About Citrix Receiver for Windows 4.6

Dec 06, 2016

This pdf file includes the Citrix Receiver for Windows 4.6 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 XenDesktop and XenApp.

What's new in this release

Keyboard layout synchronization

Starting with this release, Citrix Receiver for Windows provides dynamic synchronization of the keyboard layout from the client and the VDA in a session. This enables users to switch among preferred keyboard layouts on the client device, providing a consistent user experience when, for example, switching the touch keyboard layout from English to Spanish. When users switch layouts, they briefly see a message while the synchronization is in progress. They can then continue working with the new keyboard layout.

For more information on configuring keyboard layout, see Keyboard layout.

Support for Server Name Indicator (SNI)

Starting with this release, Citrix Receiver for Windows supports NetScaler Gateway with Server Name Indication (SNI) configured so that users can launch desktops and applications successfully. For more information on SNI, see Knowledge Center article CTX125798.

Enlightened Data Transport (for evaluation only)

Enlightened Data Transport (EDT) is a high-end data transfer protocol used for transferring data over high-speed network. EDT has an advantage where it shares the data bandwidth concurrently with TCP. EDT is recommended for use on wide-area networks.

Starting with this release, Citrix Receiver for Windows supports EDT to enhance the user experience including Thinwire display remoting, file transfer (Client Drive Mapping), printing, multimedia redirection and others from XenApp/XenDesktop. EDT helps in optimizing ICA traffic between the servers. Users have an option to choose the connection type between Receiver and the VDA. The available options are EDT and TCP. It can be enabled in a nonproduction environment with a new policy setting, Transport protocol for Receiver. Set the new policy setting to Preferred to use enlightened data transport when possible, with fallback to TCP.

For a detailed procedure on configuring EDT, see Configuring Enlightened Data Transport.

HTML5 Video Redirection - Internally Controlled Content

HTML5 video redirection for internal web sites provides the best balance between smooth audio and video display and server scalability for HTML5 video content in a virtualized environment. HTML5 video redirection controls and optimizes the way XenApp and XenDesktop servers deliver HTML5 multimedia web content to users. This feature is set on the server end and is disabled by default.

This feature is not supported with Microsoft Edge.

The following video controls are supported:

- play

- pause
- seek
- repeat
- audio
- full screen

There is no configuration required to be done in Citrix Receiver for Windows. If Citrix Receiver for Windows supports RAVE protocol, HTML5 video redirection is automatically supported.

New Citrix Receiver for Windows administrative template file

A new Citrix Receiver for Windows template file called CitrixBase.admx/CitrixBase.adml has been introduced in this release. This file is typically present in the <Installation Directory>\ICA Client\Configuration directory.

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.

For more information on template files, see Configuring Citrix Receiver for Windows with the Group Policy Object administrative template.

Extended support on Cipher suites

With this release, Citrix Receiver for Windows extends the support for the following two cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

For more information on cipher suites, see About TLS and Group Policies.

Citrix Receiver for Windows 4.6 Fixed Issues

Jan 24, 2017

Citrix Receiver for Windows 4.6

Compared to: Citrix Receiver for Windows 4.5

Keyboard

- The local on-screen keyboard might appear in the Citrix Receiver for Windows session every time you enter text while using a Microsoft Surface Pro device with an external USB or a wireless keyboard.

  [#LC5093]

Local App Access

- With Local App Access enabled, if the applications are launched inside a remote session in full-screen or windowed mode, the application icons might not be shown on the taskbar of the VDA session. The endpoint might display multiple application icons on the taskbar instead of one.

  [#LC4217]

- Certain SoftPhone applications or Chrome might not display correctly when using Local App Access.

  [#LC4327]

Memory, CPU Optimization

- The SelfServicePlugin.exe process can consume high memory.

  [#LC4509]

Printing

- On occasion, font embedding fails when fonts with symbols embedded are used with EMF printer drivers.

  [#LC3334]

Session/Connection

- The NotificationDelay registry setting controls the delay in the appearance of the connection progress bar for seamless connections. Setting this registry occasionally does not work when using the SelfService Plugin to launch the application. This fix addresses that issue.

  On 32-bit Windows:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: NotificationDelay
  Type: REG_DWORD
  Data: <Delay, in milliseconds>

  On 64-bit Windows:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Name: NotificationDelay
  Type: REG_DWORD
  Data: <Delay, in milliseconds>

  [#LC4969]

- The Single Sign-on process (SSONSvr.exe) might exit unexpectedly or the credentials might not be passed through automatically to the logon screen, causing a prompt to appear to enter the credentials manually.

  [#LC5123]

- After installing Citrix Receiver for Windows and configuring a store through a registry entry or Group Policy Object (GPO), when you log on for the first time after restarting the Virtual Machine (VM), applications might not enumerate.

  [#LC5198]

- When you dictate into SpeechMike along with another speech recognition application, the SpeechMike might stop working.

  [#LC5632]

- During the touch and drag gesture, the mouse button might remain in the down state when using a seamless EPIC application. When you release the touch input outside the seamless EPIC application window, the session might become unresponsive.

  [#LC5644]

- The HDX Engine might exit unexpectedly.

  [#LC6047]

- Attempts to launch a desktop from a Wyse thin client through NetScaler Gateway 11 might result in the following error message:

  "Your client has experienced a problem with authentication to the server."

  [#LC6145]

Smart Cards

- With Citrix Receiver for Windows 4.4 installed, an application published on XenApp 6.5 might send a transaction request

to a smart card to end a non-active transaction. Citrix Receiver for Windows might incorrectly respond to this request by causing the XenApp server to wait for the response forever or the transaction timeout value that is set can expire.

[#LC5772]

User Experience

- This fix provides improved support for sounds that play for a short period of time when using real-time mode for client audio. This fix only applies to medium quality audio.

  [#LC4941]

- File type association might not connect the type of file to the correct icon and application when using Windows 8.1 and Windows Server 2012 R2. With this fix, there are two group policies introduced under "SelfService."
  1. Enable Default FTA - To enable or disable the default behavior of FTA
  2. Enable FTA - To enable or disable the FTA feature
  To get the proper file type association icon, disable the group policy "Enable Default FTA."

  [#LC5485]

- The file type association (FTA) icon might behave like the default Citrix Receiver for Windows FTA icon when you log on to a published desktop or if you reset the Citrix Receiver for Windows configuration.

  [#LC5730]

- Desktops assigned on a client name basis are not enumerated correctly in the SelfService window. This issue occurs when using the StoreFront Unified Experience.

  [#LC5773]

User Interface

- When using VLC Media Player with skin mode and with Local App Access enabled, the endpoint might display multiple taskbar shortcuts instead of one.

  [#LC4744]

- Applications might appear in nested folders when using apps published on XenApp 6.x.

  [#LC5880]

Additional Fixes in Version 4.6

- The wfica32.exe process might not release GDI objects. When the count of GDI objects reaches 1,000, the XenDesktop session window on the user device does not get graphical updates, causing a graphics issue.

  [#654723]

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

Citrix Receiver for Windows 4.6 Known Issues

Dec 08, 2016

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 Window 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/softwareHKCU/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:

PDF Citrix Receiver for Windows Third Party Notices

System requirements and compatibility

Feb 28, 2017

Operating system

Citrix Receiver for Windows	Supported OS
4.6	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
	Windows Server 2008, 32-bit and 64-bit editions

[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 4.6 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 4.6 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 through any 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 sites

  For information about domain-joined and non-domain-joined devices, refer to the XenDesktop 7 documentation.
- For secure remote or local connections:
  - Citrix NetScaler Gateway 11.x
  - Citrix NetScaler Gateway 10.5

  Windows domain-joined, managed devices (local and remote, with or without VPN) and non-domain joined devices (with or without VPN) are supported.

  For information about the NetScaler Gateway and Access Gateway versions supported by StoreFront, see StoreFront system requirements.

About secure connections and certificates

> **Note**
>
> For additional information about security certificates, refer to topics under Secure connections and Secure communications.

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 in place of individual server certificates for any 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, alternatives to wildcard certificates, such as a certificate containing the list of server names within the Subject Alternative Name (SAN) extension, could 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	**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)**
				Yes (NetScaler plug-in)	Yes (NetScaler plug-in)

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

> **Note**
>
> Citrix Receiver for Windows 4.6 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 to 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, which may be required.
  - TLS+HTTPS

Install

Dec 12, 2016

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 Receiver user who obtains Receiver from Citrix.com or your own download site can set up an account by entering an email address instead of a server URL. Receiver determines the NetScaler Gateway (or Access Gateway) or StoreFront Server associated with the email address and then 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 Receiver installed on the device.
  - Email-based account discovery for a first-time user does not apply if Receiver is downloaded from a location other than Citrix.com (such as a Receiver for Web site).
  - If your site requires configuration of Receiver, use an alternate deployment method.
- Automatically from Receiver for Web or from a Web Interface logon screen.
  - A first-time Receiver 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 Receiver user must enter a server URL or open a provisioning file to set up an account.

Receiver does not require administrator rights to install unless it will use 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 this version of Citrix Receiver, the HDX RTME is included in the executable file (.exe).

If you 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 RealTime Media Engine.

> **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:

- The latest version of Citrix ReceiverPlusRTME contains HDX RTME; no further installation is required if you want to install RTME.
- Upgrading from a previous Receiver version to the latest bundled version (Citrix Receiver with RTME) is supported. Previously installed versions of RTME will be overwritten with the latest version; upgrading from the same Receiver version to the latest bundled version (for example, Receiver 4.6 to the bundled Receiver 4.6 plus RTME) is not supported.
- If you have an earlier version of RTME, installing the latest Receiver 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 (GA release) for

compatibility with the new RTME package; that is, RTME 2.0 cannot be used 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

Dec 06, 2016

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.

> ## Important
>
> The process for configuring pass-through authentication (Single Sign-on) has been changed for Citrix Receiver for Windows 4.x. For more information, see the /includeSSON description provided in the Configure and install Citrix Receiver for Windows using command-line parameters section.

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 using Command Line Interface

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 from a user device, 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 Citrix Receiver for Windows using Command Line parameters

Jan 20, 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 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	Installs single sign-on (pass-through) authentication. This option is required for smart card single sign on. 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. 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: • 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) 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. 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.
Sample usage	CitrixReceiver.exe /includeSSON

Enable single sign on when /includeSSON is specified

Option	ENABLE_SSON={Yes | No}

Description	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. 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.
Sample usage	CitrixReceiver.exe /ENABLE_SSON=Yes

Always-on tracing

Option	/EnableTracing={true | false}
Description	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.
Sample usage	CitrixReceiver.exe /EnableTracing=true

Using the Citrix Customer Experience Improvement Program (CEIP)

Option	/EnableCEIP={true | false}
Description	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.
Sample usage	CitrixReceiver.exe /EnableCEIP=true

Specify the installation directory

Option	INSTALLDIR=<Installation Directory>
Description	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. 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.
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... ,>
Description	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. Citrix recommends that you use the ADDLOCAL Sample Usage given below. If the Sample Usage is not used as described, it might possibly cause unexpected behavior. Components include: • 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, if verifies environment parameters and shares them with Storefront (similar to ICO 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 in 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	CitrixReceiver.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d,usb,WebHelper

Configure Citrix Receiver for Windows to manually add Stores

Option	ALLOWADDSTORE={N | S | A}
Description	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: • 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. You can also control this feature by updating the registry key HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore. 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: 1. Set HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore to A to allow users to add non-secure stores. 2. Set HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd to A to allow users to save their passwords for non-secure stores. 3. 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. 4. 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	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: • 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). You can also control this feature by updating the registry key HKLM\Software\[Wow6432Node]\Citrix\Dazzle\AllowSavePwd. Note: The following registry key must be added manually if AllowSavePwd does not work: • 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}
Description	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 notified, and given the option to use an alternate logon method if available. 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.
Sample usage	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

Use CSP components to manage Smart Card PIN entry

Option	AM_SMARTCARDPINENTRY=CSP
	Use CSP components to manage Smart Card PIN entry. By default, the PIN prompts presented to users

Description	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	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. You can also control this feature through a registry key: Create the entry REG_SZ for StartMenuDir and give it the value "\RelativePath". Location: HKLM\Software\[Wow6432Node\]Citrix\Dazzle HKCU\Software\Citrix\Dazzle 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. 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. Examples • If client application folder is \office, UseCategoryAsStartMenuPath is true, and no StartMenuDiris 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. 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.
Sample usage	CitrixReceiver.exe STARTMENUDIR=\Office

Specifying the Store Name

Option	STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On | Off]; [storedescription]" [STOREy="..."]
	Use this option to specify the Store name. Specifies up to 10 stores to use with Citrix Receiver. Values: • 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

Description	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. Note: In this release, it is important to include "/discovery" in the store URL for successful pass-through authentication.
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	SELFSERVICEMODE={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

Display an installation complete dialog during unattended installs

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

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 Citrix Receiver for Windows using Active Directory and sample startup scripts

Dec 06, 2016

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.

To modify the 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

Dec 06, 2016

You can deploy Citrix Receiver for Windows from Citrix Receiver for Web to ensure that users have it installed before they try to connect to an application from a browser. Citrix Receiver for Web sites enable users 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, the user is 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 does not apply 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

Dec 06, 2016

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.

Configure Citrix Receiver for Windows

Dec 06, 2016

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.

Configuring application delivery

Dec 06, 2016

When delivering applications with XenDesktop or XenApp, consider the following options to enhance the experience for users when they access their applications:

- Web Access Mode - Without any configuration, Citrix Receiver for Windows provides browser-based access to applications and desktops. Users simply open a browser to a Receiver for Web or Web Interface site to select and use the applications that they want. In this mode, no shortcuts are placed on the user's desktop.
- Self Service Mode - By simply 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 users 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 needed.

Note: By default, Citrix Receiver for Windows allows users to select the applications they want to display in their 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 users to find all their published apps within the familiar Windows navigation schema where users 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 GPO

Citrix recommends using the Group Policy Object 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 / receiver.adml 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.

To add or specify a NetScaler Gateway via 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.
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.

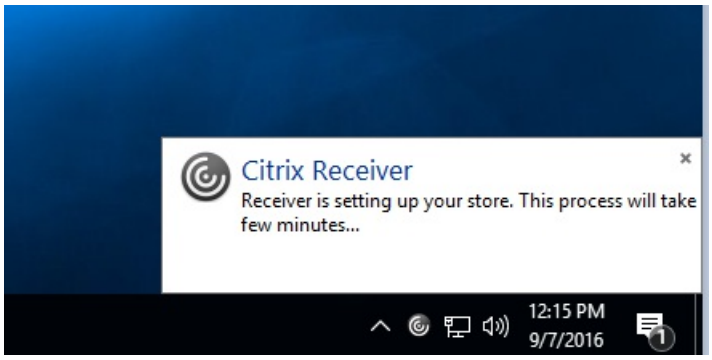
- Store name – Indicates the displayed store name
- Store URL – Indicates the URL of the store
- #Store name – Indicates the name of the store behind NetScaler Gateway

- 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 via GPO, the below message is displayed 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.

Using the Group Policy Object template to customize app shortcut locations

> **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 the return to the Group Policy Editor.
6. In the Group Policy Editor, got 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', useDontCreateAddRemoveEntry. 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.

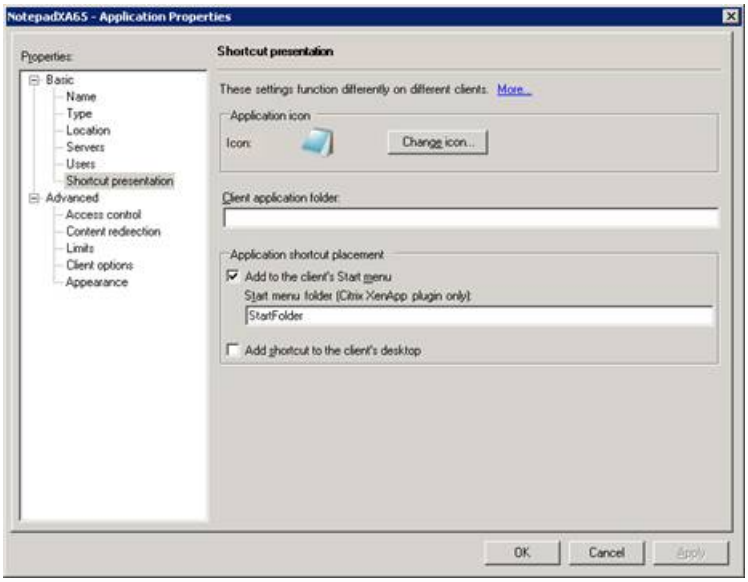
If you want to set the location of shortcuts so every user finds them in the same place use XenApp per App Settings:

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:

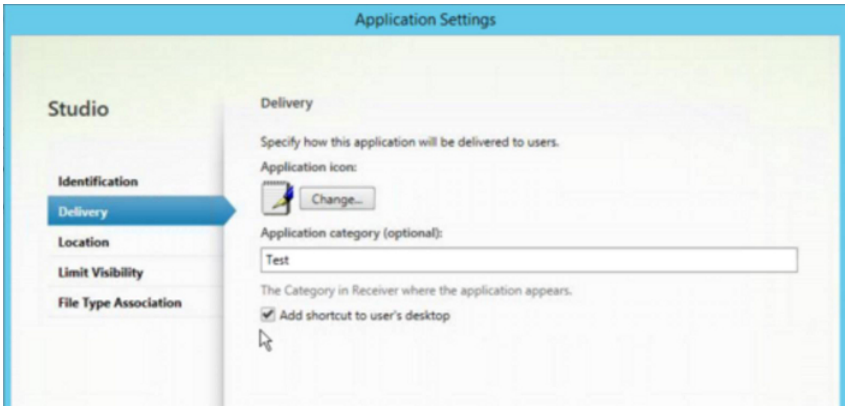
1. In the XenApp Application Properties screen, expand Basic properties.
2. Select the Shortcut presentation option.
3. In the Application shortcut placement portion of the Shortcut presentation screen, select the Add to the client's Start menu check box. After selecting the check box, enter the name 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 *auto-provisioned* and *mandatory* 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 *auto provisioned* and *mandatory* 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 shortcut 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

Dec 06, 2016

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 Enlightened Data Transport

EDT Requirements

- XenApp and XenDesktop 7.12 or higher (required to enable the feature using Studio).
- StoreFront 3.8.
- IPv4 VDAs only. IPv6 and mixed IPv6 and IPv4 configurations are not supported.

> ### Note
>
> Enlightened Data Transport is currently for evaluation purposes only and is not supported for production use. Refer to the License Agreements (EULAs) and Service Agreements (EUSAs) for terms and conditions.

EDT must be configured on the VDA by applying the Policy before it is available for communication between the VDA and Citrix Receiver.

The new data transport layer (EDT) is allowed by default in Citrix Receiver for Windows, however, by default, the client will only attempt to use EDT if the VDA has been configured to **Preferred** with in the Citrix Policy and the settings has been applied to the VDA.

If you want to disable EDT on a specific client, set the EDT options appropriately using the Citrix Group Policy Object.

To configure EDT using a Group Policy Object (GPO) (optional)

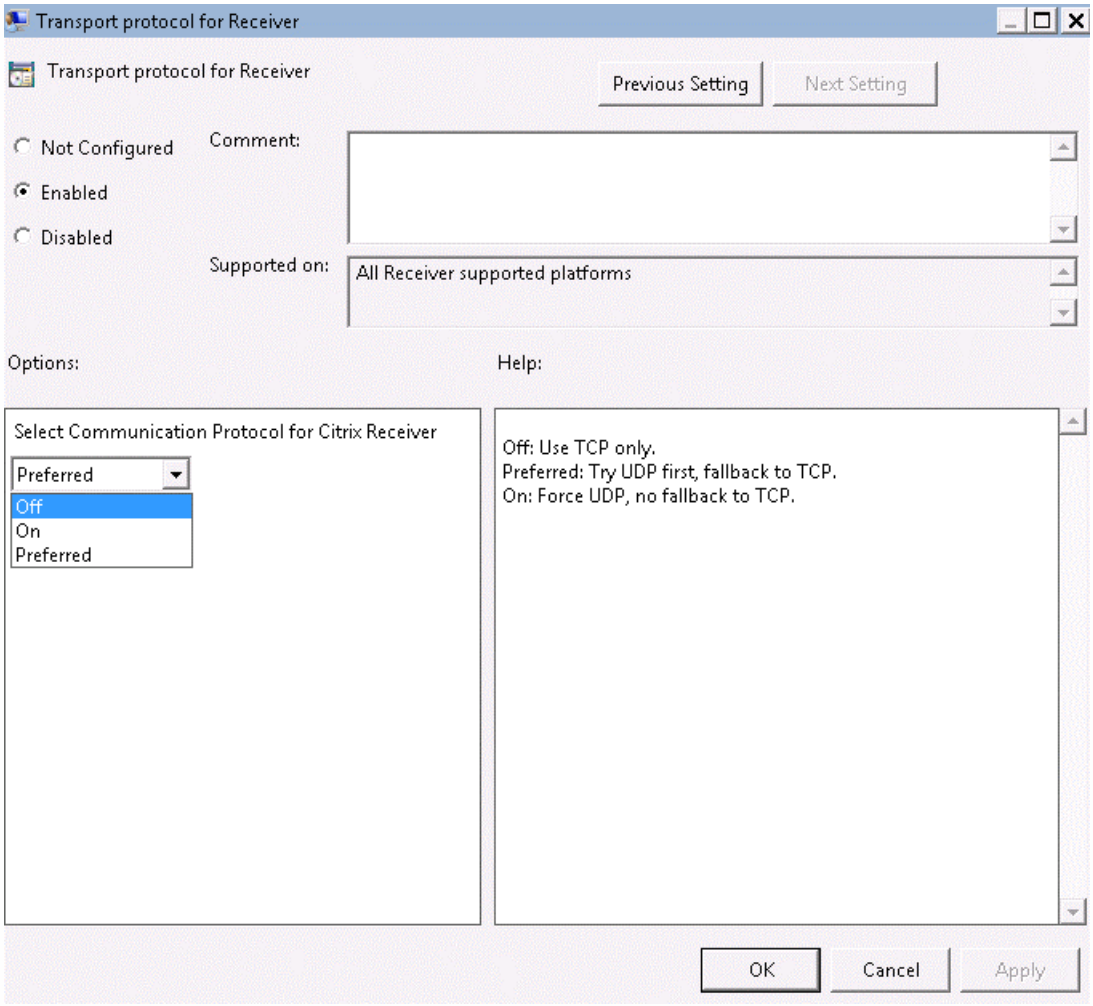
The following are optional configuration steps to customize your environment for the evaluation of this feature. For example, you may choose to disable the feature for a particular client for security reasons.

> ### Note
>
> By default, Enlightened Data Transport is disabled (Off) and TCP is always used.

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.

   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. Open command prompt.
7. Run gpupdate /force command.

Additionally, for the EDT 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:

- Check if the registry is updated to include HDXOverUDP key at HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT.

Configuring USB support for XenDesktop and XenApp connections

USB support enables users to interact with a wide range of USB devices when connected to a virtual desktop. Users 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 XenDesktop and XenApp session, and so do 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 device 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
WSCSupported	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

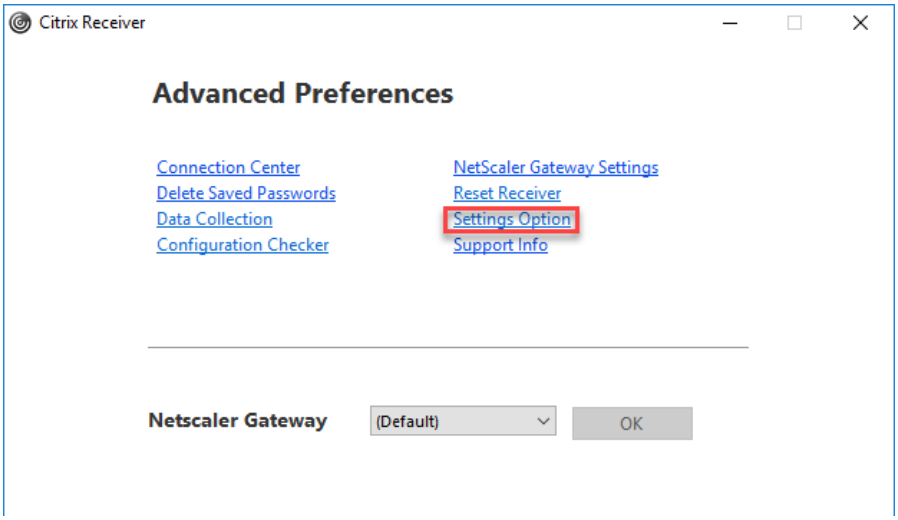
		HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	"" (empty)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle 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

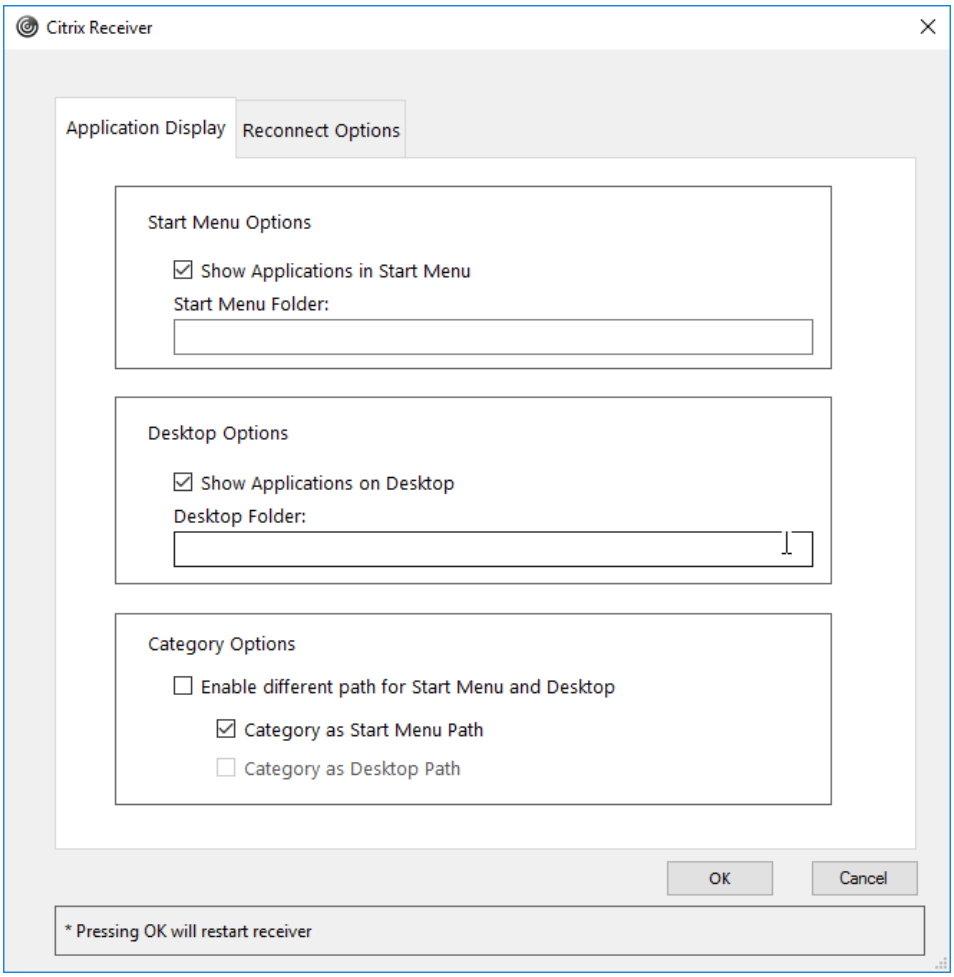
> **Note**
>
> Shortcuts can be set only for the subscribed applications and desktops.

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 Pat**h 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

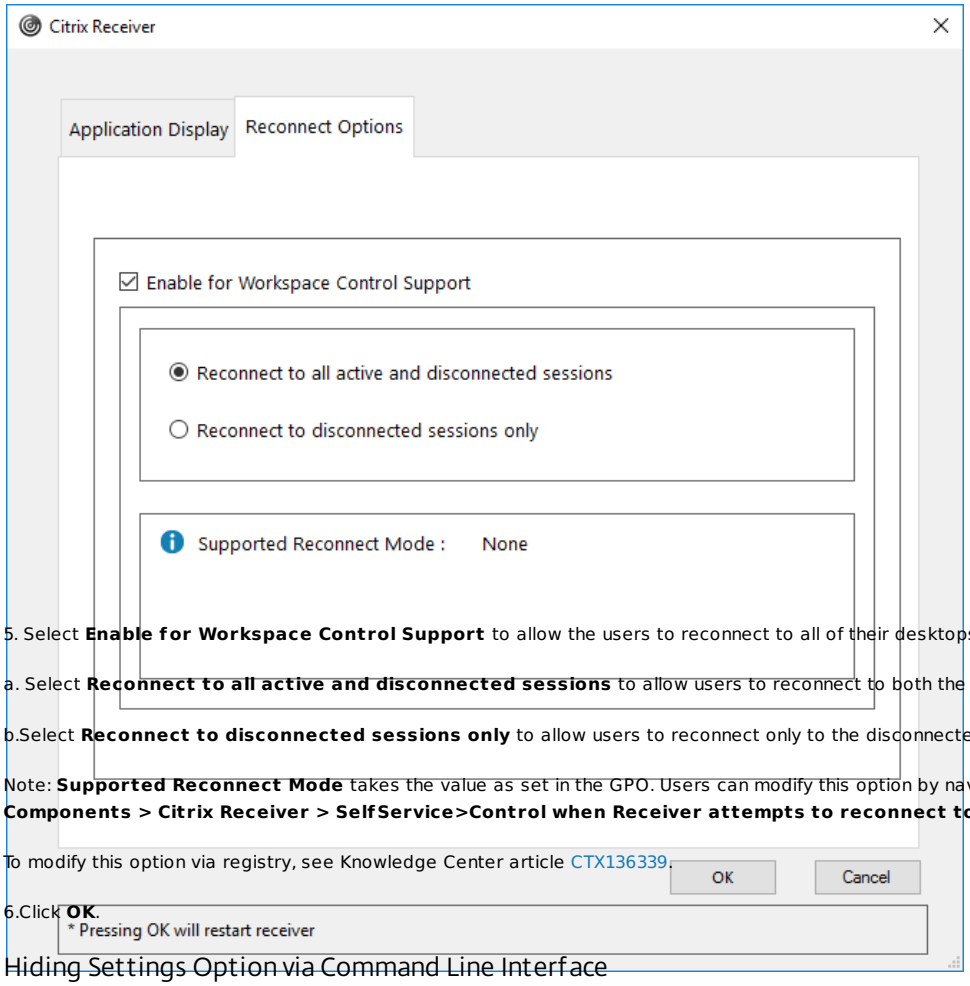
After logging on to the server, users can reconnect to all of their desktops or applications at any time. By default, Reconnect Options opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect Options to reconnect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

6.Click **OK**.

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

Configuring Citrix Receiver for Windows with the Group Policy Object administrative template

Mar 02, 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.

Note

The .adm file is for use with Windows XP Embedded platforms only. The .admx/.adml files are for use with Windows Vista/Windows Server 2008 and all later versions of Windows.

Note

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.

Note

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.

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]

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 Template**s 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

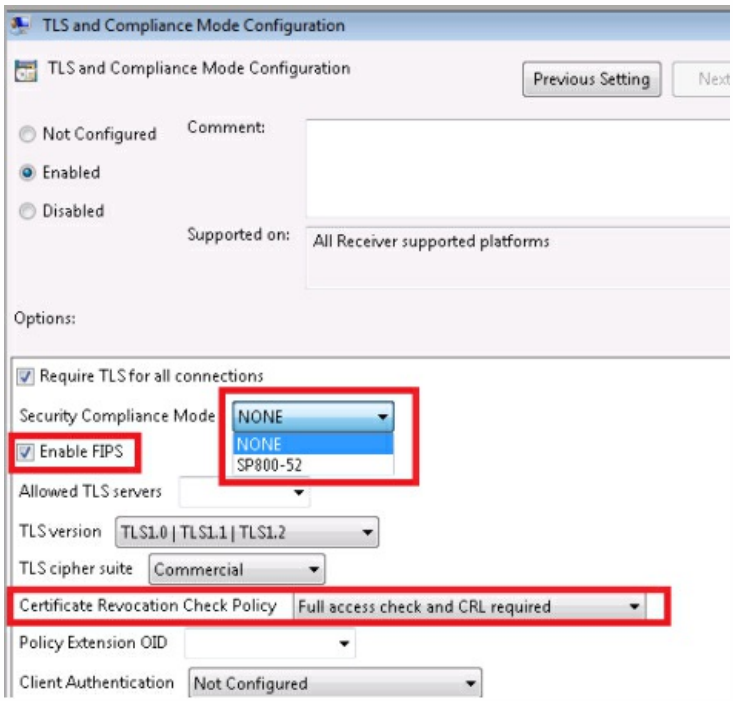
Use this policy to configure the TLS options that ensure Citrix Receiver for Windows securely identifies the server that it is connecting to, and encrypts all communication with the server.

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.

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	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.

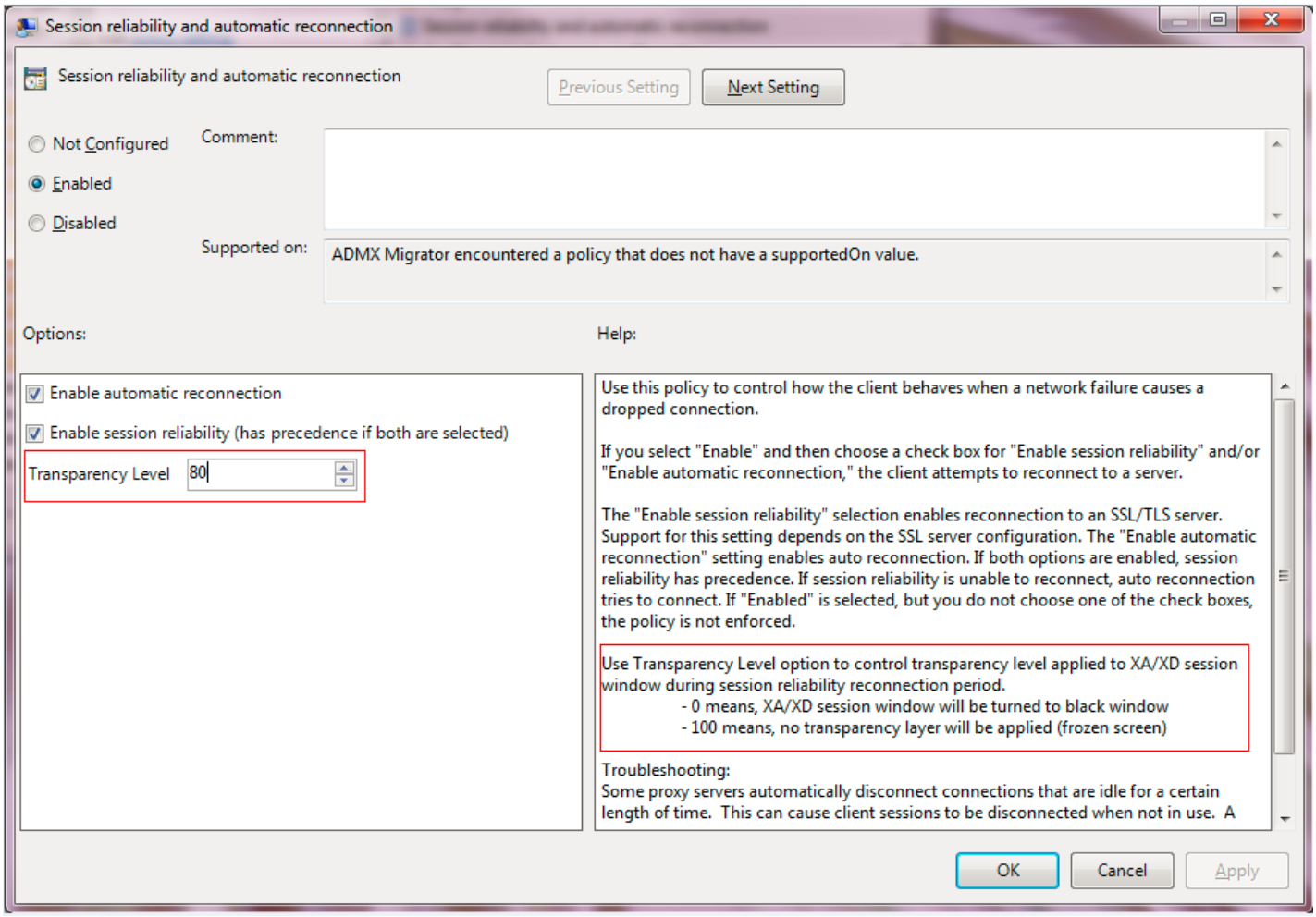
Session reliability group policy

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 - > Administrate Templates-> Citrix Components - >**

Network Routing -> Session reliability and automatic reconnection - > Transparency Level.

> **Note**
>
> By default, Transparency Level is set to 80.



Providing users with account information

Dec 06, 2016

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**
>
> Advise first-time Citrix Receiver for Windows users to restart Citrix Receiver for Windows after installing it. Restarting Citrix Receiver for Windows ensures that users can add accounts and that Citrix Receiver for Windows can discover USB devices that were in a suspended state when Citrix Receiver for Windows was installed.

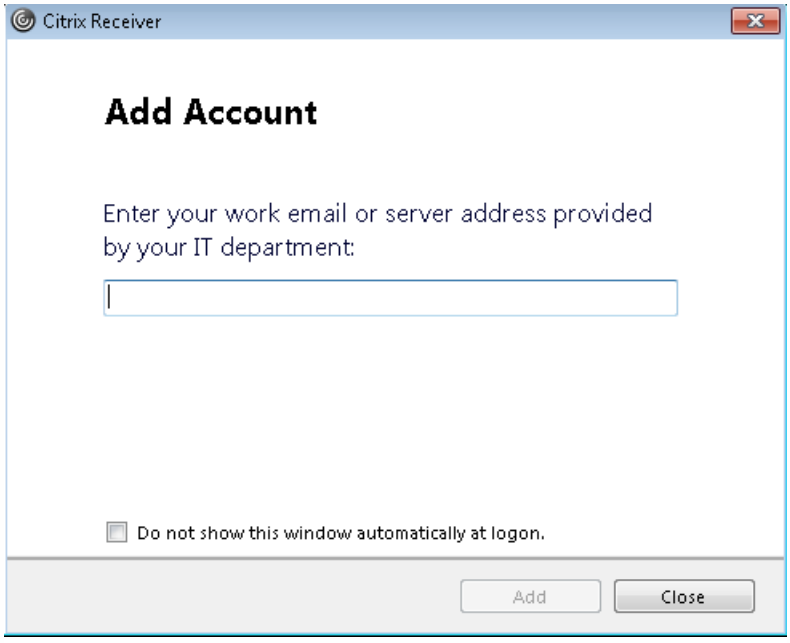
Suppressing Add Account dialog

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**



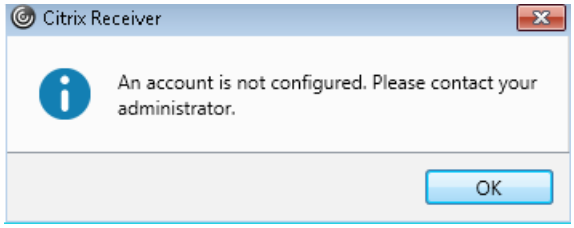
Select **Do not show this window automatically at logon** to prevent the Add Account window to pop-up on

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.

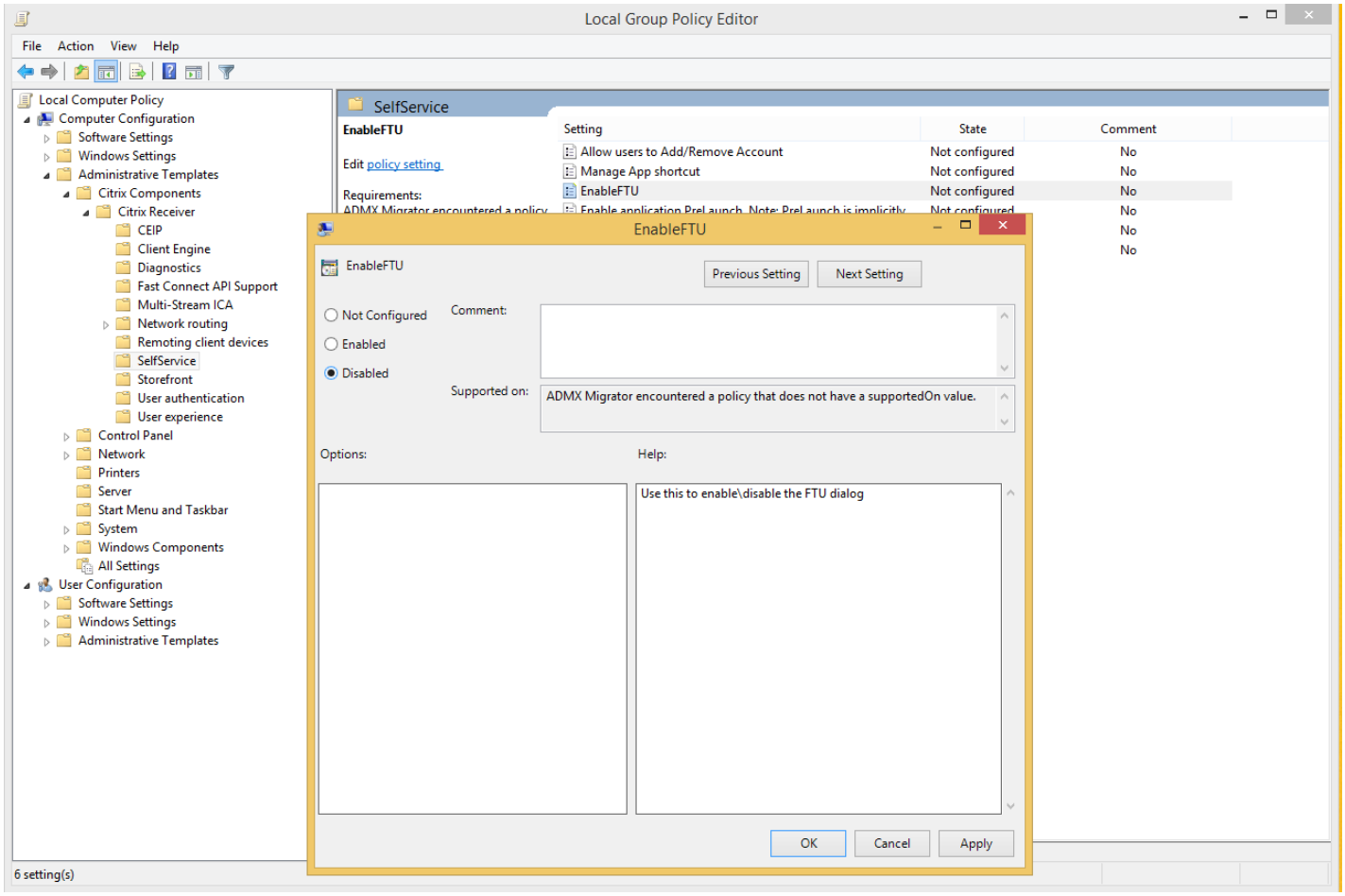
The following message is displayed when Store is not configured.



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 Citrix Receiver for Windows environment

Dec 06, 2016

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:

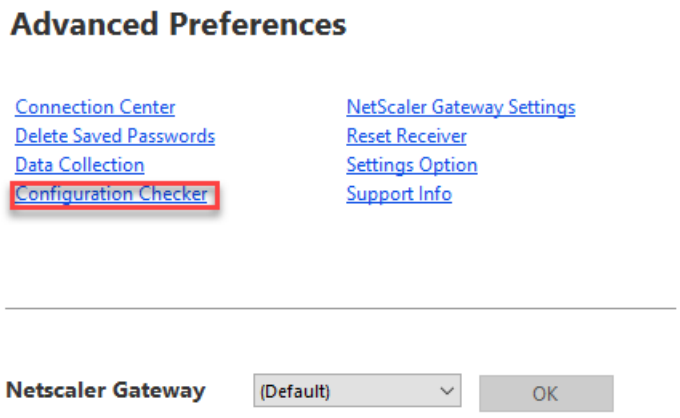
HH:MM|M:T:W:TH:F:S:SU where HH and MM are hours and minutes. M:T:W:TH:F:S:SU are the days of the week. For example, to enable scheduled pre-launch on Monday, Wednesday, and Friday at 1:45 p.m., set Schedule as Schedule=13:45|1:0:1:0:1:0:0 . The session actually launches between 1:15 p.m. and 1:45 p.m.

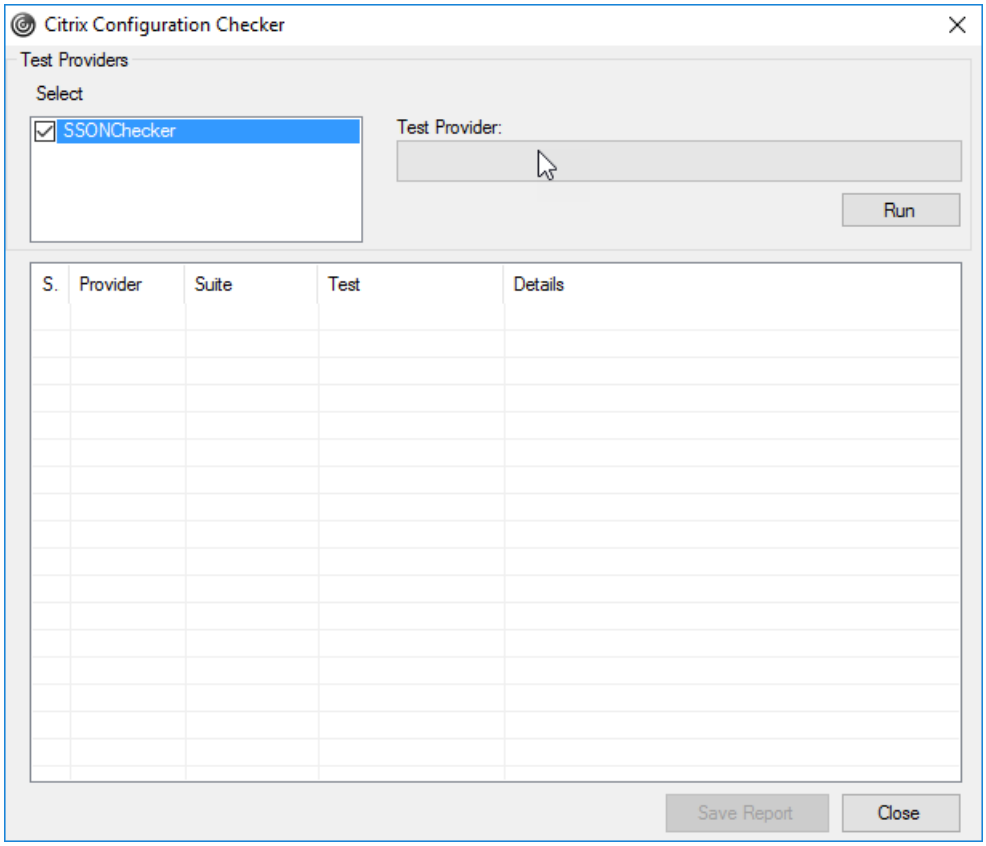
HKEY_CURRENT_USER registry values

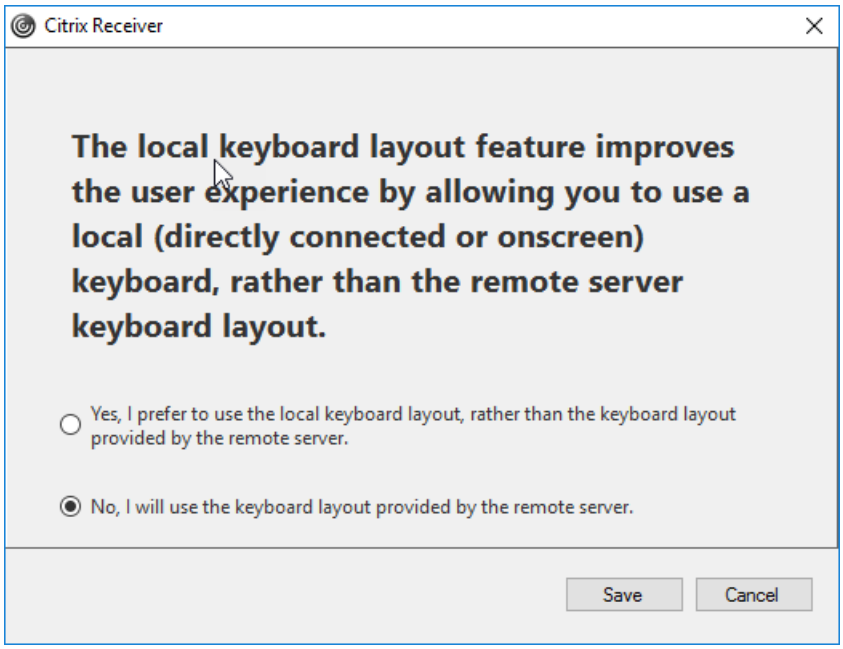
HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

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

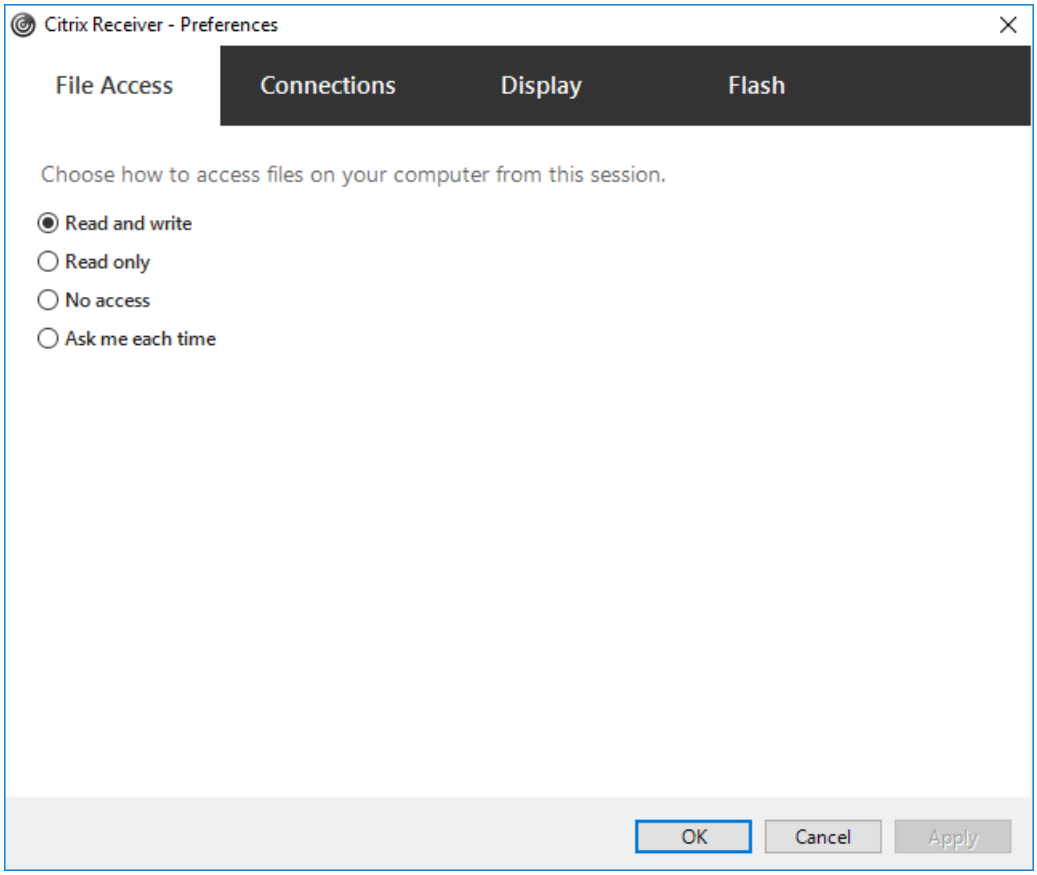
-
-
-

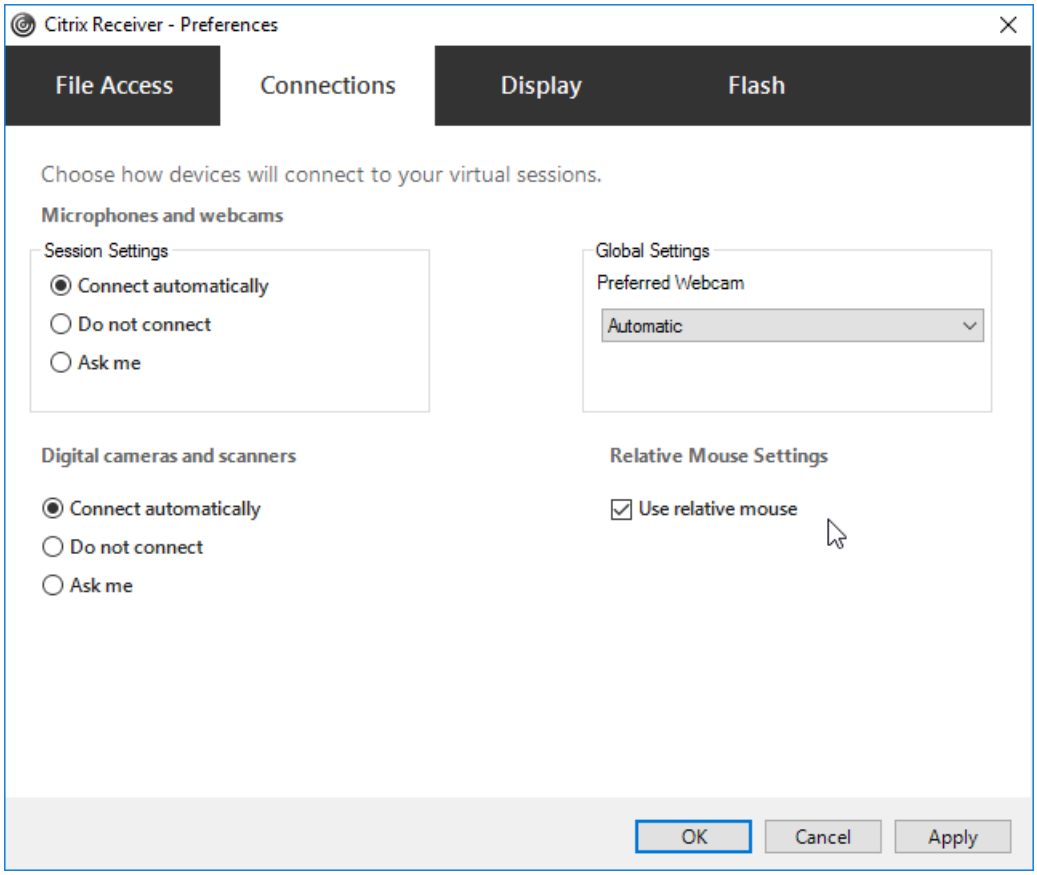


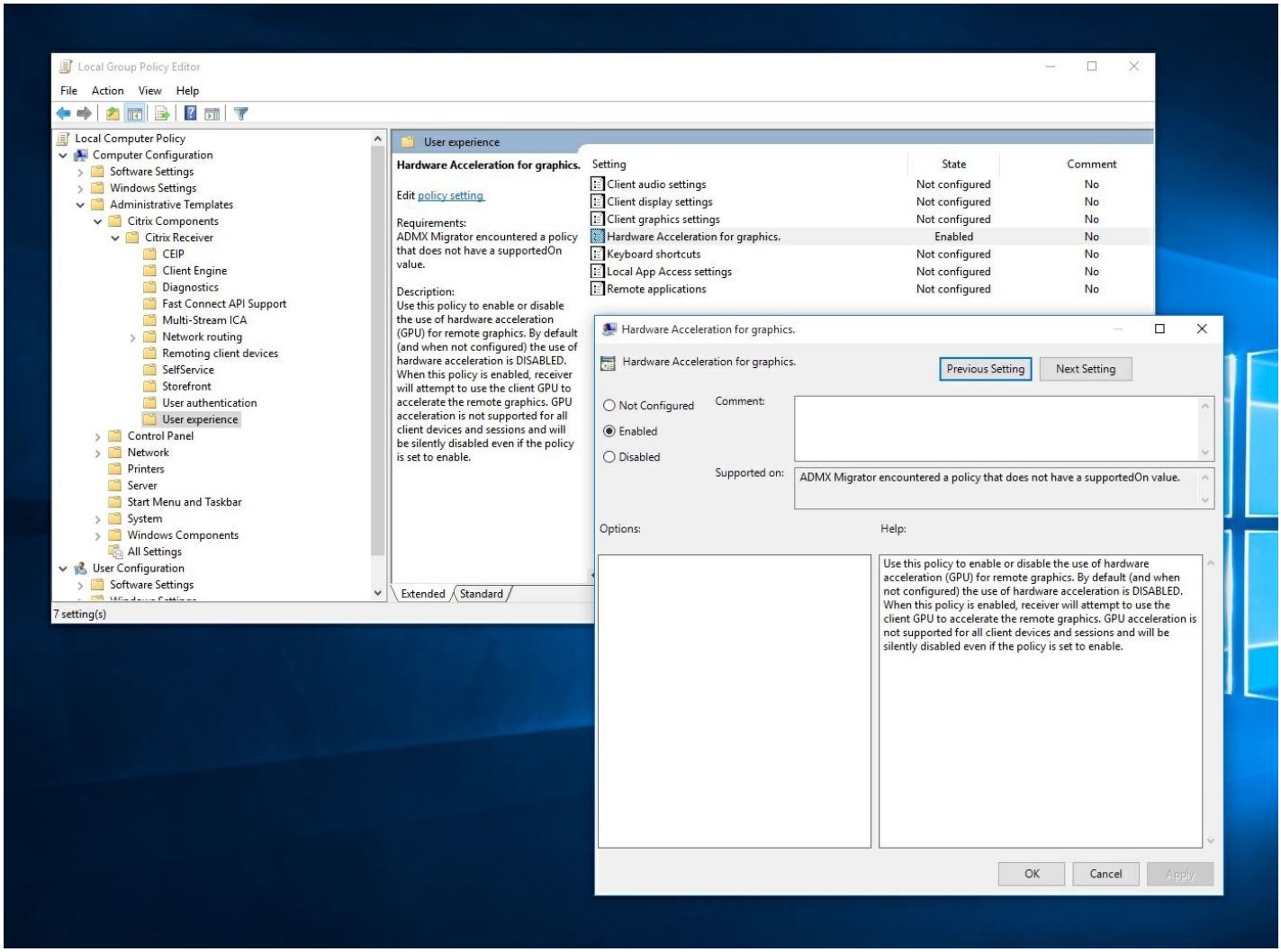




-
-
-
-







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\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.
The keys can be set to 3 different modes as given below:

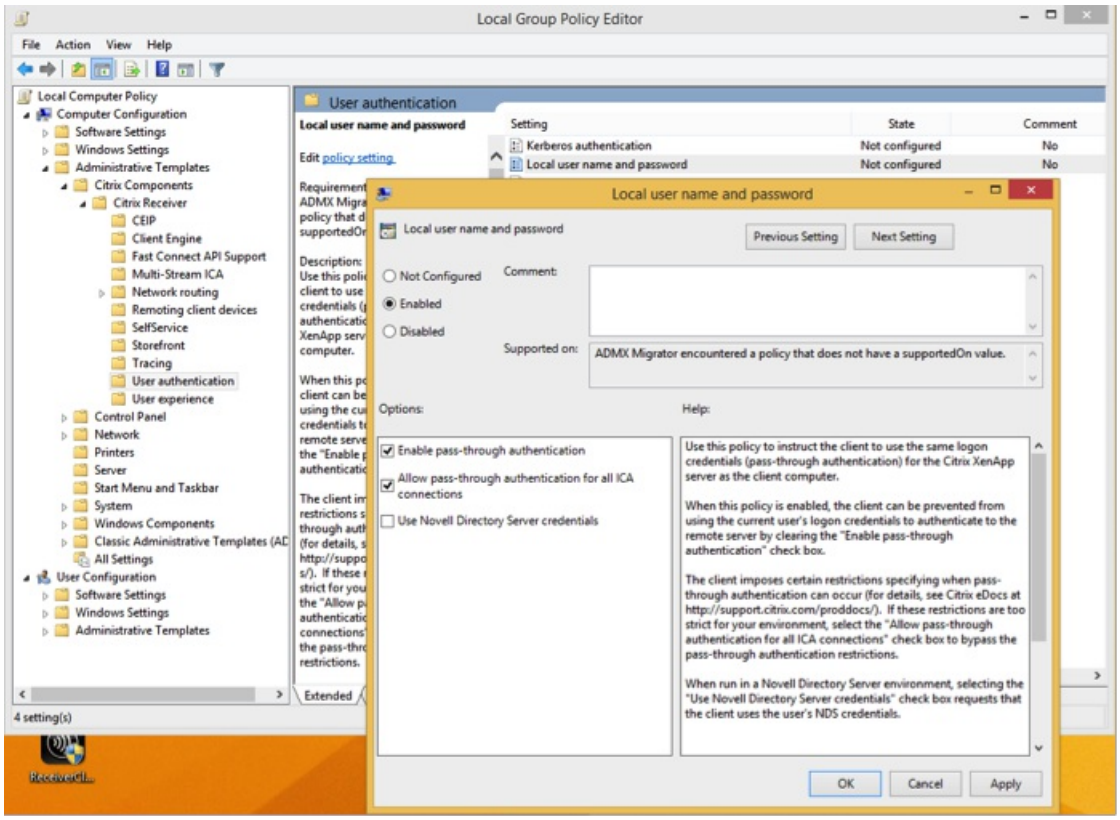
- **Automatic**: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Always popup** (on-screen keyboard): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Never popup** (on-screen keyboard): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

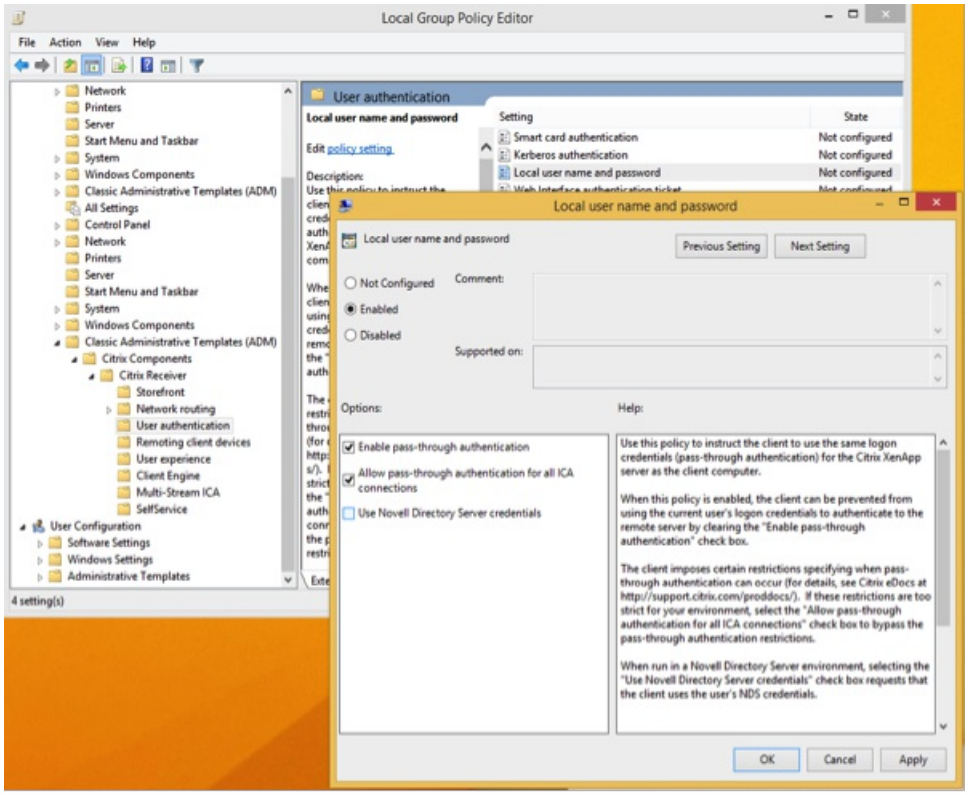
-
-
-

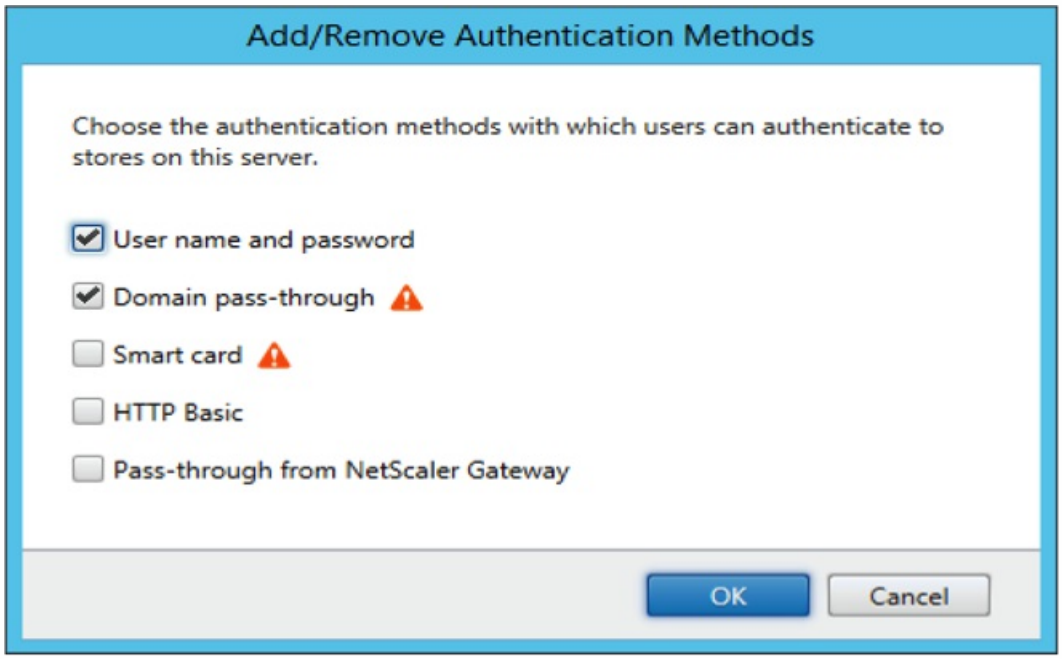
-
-

  -
  -

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.







-
-
-

-

- DisableCtrlAltDel false

-

-
  -
  -
-

DisableCtrlAltDel False

-
-
  -
  -
-
-

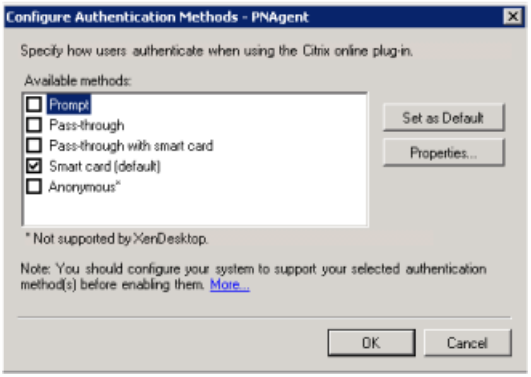
-
-
-
-
-
-
-
-
- SSONCheckEnabled false

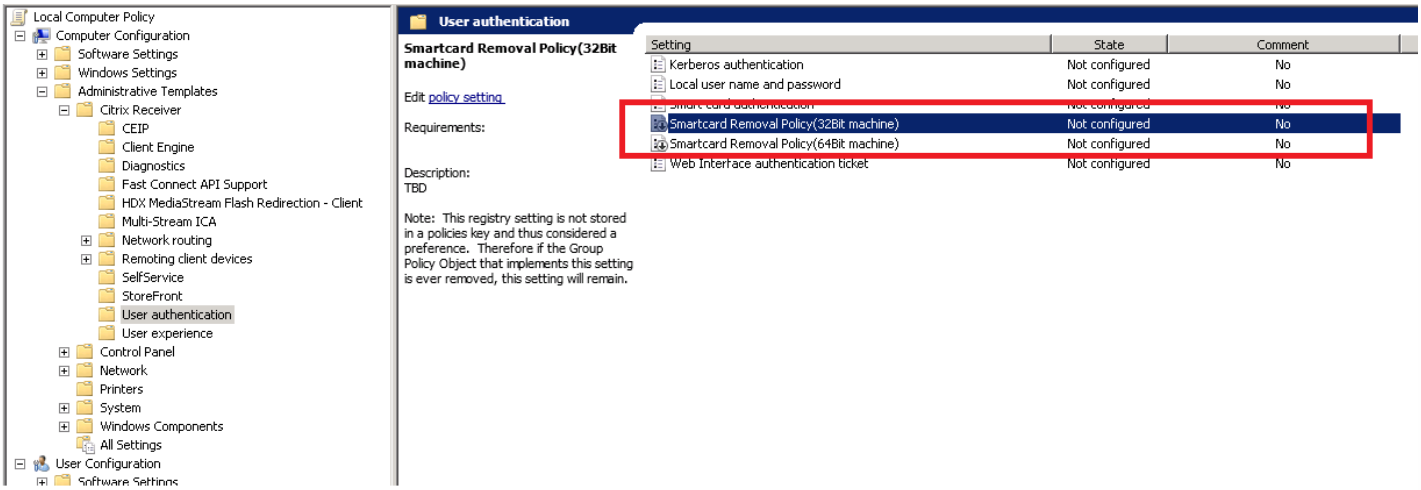
- /includeSSON
- /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
-
-
-
-
-
-
-
-

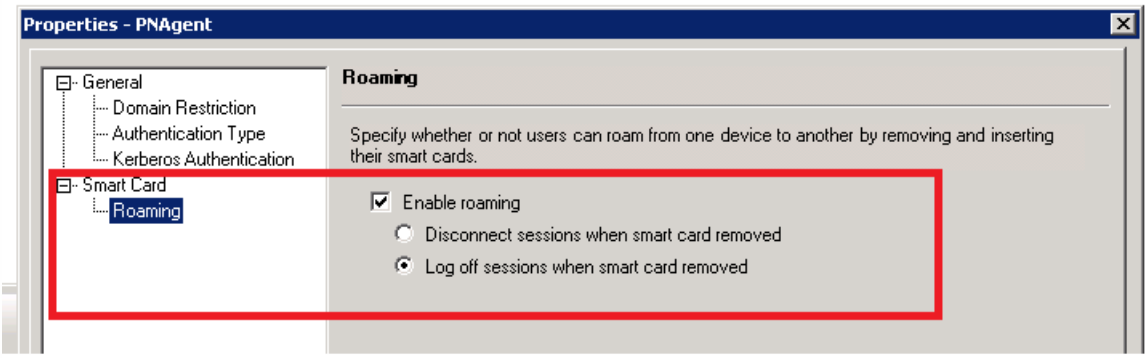
-
-
-

-
-
-
-

-
-
-
-
-
-







-
-

-
-

-
-
-
-
-
-
-

-
-

-
-
-

-
-
-
-
-
-

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.

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

-
-

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.

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, use the Group Policy template to 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. Choose Add and browse to the Receiver Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select 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 correct 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.

ICA File Signing to protect against application or desktop launches from untrusted servers

Dec 06, 2016

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).

Option	Description
launches (less secure)	

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 - > Administrate 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

check and CRL required All'.

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

Dec 06, 2016

You can use the Citrix Receiver for Windows Desktop Lock when users do not need to interact with the local desktop. Users 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.x.

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 end points.
- 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.