLS server. Support for this setting depends on the SSL server configuration. The "Enable automatic reconnection" setting enables auto reconnection. If both options are enabled, session reliability has precedence. If session reliability is unable to reconnect, auto reconnection tries to connect. If "Enabled" is selected, but you do not choose one of the check boxes, the policy is not enforced.

Use Transparency Level option to control transparency level applied to XA/XD session window during session reliability reconnection period.

- 0 means, XA/XD session window will be turned to black window
- 100 means, no transparency layer will be applied (frozen screen)

Troubleshooting:

Some proxy servers automatically disconnect connections that are idle for a certain length of time. This can cause client sessions to be disconnected when not in use. A

OK Cancel Apply

Provide users with account information

Mar 07, 2017

Provide users with the account information they need to access virtual desktops and applications. You can provide this information by:

- Configuring email-based account discovery
- Providing users with a provisioning file
- Providing users with account information to enter manually

Important

Citrix recommends you to restart Citrix Receiver for Windows after the installation. This is to ensure that users can add accounts and that Citrix Receiver for Windows can discover USB devices that were in a suspended state during installation.

A dialog appears indicating a successful installation, followed by the **Add Account** dialog. For a first time user, the **Add Account** dialog requires you to enter an email or server address to setup an account.

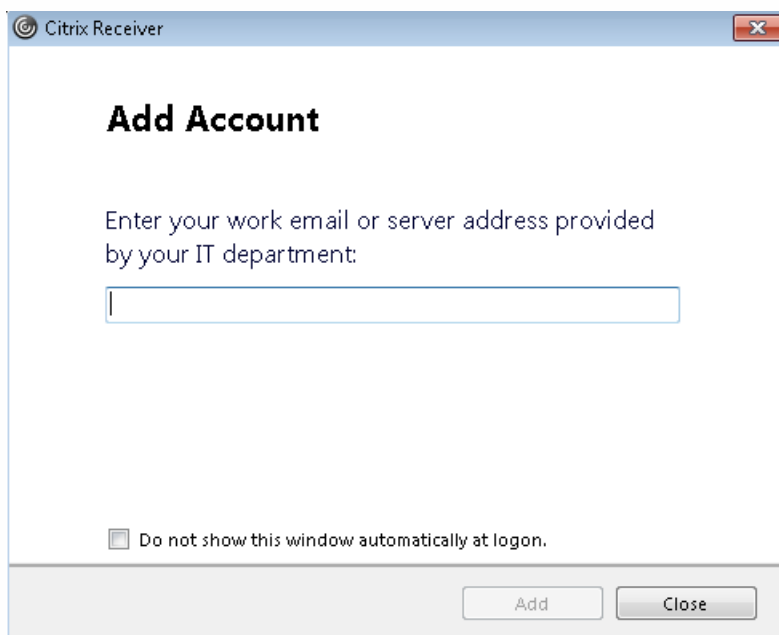
Suppressing Add Account dialog

Add Account dialog is displayed when the store is not configured. Users can use this window to set up a Citrix Receiver account by entering email address or a server URL.

Citrix Receiver for Windows determines the NetScaler Gateway, StoreFront server, or AppController virtual appliance associated with the email address and then prompts the user to log on for enumeration.

Add account dialog can be suppressed in the following ways:

1. At system logon



Select **Do not show this window automatically at logon** to prevent the Add Account window to pop-up on subsequent logon.

This setting is specific to per user and resets during Citrix Receiver for Windows Reset action.

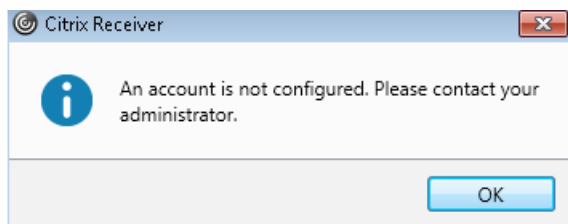
2. Command line Installation

Install Citrix Receiver for Windows as an administrator using Command Line Interface with the following switch.

CitrixReceiver.exe /ALLOWADDSTORE=N

This is a per machine setting; hence the behavior shall be applicable for all users.

The following message is displayed when Store is not configured.



Additionally, Add Account dialog can be suppressed in the following ways.

NOTE: Citrix recommends users to suppress the Add Account dialog either using System logon or Command Line Interface methods.

- **Renaming Citrix execution file:**

Rename the **CitrixReceiver.exe** to **CitrixReceiverWeb.exe** to alter the behavior of Add Account dialog. By renaming the file, Add Account dialog is not displayed from the Start menu.

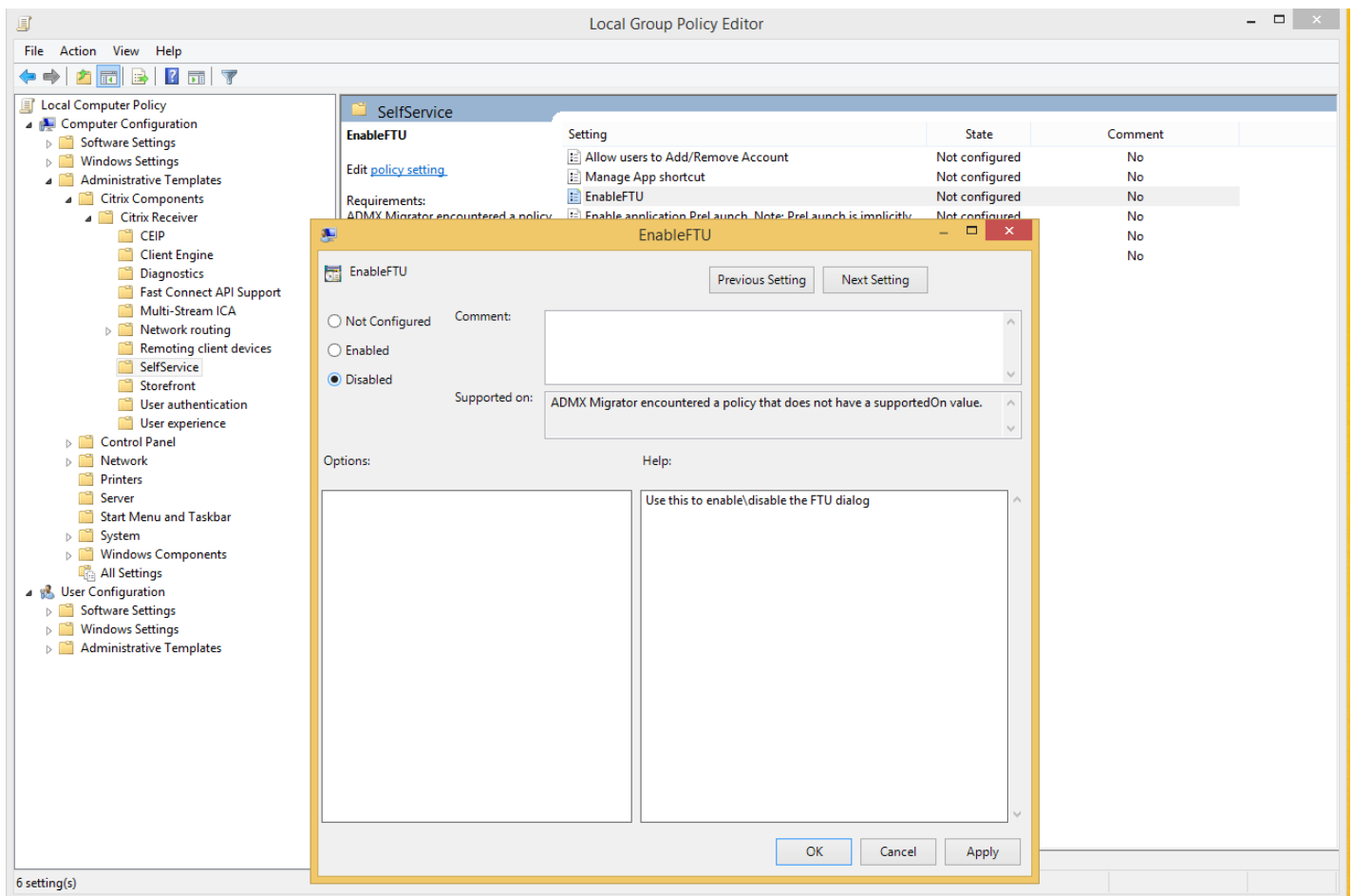
See [Deploy Receiver for Windows from Receiver for Web](#) for more information related to Citrix Receiver for Web

- **Group Policy Object:**

To hide Add Account button from the Citrix Receiver for Windows installation wizard, disable **EnableFTUpolicy** under Self-Service node in Local Group Policy editor as shown below.

This is per machine setting, hence the behavior shall be applicable for all users.

To load template file, see [Configure Receiver with the Group Policy Object template](#).



Configure email-based account discovery

When you configure Citrix Receiver for Windows for email-based account discovery, users enter their email address rather than a server URL during initial Citrix Receiver for Windows installation and configuration. Citrix Receiver for Windows determines the NetScaler Gateway or StoreFront Server associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access virtual desktops and applications.

Note

Email-based account discovery is not supported for deployments with Web Interface.

To configure your DNS server to support email-based discovery, see [Configure email-based account discovery](#) in the StoreFront documentation.

To configure NetScaler Gateway, see [Connecting to StoreFront by using email-based discovery](#) in the NetScaler Gateway documentation.

Provide users with provisioning files

StoreFront provides provisioning files that users can open to connect to stores.

You can use StoreFront to create provisioning files containing connection details for accounts. Make these files available to

your users to enable them to configure Citrix Receiver for Windows automatically. After installing Citrix Receiver for Windows, users simply open the file to configure Citrix Receiver for Windows. If you configure Citrix Receiver for Web sites, users can also obtain Citrix Receiver for Windows provisioning files from those sites.

- For more information, see [To export store provisioning files for users](#) in the StoreFront documentation.

Provide users with account information to enter manually

To enable users to set up accounts manually, be sure to distribute the information they need to connect to their virtual desktops and applications.

- For connections to a StoreFront store, provide the URL for that server. For example: `https://servername.company.com`. For web interface deployments, provide the URL for the XenApp Services site.
- For connections through NetScaler Gateway, first determine whether user should see all configured stores or just the store that has remote access enabled for a particular NetScaler Gateway.
 - To present all configured stores: Provide users with the NetScaler Gateway fully-qualified domain name.
 - To limit access to a particular store: Provide users with the NetScaler Gateway fully-qualified domain name and the store name in the form:

NetScalerGatewayFQDN?MyStoreName

For example, if a store named "SalesApps" has remote access enabled for server1.com and a store named "HRApps" has remote access enabled for server2.com, a user must enter `server1.com?SalesApps` to access SalesApps or enter `server2.com?HRApps` to access HRApps. This feature requires that a first-time user create an account by entering a URL and is not available for email-based discovery.

When a user enters the details for a new account, Citrix Receiver for Windows attempts to verify the connection. If successful, Citrix Receiver for Windows prompts the user to log on to the account.

To manage accounts, a Citrix Receiver user opens the Citrix Receiver for Windows home page, clicks , and then clicks **Accounts**.

Sharing multiple store accounts automatically

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.

If you have more than one store account, you can configure Citrix Receiver for Windows to automatically connect to all accounts when establishing a session. To automatically view all accounts when opening Citrix Receiver for Windows:

For 32-bit systems, create the key "CurrentAccount":

Location: HKLM\Software\Citrix\Dazzle

KeyName: CurrentAccount

Value: AllAccount

Type: REG_SZ

For 64-bit systems, create the key "CurrentAccount":

Location: HKLM\Software\Wow6432Node\Citrix\Dazzle

KeyName: CurrentAccount

Value: AllAccount

Type: REG_SZ

Optimize the environment

Mar 07, 2017

You can optimize the environment.

- Reduce application launch time
- Facilitate the connection of devices to published resources
- Support DNS name resolution
- Use proxy servers with XenDesktop connections
- [Provide support for NDS users](#)
- [Use Receiver with XenApp for UNIX](#)
- Enable access to anonymous applications
- Checking Single-Sign on configuration

For information about other optimization options, refer to topics in the XenDesktop documentation related to maintaining session activity and optimizing the user HDX experience.

Reducing application launch time

Dec 06, 2016

Use the session pre-launch feature to reduce application launch time during normal or high traffic periods, thus providing users with a better experience. The pre-launch feature allows a pre-launch session to be created when a user logs on to Citrix Receiver for Windows, or at a scheduled time if the user is already logged on.

This pre-launch session reduces the launch time of the first application. When a user adds a new account connection to Citrix Receiver for Windows, session pre-launch does not take effect until the next session. The default application `ctxprelaunch.exe` is running in the session, but it is not visible to the user.

Session pre-launch is supported for StoreFront deployments as of the StoreFront 2.0 release. For Web Interface deployments, be sure to use the Web Interface Save Password option to avoid logon prompts. Session pre-launch is not supported for XenDesktop 7 deployments.

Session pre-launch is disabled by default. To enable session pre-launch, specify the `ENABLEPRELAUNCH=true` parameter on the Receiver command line or set the `EnablePreLaunch` registry key to true. The default setting, null, means that pre-launch is disabled.

Note: If the client machine has been configured to support Domain Passthrough (SSON) authentication, then prelaunch is automatically enabled. If you want to use Domain Passthrough (SSON) without prelaunch, then set the `EnablePreLaunch` registry key value to false.

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.

The registry locations are:

`HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\Dazzle`

`HKEY_CURRENT_USER\Software\Citrix\Dazzle`

There are two types of pre-launch:

- **Just-in-time pre-launch.** Pre-Launch starts immediately after the user's credentials are authenticated whether or not it is a high-traffic period. Typically used for normal traffic periods. A user can trigger just-in-time pre-launch by restarting Citrix Receiver for Windows.
- **Scheduled pre-launch.** Pre-launch starts at a scheduled time. Scheduled pre-launch starts only when the user device is already running and authenticated. If those two conditions are not met when the scheduled pre-launch time arrives, a session does not launch. To spread network and server load, the session launches within a window of when it is scheduled. For example, if the scheduled pre-launch is scheduled for 1:45 p.m., the session actually launches between 1:15 p.m. and 1:45 p.m. Typically used for high-traffic periods.

Configuring pre-launch on a XenApp server consists of creating, modifying, or deleting pre-launch applications, as well as updating user policy settings that control the pre-launch application. See "To pre-launch applications to user devices" in the XenApp documentation for information about configuring session pre-launch on the XenApp server.

Customizing the pre-launch feature using the `receiver.admx` file is not supported. However, you can change the pre-launch configuration by modifying registry values during or after Citrix Receiver for Windows installation. There are three HKLM values and two HKCU values:

- The HKLM values are written during client installation.
- The HKCU values enable you to provide different users on the same machine with different settings. Users can change the HKCU values without administrative permission. You can provide your users with scripts to accomplish this.

HKEY_LOCAL_MACHINE registry values

For Windows 7 and 8, 64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

For all other supported 32-bit Windows operating systems: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

Name: UserOverride

Values:

0 - Use the HKEY_LOCAL_MACHINE values even if HKEY_CURRENT_USER values are also present.

1 - Use HKEY_CURRENT_USER values if they exist; otherwise, use the HKEY_LOCAL_MACHINE values.

Name: State

Values:

0 - Disable pre-launch.

1 - Enable just-in-time pre-launch. (Pre-Launch starts after the user's credentials are authenticated.)

2 - Enable scheduled pre-launch. (Pre-launch starts at the time configured for Schedule.)

Name: Schedule

Value:

The time (24 hour format) and days of week for scheduled pre-launch entered in the following format:

HH:MM | M:T:W:TH:F:S:SU where HH and MM are hours and minutes. M:T:W:TH:F:S:SU are the days of the week. For example, to enable scheduled pre-launch on Monday, Wednesday, and Friday at 1:45 p.m., set Schedule as Schedule=13:45 | 1:0:1:0:1:0:0 . The session actually launches between 1:15 p.m. and 1:45 p.m.

HKEY_CURRENT_USER registry values

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

The State and Schedule keys have the same values as for HKEY_LOCAL_MACHINE.

Map client devices

Mar 07, 2017

Citrix Receiver for Windows supports device mapping on user devices so they are available from within a session. Users can:

- Transparently access local drives, printers, and COM ports
- Cut and paste between the session and the local Windows clipboard
- Hear audio (system sounds and .wav files) played from the session

During logon, Citrix Receiver for Windows informs the server of the available client drives, COM ports, and LPT ports. By default, client drives are mapped to server drive letters and server print queues are created for client printers so they appear to be directly connected to the session. These mappings are available only for the current user during the current session. They are deleted when the user logs off and recreated the next time the user logs on.

You can use the redirection policy settings to map user devices not automatically mapped at logon. For more information, see the XenDesktop or XenApp documentation.

Turn off user device mappings

You can configure user device mapping including options for drives, printers, and ports, using the Windows Server Manager tool. For more information about the available options, see your Remote Desktop Services documentation.

Redirect client folders

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. For more information, including how to configure client folder redirection for user devices, see the XenDesktop 7 documentation.

Map client drives to host-side drive letters

Client drive mapping allows drive letters on the host-side to be redirected to drives that exist on the user device. For example, drive H in a Citrix user session can be mapped to drive C of the user device running Citrix Receiver for Windows.

Client drive mapping is built into the standard Citrix device redirection facilities transparently. To File Manager, Windows Explorer, and your applications, these mappings appear like any other network mappings.

The server hosting virtual desktops and applications can be configured during installation to map client drives automatically to a given set of drive letters. The default installation maps drive letters assigned to client drives starting with V and works backward, assigning a drive letter to each fixed drive and CD-ROM drive. (Floppy drives are assigned their existing drive letters.) This method yields the following drive mappings in a session:

Client drive letter	Is accessed by the server as:
A	A

Client drive letter	Is accessed by the server as:
C	V
D	U

The server can be configured so that the server drive letters do not conflict with the client drive letters; in this case the server drive letters are changed to higher drive letters. For example, changing server drives C to M and D to N allows client devices to access their C and D drives directly. This method yields the following drive mappings in a session:

Client drive letter	Is accessed by the server as:
A	A
B	B
C	C
D	D

The drive letter used to replace the server drive C is defined during Setup. All other fixed drive and CD-ROM drive letters are replaced with sequential drive letters (for example; C > M, D > N, E > O). These drive letters must not conflict with any existing network drive mappings. If a network drive is mapped to the same drive letter as a server drive letter, the network drive mapping is not valid.

When a user device connects to a server, client mappings are reestablished unless automatic client device mapping is disabled. Client drive mapping is enabled by default. To change the settings, use the Remote Desktop Services (Terminal Services) Configuration tool. You can also use policies to give you more control over how client device mapping is applied. For more information about policies, see the XenDesktop or XenApp documentation in Citrix Product Documentation.

HDX Plug and Play USB device redirection

Updated: 2015-01-27

HDX Plug and Play USB device redirection enables dynamic redirection of media devices, including cameras, scanners, media players, and point of sale (POS) devices to the server. You or the user can restrict redirection of all or some of the devices. Edit policies on the server or apply group policies on the user device to configure the redirection settings. For more information, see [USB and client drive considerations](#) in the XenApp and XenDesktop documentation.

Important: If you prohibit Plug and Play USB device redirection in a server policy, the user cannot override that policy setting. A user can set permissions in Citrix Receiver for Windows to always allow or reject device redirection or to be prompted each time a device is connected. The setting affects only devices plugged in after the user changes the setting.

To map a client COM port to a server COM port

Client COM port mapping allows devices attached to the COM ports of the user device to be used during sessions. These

mappings can be used like any other network mappings.

You can map client COM ports at the command prompt. You can also control client COM port mapping from the Remote Desktop (Terminal Services) Configuration tool or using policies. For information about policies, see the XenDesktop or XenApp documentation.

Important: COM port mapping is not TAPI-compatible.

1. For XenDesktop 7 deployments, enable the Client COM port redirection policy setting.
2. Log on to Citrix Receiver for Windows.
3. At a command prompt, type:

```
net use comx: \\client\comz:
```

where x is the number of the COM port on the server (ports 1 through 9 are available for mapping) and z is the number of the client COM port you want to map.

4. To confirm the operation, type:

```
net use
```

at a command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.

To use this COM port in a virtual desktop or application, install your user device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session. Use this mapped COM port as you would a COM port on the user device.

Supporting DNS name resolution

Dec 06, 2016

You can configure Citrix Receiver for Windows that use the Citrix XML Service to request a Domain Name Service (DNS) name for a server instead of an IP address.

Important: Unless your DNS environment is configured specifically to use this feature, Citrix recommends that you do not enable DNS name resolution in the server farm.

Citrix Receiver for Windows connecting to published applications through the Web Interface also use the Citrix XML Service. For Citrix Receiver for Windows connecting through the Web Interface, the Web server resolves the DNS name on behalf of the Citrix Receiver for Windows.

DNS name resolution is disabled by default in the server farm and enabled by default on the Citrix Receiver for Windows . When DNS name resolution is disabled in the farm, any Citrix Receiver for Windows request for a DNS name returns an IP address. There is no need to disable DNS name resolution on Citrix Receiver for Windows.

To disable DNS name resolution for specific user devices

If your server deployment uses DNS name resolution and you experience issues with specific user devices, you can disable DNS name resolution for those devices.

Caution: 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.

1. Add a string registry key `xmlAddressResolutionType` to `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing`.
2. Set the value to `IPv4-Port`.
3. Repeat for each user of the user devices.

Using proxy servers with XenDesktop

Dec 06, 2016

If you do not use proxy servers in your environment, correct the Internet Explorer proxy settings on any user devices running Internet Explorer 7.0 on Windows XP. By default, this configuration automatically detects proxy settings. If proxy servers are not used, users will experience unnecessary delays during the detection process. For instructions on changing the proxy settings, consult your Internet Explorer documentation. Alternatively, you can change proxy settings using the Web Interface. For more information, consult the [Web Interface documentation](#).

Using Configuration Checker to validate Single Sign-on configuration

Mar 13, 2017

Starting with Release 4.5 of Citrix Receiver for Windows, Configuration Checker helps users to run a test to ensure Single Sign-on is configured properly. The test runs on different checkpoints of the Single Sign-on configuration and displays the configuration results.

1. Logon to Citrix Receiver for Windows.
2. Right-click Citrix Receiver for Windows in the notification area and select **Advanced Preferences**.
The Advanced Preferences window appears.

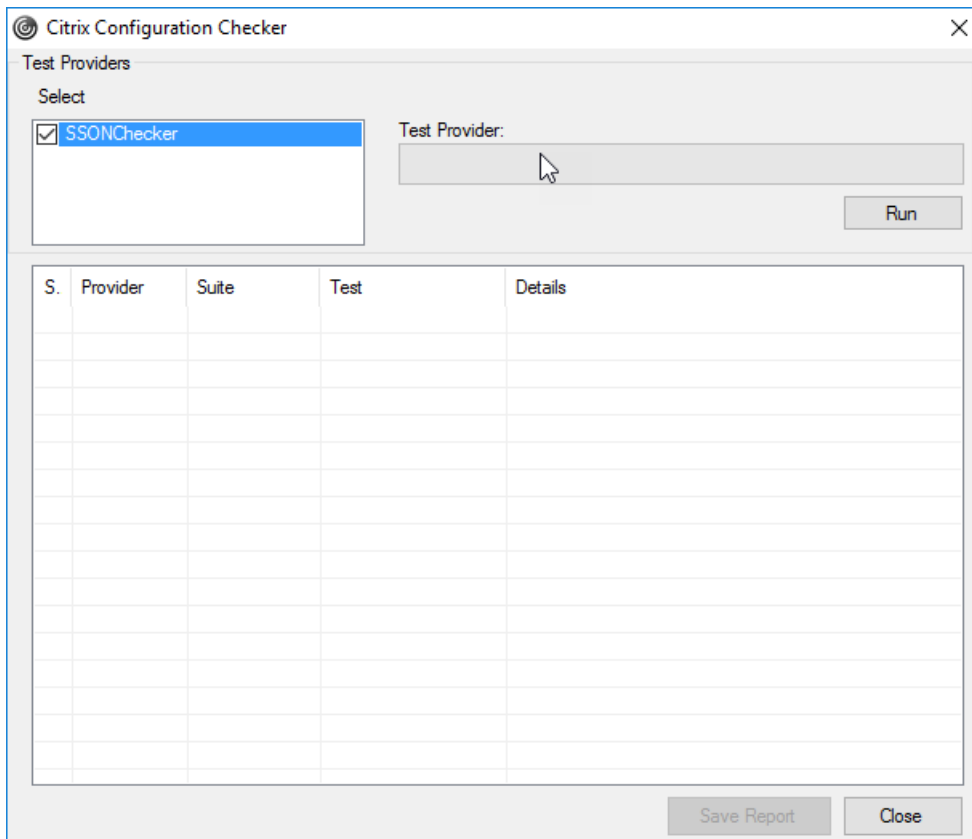
Advanced Preferences

Connection Center	NetScaler Gateway Settings
Delete Saved Passwords	Reset Receiver
Data Collection	Settings Option
Configuration Checker	Support Info

Netscaler Gateway (Default)

3. Select **Configuration Checker**.

The Citrix Configuration Checker window appears.



4. Select **SSONChecker** from the **Select** pane.
 5. Click **Run**.
- A progress bar appears, displaying the status of the test.

The Configuration Checker window has the following columns:

1. **Status:** Displays the result of a test on a specific check point.
 - A green check mark indicates that the specific checkpoint is configured properly.
 - A blue I indicates information about the checkpoint.
 - A Red X indicates that the specific checkpoint is not configured properly.
 2. **Provider:** Displays the name of the module on which the test is run. In this case, Single Sign-on.
 3. **Suite:** Indicates the category of the test. For example, Installation.
 4. **Test:** Indicates the name of the specific test that is run.
 5. **Details:** Provides additional information about the test, irrespective of pass or fail.
- The user gets more information about each checkpoint and the corresponding results.

The following tests are performed:

1. Installed with Single Sign-on
2. Logon credential capture
3. Network Provider registration

The test result against Network Provider registration displays a green check mark only when “Citrix Single Sign-on” is set to be first in the list of Network Providers. If Citrix Single Sign-on appears anywhere else in the list, the test result against Network Provider registration appears with a blue I and additional information.

4. Single Sign-on process is running
5. Group Policy

By default, this policy is configured on the client.

6. Internet Settings for Security Zones

Ensure that you add the Store/XenApp Service URL to the list of Security Zones in the Internet Options.

If the Security Zones is configured via Group policy, any change in the policy requires the Advanced Preference window to be reopened for the changes to take effect and to display the correct status of the test.

7. Authentication method for Web Interface/StoreFront.

Note: If the user is accessing Receiver for Web, the test results are not applicable.

If Citrix Receiver for Windows is configured with multiple stores, the authentication method test runs on all configured stores.

Note: The test results can be saved as reports and the default format for the report is .txt.

Hiding the Configuration Checker option from the Advanced Preferences dialog

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer, or by using the Group Policy Management Console when applying domain policies.
2. In the Group Policy Editor, go to Citrix Components > Citrix Receiver > Self Service > DisableConfigChecker.
3. Select **Enabled**.
This hides the Configuration Checker option from the Advanced Preferences window.
4. Click Apply and OK.
5. Open a command prompt.
6. Run gpupdate /force command.

For the changes to take effect, close and reopen the Advance Preferences dialog.

Limitations

Configuration Checker does not include the checkpoint for the configuration of Trust requests sent to the XML service on XenApp/XenDesktop servers.

Improve the user experience

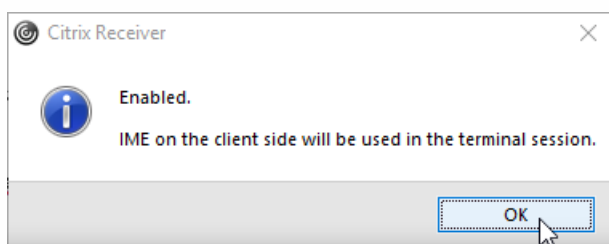
Feb 23, 2017

You can improve your user experience with the following features:

Configuring generic client Input Method Editors (IME)

Configuring generic client IME using the command line interface

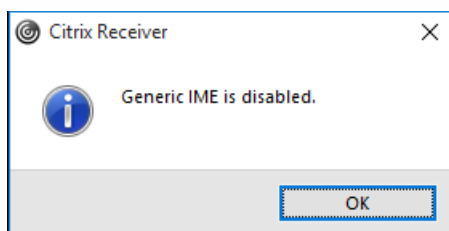
To enable generic client IME, run the **wfica32.exe /localime:on** command from the Citrix Receiver for Windows installation folder (C:\Program Files (x86)\Citrix\ICA Client).



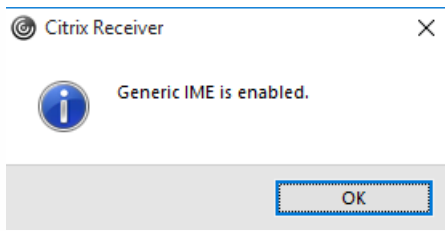
Note

You can use the command line switch **wfica32.exe /localime:on** to enable both generic client IME and keyboard layout synchronization.

To disable generic client IME, run the **wfica32.exe /localgenericime:off** command from the Citrix Receiver for Windows installation folder (C:\Program Files (x86)\Citrix\ICA Client). This command does not affect keyboard layout synchronization settings.



If you have disabled generic client IME using the command line interface, you can enable the feature again by running the **wfica32.exe /localgenericime:on** command.



Toggle

Citrix Receiver for Windows supports toggle functionality for this feature. You can run the **wfica32.exe /localgenericime:on** command to enable or disable the feature. However, the keyboard layout synchronization settings take precedence over the toggle switch. If keyboard layout synchronization is set to **Off**, toggling does not enable generic client IME.

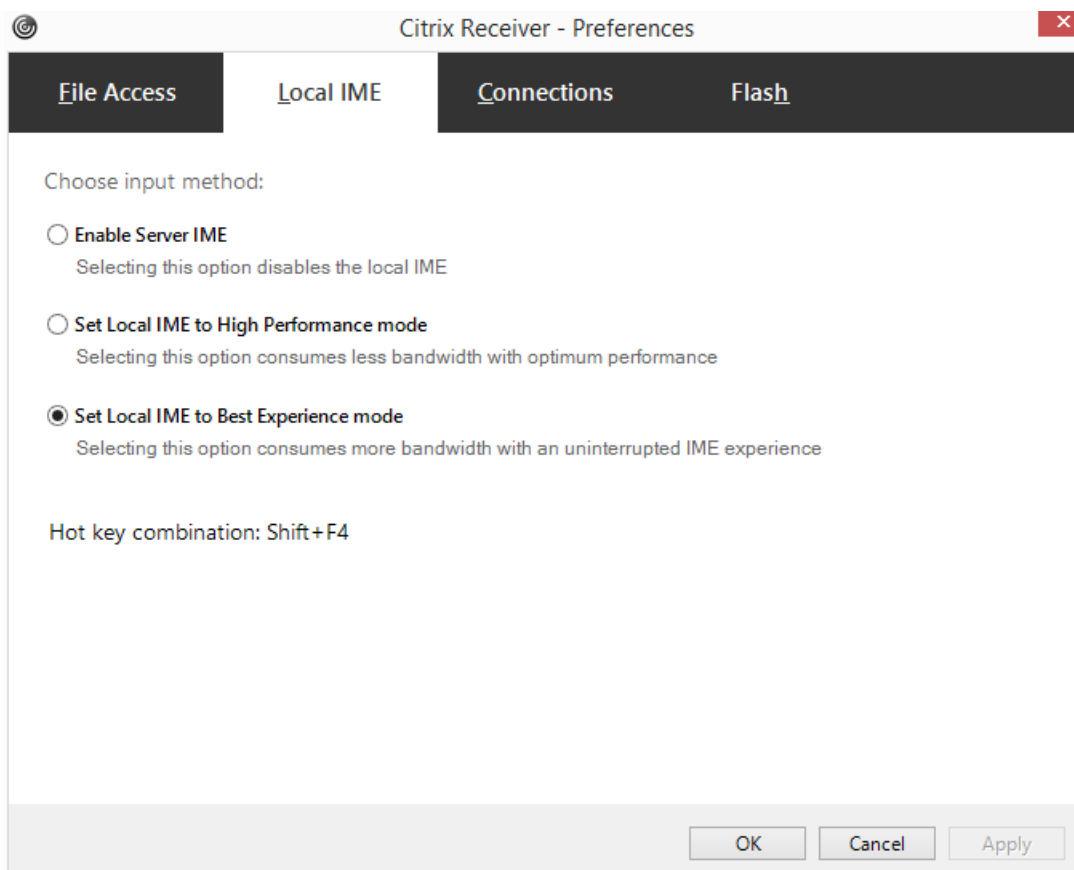
Configuring generic client IME using the graphical user interface

Generic client IME requires VDA Version 7.13 or later.

Generic client IME feature can be enabled by enabling keyboard layout synchronization. For more information, see [Keyboard layout synchronization](#).

Citrix Receiver for Windows allows you to configure different options to use generic client IME. You can select from one of these options based on your requirements and usage.

1. In an active application session, right-click the Citrix Receiver icon in the notification area and select **Connection Center**.
2. Select **Preferences** and click **Local IME**.



The options below are available to support different IME modes:

1. **Enable Server IME** – select this option to disable local IME. This option means that only the languages set on the server can be used.
2. **Set Local IME to High Performance mode** – select this option to use local IME with limited bandwidth. This option restricts the candidate window functionality.
3. **Set Local IME to Best Experience mode** – select this option to use local IME with best user experience. This option consumes high bandwidth. By default, this option is selected when generic client IME is enabled.

The change in settings is applied only in the current session.

Enabling hotkey configuration using a registry editor

When generic client IME is enabled, you can use the **Shift+F4** hotkeys to select different IME modes. The different options for IME modes appear in the top-right corner of the session.

By default, the hotkey for generic client IME is disabled.

In the registry editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys.

Select **AllowHotKey** and change the default value to 1.

Local IME Off

High IME Performance

Best IME Experience

Note

Hotkey functionality is supported in both desktop and application sessions.

Limitations

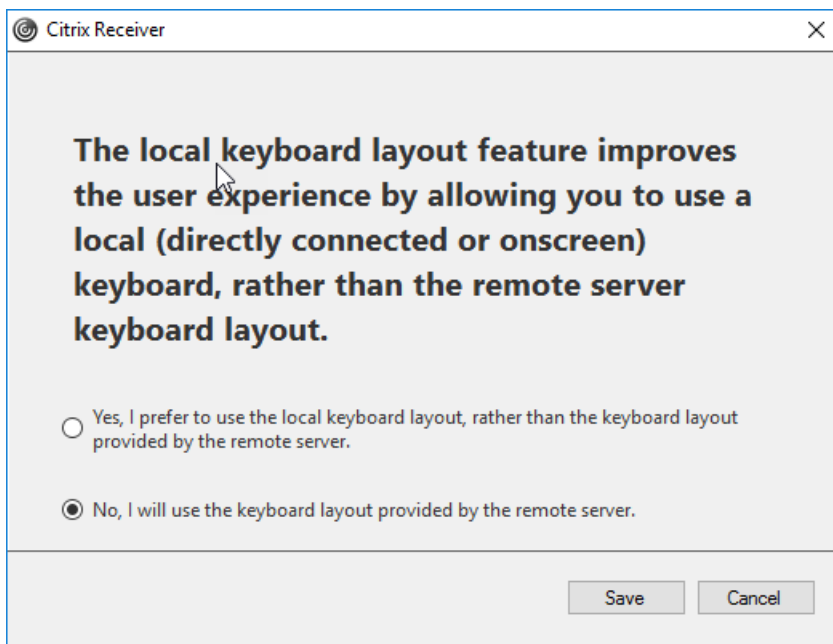
1. Generic client IME does not support UWP (Universal Windows Platform) apps such as Search UI, and the Edge browser of the Windows 10 operating system. As a workaround, use the server IME instead.
2. Generic client IME is not supported on Internet Explorer Version 11 in Protected Mode. As a workaround, you can disable Protected Mode by using **Internet Options**. To do this, click **Security** and clear **Enable Protected Mode**.

Keyboard layout

Keyboard layout synchronization enables users to switch among preferred keyboard layouts on the client device. This feature is disabled by default.

To enable keyboard layout synchronization:

1. From the Citrix Receiver for Windows notification area icon, select **Advanced Preferences > Local keyboard layout setting > Yes**.



2. Click **Save**.

You can disable the feature by selecting **No**.

You can also enable and disable keyboard layout synchronization through the command line by running **wfica32.exe /localime:on** or **wfica32.exe /localime:off** from the Citrix Receiver for Windows installation folder (C:\program files (x86)\Citrix\ICA Client).

Note: Using the local keyboard layout option activates the Client IME (Input Method Editor). If users working in Japanese, Chinese or Korean prefer to use the Server IME, they must disable the local keyboard layout option by selecting **No**, or running **wfica32.exe /localime:off**. The session will revert to the keyboard layout provided by the remote server when they connect to the next session.

Sometimes, switching the client keyboard layout does not take effect in an active session. To resolve this issue, log off from Citrix Receiver for Windows and login again.

Limitations:

- Remote applications which run with elevated privilege (for example, right click an application icon > Run as administrator) can't be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the server side (VDA) or disable UAC.
- If the user changes the keyboard layout on the client to a layout which is not supported on the server, then the keyboard layout synchronization feature will be disabled for security reasons - an unrecognized keyboard layout is treated as a potential security threat. To restore the keyboard layout synchronization feature, the user should log off and back on to the session.
- When RDP is deployed as an application and the user is working within an RDP session, it is not possible to change the keyboard layout using Alt + Shift shortcuts. To work around this, the user can use the language bar in the RDP session to switch the keyboard layout.
- This feature is disabled in Windows Server 2016 due to a third-party issue which may introduce performance risk. The feature can be enabled with a registry setting on the VDA: in HKLM\Software\Citrix\ICA\Icalme, add a new key called DisableKeyboardSync and set the value to 0.

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.

Relative Mouse

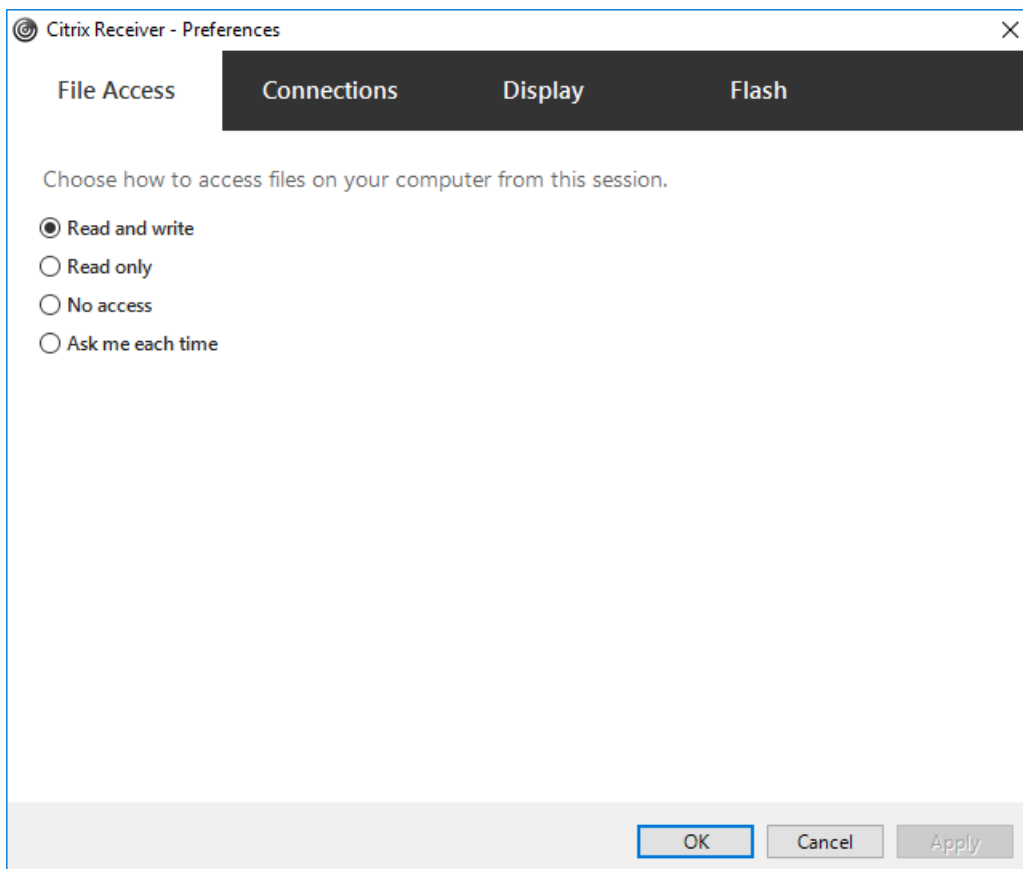
Relative Mouse support provides an option to interpret the mouse position in a relative rather than an absolute manner. This capability is required for applications that demand relative mouse input rather than absolute.

Note: This feature can be applied in a published desktop session only.

To enable Relative Mouse support

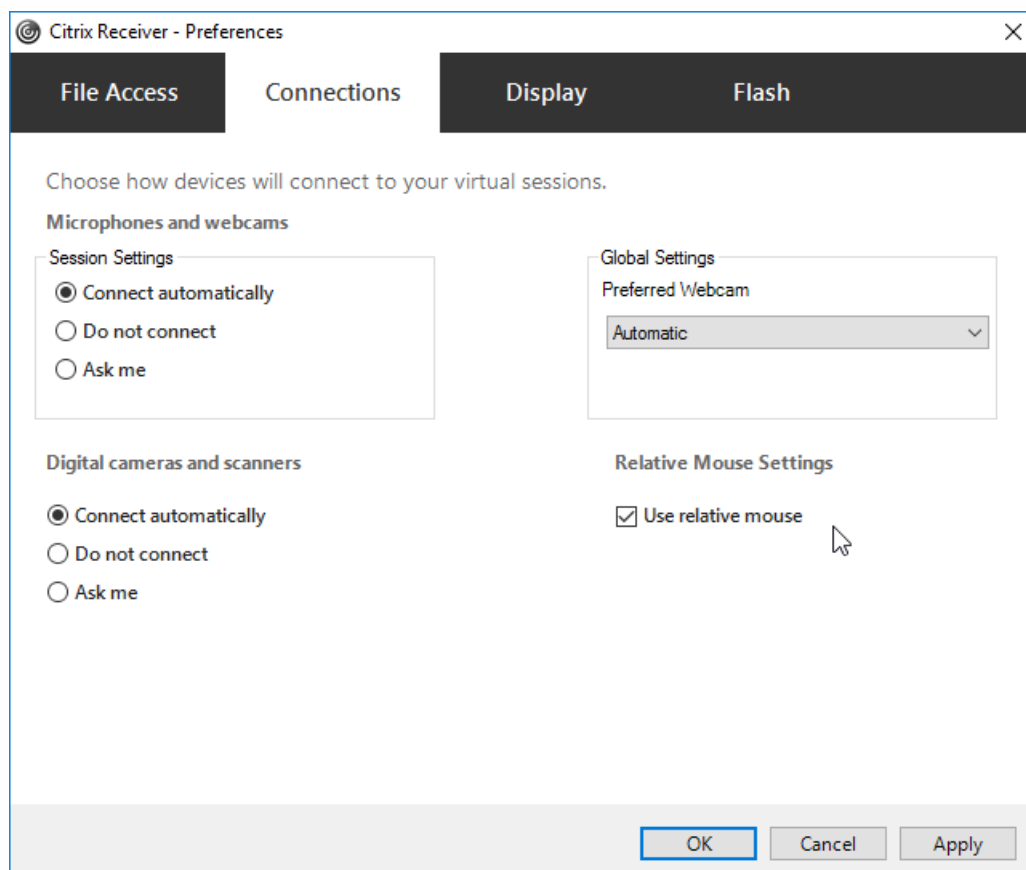
1. Logon to Citrix Receiver for Windows
2. Launch a published desktop session
3. From the Desktop Viewer toolbar, select **Preferences**.

The Citrix Receiver - Preferences window appears.



4. Select Connections.

5. Under Relative Mouse settings, enable **Use relative mouse**.



6. Click **Apply** and **OK**.

NOTE: This is a per session feature. It does not persist after reconnecting to a disconnected session. Users must re-enable the feature every time they connect or reconnect to the published desktop.

Hardware decoding

When using Citrix Receiver for Windows (with HDX engine 14.4), the GPU can be used for H.264 decoding wherever it is available at the client. The API layer used for GPU decoding is [DXVA](#) (DirectX Video Acceleration).

For more information, see [Improved User Experience: Hardware Decoding for Citrix Windows Receiver](#).

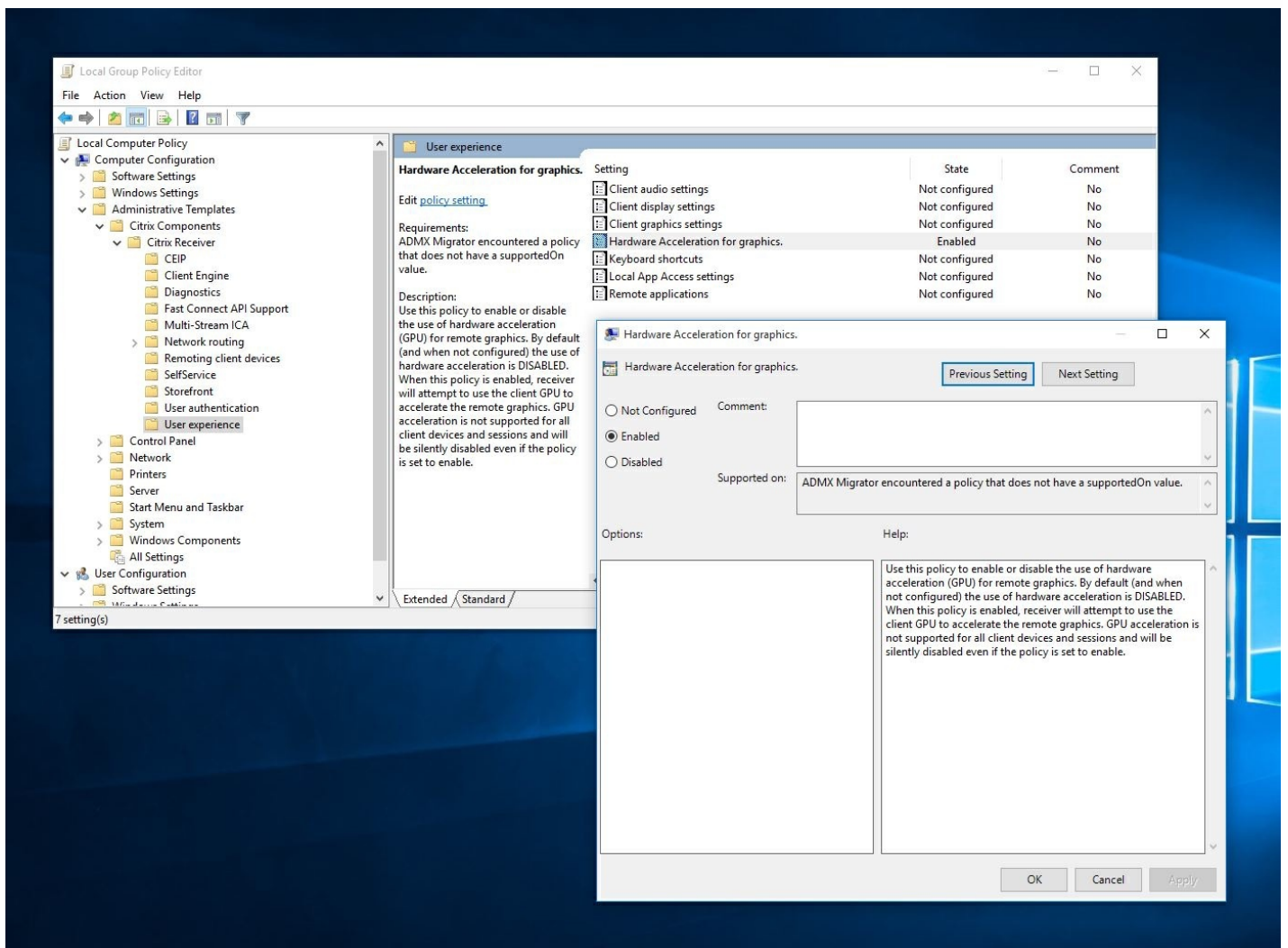
Note

This feature is not enabled by default for embedded GPUs.

To enable hardware decoding:

1. Copy "receiver.adml" from "root\Citrix\ICA Client\Configuration\en" to "C:\Windows\PolicyDefinitions\en-US".
2. Copy "receiver.admx" from "root\Citrix\ICA Client\Configuration" to "C:\Windows\PolicyDefinitions\".

3. Navigate to **Local Group policy editor**.
4. Under Computer Configuration-> Administrative Templates -> Citrix Receiver -> User Experience, open **Hardware Acceleration for graphics**.
5. Select **Enabled** and click **OK**.



To validate if the policy was applied and hardware acceleration is being used for an active ICA session, look for the following registry entries:

Registry Path: HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\<session ID>

Tip

The value for **Graphics_GfxRender_Decoder** and **Graphics_GfxRender_Renderer** should be 2. If the value is 1, that means CPU based decoding is being used.

When using the hardware decoding feature, consider the following limitations:

- If the client has two GPU's and if one of the monitors is active on the 2nd GPU, CPU decoding will be used.

- When connecting to a XenApp 7.x server running on Windows Server 2008 R2, Citrix recommends that you do not to use hardware decoding on the user's Windows device. If enabled, issues like slow performance while highlighting text and flickering issues will be seen.

Client-side microphone input

Citrix Receiver for Windows supports multiple client-side microphone input. Locally installed microphones can be used for:

- Real-time activities, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Citrix Receiver for Windows users can select whether to use microphones attached to their device by changing a Connection Center setting. XenDesktop users can also use the XenDesktop Viewer Preferences to disable their microphones and webcams.

Multi-monitor support

You can use up to eight monitors with Citrix Receiver for Windows.

Each monitor in a multiple monitor configuration has its own resolution designed by its manufacturer. Monitors can have different resolutions and orientations during sessions.

Sessions can span multiple monitors in two ways:

- Full screen mode, with multiple monitors shown inside the session; applications snap to monitors as they would locally.
XenDesktop: To display the Desktop Viewer window across any rectangular subset of monitors, resize the window across any part of those monitors and click **Maximize**.
- Windowed mode, with one single monitor image for the session; applications do not snap to individual monitors.

XenDesktop: When any desktop in the same assignment (formerly "desktop group") is launched subsequently, the window setting is preserved and the desktop is displayed across the same monitors. Multiple virtual desktops can be displayed on one device provided the monitor arrangement is rectangular. If the primary monitor on the device is used by the XenDesktop session, it becomes the primary monitor in the session. Otherwise, the numerically lowest monitor in the session becomes the primary monitor.

To enable multi-monitor support, ensure the following:

- The user device is configured to support multiple monitors.
- The user device operating system must be able to detect each of the monitors. On Windows platforms, to verify that this detection occurs, on the user device, view the Settings tab in the Display Settings dialog box and confirm that each monitor appears separately.
- After your monitors are detected:
 - **XenDesktop:** Configure the graphics memory limit using the Citrix Machine Policy setting Display memory limit.
 - **XenApp:** Depending on the version of the XenApp server you have installed:
 - Configure the graphics memory limit using the Citrix Computer Policy setting Display memory limit.
 - From the Citrix management console for the XenApp server, select the farm and in the task pane, select Modify Server Properties > Modify all properties > Server Default > HDX Broadcast > Display (or Modify Server Properties > Modify all properties > Server Default > ICA > Display) and set the Maximum memory to use for each session's graphics.

Ensure the setting is large enough (in kilobytes) to provide sufficient graphic memory. If this setting is not high enough, the

published resource is restricted to the subset of the monitors that fits within the size specified.

For information about calculating the session's graphic memory requirements for XenApp and XenDesktop, see Knowledge Center article [CTX115637](#).

Printer setting overrides on devices

If the Universal printing optimization defaults policy setting Allow non-administrators to modify these settings is enabled, users can override the Image Compression and Image and Font Caching options specified in that policy setting.

To override the printer settings on the user device

1. From the Print menu available from an application on the user device, choose Properties.
2. On the Client Settings tab, click Advanced Optimizations and make changes to the Image Compression and Image and Font Caching options.

On-screen keyboard control

To enable touch-enabled access to virtual applications and desktops from Windows tablets, Citrix Receiver for Windows automatically displays the on-screen keyboard when you activate a text entry field, and when the device is in tent or tablet mode.

On some devices and in some circumstances, Citrix Receiver for Windows cannot accurately detect the mode of the device, and the on-screen keyboard may appear when you do not want it to.

To suppress the on-screen keyboard from appearing when using a convertible device, create a REG_DWORD value DisableKeyboardPopup in HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver and set the value to 1.

Note: On a x64 machine, create the value in HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

The keys can be set to 3 different modes as given below:

- **Automatic:** AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Always popup** (on-screen keyboard): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Never popup** (on-screen keyboard): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

Keyboard shortcuts

You can configure combinations of keys that Receiver interprets as having special functionality. When the keyboard shortcuts policy is enabled, you can specify Citrix Hotkey mappings, behavior of Windows hotkeys, and keyboard layout for sessions.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

Note: If you already imported the Citrix Receiver for Windows template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Receiver Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select the Citrix Receiver for Windows template file.

Note: Depending on the version of the Windows Operating System, select the Citrix Receiver for Windows template file (receiver.adm or receiver.admx/receiver.adml).

5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Experience > Keyboard shortcuts.
7. From the Action menu, choose Properties, select Enabled, and choose the desired options.

Citrix Receiver for Windows support for 32-bit color icons

Citrix Receiver for Windows supports 32-bit high color icons and automatically selects the color depth for applications visible in the Citrix Connection Center dialog box, the Start menu, and task bar to provide for seamless 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.

To set a preferred depth, you can add a string registry key named TWIDesiredIconColor to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences and set it to the desired value. The possible color depths for icons are 4, 8, 16, 24, and 32 bits-per-pixel. The user can select a lower color depth for icons if the network connection is slow.

Enabling Desktop Viewer

Different enterprises have different corporate needs. Your requirements for the way users access virtual desktops may vary from user to user and may vary as your corporate needs evolve. The user experience of connecting to virtual desktops and the extent of user involvement in configuring the connections depend on how you set up Citrix Receiver for Windows.

Use the **Desktop Viewer** when users need to interact with their virtual desktop. The user's virtual desktop can be a published virtual desktop, or a shared or dedicated desktop. In this access scenario, the Desktop Viewer toolbar functionality allows the user to open a virtual desktop in a window and pan and scale that desktop inside their local desktop. Users can set preferences and work with more than one desktop using multiple XenDesktop connections on the same user device.

Note: Your users must use Citrix Receiver for Windows to change the screen resolution on their virtual desktops. They cannot change Screen Resolution using Windows Control Panel.

Keyboard input in Desktop Viewer sessions

In Desktop Viewer sessions, Windows logo key+L is directed to the local computer.

Ctrl+Alt+Delete is directed to the local computer.

Key presses that activate StickyKeys, FilterKeys, and ToggleKeys (Microsoft accessibility features) are normally directed to the local computer.

As an accessibility feature of the Desktop Viewer, pressing Ctrl+Alt+Break displays the Desktop Viewer toolbar buttons in a pop-up window.

Ctrl+Esc is sent to the remote, virtual desktop.

Note: By default, if the Desktop Viewer is maximized, Alt+Tab switches focus between windows inside the session. If the Desktop Viewer is displayed in a window, Alt+Tab switches focus between windows outside the session.

Hotkey sequences are key combinations designed by Citrix. For example, the Ctrl+F1 sequence reproduces Ctrl+Alt+Delete, and Shift+F2 switches applications between full-screen and windowed mode. You cannot use hotkey sequences with virtual desktops displayed in the Desktop Viewer (that is, with XenDesktop sessions), but you can use them with published applications (that is, with XenApp sessions).

Connect to virtual desktops

From within a desktop session, users cannot connect to the same virtual desktop. Attempting to do so will disconnect the existing desktop session. Therefore, Citrix recommends:

- Administrators should not configure the clients on a desktop to point to a site that publishes the same desktop
- Users should not browse to a site that hosts the same desktop if the site is configured to automatically reconnect users to existing sessions
- Users should not browse to a site that hosts the same desktop and try to launch it

Be aware that a user who logs on locally to a computer that is acting as a virtual desktop blocks connections to that desktop.

If your users connect to virtual applications (published with XenApp) from within a virtual desktop and your organization has a separate XenApp administrator, Citrix recommends working with them to define device mapping such that desktop devices are mapped consistently within desktop and application sessions. Because local drives are displayed as network drives in desktop sessions, the XenApp administrator needs to change the drive mapping policy to include network drives.

Changing the status indicator time-out

You can change the amount of time the status indicator displays when a user is launching a session. To alter the time out period, create a REG_DWORD value SI_INACTIVE_MS in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\.. The REG_DWORD value can be set to 4 if you want the status indicator to disappear sooner.

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.

Secure connections

Mar 07, 2017

To maximize the security of your environment, the connections between Citrix Receiver for Windows and the resources you publish must be secured. You can configure various types of authentication for your Citrix Receiver for Windows software, including smart card authentication, certificate revocation list checking, and Kerberos pass-through authentication.

Windows NT Challenge/Response (NTLM) authentication is supported by default on Windows computers.

Configure domain pass-through authentication

Apr 10, 2017

For information on configuring domain pass-through authentication, see Knowledge Center article [CTX133982](#).

Citrix Receiver for Windows installation with Single Sign-on

There are two ways to enable domain pass-through (SSON) when installing Citrix Receiver for Windows:

- using the command line installation
- using the graphical user interface

Enable domain pass-through using the command line interface

To enable domain pass-through (SSON) using the command line interface:

1. Install Citrix Receiver 4.x with the **/includeSSON** switch.
 - Install one or more StoreFront stores (you can complete this step at a later stage); installing StoreFront stores is not a prerequisite for setting up domain pass-through authentication.
 - Verify that pass-through authentication is enabled by starting Citrix Receiver, then confirm that the `ssonsvr.exe` process is running in Task Manager after rebooting the end point where Citrix Receiver is installed.

Note

For information on the syntax for adding one or more StoreFront stores, see [Configure and install Receiver for Windows using command-line parameters](#).

Enable domain pass-through using the graphical user interface

To enable domain pass-through using the graphical user interface:

1. Locate the Citrix Receiver for Windows installation file (CitrixReceiver.exe).
2. Double click **CitrixReceiver.exe** to launch the installer.
3. In the Enable Single Sign-on installation wizard, select the Enable single sign-on checkbox to install Citrix Receiver for Windows with the SSON feature enabled; this is equivalent to installing Citrix Receiver for Windows using the command line switch **/includeSSON**.

The image below illustrates how to enable Single Sign-on:



Note

The Enable Single Sign-on installation wizard is available only for fresh installation on a domain joined machine.

Verify that pass-through authentication is enabled by restarting Citrix Receiver for Windows, and then confirm that the **ssonsvr.exe** process is running in Task Manager after rebooting the endpoint on which Citrix Receiver for Windows is installed.

Group policy settings for SSON

Use the information in this section to configure group policy settings for SSON authentication.

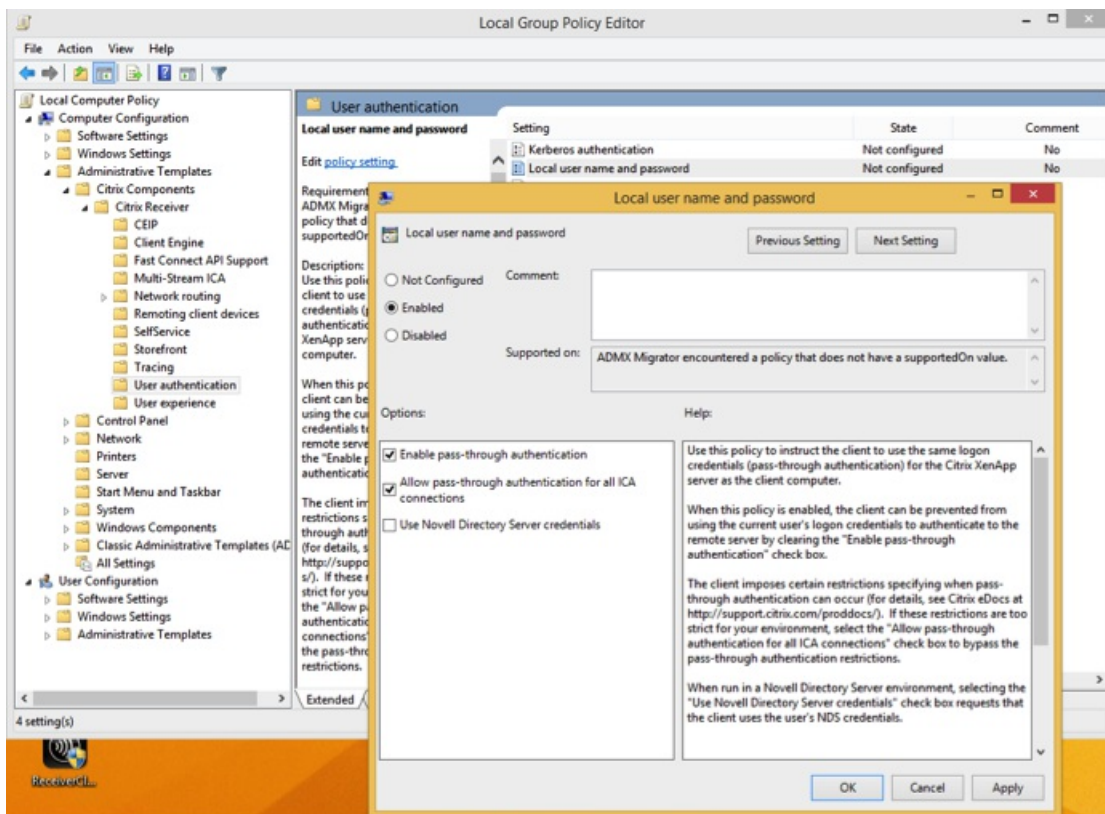
Note

The default value of the GPO policy setting related to SSON is **Enable pass-through authentication**.

Using a Citrix Receiver for Windows template file for SSON group policy

Use the following procedure to configure group policy settings using an ADMX file:

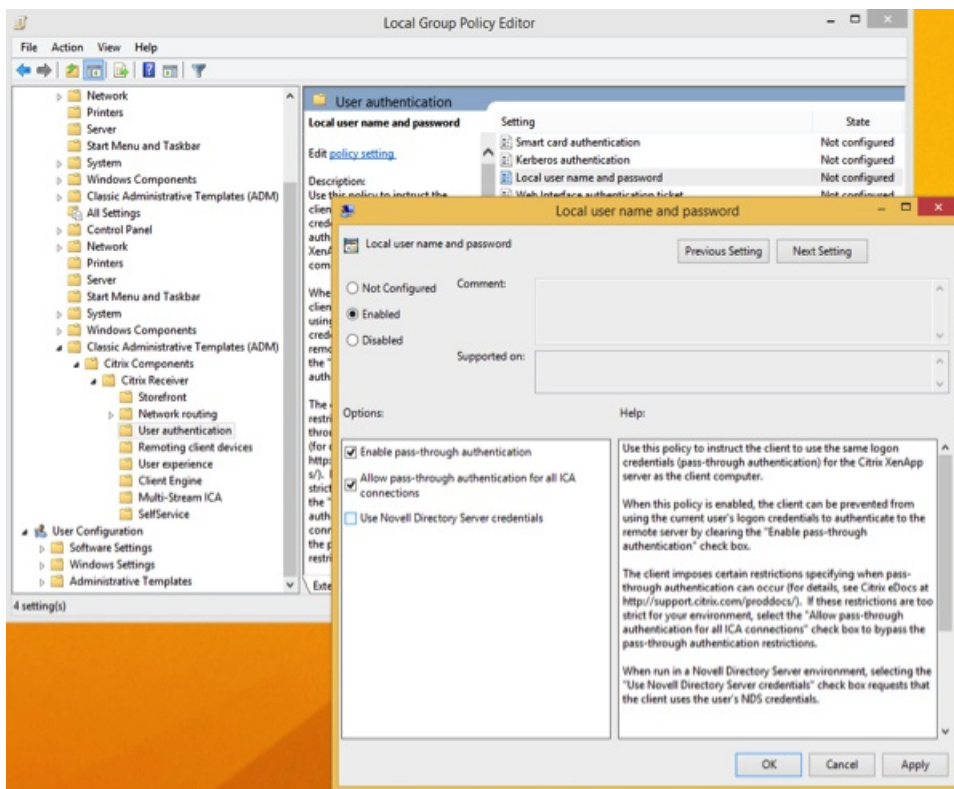
1. Load group policy files. For installations using Citrix Receiver for Windows 4.3 and later, use **receiver.ADMX** or **receiver.ADML** located in the %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration folder.
2. Open **gpedit.msc**, right-click **Computer Configuration > Administrative Templates - > Citrix Component-> Citrix Receiver->User Authentication**.
3. Enable the following local computer GPO settings (on the user's local machine and/or on the VDA desktop golden image):
 - Choose the local user name and password.
 - Select **Enabled**.
 - Select **Enable pass-through authentication**.
4. Reboot the end point (on which Citrix Receiver for Windows is installed) or the VDA desktop golden image.



Using an ADM file for SSON group policy

Use the following procedure to configure group policy settings using an ADM file:

1. Open the local group policy editor by selecting **Computer Configuration > Right-click Administrative Templates > Choose Add/Remove Templates**.
2. Click **Add** to add a ADM template.
3. After successfully adding the **receiver.adm** template, expand **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication**.



4. Open Internet Explorer on the local machine and/or on the VDA desktop golden image.

5. In **Internet Settings > Security > Trusted Sites**, add the StoreFront server(s) fully qualified domain name (FQDN), without the store path, to the list. For example, <https://storefront.example.com>.

Note

You can also add the StoreFront server to the Trusted Sites using a Microsoft GPO. The GPO is called **Site to Zone Assignment List**; you can find this list in **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page**.

6. Log off, and log back on to the Citrix Receiver endpoint.

When Citrix Receiver opens, if the current user is logged on to the domain, the user's credentials are passed through to StoreFront, along with enumerated apps and desktops within Citrix Receiver, including the user's Start menu settings. When the user clicks an icon, Citrix Receiver passes through the user's domain credentials to the Delivery Controller and the app (or desktop) opens.

Enable Delivery Controller to trust XML

Use the following procedure to configure SSON on StoreFront and Web Interface:

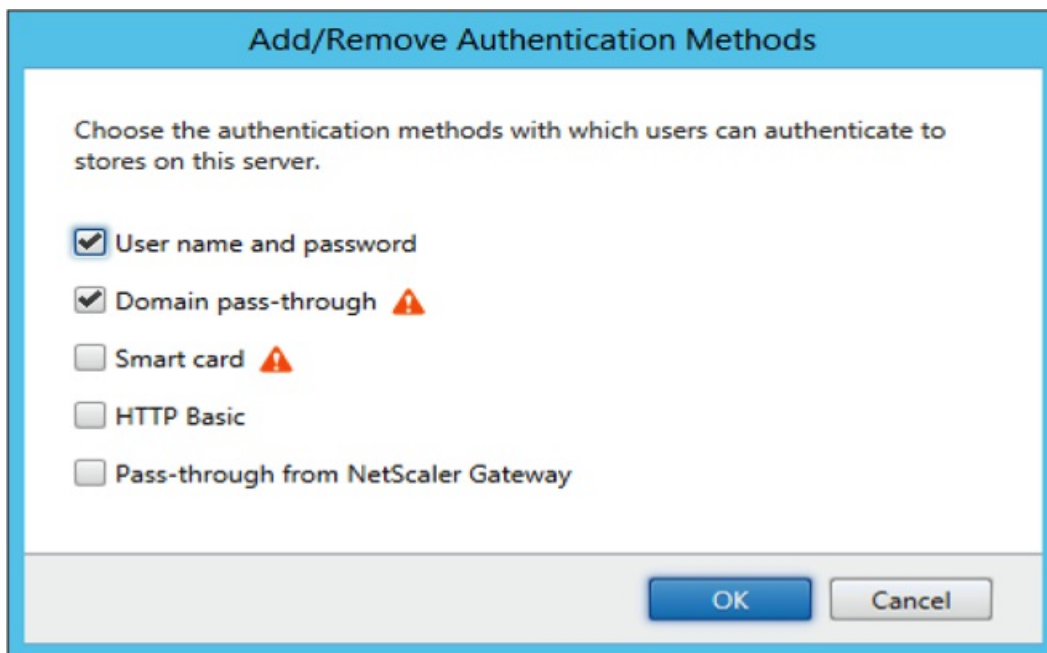
1. Log onto the Delivery Controller(s) as an administrator.
2. Open Windows PowerShell (with administrative privileges). Using PowerShell, you can issue commands to enable the Delivery Controller to trust XML requests sent from StoreFront.

3. If not already loaded, load the Citrix cmdlets by typing **Add-PSSnapin Citrix***, and press **Enter**.
4. Press **Enter**.
5. Type **Add-PSSnapin citrix.broker.admin.v2**, and press **Enter**.
6. Type **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$True**, and press **Enter**.
7. Close PowerShell.

Configuring SSON on StoreFront and Web Interface

StoreFront configuration

To configure SSON on StoreFront and Web Interface, open Citrix Studio on the StoreFront Server and select **Authentication->Add /Remove Methods**. Select **Domain pass-through**.



Web Interface configuration

To configure SSON on the Web Interface, select **Citrix Web Interface Management > XenApp Services Sites > Authentication Methods** and enable **Pass-through**.



Configure domain pass-through authentication with Kerberos

Dec 06, 2016

This topic applies only to connections between Citrix Receiver for Windows and StoreFront, XenDesktop, or XenApp.

Citrix Receiver for Windows supports Kerberos for domain pass-through authentication for deployments that use smart cards. Kerberos is one of the authentication methods included in Integrated Windows Authentication (IWA).

When Kerberos authentication is enabled, Kerberos authenticates without passwords for Citrix Receiver for Windows, thus preventing Trojan horse-style attacks on the user device to gain access to passwords. Users can log on to the user device with any authentication method; for example, a biometric authenticator such as a fingerprint reader, and still access published resources without further authentication.

Citrix Receiver for Windows handles pass-through authentication with Kerberos as follows when Citrix Receiver for Windows, StoreFront, XenDesktop and XenApp are configured for smart card authentication and a user logs on with a smart card:

1. The Citrix Receiver for Windows Single Sign-on service captures the smart card PIN.
2. Citrix Receiver for Windows uses IWA (Kerberos) to authenticate the user to StoreFront. StoreFront then provides Citrix Receiver for Windows with information about available virtual desktops and apps.
Note: You do not have to use Kerberos authentication for this step. Enabling Kerberos on Citrix Receiver for Windows is only needed to avoid an extra PIN prompt. If you do not use Kerberos authentication, Citrix Receiver for Windows authenticates to StoreFront using the smart card credentials.
3. The HDX engine (previously referred to as the ICA client) passes the smart card PIN to XenDesktop or XenApp to log the user on to the Windows session. XenDesktop or XenApp then deliver the requested resources.

To use Kerberos authentication with Citrix Receiver for Windows, make sure your Kerberos configuration conforms to the following.

- Kerberos works only between Citrix Receiver for Windows and servers that belong to the same or to trusted Windows Server domains. Servers must also be trusted for delegation, an option you configure through the Active Directory Users and Computers management tool.
- Kerberos must be enabled on the domain and in XenDesktop and XenApp. For enhanced security and to ensure that Kerberos is used, disable on the domain any non-Kerberos IWA options.
- Kerberos logon is not available for Remote Desktop Services connections configured to use Basic authentication, to always use specified logon information, or to always prompt for a password.

The remainder of this topic describes how to configure domain pass-through authentication for the most common scenarios. If you are migrating to StoreFront from Web Interface and previously used a customized authentication solution, contact your Citrix Support representative for more information.

Warning

Some of the configurations described in this topic include registry edits. 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.

To configure domain pass-through authentication with Kerberos for use with smart cards

If you are not familiar with smart card deployments in a XenDesktop environment, we recommend that you review the smart card information in the [Secure your deployment](#) section in the XenDesktop documentation before continuing.

When you install Citrix Receiver for Windows, include the following command-line option:

- /includeSSON

This option installs the single sign-on component on the domain-joined computer, enabling Citrix Receiver for Windows to authenticate to StoreFront using IWA (Kerberos). The single sign-on component stores the smart card PIN, which is then used by the HDX engine when it remotes the smart card hardware and credentials to XenDesktop. XenDesktop automatically selects a certificate from the smart card and obtains the PIN from the HDX engine.

A related option, ENABLE_SSON, is enabled by default and should remain enabled.

If a security policy prevents enabling single sign-on on a device, configure Citrix Receiver for Windows through the following policy:

Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password

Note: In this scenario you want to allow the HDX engine to use smart card authentication and not Kerberos, so do not use the option ENABLE_KERBEROS=Yes, which would force the HDX engine to use Kerberos.

To apply the settings, restart Citrix Receiver for Windows on the user device.

To configure StoreFront:

- In the default.ica file located on the StoreFront server, set DisableCtrlAltDel to false.
Note: This step is not required if all client machines are running Citrix Receiver for Windows 4.2 or above.
- When you configure the authentication service on the StoreFront server, select the Domain pass-through check box. That setting enables Integrated Windows Authentication. You do not need to select the Smart card check box unless you also have non domain joined clients connecting to Storefront with smart cards.

For more information about using smart cards with StoreFront, refer to [Configure the authentication service](#) in the StoreFront documentation.

About FastConnect API and HTTP basic authentication

The FastConnect API uses the HTTP Basic Authentication method, which is frequently confused with authentication methods associated with domain pass-through, Kerberos, and IWA. Citrix recommends that you disable IWA on StoreFront and in ICA group policy.

Configure smart card authentication

Dec 06, 2016

Citrix Receiver for Windows supports the following smart card authentication features. For information about XenDesktop and StoreFront configuration, refer to the documentation for those components. This topic describes Citrix Receiver for Windows configuration for smart cards.

- **Pass-through authentication (single sign-on)** – Pass-through authentication captures smart card credentials when users log on to Citrix Receiver for Windows. Citrix Receiver for Windows uses the captured credentials as follows:
 - Users of domain-joined devices who log on to Citrix Receiver for Windows with smart card credentials can start virtual desktops and applications without needing to re-authenticate.
 - Users of non-domain-joined devices who log on to Citrix Receiver for Windows with smart card credentials must enter their credentials again to start a virtual desktop or application.

Pass-through authentication requires StoreFront and Citrix Receiver for Windows configuration.

- **Bimodal authentication** – Bimodal authentication offers users a choice between using a smart card and entering their user name and password. This feature is useful if the smart card cannot be used (for example, the user has left it at home or the logon certificate has expired). Dedicated stores must be set up per site to allow this, using the `DisableCtrlAltDel` method set to `False` to allow smart cards. Bimodal authentication requires StoreFront configuration. If NetScaler Gateway is present in the solution, is also requires configuration. Bimodal authentication also now gives the StoreFront administrator the opportunity to offer the end user both user name and password and smart card authentication to the same store by selecting them in the StoreFront Console. See [StoreFront](#) documentation.
- **Multiple certificates** – Multiple certificates can be available for a single smart card and if multiple smart cards are in use. When a user inserts a smart card into a card reader, the certificates are available to all applications running on the user device, including Citrix Receiver for Windows. To change how certificates are selected, configure Citrix Receiver for Windows.
- **Client certificate authentication** – Client certificate authentication requires NetScaler Gateway and StoreFront configuration.
 - For access to StoreFront resources through NetScaler Gateway, users might have to re-authenticate after removing a smart card.
 - When the NetScaler Gateway SSL configuration is set to mandatory client certificate authentication, operation is more secure. However mandatory client certificate authentication is not compatible with bimodal authentication.
- **Double hop sessions** – If a double-hop is required, a further connection is established between Receiver and the user's virtual desktop. Deployments supporting double hops are described in the XenDesktop documentation.
- **Smart card-enabled applications** – Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office, allow users to digitally sign or encrypt documents available in virtual desktop or application sessions.

Prerequisites

This topic assumes familiarity with the smart card topics in the XenDesktop and StoreFront documentation.

Limitations

- Certificates must be stored on a smart card, not the user device.
- Citrix Receiver for Windows does not save the user certificate choice, but can store the PIN when configured. The PIN is only cached in non-paged memory for the duration of the user session and is not stored to disk at any point.

- Citrix Receiver for Windows does not reconnect sessions when a smart card is inserted.
- When configured for smart card authentication, Citrix Receiver for Windows does not support virtual private network (VPN) single-sign on or session pre-launch. To use VPN tunnels with smart card authentication, users must install the NetScaler Gateway Plug-in and log on through a web page, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the NetScaler Gateway Plug-in is not available for smart card users.
- Citrix Receiver for Windows Updater communications with citrix.com and the Merchandising Server is not compatible with smart card authentication on NetScaler Gateway.

Warning

Some of the configuration described in this topic include registry edits. 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.

To enable single sign-on for smart card authentication

To configure Citrix Receiver for Windows, include the following command-line option when you install it:

- `ENABLE_SSON=Yes`
Single sign-on is another term for pass-through authentication. Enabling this setting prevents Citrix Receiver for Windows from displaying a second prompt for a PIN.

Alternatively, you can perform the configuration through these policy and registry changes:

- Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password
- Set `SSONCheckEnabled` to false in either of the following registry keys if the single sign-on component is not installed. The key prevents the Citrix Receiver for Windows authentication manager from checking for the single sign-on component, thus allowing Citrix Receiver for Windows to authenticate to StoreFront.
`HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\`
`HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\`

Alternatively, it is possible to enable smart card authentication to Storefront instead of Kerberos. To enable smart card authentication to StoreFront instead of Kerberos, install Citrix Receiver for Windows with the command line options below. This requires administrator privileges. The machine does not need to be joined to a domain.

- `/includeSSON` installs single sign-on (pass-through) authentication. Enables credential caching and the use of pass-through domain-based authentication.
- If the user is logging on to the endpoint with a different method to smart card for Receiver authentication (for example, user name and password), the command line is:
`/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No`
 This prevents the credentials being captured at log on time and allows Citrix Receiver for Windows to store the PIN when logging on to Citrix Receiver for Windows.
- Go to Policy > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Authentication > Local user name and password.

Enable pass-through authentication. Depending on the configuration and security settings, you may need to select the Allow pass-through authentication for all ICA option for pass-through authentication to work.

To configure StoreFront:

- When you configure the authentication service, select the Smart card check box.

For more information about using smart cards with StoreFront, see [Configure the authentication service](#) in the StoreFront documentation.

To enable user devices for smart card use

1. Import the certificate authority root certificate into the device's keystore.
2. Install your vendor's cryptographic middleware.
3. Install and configure Citrix Receiver for Windows.

To change how certificates are selected

By default, if multiple certificates are valid, Citrix Receiver for Windows prompts the user to choose a certificate from the list. Alternatively, you can configure Citrix Receiver for Windows to use the default certificate (per the smart card provider) or the certificate with the latest expiry date. If there are no valid logon certificates, the user is notified, and given the option to use an alternate logon method if available.

A valid certificate must have all of these characteristics:

- The current time of the clock on the local computer is within the certificate validity period.
- The Subject public key must use the RSA algorithm and have a key length of 1024, 2048, or 4096 bits.
- Key Usage must contain Digital Signature.
- Subject Alternative Name must contain the User Principal Name (UPN).
- Enhanced Key Usage must contain Smart Card Logon and Client Authentication, or All Key Usages.
- One of the Certificate Authorities on the certificate's issuer chain must match one of the permitted Distinguished Names (DN) sent by the server in the TLS handshake.

Change how certificates are selected by using either of the following methods:

- On the Citrix Receiver for Windows command line, specify the option `AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`.
Prompt is the default. For SmartCardDefault or LatestExpiry, if multiple certificates meet the criteria, Citrix Receiver for Windows prompts the user to choose a certificate.
- Add the following key value to the registry key `HKCU or HKLM\Software\[Wow6432Node\]Citrix\AuthManager`:
`CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }`.
Values defined in HKCU take precedence over values in HKLM to best assist the user in selecting a certificate.

To use CSP PIN prompts

By default, the PIN prompts presented to users are provided by Citrix Receiver for Windows rather than the smart card Cryptographic Service Provider (CSP). Citrix Receiver for Windows prompts users to enter a PIN when required and then passes the PIN to the smart card CSP. If your site or smart card has more stringent security requirements, such as to disallow caching the PIN per-process or per-session, you can configure Citrix Receiver for Windows to instead use the CSP components to manage the PIN entry, including the prompt for a PIN.

Change how PIN entry is handled by using either of the following methods:

- On the Citrix Receiver for Windows command line, specify the option `AM_SMARTCARDPINENTRY=CSP`.
- Add the following key value to the registry key `HKLM\Software\[Wow6432Node\Citrix\AuthManager:SmartCardPINEntry=CSP`.

Enable certificate revocation list checking for improved security

Mar 07, 2017

When certificate revocation list (CRL) checking is enabled, Citrix Receiver checks whether or not the server's certificate is revoked. By forcing Citrix Receiver to check this, you can improve the cryptographic authentication of the server and the overall security of the TLS connection between a user device and a server.

You can enable several levels of CRL checking. For example, you can configure Citrix Receiver to check only its local certificate list or to check the local and network certificate lists. In addition, you can configure certificate checking to allow users to log on only if all CRLs are verified.

If you are making this change on a local computer, exit Citrix Receiver if it is running. Make sure all Citrix Receiver components, including the Connection Center, are closed.

1. As an administrator, open the Group Policy Editor by either running `gpedit.msc` locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
Note: If you already imported the Citrix Receiver for Windows template into the Group Policy Editor, you can omit Steps 2 to 5.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Configuration folder for the Receiver (usually `C:\Program Files\Citrix\ICA Client\Configuration`) and select the Citrix Receiver for Windows template file.
Note: Depending on the version of the Windows operating system, select the Citrix Receiver for Windows template file (`receiver.adm` or `receiver.admx/receiver.adml`).
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. From the Action menu, choose Properties and select Enabled.
8. From the CRL verification drop-down menu, select one of the options.
 - Disabled. No certificate revocation list checking is performed.
 - Only check locally stored CRLs. CRLs that were installed or downloaded previously are used in certificate validation. Connection fails if the certificate is revoked.
 - Require CRLs for connection. CRLs locally and from relevant certificate issuers on the network are checked. Connection fails if the certificate is revoked or not found.
 - Retrieve CRLs from network. CRLs from the relevant certificate issuers are checked. Connection fails if the certificate is revoked.

If you do not set CRL verification, it defaults to Only check locally stored CRLs.

Secure communications

Mar 07, 2017

To secure the communication between XenDesktop Sites or XenApp server farms and Citrix Receiver for Windows, you can integrate your Citrix Receiver for Windows connections using security technologies such as the following:

- Citrix NetScaler Gateway. For information, refer to topics in this section as well as the NetScaler Gateway, and StoreFront documentation.
Note: Citrix recommends using NetScaler Gateway to secure communications between StoreFront servers and user devices.
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Citrix Receiver for Windows through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.
- Trusted server configuration.
- For XenApp or Web Interface deployments only; not applicable to XenDesktop 7: A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Receiver and servers. Receiver supports SOCKS and secure proxy protocols.
- For XenApp or Web Interface deployments only; not applicable to XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5, or XenApp 7.5: SSL Relay solutions with Transport Layer Security (TLS) protocols.
- For XenApp 7.6 and XenDesktop 7.6, you can enable an SSL connection directly between users and VDAs. (See [SSL](#) for information about configuring SSL for XenApp 7.6 or XenDesktop 7.6.)

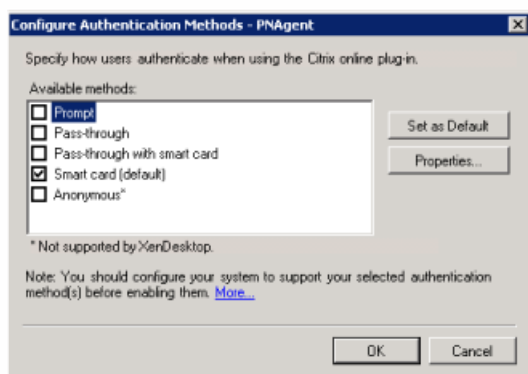
Citrix Receiver for Windows is compatible with and functions in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates are used. These templates are supported on various Windows platforms. Refer to the Windows security guides available at <http://technet.microsoft.com> for more information about the templates and related settings.

Configure smart card authentication for Web Interface 5.4

Mar 07, 2017

If Citrix Receiver for Windows is installed with a SSON component, pass-through authentication is enabled by default even if the PIN pass-through for smart card is not enabled on the XenApp PNAgent site; the pass-through setting for authentication methods will no longer be effective. The screen below illustrates how to enable smart card as the authentication method when Citrix Receiver for Windows is properly configured with SSON.

See [How to Manually install and configure Citrix Receiver for Pass-through Authentication](#) for more information.



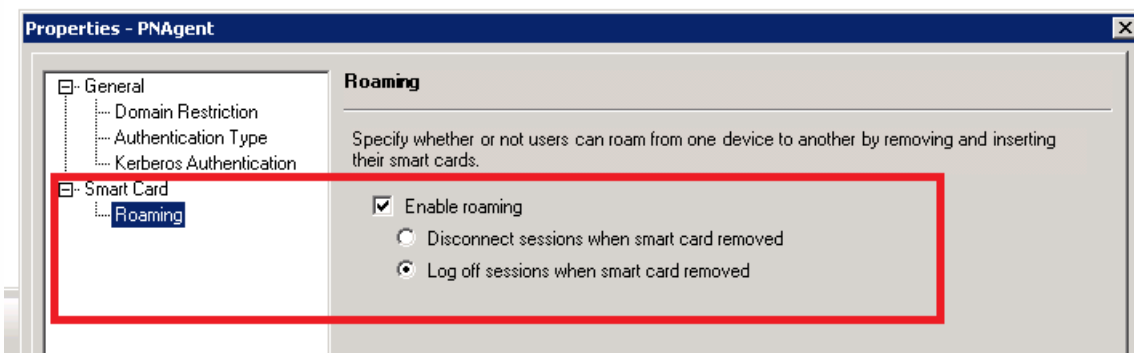
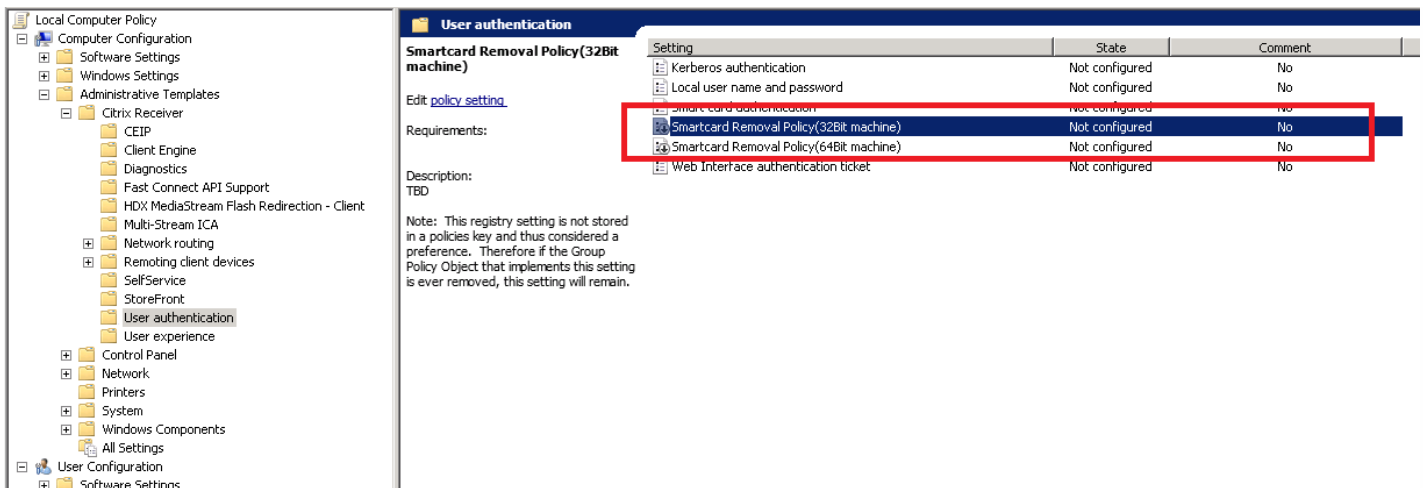
Use the smart card removal policy to control the behavior for smart card removal when a user authenticates to the Citrix Web Interface 5.4 PNAgent site.

When this policy is enabled, the user is logged off from the XenApp session if the smart card is removed from the client device. However, the user is still logged into Citrix Receiver for Windows.

For this policy to take effect, the smart card removal policy must be set in Web Interface XenApp Services site. The settings can be found on Web Interface 5.4, **XenApp Services Site > Pass-through with smart card > Enable Roaming > Logoff the sessions when smart card removed.**

When the smart card removal policy is disabled, the user's XenApp session is disconnected if the smart card is removed from the client device; smart card removal on the Web Interface XenApp Services site does not have any effect.

Note: There are separate policies for 32bit and 64bit clients. For 32bit devices, the policy name is **Smartcard Removal Policy (32Bit machine)** and for 64bit devices, the policy name is **Smartcard Removal Policy (64Bit machine)**.



Smart card support and removal changes

Consider the following when connecting to a XenApp 6.5 PNAgent site:

- Beginning with Citrix Receiver for Windows 4.5, smart card login is supported for PNAgent site logins.
- The smart card removal policy has changed on the PNAgent Site:
A XenApp session is logged off when the smart card is removed – if the PNAgent site is configured with smart card as the authentication method, the corresponding policy has to be configured on Receiver for Windows to enforce the XenApp session for logoff. Enable roaming for smart card authentication on the XenApp PNAgent site and enable the smart card removal policy, which logs off XenApp from the Receiver session; the user is still logged into the Receiver session.

Known issue

When a user logs in to the PNAgent site using smart card authentication, the username is displayed as **Logged On**.

Connect with NetScaler Gateway

Dec 06, 2016

To enable remote users to connect through NetScaler Gateway, configure NetScaler Gateway to work with StoreFront and AppController (a component of CloudGateway).

- For StoreFront deployments: Allow connections from internal or remote users to StoreFront through NetScaler Gateway by integrating NetScaler Gateway and StoreFront. This deployment allows users to connect to StoreFront to access virtual desktops and applications. Users connect through Citrix Receiver for Windows.
- For AppController deployments: Allow connections from remote users to AppController by integrating Access Gateway and AppController. This deployment allows users to connect to AppController to obtain their web and Software as a Service (SaaS) apps and provides ShareFile Enterprise services to Citrix Receiver for Windows users. Users connect through either Citrix Receiver for Windows or the NetScaler Gateway Plug-in.

Note

The NetScaler Gateway End Point Analysis Plug-in (EPA) does not support native Citrix Receiver for Windows.

For information about configuring these connections, see [Integrating NetScaler Gateway with XenMobile App Edition](#) and related topics. Information about the settings required for Citrix Receiver for Windows are in the following topics:

- [Configuring Session Policies and Profiles for XenMobile App Edition](#)
- [Creating the Session Profile for Receiver for XenMobile App Edition](#)
- [Configuring Custom Clientless Access Policies for Receiver](#)
- [Configuring Session Policies and Profiles for CloudGateway](#)
- [Creating the Session Profile for Receiver for CloudGateway Enterprise](#)
- [Creating the Session Profile for Receiver for CloudGateway Express](#)
- [Configuring Custom Clientless Access Policies for Receiver](#)

To enable remote users to connect through NetScaler Gateway to your Web Interface deployment, configure NetScaler Gateway to work with Web Interface, as described in [Providing Access to Published Applications and Virtual Desktops Through the Web Interface](#) and its sub-topics.

Connect with Secure Gateway

Dec 06, 2016

This topic applies only to deployments using the Web Interface.

You can use the Secure Gateway in either Normal mode or Relay mode to provide a secure channel for communication between Citrix Receiver for Windows and the server. No Citrix Receiver for Windows configuration is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

Citrix Receiver for Windows uses settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway. See the topics for the Web Interface for information about configuring proxy server settings for Citrix Receiver for Windows.

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. See the topics for the Secure Gateway for more information about Relay mode.

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure Citrix Receiver for Windows to use:

- The fully qualified domain name (FQDN) of the Secure Gateway server.
- The port number of the Secure Gateway server. Note that Relay mode is not supported by Secure Gateway Version 2.0.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example: `my_computer.my_company.com` is an FQDN, because it lists, in sequence, a host name (`my_computer`), an intermediate domain (`my_company`), and a top-level domain (`com`). The combination of intermediate and top-level domain (`my_company.com`) is generally referred to as the domain name.

Connect through a firewall

Dec 06, 2016

Network firewalls can allow or block packets based on the destination address and port. If you are using a firewall in your deployment, Citrix Receiver for Windows must be able to communicate through the firewall with both the Web server and Citrix server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for user device to Web server communication. For Receiver to Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

If the firewall is configured for Network Address Translation (NAT), you can use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your XenApp or XenDesktop server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to Receiver. Citrix Receiver for Windows then connects to the server using the external address and port number. For more information, see the [Web Interface](#) documentation.

Enforce trust relations

Dec 06, 2016

Trusted server configuration is designed to identify and enforce trust relations involved in Citrix Receiver for Windows connections. This trust relationship increases the confidence of Citrix Receiver for Windows administrators and users in the integrity of data on user devices and prevents the malicious use of Citrix Receiver for Windows connections.

When this feature is enabled, Citrix Receiver for Windows can specify the requirements for trust and determine whether or not they trust a connection to the server. For example, a Citrix Receiver for Windows connecting to a certain address (such as https://*.citrix.com) with a specific connection type (such as TLS) is directed to a trusted zone on the server.

When trusted server configuration is enabled, connected servers must reside in a Windows Trusted Sites zone. (For step-by-step instructions about adding servers to the Windows Trusted Sites zone, see the Internet Explorer online help.)

To enable trusted server configuration

If you are changing this on a local computer, close all Citrix Receiver for Windows components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by either running `gpedit.msc` locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
Note: If you already imported the Citrix Receiver for Windows template into the Group Policy Editor, you can omit Steps 2 to 5.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Receiver Configuration folder (usually `C:\Program Files\Citrix\ICA Client\Configuration`) and select the Citrix Receiver for Windows template file.
Note: Depending on the version of the Windows Operating System, select the Citrix Receiver for Windows template file (`receiver.adm` or `receiver.admx/receiver.adml`).
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. Expand the Administrative Templates folder under the User Configuration node.
7. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network Routing > Configure trusted server configuration.
8. From the Action menu, choose Properties and select Enabled.

Elevation level and wfcrun32.exe

Dec 06, 2016

When User Access Control (UAC) is enabled on devices running Windows 8, Windows 7, or Windows Vista, only processes at the same elevation/integrity level as wfcrun32.exe can launch virtual applications.

Example 1:

When wfcrun32.exe is running as a normal user (un-elevated), other processes such as Receiver must be running as a normal user to launch applications through wfcrun32.

Example 2:

When wfcrun32.exe is running in elevated mode, other processes such as Receiver, Connection Center, and third party applications using the ICA Client Object that are running in non-elevated mode cannot communicate with wfcrun32.exe.

Connect through a proxy server

Mar 07, 2017

This topic applies only to deployments using Web Interface.

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Receiver for Windows and servers. Citrix Receiver for Windows supports SOCKS and secure proxy protocols.

When communicating with the server farm, Receiver uses proxy server settings that are configured remotely on the server running Receiver for Web or the Web Interface. For information about proxy server configuration, refer to StoreFront or Web Interface documentation.

In communicating with the Web server, Receiver uses the proxy server settings that are configured through the Internet settings of the default Web browser on the user device. You must configure the Internet settings of the default Web browser on the user device accordingly.

Connect with Secure Sockets Layer (SSL) Relay

Dec 06, 2016

This topic does not apply to XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5, or XenApp 7.5.

You can integrate Citrix Receiver for Windows with the Secure Sockets Layer (SSL) Relay service. Citrix Receiver for Windows supports TLS protocols.

- TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

Connecting with Citrix SSL Relay

This topic does not apply to XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5, or XenApp 7.5.

By default, Citrix SSL Relay uses TCP port 443 on the XenApp server for TLS-secured communication. When the SSL Relay receives an TLS connection, it decrypts the data before redirecting it to the server, or, if the user selects TLS+HTTPS browsing, to the Citrix XML Service.

If you configure SSL Relay to listen on a port other than 443, you must specify the nonstandard listening port number to the plug-in.

You can use Citrix SSL Relay to secure communications:

- Between an TLS-enabled client and a server. Connections using TLS encryption are marked with a padlock icon in the Citrix Connection Center.
- With a server running the Web Interface, between the XenApp server and the Web server.

For information about configuring SSL Relay to secure your installation, refer to the XenApp documentation.

User device requirements

In addition to the System Requirements, you also must ensure that:

- The user device supports 128-bit encryption
- The user device has a root certificate installed that can verify the signature of the Certificate Authority on the server certificate
- Citrix Receiver for Windows is aware of the TCP listening port number used by the SSL Relay service in the server farm
- Any service packs or upgrades that Microsoft recommends are applied

If you are using Internet Explorer and you are not certain about the encryption level of your system, visit the Microsoft Web site at <http://www.microsoft.com> to install a service pack that provides 128-bit encryption.

Important: Citrix Receiver for Windows supports certificate key lengths of up to 4096 bits. Ensure that the bit lengths of your Certificate Authority root and intermediate certificates, and those of your server certificates, do not exceed the bit length your Citrix Receiver for Windows supports or connection might fail.

To apply a different listening port number for all connections

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

Note: If you already imported the Citrix Receiver for Windows template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select the Citrix Receiver for Windows template file.
Note: Depending on the version of the Windows Operating System, select the Citrix Receiver for Windows template file (receiver.adm or receiver.admx/receiver.adml).
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. From the Action menu, choose Properties, select Enabled, and type a new port number in the Allowed SSL servers text box in the following format: server:SSL relay port number where SSL relay port number is the number of the listening port. You can use a wildcard to specify multiple servers. For example, *.Test.com:SSL relay port number matches all connections to Test.com through the specified port.

To apply a different listening port number to particular connections only

If you are changing this on a local computer, close all Receiver components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

Note: If you already added the Citrix Receiver for Windows template to the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Receiver Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select the Citrix Receiver for Windows template file.

Note: Depending on the version of the Windows Operating System, select the Citrix Receiver for Windows template file (receiver.adm or receiver.admx/receiver.adml).

5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. From the Action menu, choose Properties, select Enabled, and type a comma-separated list of trusted servers and the new port number in the Allowed SSL servers text box in the following format: servername:SSL relay port number,servername:SSL relay port number where SSL relay port number is the number of the listening port. You can specify a comma-separated list of specific trusted SSL servers similar to this example:

csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
which translates into the following in an example appsrv.ini file: [Word]
SSLProxyHost=csghq.Test.com:443

[Excel]
SSLProxyHost=csghq.Test.com:444

[Notepad]
SSLProxyHost=fred.Test.com:443

Configure and enable TLS

Dec 06, 2016

This topic applies to XenApp and XenDesktop Version 7.6 and later.

To force Citrix Receiver for Windows to connect with TLS, you must specify TLS on the Secure Gateway server or SSL Relay service. See the topics for the Secure Gateway or your SSL Relay service documentation for more information.

In addition, make sure that the user device meets all system requirements.

To use TLS encryption for all Citrix Receiver for Windows communications, configure the user device, Citrix Receiver for Windows, and, if using Web Interface, the server running the Web Interface. For information about securing StoreFront communications, see [Secure](#) section in the StoreFront documentation. For information about securing Web Interface, see [Secure](#) section in the Web Interface documentation.

Install root certificates on user devices

To use TLS to secure communications between a TLS-enabled Citrix Receiver for Windows and the server farm, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate.

Citrix Receiver for Windows supports the Certificate Authorities that are supported by the Windows operating system. The root certificates for these Certificate Authorities are installed with Windows and managed using Windows utilities. They are the same root certificates that are used by Microsoft Internet Explorer.

If you use your own Certificate Authority, you must obtain a root certificate from that Certificate Authority and install it on each user device. This root certificate is then used and trusted by both Microsoft Internet Explorer and Receiver.

You might be able to install the root certificate using other administration or deployment methods, such as:

- Using the Microsoft Internet Explorer Administration Kit (IEAK) Configuration Wizard and Profile Manager
- Using third-party deployment tools

Make sure that the certificates installed by your Windows operating system meet the security requirements for your organization or use the certificates issued by your organization's Certificate Authority.

To configure Web Interface to use TLS for Citrix Receiver for Windows

1. To use TLS to encrypt application enumeration and launch data passed between Citrix Receiver for Windows and the server running the Web Interface, configure the appropriate settings using the Web Interface. You must include the computer name of the XenApp server that is hosting the SSL certificate.
2. To use secure HTTP (HTTPS) to encrypt the configuration information passed between Citrix Receiver for Windows and the server running the Web Interface, enter the server URL in the format `https://servername`. In the Windows notification area, right-click the Citrix Receiver for Windows icon and choose Preferences.
3. Right-click the Online Plug-in entry in the Plug-in Status and choose Change Server.

To configure TLS support

If you are changing this on a local computer, close all Receiver components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by running gpedit.msc locally from the Start menu when applying this to a single computer or by using the Group Policy Management Console when using Active Directory.
Note: If you already imported the Citrix Receiver for Windows template into the Group Policy Editor, you can omit Steps 2 to 5
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Receiver Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select the Citrix Receiver for Windows template file.
Note: Depending on the version of the Windows Operating System, select the Citrix Receiver for Windows template file (receiver.adm or receiver.admx/receiver.adml).
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. From the Action menu, choose Properties, select Enabled, and from the drop-down menus, select the TLS settings.
 - Set TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Citrix Receiver for Windows connects using TLS encryption.
 - Set SSL cipher suite to Detect version to have Citrix Receiver for Windows negotiate a suitable cipher suite from the Government and Commercial cipher suits. You can restrict the cipher suites to either Government or Commercial.
 - Set CRL verification to Require CRLs for connection requiring Citrix Receiver for Windows to try to retrieve Certificate Revocation Lists (CRLs) from the relevant certificate issuers.

To use the Group Policy Object administrative template on Web Interface

If you are changing this on a local computer, close all Citrix Receiver for Windows components, including the Connection Center.

To meet FIPS 140 security requirements, configure the parameters or include the parameters in the default.ica file on the server running the Web Interface. See the information about Web Interface for additional information about the default.ica file.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
Note: If you already imported the Citrix Receiver for Windows template file into the Group Policy Editor, you can omit Steps 3 to 5.
2. In the left pane of the Group Policy Editor, select the **Administrative Templates** folder.
3. From the Action menu, choose Add/Remove Templates.
4. Click **Add** and browse to the Receiver Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select the Citrix Receiver for Windows template file (receiver.adm or receiver.admx/receiver.adml, depending on the version of the Windows operating system).
5. Click **Open** to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to **Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification**.
7. From the Action menu, choose **Properties**, select **Enabled**, and from the drop-down menus, select the appropriate settings.
 - Set **TLS Version to TLS or Detect all** to enable TLS. If Detect all is selected, Receiver tries to connect using TLS encryption.
 - Set **SSL cipher suite** to Government.

- Set **CRL verification** to Require CRLs for connection.

To configure the Web Interface to use TLS when communicating with Citrix Receiver for Windows

When using the Web Interface, specify the computer name of the server hosting the SSL certificate.

For more details on using TLS to secure communications between Citrix Receiver for Windows and the Web server, see [Web Interface](#) documentation.

1. From the Configuration settings menu, select **Server Settings**.
2. Select **Use SSL/TLS** for communications between clients and the Web server.
3. Save your changes.

Selecting SSL/TLS changes all URLs to use HTTPS protocol.

To configure XenApp to use TLS when communicating with Citrix Receiver for Windows

You can configure the XenApp server to use TLS to secure the communications between Citrix Receiver for Windows and the server.

1. From the Citrix management console for the XenApp server, open the Properties dialog box for the application you want to secure.
2. Select Advanced > Client options and ensure that you select Enable SSL and TLS protocols.
3. Repeat these steps for each application you want to secure.

When using the Web Interface, specify the computer name of the server hosting the SSL certificate. See the information about Web Interface for more details about using TLS to secure communications between Citrix Receiver for Windows and the Web server.

To configure Citrix Receiver to use TLS when communicating with the server running the Web Interface

You can configure Citrix Receiver for Windows to use TLS to secure the communications between Citrix Receiver for Windows and the server running the Web Interface.

Ensure that a valid root certificate is installed on the user device. For more information, see [Install root certificates on user devices](#).

1. In the Windows notification area, right-click the Citrix Receiver for Windows icon and choose Preferences.
2. Right-click the Online Plug-in entry in the Plug-in Status and choose Change Server.
3. The Change Server screen displays the currently configured URL. Enter the server URL in the text box in the format `https://servername` to encrypt the configuration data using TLS.
4. Click Update to apply the change.
5. Enable TLS in the user device browser. For more information, see the online Help for the browser.

TLS and HTML5 video redirection

HTML5 video redirection includes support for video content over TLS (HTTPS). To achieve this, custom certificates are placed in the computer's certificate store on the VDA.

HTML5 video redirection is disabled by default.

If you do not intend to use HTML5 video redirection with video content over TLS, Citrix recommends that you delete the two certificates from the Trusted Root Certificates store on the VDA. These certificates are Issued to "Citrix HDX" /Issued by "Citrix HDX", and Issued to "127.0.0.1"/Issued by "Citrix HDX".

ICA file signing to protect against application or desktop launches from untrusted servers

Mar 07, 2017

This topic applies only to deployments with Web Interface using Administrative Templates.

The ICA File Signing feature helps protect users from unauthorized application or desktop launches. Citrix Receiver for Windows verifies that a trusted source generated the application or desktop launch based on administrative policy and protects against launches from untrusted servers. You can configure this Citrix Receiver for Windows security policy for application or desktop launch signature verification using Group Policy Objects, StoreFront, or Citrix Merchandising Server. ICA file signing is not enabled by default. For information about enabling ICA file signing for StoreFront, refer to the StoreFront documentation.

For Web Interface deployments, the Web Interface enables and configures application or desktop launches to include a signature during the launch process using the Citrix ICA File Signing Service. The service can sign ICA files using a certificate from the computer's personal certificate store.

The Citrix Merchandising Server with Citrix Receiver for Windows enables and configures launch signature verification using the Citrix Merchandising Server Administrator Console > Deliveries wizard to add trusted certificate thumbprints.

To use Group Policy Objects to enable and configure application or desktop launch signature verification, follow this procedure:

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
Note: If you already imported the ica-file-signing.adm template into the Group Policy Editor, you can omit Steps 2 to 5.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Citrix Receiver for Windows configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select ica-file-signing.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver and navigate to Enable ICA File Signing.
7. If you choose Enabled, you can add signing certificate thumbprints to the white list of trusted certificate thumbprints or remove signing certificate thumbprints from the white list by clicking Show and using the Show Contents screen. You can copy and paste the signing certificate thumbprints from the signing certificate properties. Use the Policy drop-down menu to select Only allow signed launches (more secure) or Prompt user on unsigned launches (less secure).

Option	Description
Only allow signed launches (more secure)	Allows only properly signed application or desktop launches from a trusted server. The user sees a Security Warning message in Citrix Receiver for Windows if an application or desktop launch has an invalid signature. The user cannot continue and the unauthorized launch is blocked.
Prompt user on unsigned	Prompts the user every time an unsigned or invalidly signed application or desktop attempts to launch. The user can either continue the application launch or abort the launch (default).

launches (less Option secure)	Description
-------------------------------------	-------------

To select and distribute a digital signature certificate

When selecting a digital signature certificate, Citrix recommends you choose from this prioritized list:

1. Buy a code-signing certificate or SSL signing certificate from a public Certificate Authority (CA).
2. If your enterprise has a private CA, create a code-signing certificate or SSL signing certificate using the private CA.
3. Use an existing SSL certificate, such as the Web Interface server certificate.
4. Create a new root CA certificate and distribute it to user devices using GPO or manual installation.

Configure a Web browser and ICA file to enable single sign-on and manage secure connections to trusted servers

Dec 06, 2016

This topic applies only to deployments using Web Interface.

To use Single sign-on (SSO) and to manage secure connections to trusted servers, add the Citrix server's site address to the Local intranet or Trusted sites zones in Internet Explorer under Tools > Internet Options > Security on the user device. The address can include the wildcard (*) formats supported by the Internet Security Manager (ISM) or be as specific as protocol://URL[:port].

The same format must be used in both the ICA file and the sites entries. For example, if you use a fully qualified domain name (FQDN) in the ICA file, you must use an FQDN in the sites zone entry. XenDesktop connections use only a desktop group name format.

Supported formats (including wildcards)

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://hostname

http[s]://fqdn.example.com

http[s]://*.example.com

http[s]://cname.*.example.com

http[s]://*.example.co.uk

desktop://group-20name

ica[s]://xaserver1

ica[s]://xaserver1.example.com

Launch SSO or use secure connections with a Web site

Add the exact address of the Web Interface site in the sites zone.

Example Web site addresses

https://my.company.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

XenDesktop connections with Desktop Viewer

Add the address in the form `desktop://Desktop Group Name`. If the desktop group name contains spaces, replace each space with `-20`.

Custom ICA entry formats

Use one of the following formats in the ICA file for the Citrix server site address. Use the same format to add it to the Local intranet or Trusted sites zones in Internet Explorer under Tools > Internet Options > Security on the user device:

Example of ICA file `HttpBrowserAddress` entry

```
HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080
```

Examples of ICA file XenApp server address entries

If the ICA file contains only the XenApp server **Address** field, use one of the following entry formats:

```
icas://10.20.30.40:1494
```

```
icas://my.xenapp-server.company.com
```

```
ica://10.20.30.40
```


Set client resource permissions

Dec 06, 2016

This topic applies only to deployments using Web Interface.

You can set client resource permissions using trusted and restricted site regions by:

- Adding the Web Interface site to the Trusted Site list
- Making changes to new registry settings

Note

Due to recent enhancements to Citrix Receiver, the .ini procedure available in earlier versions of the plug-in/Receiver is replaced with these procedures.

To add the Web Interface site to the trusted site list

1. From the Internet Explorer Tools menu, choose Internet Options > Security.
2. Select the Trusted sites icon and click the Sites button..
3. In the Add this website to the zone text field, type the URL to your Web Interface site and click Add.
4. Download the registry settings from <http://support.citrix.com/article/CTX133565> and make any registry changes. Use SsonRegUpX86.reg for Win32 user devices and SsonRegUpX64.reg for Win64 user devices.
5. Log off and then log on to the user device.

To change client resource permissions in the registry

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.

1. Download the registry settings from <http://support.citrix.com/article/CTX133565> and import the settings on each user device. Use SsonRegUpX86.reg for Win32 user devices and SsonRegUpX64.reg for Win64 user devices.
2. In the registry editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust and in the appropriate regions, change the default value to the required access values for any of the following resources:

Resource key	Resource description
FileSecurityPermission	Client drives
MicrophoneAndWebcamSecurityPermission	Microphones and webcams
ScannerAndDigitalCameraSecurityPermission	USB and other devices

Resource key		Resource description
Value	Description	
0	No Access	
1	Read-only access	
2	Full access	
3	Prompt user for access	

Supported TLS cipher suites

When Citrix Receiver for Windows is enumerating applications and communicating with Storefront, Windows platform cryptography is used.

For TCP connections between Citrix Receiver for Windows and XenApp/XenDesktop, Citrix Receiver for Windows supports TLS 1.0, 1.1 and 1.2 with the following cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

For UDP based connections Citrix Receiver for Windows supports DTLS 1.0 with the following cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Enable SP 800-52 compliance mode

A new check box has been introduced under Computer Configuration -> Administrative Templates-> Citrix Components -> Network Routing -> TLS and Compliance Mode Configuration, called **Enable FIPS**. This will ensure that only FIPS approved cryptography is used for all ICA connections. By fault this option will be disabled or unchecked.

A new Security Compliance Mode is introduced called SP 800-52. By fault this option will be NONE and is not enabled. Please follow the link that describes the compliance required for NIST SP 800-52: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295.

Note

The SP800-52 compliance mode requires FIPS Compliance. When SP800-52 is enabled FIPS mode is also enabled regardless of the FIPS setting. The allowed 'Certificate Revocation Check policy' values are either 'Full access check and CRL required' or 'Full access

Limiting TLS versions and cipher suites

You can configure Citrix Receiver for Windows r to limit TLS versions and cipher suites. An option is provided to select the allowed TLS protocol versions, which determines TLS protocol for ICA connections. Highest and mutually available TLS version between Client and Server will be selected. Options include:

- TLS 1.0 | TLS 1.1 | TLS 1.2 (default).
- TLS 1.1 | TLS 1.2
- TLS 1.2

An option is available for TLS cipher suite selection. Citrix Receiver for Windows can choose between:

- Any
- Commercial
- Government

Commercial Cipher suites

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Government Cipher suites

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Note

If **Require TLS for all connections** is enabled, connection requests to Storefront must also adhere to HTTPS; adding a store as HTTP fails, and non-SSL VDA (XenDesktop and XenApp) cannot be launched.

Citrix Receiver for Windows Desktop Lock

Feb 23, 2017

You can use the Citrix Receiver for Windows Desktop Lock when you do not need to interact with the local desktop. You can still use the Desktop Viewer (if enabled), however it has only the required set of options on the toolbar: Ctrl+Alt+Del, Preferences, Devices, and Disconnect.

Citrix Receiver for Windows Desktop Lock works on domain-joined machines, which are SSON-enabled (Single Sign-On) and store configured; it can also be used on non-domain joined machines without SSON enabled. It does not support PNA sites. Previous versions of Desktop Lock are not supported when you upgrade to Citrix Receiver for Windows 4.2 or later.

You must install Citrix Receiver for Windows with the /includeSSON flag. You must configure the store and Single Sign-on, either using the adm/admx file or cmdline option. For more information, see [Install and configure Citrix Receiver using the command line](#).

Then, install the Citrix Receiver for Windows Desktop Lock as an administrator using the CitrixReceiverDesktopLock.MSI available in the [Citrix Downloads](#) page.

System requirements for Citrix Receiver Desktop Lock

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. For more information, see the [Microsoft Download](#) page.
- Supported on Windows 7 (including Embedded Edition), Windows 7 Thin PC, Windows 8, and Windows 8.1 and Windows 10 (Anniversary update included).
- Connects to StoreFront through native protocols only.
- Domain-joined and non-domain joined endpoints.
- User devices must be connected to a local area network (LAN) or wide area network (WAN).

Local App Access

Important

Enabling Local App Access may permit local desktop access, unless a full lock down has been applied with the Group Policy Object template, or a similar policy. See [Configure Local App Access and URL redirection](#) in XenApp and XenDesktop for more information.

Working with Citrix Receiver for Windows Desktop Lock

- You can use Citrix Receiver for Windows Desktop Lock with the following Citrix Receiver for Windows features:
 - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013 plug-in, and local app access
 - Domain, two-factor, or smart card authentication only
- Disconnecting the Citrix Receiver for Windows Desktop Lock session logs out the end device.
- Flash redirection is disabled on Windows 8 and later versions. Flash redirection is enabled on Windows 7.
- The Desktop Viewer is optimized for Citrix Receiver for Windows Desktop Lock with no Home, Restore, Maximize, and Display properties.
- Ctrl+Alt+Del is available on the Viewer toolbar.
- Most windows shortcut keys are passed to the remote session, with the exception of Windows+L. For details, see

[Passing Windows shortcut keys to the remote session.](#)

- Ctrl+F1 triggers Ctrl+Alt+Del when you disable the connection or Desktop Viewer for desktop connections.

To install Citrix Receiver for Windows Desktop Lock

This procedure installs Citrix Receiver for Windows so that virtual desktops appear using Citrix Receiver for Windows Desktop Lock. For deployments that use smart cards, see [To configure smart cards for use with devices running Receiver Desktop Lock](#).

1. Log on using a local administrator account.
2. At a command prompt, run the following command (located in the Citrix Receiver and Plug-ins > Windows > Citrix Receiver for Windows folder on the installation media).
For example:
`CitrixReceiver.exe /includeSSON
STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/discovery;on;Desktop Store"`
For command details, see the Citrix Receiver for Windows install documentation at [Configure and install Receiver for Windows using command-line parameters](#).
3. In the same folder on the installation media, double-click CitrixReceiverDesktopLock.MSI . The Desktop Lock wizard opens. Follow the prompts.
4. When the installation completes, restart the user device. If you have permission to access a desktop and you log on as a domain user, the device appears using Receiver Desktop Lock.

To allow administration of the user device after installation, the account used to install CitrixReceiverDesktopLock.msi is excluded from the replacement shell. If that account is later deleted, you will not be able to log on and administer the device.

To run a **silent install** of Receiver Desktop Lock, use the following command line: `msiexec /i CitrixReceiverDesktopLock.msi /qn`

To configure Citrix Receiver for Windows Desktop Lock

Grant access to only one virtual desktop running Citrix Receiver for Windows Desktop Lock per user.

Using Active Directory policies, prevent users from hibernating virtual desktops.

Use the same administrator account to configure Citrix Receiver for Windows Desktop Lock as you did to install it.

- Ensure that the receiver.admx (or receiver.adml) and receiver_usb.admx (.adml) files are loaded into Group Policy (where the policies appear in Computer Configuration or User Configuration > Administrative Templates > Classic Administrative Templates (ADMX) > Citrix Components). The .admx files are located in %Program Files%\Citrix\ICA Client\Configuration\.
- USB preferences - When a user plugs in a USB device, that device is automatically remoted to the virtual desktop; no user interaction is required. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.
 - Enable the USB policy rule.
 - In Citrix Receiver > Remoting client devices > Generic USB Remoting, enable and configure the Existing USB Devices and New USB Devices policies.
- Drive mapping - In Citrix Receiver > Remoting client devices, enable and configure the Client drive mapping policy.
- Microphone - In Citrix Receiver > Remoting client devices, enable and configure the Client microphone policy.

To configure smart cards for use with devices running Citrix Receiver for Windows Desktop Lock

1. Configure StoreFront.
 1. Configure the XML Service to use DNS Address Resolution for Kerberos support.
 2. Configure StoreFront sites for HTTPS access, create a server certificate signed by your domain certificate authority, and add HTTPS binding to the default website.
 3. Ensure pass-through with smart card is enabled (enabled by default).
 4. Enable Kerberos.
 5. Enable Kerberos and Pass-through with smart card.
 6. Enable Anonymous access on the IIS Default Web Site and use Integrated Windows Authentication.
 7. Ensure the IIS Default Web Site does not require SSL and ignores client certificates.
2. Use the Group Policy Management Console to configure Local Computer Policies on the user device.
 1. Import the Receiver.admx template from %Program Files%\Citrix\ICA Client\Configuration\.
 2. Expand Administrative Templates > Classic Administrative Templates (ADMX) > Citrix Components > Citrix Receiver > User authentication.
 3. Enable Smart card authentication.
 4. Enable Local user name and password.
3. Configure the user device before installing Citrix Receiver for Windows Desktop Lock.
 1. Add the URL for the Delivery Controller to the Windows Internet Explorer Trusted Sites list.
 2. Add the URL for the first Delivery Group to the Internet Explorer Trusted Sites list in the form desktop://delivery-group-name.
 3. Enable Internet Explorer to use automatic logon for Trusted Sites.

When Citrix Receiver for Windows Desktop Lock is installed on the user device, a consistent smart card removal policy is enforced. For example, if the Windows smart card removal policy is set to Force logoff for the desktop, the user must log off from the user device as well, regardless of the Windows smart card removal policy set on it. This ensures that the user device is not left in an inconsistent state. This applies only to user devices with the Citrix Receiver for Windows Desktop Lock.

To remove Citrix Receiver for Windows Desktop Lock

Be sure to remove both of the components listed below.

1. Log on with the same local administrator account that was used to install and configure Citrix Receiver for Windows Desktop Lock.
2. From the Windows feature for removing or changing programs:
 - Remove Citrix Receiver for Windows Desktop Lock.
 - Remove Citrix Receiver for Windows.

Passing Windows shortcut keys to the remote session

Most windows shortcut keys are passed to the remote session. This section highlights some of the common ones.

Windows

- Win+D - Minimize all windows on the desktop.
- Alt+Tab - Change active window.
- Ctrl+Alt+Delete - via Ctrl+F1 and the Desktop Viewer toolbar.
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+All Character keys

Windows 8

- Win+C - Open charms.
- Win+Q - Search charm.
- Win+H - Share charm.
- Win+K - Devices charm.
- Win+I - Settings charm.
- Win+Q - Search apps.
- Win+W - Search settings.
- Win+F - Search files.

Windows 8 apps

- Win+Z - Get to app options.
- Win+. - Snap app to the left.
- Win+Shift+. - Snap app to the right.
- Ctrl+Tab - Cycle through app history.
- Alt+F4 - Close an app.

Desktop

- Win+D - Open desktop.
- Win+, - Peek at desktop.
- Win+B - Back to desktop.

Other

- Win+U - Open Ease of Access Center.
- Ctrl+Esc - Start screen.
- Win+Enter - Open Windows Narrator.
- Win+X - Open system utility settings menu.
- Win+PrintScrn - Take a screen shot and save to pictures.
- Win+Tab - Open switch list.
- Win+T - Preview open windows in taskbar.

SDK and API for Citrix Receiver for Windows

Mar 08, 2017

Citrix Virtual Channel SDK

The Citrix Virtual Channel software development kit (SDK) supports writing server-side applications and client-side drivers for additional virtual channels using the ICA protocol. The server-side virtual channel applications are on XenApp or XenDesktop servers. This version of the SDK supports writing new virtual channels for Receiver for Windows. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) is used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.
- The Windows Monitoring API, which enhances the visual experience and support for third-party applications integrated with ICA.
- Working source code for virtual channel sample programs to demonstrate programming techniques.
- The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

For more information on SDK, see [Citrix Virtual Channel SDK for Citrix Receiver for Windows](#).

Fast Connect 3 Credential Insertion API

The Fast Connect 3 Credential Insertion API provides an interface that supplies user credentials to the Single Sign-on (SSON) feature. This feature is available from Citrix Receiver for Windows Version 4.2 and later. Using this API, Citrix partners can provide authentication and SSO products that use StoreFront or the Web Interface to log users on to virtual applications or desktops and then disconnect users from those sessions.

For more information on Fast Connect API, see [Fast Connect 3 Credential Insertion API for Citrix Receiver for Windows](#).