Receiver for Windows 3.3

2015-01-12 12:44:51 UTC

Contents

Receiver for Windows 3.3

Quick Links

About this Release	Configuring Receiver for Windows
Issues Fixed in Receiver for Windows 3.3	Optimizing the Receiver Environment
System Requirements and Compatibility	Improving the User Experience
Licensing Your Product	Securing Your Connections
Installing Receiver for Windows	Securing Receiver Communication
Configuring and Installing Receiver for Windows Using Command-Line Parameters	

Product documentation is also available for Receiver for Windows Enterprise 3.4 and 3.3.

About Receiver for Windows 3.3

Citrix Receiver for Windows provides users with self-service access to resources published on XenApp or XenDesktop servers. Receiver combines ease of deployment and use, and offers quick, secure access to hosted applications, desktops, and data. Receiver also provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications. You can use it for Web access or configure it for use with Citrix CloudGateway.

What's New

Citrix Receiver for Windows 3.3 provides the following new features and enhancements.

- **Simplified use for first-time and returning users:**
  - Users have just one package choice when installing Receiver for Windows 3.3 from the Citrix.com or your own download site.
  - Users can set up a Receiver account by entering an email address or a server URL. Receiver determines the Access Gateway, StoreFront server, or AppController virtual appliance associated with the email address and then prompts the user to log on and proceed with the installation.
  - The simplified interface no longer includes a Preferences panel.
- **Template to create a site-specific download site.** For administrators who need more control, Citrix provides a template that you can use to create a download site for Receiver.
- **Automatic updates.** For Receivers installed from Citrix.com or your download site, a new update service built in to Receiver automatically handles updates, in most cases silently. Receiver Updater for Windows is needed only if you prefer to use Merchandising Server to distribute Receiver and its updates.
- **Access to SaaS apps from outside the firewall without a VPN.** Receiver for Windows 3.3 does not require a VPN connection to access SaaS apps remotely. (Enterprise Web apps published and accessed through CloudGateway still require a VPN connection.)
- **Hosted Shared desktops.** Receiver for Windows now supports server desktops published with Citrix XenApp. The desktops are displayed through the Desktop Viewer. To configure this feature, see the XenApp, StoreFront, or Web Interface documentation.

Receiver for Windows Enterprise

The only changes to the Receiver Enterprise package (CitrixReceiverEnterprise.exe) in this release are the fixed issues referenced at the end of this topic. For information, refer to Receiver for Windows Enterprise.

Known Issues

This section contains:

- Installation and upgrade issues
- General issues
- Known issues - Desktop connections
- Third-party issues

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.

Installation and upgrade issues

- Installation of Receiver for Windows 3.3 by a user fails if Receiver for Windows was previously installed by an administrator. [#300624]

- The documented syntax for uninstalling Receiver from a command line does not work. To uninstall Receiver from a command line, use CitrixReceiver.exe -uninstall. [#335780]

- If a user uninstalls a plug-in using the Control Panel and restarts the computer, the plug-in continues to display in the list that appears when you right-click the Receiver icon, click About and then expand Advanced. This occurs only when Receiver is installed from Citrix.com or your own download site. [#320277]

- Plug-in updates on Windows XP, 64-bit edition, fail. To work around this issue, install the hotfix available from http://support.microsoft.com/kb/968730/en-us. [328081]

- If you previously installed the ShareFile for Receiver for Windows Tech Preview, follow these steps to remove the Technology Preview software and perform a clean installation of Receiver for Windows 3.3:

    1. Uninstall the ShareFile plug-in using the ShareFilePlugin.exe file, located in C:\Program Files\Citrix\ShareFilePluginForReceiver.

    2. Download the Receiver for Windows 3.3 installation package, CitrixReceiver.exe, and open it.

    3. Select Uninstall Citrix Receiver and follow the on-screen instructions.

    4. When the uninstallation is complete, select Install CitrixReceiver.exe and follow the on-screen instructions. [#327752]

- You might receive an error message when trying to launch an application with Web Interface after installing a previous version of the Receiver (Online plug-in) while logged in as one user, upgrading with CitrixReceiver.exe as another user, logging off the Receiver, and logging back on with the previous user name. The error message is: Citrix online plug-in Configuration Manager: No value could be found for (ClientHostedApps) that satisfies all lock down requirements. The lockdown requirements in force may be conflicting. [#261877]

    As a workaround, set the following registry key:

    HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Control

    Name: ClientHostedApps

    Value: FALSE (or set to * / TRUE if you have overridden the defaults in HKEY_LOCAL_MACHINE)

- If you use Web Interface with Internet Explorer 8 and Windows 7 to upgrade to this version of Citrix Receiver, the upgrade finishes, but the Upgrade in Progress message remains on the screen and the log on screen does not appear. Workaround: Restart the browser [#247858]

- Before installing Receiver for Windows on a Windows XP Embedded thin client device, increase the RAM disk limit of the device to 100 MB. [#266384]

- When the offline plug-in is not installed and a streamed application is configured to fallback to ICA and the XenApp server is down, an incorrect error message appears informing you that the correct plug-in is not installed. [#273813]

General Issues

- When configured with multiple stores, Receiver might confuse the gateways required to connect to a store causing incorrect apps being available to users. Work around: Configure only one store. [#263165]

- Receiver for Windows can experience issues with automatic reconnection under the following conditions: CitrixReceiver.exe or CitrixReceiverEnterprise.exe is connected to a Web Interface site and the default.ica file contains the entry SessionReliabilityTTL=60. To work around this issue, edit the default.ica file and either remove the SessionReliabilityTTL entry (to use the default value of 180) or change the entry to SessionReliabilityTTL=180. [#373506]

- When StoreFront is configured with multiple external beacon points, Receiver for Windows does not enumerate applications if all of the beacons respond with the same URL. Workaround: Retain the configuration for only one external beacon. Alternatively, keep all beacons and add a beacon that points to a non-existing URL. [#299560]

- If you use the Receiver with XenApp 5.0 Feature Pack 2 for Windows Server 2003 (32- or 64-bit editions), the Receiver plays audio even when you configure the Turn off speakers policy setting to disable the audio. [#242703]

- When you launch applications using the Web Interface, Connection Center does not enumerate the sessions. [#261177]

- After you launch a published application that is filtered by XenApp for Access Gateway, other published applications do not launch. [#263003]

- In some environments, content redirection may not work until the published application is launched for the first time. [#252515]

- When versions of Receiver are localized in Traditional Chinese, Korean, or Russian and integrated with Access Gateway Standard Edition, the Receiver log on screen displays in English because of an Access Gateway Standard Edition language limitation. [#263442]

- If Certificate Revocation List (CRL) checking is disabled in Internet Options on the user device, this overrides the CertificateRevocationCheck registry setting for Receiver for Windows. This means users may be able to access Web sites that do not have valid certificates. As a workaround, ensure that the Check server revocation option located at Settings > Control Panel > Internet Options > Advanced is enabled. [#32682]

- Receiver does not support the VPN keyword in Access Gateway ClientChoices mode. [#274828]

- If the VPN keyword is removed from an application after a user subscribes to it, Receiver continues to attempt an Access Gateway connection for the application. Workaround: Unsubscribe and then re-subscribe to the application to synchronize the VPN keyword removal on Receiver. [#298387]

- If synchronization progress overlays do not appear in Windows Explorer for files and folders, restart your computer. [#319284]

- The Receiver icon is displayed instead of an application icon in the task bar when an application is launched from Receiver using XenApp 5.0 and earlier versions. [#310366]

Desktop Connections

- The documentation for Receiver for Windows 3.3 contains information about desktop lock. That feature is available only for Receiver for Windows Enterprise.
- Loss of video is experienced if files are being played with a published version of Windows Media Player through a virtual desktop session, and the Desktop Viewer window is changed from full-screen to window mode. As a workaround, minimize and restore the Media Player window, and then pause and resume the application (or stop and restart it). [#246230]
- You cannot log off normally from Windows XP 32-bit virtual desktops if you start (but do not log on to) the Receiver in the desktop session. If the Receiver logon dialog box is not completed, you cannot log off from the desktop. To work around the issue, complete the logon dialog box or close it. This issue is not observed on other virtual desktop operating systems. [#246516]
- If virtual desktops are installed with the Virtual Desktop Agent supplied with XenDesktop 5.0, Receiver for Windows 3.0 displays an error if the user starts a published application from the desktop. The workaround is to use the Virtual Desktop Agent supplied with XenDesktop 5.5. [#263079]
- The Citrix Desktop Lock does not redirect Adobe Flash content to domain-joined user devices. The content can be viewed but is rendered on the server, not locally. As a workaround, Adobe Flash redirection can be configured for server-side content fetching to pass the content from the server to the user device. This issue does not occur on non-domain-joined devices or when the content is viewed with the Desktop Viewer. [#263092]
- The Desktop Viewer Devices menu may not close when the user clicks the Devices icon. It also may remain open after its corresponding dialog box closes. If this occurs, click the Devices icon again. [#262202]
- Windows Media Player, when displayed in the non-primary monitor of a two-monitor Windows user device, may not work as expected. Due to an issue with the DirectX video mixing renderer filter VMR-9, the screen is black and there is no sound, although the player's progress bar advances. To correct this issue, edit the registry on the user device from which the XenDesktop connection is launched. In the HKEY_CURRENT_USER\Software\Citrix subkey, create the HdxMediaStream key. Name the key DisableVMRSupport. Set the type as REG_DWORD. Give the key the value 3. [#262852]

Third-Party Issues

- When using Internet Explorer to open a Microsoft Office document in Edit mode from SharePoint, Microsoft Office might display the message, “Access denied.” Workaround: Go to the SharePoint site and check out the document, edit it, and check the file back in to SharePoint. [#258725]

Fixed Issues

For issues fixed in this release, click the link for Receiver for Windows 3.3 in Issues Fixed in XenApp, XenDesktop, and Component Technologies.

System Requirements and Compatibility for Receiver for Windows

Device

Operating system

The following list of requirements specifies edition or service pack only where support is limited.

- Windows 8, 32-bit and 64-bit editions (including Embedded Edition)
- Windows 7, 32-bit and 64-bit editions
- Windows XP Professional, 32-bit and 64-bit editions (including Embedded Edition)

  Support for Windows XP ends April 8, 2014 when Microsoft ends extended support for Windows XP. Support for Windows XP Embedded will continue.
- Windows Vista, 32-bit and 64-bit editions
- Windows Thin PC
- Windows Server 2008 R1, 32-bit and 64-bit editions
- Windows Server 2008 R2, 64-bit edition
- Windows Server 2003, 32-bit and 64-bit editions

Hardware

- VGA or SVGA video adapter with color monitor
- Windows-compatible sound card for sound support (optional)
- For network connections to the server farm, a network interface card (NIC) and the appropriate network transport software

Server

- XenApp (any of the following products):
    - Citrix XenApp 6.5 for Windows Server 2008 R2
    - Citrix XenApp 6 for Windows Server 2008 R2
    - Citrix XenApp 5 for Windows Server 2008
    - Citrix XenApp 5 for Windows Server 2003
    - Citrix XenApp 4, Feature Pack 1 or 2, for UNIX operating systems
- XenDesktop (any of the following products):
    - XenDesktop 5.6
    - XenDesktop 5.5
    - XenDesktop 5
    - XenDesktop 4
- To manage connections to apps and desktops, Citrix Receiver supports CloudGateway or Web Interface.

  CloudGateway:

    - CloudGateway Express, with StoreFront 1.2, 1.1 or 1.0

      For direct access to StoreFront stores.
    - CloudGateway Express, with StoreFront 1.2, 1.1 or 1.0 configured with a Receiver for Web site

      For access to StoreFront stores from a web browser.
    - CloudGateway Enterprise 2.0 or 1.0, with StoreFront 1.2, 1.1 or 1.0

      For access to Windows, Web, and Software as a Service (SaaS) apps.

  Web Interface:

    - Web Interface 5.4 for Windows with Web Interface sites

      For access to apps and desktops from a Web browser.
    - Web Interface 5.4 for Windows with XenApp Services or XenDesktop Services sites and the PNAgent plugin
- Merchandising Server 2.*x*

Browser

- Internet Explorer Version 6.0 through 9.0

  Connections to StoreFront or Web Interface support the 32-bit mode of Internet Explorer.

- Mozilla Firefox Version 1.*x* through 5.*x*

- Google Chrome Version 10.0 and later (requires StoreFront)

Connectivity

Citrix Receiver for Windows supports HTTPS and ICA-over-SSL connections through any one of the following configurations.

- For LAN connections:

  - StoreFront using StoreFront services or Receiver for Web sites

    Single sign on to Web and SaaS apps published through AppController requires StoreFront 1.2 or 1.1.

  - Web Interface 5.*x* for Windows, using Web Interface sites

  Windows non-domain joined, kiosk, managed devices (with or without Desktop Lock) and domain-joined (with Desktop Lock), managed devices (repurposed PCs) are supported for LAN only connections.

- For secure remote or local connections:

  - Citrix Access Gateway Enterprise Edition 10

  - Citrix Access Gateway Enterprise Edition 9.*x*

  - Citrix Access Gateway VPX

  - Citrix Access Gateway 5.0

  - Citrix Secure Gateway 3.*x* (for use with Web Interface only)

  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 Access Gateway versions supported by StoreFront, refer to the Access Gateway and StoreFront documentation in eDocs.

Certificates

For information about security certificates, refer to topics under Secure Connections and Secure Communications.

Authentication

Receiver for Windows 3.3, when used with StoreFront 1.2, 1.1 or 1.0, supports the following authentication methods:

- Domain
- Domain pass-through

  Receiver for Web sites do not support domain pass-through authentication.
- Security token*
- Two-factor (domain plus security token)*

* Available only in deployments that include Access Gateway.

Receiver for Windows 3.3, when used with Web Interface 5.X, supports the following authentication methods. (Web Interface uses the term "Explicit" for domain and security token authentication.)

- Domain
- Domain pass-through
- Security token*
- Two-factor (domain plus security token)*
- SMS*
- Client certificate* (can be used alone or with other authentication methods)

* Available only in deployments that include Access Gateway.

For information about authentication, refer to the Access Gateway documentation and the "Manage" topics in the StoreFront documentation in eDocs. For information about other authentication methods supported by Web Interface, refer to "Configuring Authentication for the Web Interface" in the Web Interface documentation in eDocs.

Upgrades

Upgrades are supported only for Citrix online plug-in 11.2/12.x and Receiver for Windows 3.x releases.

Availability of Receiver for Windows 3.3 features

Some of the features and functionality of Receiver are available only when connecting to newer XenApp and XenDesktop versions and might require the latest hotfixes for XenApp, XenDesktop, and Secure Gateway.

Other

- **Compatible plug-ins**

  For a list of compatible plug-ins, refer to information about managing Receiver updates in the StoreFront documentation in Citrix eDocs.

- **.NET Framework requirements**

  - 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.
- **HDX MediaStream Multimedia Acceleration**

  For applications and media formats supported by HDX MediaStream Multimedia Acceleration, refer to information about optimizing audio and video playback in the XenApp documentation in Citrix eDocs.

- **Supported connection methods and network transports:**

  - TCP/IP+HTTP

  - SSL/TLS+HTTPS
- Previous versions of the Presentation Server Client/Online Plug-in and the current icaclient.adm file. Previous versions of the Presentation Server Client and Online Plug-in are not compatible with the Receiver for Windows 3.3 icaclient.adm file.

Installing Receiver for Windows

The CitrixReceiver.exe installation package can be installed:

- 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 Access Gateway, StoreFront server, or the AppController virtual appliance 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) or if Receiver Updater for Windows is installed.
  - Receiver users can manually check for updates from the Receiver interface.
  - If your site requires configuration of Receiver, use an alternate deployment method.
- Automatically from Deploying Receiver from Receiver for Web or from Deploying Receiver 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 file.
  - This installation method does not provide automatic updates.
- Using an Electronic Software Distribution (ESD) tool
  - A first-time Receiver user must enter a server URL to set up an account.
  - You can use Merchandising Server or other methods to provide updates.

    If you are using email-based or URL-based account discovery for account setup, you can use Merchandising Server to add stores to Receiver. However, do not use Merchandising Server to deliver the same stores that are provided through email-based or URL-based account discovery.

Refer also to Configuring and Installing Receiver for Windows Using Command-Line Parameters, Install and uninstall Receiver for Windows manually, and Delivering Receiver Using Active Directory and Sample Startup Scripts.

Receiver does not require administrator rights to install unless it will use pass-through authentication.

Upgrading to Receiver for Windows 3.3

Note: Sites that use smart card authentication or legacy PNA Services sites do not need to upgrade and should continue to use Receiver Enterprise.

For deployments with StoreFront:

- Best practice is to configure Access Gateway Enterprise Edition and StoreFront 1.2 as described in the documentation for those products in Citrix eDocs. Attach the provisioning file created by StoreFront to an email and inform users how to upgrade and to open the provisioning file after installing Receiver.

- As an alternative to using a provisioning file, inform users to enter either the URL of an Access Gateway Enterprise Edition or, if you have configured email-based account discovery as described in the StoreFront documentation, their email address.

- Another method is to configure a Receiver for Web site as described in the StoreFront documentation and complete the configuration described in Deploying Receiver from Receiver for Web. Inform users how to upgrade Receiver, access the Receiver for Web site, and download the provisioning file from the Receiver for Web interface (click the user name and click Activate).

For deployments with Web Interface

- If you are using AppController, configure the connectors as described in the AppController documentation in eDocs.

- Upgrade your Web Interface site with Receiver for Windows 3.3 and complete the configuration described in Deploying Receiver from a Web Interface Logon Screen. Let your users know how to upgrade Receiver. You can, for example, create a download site where users can obtain the renamed Receiver installer.

Considerations When Upgrading

Receiver for Windows 3.3 (CitrixReceiver.exe) can be used to upgrade Receiver for Windows 3.0 through 3.2 as well as Citrix online plug-in 11.2 and 12.*x*. Remove versions older than 11.2 before installing the new version.

To upgrade the Online plug-in (full) configured for PNA or Citrix Receiver (Enterprise) to Receiver for Windows 3.3 (CitrixReceiver.exe), first uninstall the older version and then install the new version.

If CitrixReceiver.exe is already installed with no Online plug-in or with the Online plug-in (web), upgrading to Receiver for Windows 3.3 provides Web-based access to Citrix Receiver.

If Receiver for Windows 3.0 through 3.2 was installed per machine, a per-user upgrade (by a user without administrative privileges) is not supported.

If Receiver for Windows 3.0 through 3.2 was installed per user, a per-machine upgrade is not supported.

Disabling Automatic Updates for Pooled Desktops

For desktops delivered from pooled machines, disable automatic updating of Receiver so that updates to it are controlled from the master VM used to create the desktops.

When you prepare the master VM, disable automatic updates as follows:

- If updates are obtained from Citrix.com or your own site, set the following registry key on the master VM:

  > **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.

  On 32-bit machines:

  DWORD:00000001 HKLM\SOFTWARE\Citrix\Receiver\Inventory\NoPluginUpdates

  On 64-bit machines:

  DWORD:00000001
  HKLM\Software\Wow6432Node\Citrix\Receiver\Inventory\NoPluginUpdates

- If updates are obtained from the Merchandising Server, follow the instructions in *To use Merchandising Server to install and set up Citrix Receiver for Windows on a shared XenDesktop image* in the Merchandising Server documentation and also set the registry key noted above.

Install and uninstall Receiver for Windows manually

You can install Receiver from the installation media, a network share, Windows Explorer, or a command line by manually running the CitrixReceiver.exe installer package.

When you cancel the installation before completion, some components might be installed. In that case, remove the Receiver with the Add/Remove Programs utility from the Control Panel on Windows XP or Windows Server 2003 (Programs and Features utility from the Control Panel on Windows Vista, Windows 7, Windows 8, and Windows Server 2008).

For command line installation parameters and space requirements, see Configuring and Installing Receiver for Windows Using Command-Line Parameters.

If company policies prohibit you from using an .exe file, refer to How to Manually Extract, Install, and Remove Individual .msi Files.

Remove Receiver for Windows

If Citrix Receiver Updater was used to install Receiver, you can use Updater to uninstall Receiver. If Citrix Receiver Updater was not used to install Receiver, you can uninstall Receiver by running the Add/Remove Programs utility (from the Control Panel on Windows XP or Windows Server 2003) or the Programs and Features utility (from the Control Panel on Windows Vista, Windows 7, Windows 8, and Windows Server 2008).

In some cases, uninstalling Receiver for Windows does not remove all component files or registry entries. If you are unable to install Receiver after uninstalling an older version, use the Receiver Clean-Up Utility to remove old files and registry entries.

If you delete Receiver-related files or registry entries just before uninstalling Receiver with Add/Remove Programs or Programs and Features, uninstall might fail. The Microsoft Windows Installer (MSI) is trying to repair and uninstall at the same time. If this occurs, use Receiver to start an auto-repair. After the auto-repair completes, you can cleanly uninstall Receiver from Add/Remove Programs or Programs and Features.

Auto-repair occurs if there is a problem with Receiver; however, there is no Add/Remove Programs or Programs and Features Repair option. If the Receiver repair option prompts for the location of the .msi file, browse to one of these locations to find the file:

- If installed per computer:
  - Operating system: Windows XP and Windows 2003

    C:\Documents and Settings\All Users\Application Data\Citrix\Citrix Receiver\
  - Operating system: Windows Vista, Windows 7, and Windows 8

    C:\ProgramData\Citrix\Citrix Receiver\

- If installed per user:
  - Operating system: Windows XP and Windows 2003

    %USERPROFILE%\Local Settings\Application Data\Citrix\Citrix Receiver\
  - Operating system: Windows Vista, Windows 7, and Windows 8

    %USERPROFILE%\Appdata\local\Citrix\Citrix Receiver\

To remove Receiver using the command line

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

```
CitrixReceiver.exe /uninstall
```

After uninstalling Receiver from a user device, the custom Receiver registry keys created by icaclient.adm remain in the Software\Policies\Citrix\ICA Client directory under HKEY_LOCAL_MACHINE and HKEY_LOCAL_USER. If you reinstall Receiver, these policies might be enforced, possibly causing unexpected behavior. If you want to remove these customizations, delete them manually.

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

Upgrading the Desktop Viewer and Desktop Appliance Lock

You can upgrade the Desktop Viewer component contained in Citrix online plug-in 12.1 by installing this version of the Citrix Receiver for Windows.

To upgrade the Desktop Appliance Lock, remove Citrix online plug-in 12.1 and the Desktop Appliance Lock, and then install this version of the Receiver and the Citrix Desktop Lock.

To install the Citrix Desktop Lock

Important: Log on using a local administrator account to carry out this installation procedure.

This procedure installs the plug-in so that virtual desktops are displayed using the Citrix Desktop Lock. Do not use this procedure if you want the Desktop Viewer to be available to users.

1. On the installation media, navigate to the folder called Citrix Receiver and Plug-ins\Windows\Receiver, and run CitrixReceiverEnterprise.exe from the command line using the following syntax:

   ```
   CitrixReceiverEnterprise.exe ADDLOCAL="ReceiverInside,ICA_Client,SSON,USB,DesktopViewer,
   Flash,PN_Agent,Vd3d" SERVER_LOCATION="my.server" ENABLE_SSON="Yes"
   ```

   ReceiverInside and ICA_Client are prerequisites and must be installed. For other information about the properties used in this command, see Configuring and Installing Receiver for Windows Using Command-Line Parameters.

2. Enter the URL of the XenDesktop Services site where your virtual desktops are located. The URL must be in the format http://*servername* or https://*servername*. If you are using hardware or software for load balancing or failover, you can enter a load-balanced address.

   Important: Check that the URL you enter is correct. If the URL is incorrectly typed, or you leave the field empty and the user does not enter a valid URL when prompted after installation, no virtual desktop or local desktop will be available.

3. On the XenDesktop installation media, navigate to the Citrix Receiver and Plug-ins\Windows\Receiver folder and double-click CitrixDesktopLock.msi. The Citrix Desktop Lock wizard appears.

4. On the License Agreement page, read and accept the Citrix license agreement and click Install. The Installation Progress page appears.

5. In the Installation Completed dialog box, click Close.

6. When prompted, restart the user device. If you have been granted access to a desktop and you log on as a domain user, the restarted device is displayed using the Desktop Lock.

User Accounts Used to Install the Citrix Desktop Lock

When you install the Citrix Desktop Lock, a replacement shell is used. To allow administration of the user device after you complete the installation, the account used to install CitrixDesktopLock.msi is excluded from the shell replacement. If the account used to install CitrixDesktopLock.msi is later deleted, you will not be able to log on and administer the device.

Note that because a replacement shell is used, Citrix does not recommend the use of custom shells with desktops accessed through the Desktop Lock.

To remove the Citrix Desktop Lock

If you installed the Citrix Desktop Lock, two separate items are displayed in Add/Remove Programs. You must remove both to complete the removal process.

1. Log on with the same local administrator credentials that were used to install the Desktop Lock.
2. Run the Add/Remove programs utility from the Control Panel.
3. Remove Citrix Desktop Lock.
4. Remove Citrix Receiver or Citrix Receiver (Enterprise).

Canadian Keyboard Layouts and Updating from Presentation Server Clients Version 10.200

The Canadian keyboard layouts are aligned with those supported by Microsoft. If users install Receivers without uninstalling the Presentation Server Clients Version 10.200 first, they must manually edit the module.ini file (usually in C:\Program Files\Citrix\ICA Client) to upgrade the keyboard layout settings:

Replace:

Canadian English (Multilingual)=0x00001009

Canadian French=0x00000C0C

Canadian French (Multilingual)=0x00010C0C

With:

Canadian French=0x00001009

Canadian French (Legacy)=0x00000C0C

Canadian Multilingual Standard=0x00011009

Configuring and Installing Receiver for Windows Using Command-Line Parameters

Note: This topic describes configuring and installing Receiver for Windows 3.3. For information on using the command line to configure and install Receiver for Windows Enterprise, see Configuring and Installing Receiver for Windows Using Command-Line Parameters in the Receiver for Windows Enterprise 3.4 and 3.3 eDocs documentation.

Customize the Receiver installer by specifying command line options. The installer package self-extracts to the user's temp directory before launching the setup program and requires 78.8 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 Receiver for Windows from a command prompt, use the syntax:

CitrixReceiver.exe [*Options*]

where the *Options* are as follows:

- /? or /help displays usage information.
- /noreboot suppresses reboot during UI installations. This option is not necessary during silent installs.
- /silent disables the error and progress dialogs to execute a completely silent installation.
- /includeSSON enables single sign on. If you are using ADDLOCAL= to specify features and you want to install single sign on, you must also specify the SSON value. Requires administrator rights. For information about related requirements, see Configuring a Web Browser and ICA File to Enable Single Sign-on and Manage Secure Connections to Trusted Servers.
- *PROPERTY=Value*

  Where *PROPERTY* is one of the following all-uppercase variables (keys) specified with a *Value*.

  - INSTALLDIR=*Installation directory*, where *Installation directory* is the location where the Receiver software is installed. The default value is C:\Program Files\Citrix\Receiver. If you use this option and specify an *Installation directory*, you must install the RIInstaller.msi in the *Installation directory*\Receiver directory and the other .msi files in the *Installation directory*.
  - CLIENT_NAME=*ClientName*, where *ClientName* is the name used to identify the user device to the server farm. The default value is %COMPUTERNAME%.

- ENABLE_DYNAMIC_CLIENT_NAME={Yes | No} 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.

- ADDLOCAL=*feature*[,...] Install 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.

  Note: ReceiverInside and ICA_Client are prerequisites for all other components and must be installed.

  ReceiverInside – Installs the Receiver experience. (Required)

  ICA_Client – Installs the standard Receiver. (Required)

  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.

  USB – Installs USB support.

  DesktopViewer – Installs the Desktop Viewer.

  Flash – Installs HDX media stream for Flash.

  Vd3d – Enables the Windows Aero experience (for operating systems that support it)

- ALLOWADDSTORE={N | S | A} – 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.)

  N – Never allow users to add their own store.

  S – Allow only secure stores (configured with HTTPS).

  A – Allow users to add their own store.

  The default depends on the following situations:

  N if Merchandising Server is used or stores are specified on the installation command line.

  S if Receiver is installed per machine.

  A if Receiver is installed per user.

  Important: To add a store that is configured in StoreFront with a Transport type of HTTP, you must also add the following key value to the registry key HKLM\Software\Citrix\AuthManager: ConnectionSecurityMode=Any.

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

- ALLOWSAVEPWD={N | S | A} – The default is the value specified from the PNAgent server at run time. Specifies whether users can save credentials for stores locally on their computers and applies only to stores using the PNAgent protocol. Setting this argument to N prevents users from saving their credentials. If the argument is set to S, users can only save credentials for stores accessed through HTTPS connections. Using the value A allows users to save credentials for all their stores.

- ENABLE_SSON={Yes | No} – The default value is Yes. Note that users must log off and log back onto their devices after an installation with pass-through authentication enabled. Requires administrator rights.

  > **Important:** If you disable single sign on pass-through authentication, users must reinstall Receiver if you decide to use pass-through authentication at a later time.

- ENABLE_KERBEROS={Yes | No} – The default value is No. Specifies that Kerberos should be used; applies only when pass-through authentication (SSON) is enabled.

- LEGACYFTAICONS={False | True} – 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 on delivering Microsoft Office applications to users running Windows 7.

- STARTMENUDIR=*Text string* – By default, applications appear under Start > All Programs. You can specify the name of a default folder to be added to the Start menu to contain the shortcuts to subscribed applications. Users can change the folder name and/or move the folder at any time.

- STORE*x*="*storename*;http[s]://*servername.domain*/*IISLocation*/resources/v1;[On | Off];[*storedescription*]"[STORE*y*="..."] – Specifies up to 10 stores to use with 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/MyStore/resources/v1" (for StoreFront 1). To obtain the URL, export a provisioning file from StoreFront, open it in notepad and copy the URL from the `<Address>` element.

- On | Off – The optional Off configuration setting enables you to deliver disabled stores, giving users the choice of whether or not they access them. When the store status is not specified, the default setting is On.
- *storedescription* – An optional description of the store, such as Apps on XenApp.

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

CtxInstall-ICAWebWrapper.log

TrollyExpress-20090807-123456.log

Examples of a Command-Line Installation

```
CitrixReceiver.exe /silent /includeSSON STORE0="AppStore;https://testserver.net/Citrix/MyStore/resources/v1;on;Apps on XenApp" STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/resources/v1;on;Backup Store Apps on XenApp"
```

This example:

- Installs Receiver with single sign on.
- Installs all components silently.
- Specifies two application stores.

Delivering Receiver Using Active Directory and Sample Startup Scripts

You can use Active Directory Group Policy scripts to pre-deploy Receiver 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 Receiver that is deployed. Use the Scripts setting in the Group Policy Management Console (GPMC) under Computer Configuration or User Configuration. Microsoft documents the advantages and disadvantages of using scripts at Microsoft Technet - Use Group Policy to assign computer startup scripts.

Citrix includes sample per-computer startup scripts to install and uninstall CitrixReceiver.exe. The scripts are located on recent XenApp and XenDesktop media in the Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts folder.

- 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 Configuring and Installing 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 Receiver 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 Receiver 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.

Using the Per-User Sample Startup Scripts

Citrix recommends using per-computer startup scripts but does include two Citrix Receiver per-user scripts on the XenApp media in the Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts folder for situations where you require Receiver (standard) per-user deployments.

- 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 Receiver 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 Receiver 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.

Deploying Receiver from Receiver for Web

You can deploy Receiver from Receiver for Web to ensure that users have it installed before they try to connect to an application from a browser. Receiver for Web sites enable users to access StoreFront stores through a Web page. If the Receiver for Web site detects that a user does not have a compatible version of Receiver, the user is prompted to download and install Receiver. For more information, refer to the StoreFront documentation on Citrix eDocs.

Email-based account discovery does not apply when Receiver is deployed from Receiver for Web. If email-based account discovery is configured and a first-time user installs Receiver from Citrix.com, Receiver 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.

   Important: The name CitrixReceiverWeb.exe is case sensitive.
3. Deploy the renamed executable using your regular deployment method. If you use StoreFront, refer to "Configuring Receiver for Web Using the Configuration Files" in the StoreFront documentation.

Deploying Receiver from a Web Interface Logon Screen

You can deploy Receiver 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 Web site. If the Web Interface detects that a user does not have compatible version of Receiver, the user is prompted to download and install Receiver.

For more information, see the Web Interface documentation.

Email-based account discovery does not apply when Receiver is deployed from Web Interface. If email-based account discovery is configured and a first-time user installs Receiver from Citrix.com, Receiver 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.

   Important: The name CitrixReceiverWeb.exe is case sensitive.
3. Specify the changed filename in the ClientIcaWin32 parameter in the configuration files for your XenApp Web sites.

   To use the client detection and deployment process, the Receiver installation files must be available on the Web Interface server. By default, the Web Interface assumes that the file names of the Receiver 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.

Configuring Receiver for Windows

The following configuration steps allow users to access their hosted applications and desktops:

- Configure your XenApp environment and XenDesktop environment. Ensure your XenApp or XenDesktop environment is configured correctly. Set up any Web Interface sites you require and configure the Access Gateway or Secure Gateway to provide users with secure access to their hosted applications and desktops.
- Configure StoreFront. Create stores that enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users.
- Configure access to accounts. In some environments, users must manually set up access to accounts hosting their applications and desktops.
- Use a GPO template file to customize Receiver. Configure rules for routing, proxy servers, remote client devices, and more.

You can also configure Receiver using Merchandising Server. For more information, see the Merchandising Server documentation in Citrix eDocs.

Configuring Your XenApp Environment

Before your users access applications hosted in your XenApp deployment, configure the following components in your deployment as described here.

- When publishing applications on your XenApp farms, consider the following options to enhance the experience for users accessing those applications through Storefront stores:

    - Ensure that you include meaningful descriptions for published applications, as these descriptions are visible to users in Citrix Receiver.

    - To automatically subscribe all users of a store to an application, append the string KEYWORDS:Auto to the description you provide when you publish the application in XenApp. 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 make commonly used applications easier to find by listing them in Citrix Receiver's Featured list, append the string KEYWORDS:Featured to the application description.

  For more information see the StoreFront documentation in Citrix eDocs.

- If the Web Interface of your XenApp deployment does not have a XenApp Services site, create one. The name of the site and how you create it depends on the version of the Web Interface you have installed. For more information, see the Web Interface documentation in Citrix eDocs.

Configuring Your XenDesktop Environment

The topics in this section describe how to configure USB support, allow users to restart their desktops, prevent the Desktop Viewer window from dimming, and configure Desktop Lock.

Configuring USB Support for XenDesktop 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 session, and so do not use USB support:

- Keyboards
- Mice
- Smart cards

Note: Specialist USB devices (for example, Bloomberg keyboards and 3D mice) can be configured to use USB support. For information on configuring Bloomberg keyboards, see Configuring Bloomberg Keyboards. For information on configuring policy rules for other specialist USB devices, see CTX 119722.

By default, certain types of USB devices are not supported for remoting through XenDesktop. For example, a user may have a network interface card attached to the system board by internal USB. Remoting this 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.

For instructions on modifying the range of USB devices that are available to users, see Updating the List of USB Devices Available for Remoting.

For instructions on automatically redirecting specific USB devices, see 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.

The user experience depends upon the type of desktop to which users are connecting.

For desktops accessed through the Citrix Desktop Lock, 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.

For desktops accessed through the Desktop Viewer, when a user plugs in a USB device, a dialog box appears asking the user if they want that device remoted to the virtual desktop. 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 Mappings rule. When this rule 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 Citrix Mappings rule is in the Drives subfolder of the Client Devices Resources folder in the Presentation Server Console.

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

Feature	Client Drive Mapping	USB Rule
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 USB support and the Citrix Mappings rule 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 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.

  Note: Some specialty devices (for example, VOIP phones) require additional configuration. For instructions on this, see 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 that 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 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. 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 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

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 them 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 it is appropriate to provide access to using USB support.

Updating the List of USB Devices Available for Remoting

You can update the range of USB devices available for remoting to desktops by editing the file icaclient_usb.adm. This allows you to make changes to the Receiver 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:

HKLM\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:

HKLM\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 http://support.citrix.com/article/ctx119722/.

Configuring Bloomberg Keyboards

Bloomberg keyboards are supported by XenDesktop 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.

Configuring User-Driven Desktop Restart

You can allow users to restart their desktops themselves. They may need to do this if a desktop fails to connect or becomes unresponsive.

This feature is disabled by default. You enable user-driven desktop restart for a desktop group in Desktop Studio. For information on this, see the XenDesktop documentation in eDocs.

The procedures for restarting desktops differ depending on whether users are connecting to desktops through the Desktop Viewer or the Citrix Desktop Lock.

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:

   - HKCU\Software\Citrix\XenDesktop\DesktopViewer

   - HKLM\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:

   - HKCU\Software\Policies\Citrix\XenDesktop\DesktopViewer

   - HKLM\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. HKCU\Software\Policies\Citrix\...

2. HKLM\Software\Policies\Citrix\...

3. HKCU\Software\Citrix\...

4. HKLM\Software\Citrix\...

To configure the Citrix Desktop Lock

This topic contains instructions for configuring USB preferences, drive mappings, and microphones for a virtual desktop accessed through the Citrix Desktop Lock. In addition, some general advice on configuring the Desktop Lock is also provided.

Typically, this is used in non-domain-joined environments such as on a thin client or desktop appliance. In this access scenario, the Desktop Viewer is unavailable, so only administrators (not users) can perform the configuration.

Two .adm files are provided that allow you to perform this task using policies:

- icaclient.adm. For information on obtaining this file, see To configure settings for multiple users and devices.

- icaclient_usb.adm. The file is located in the following installed folder: <root drive>:\Program Files\Citrix\ICA Client\Configuration\en.

This topic assumes you have loaded both files into Group Policy, where the policies appear in Computer Configuration or User Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components.

To configure USB preferences

As a prerequisite, you must turn on USB support in XenDesktop deployments by enabling the USB policy rule. For information on this, see the XenDesktop documentation.

In Citrix Receiver > Remoting client devices > Generic USB Remoting, enable and configure as desired the Existing USB Devices, New USB Devices, and USB Devices List In Desktop Viewer policies. You can use the Show All Devices policy to display all connected USB devices, including those using the Generic USB virtual channel (for example, webcams and memory sticks).

To configure drive mapping

In Citrix Receiver > Remoting client devices, enable and configure as desired the Client drive mapping policy.

To configure a microphone

In Citrix Receiver > Remoting client devices, enable and configure as desired the Client microphone policy.

General Advice On Configuring the Desktop Lock

Grant access to only one virtual desktop running the Desktop Lock per user.

Do not allow users to hibernate virtual desktops. Use Active Directory policies appropriately to prevent this.

To configure settings for multiple users and devices

In addition to the configuration options offered by the Receiver user interface, you can use the Group Policy Editor and the icaclient.adm template file to configure settings. Using the Group Policy Editor, you can:

- Extend the icaclient template to cover any Receiver setting by editing the icaclient.adm file. See the Microsoft Group Policy documentation for more information about editing .adm files and about applying settings to a particular computer.
- Make changes that apply only to either specific users or all users of a client device.
- Configure settings for multiple user devices

Citrix recommends using Group Policy to configure user devices remotely; however you can use any method, including the Registry Editor, which updates the relevant registry entries.

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 icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Configuration folder for Receiver (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. Under the User Configuration node or the Computer Configuration node, edit the relevant settings as required.

Configuring StoreFront

To configure StoreFront

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Receiver. Create stores that enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users.

1. Install and configure StoreFront. For more information, see the StoreFront documentation in Citrix eDocs.

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

2. Configure stores for CloudGateway just as you would for other XenApp and XenDesktop applications. No special configuration is needed for Receiver. For more information, see *Configuring Stores* in the StoreFront documentation in Citrix eDocs.

To configure the AppController

In addition to providing access to applications published for XenApp and XenDesktop, you can use AppController, a component of CloudGateway Enterprise, to provide URLs for Web applications and applications on your internal network.

Use AppController to configure Web and SaaS apps for users. For more information about installing and configuring AppController, see the AppController documentation in Citrix eDocs.

To configure Access Gateway or CloudGateway

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 Access Gateway. For more information see the Access Gateway or CloudGateway documentation in Citrix eDocs.

Using the Group Policy Object Template to Customize Receiver

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

You can use the icaclient.adm 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 Receiver 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.

For details about Group Policy management, see the Microsoft Group Policy documentation.

To import the icaclient template using the Group Policy Management Console

To affect domain-based group policies, import the icaclient.adm file with the Group Policy Management Console.

1. As an administrator, open the Group Policy Management Console.
2. In the left pane, select a group policy and from the Action menu, choose Edit.
3. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
4. From the Action menu, choose Add/Remove Templates.
5. Choose Add and browse to the Configuration folder for Receiver (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
6. Select Open to add the template and then Close to return to the Group Policy Editor.

To import the icaclient template using the local Group Policy Editor

To affect the policies on a local computer, import the icaclient.adm file with the local Group Policy Editor.

1. As an administrator, open the Group Policy Editor by running gpedit.msc from the Start menu.
2. In the left pane, 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 (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.

Providing Users with Account Information

After installation, you must provide users with the account information they need to access their hosted applications, desktops, and data. 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

Configuring Email-based Account Discovery

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

To configure your DNS server to support email-based discovery, see *Configuring Email-based Account Discovery* in the StoreFront documentation in Citrix eDocs.

To configure Access Gateway to accept user connections by using an email address to discover the StoreFront or Access Gateway URL, see *Connecting to StoreFront by Using Email-Based Discovery* in the Access Gateway documentation in Citrix eDocs.

Providing Users with a Provisioning File

You can use StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Receiver automatically. After installing Receive, users simply open the file to configure Receiver. If you configure Receiver for Web sites, users can also obtain Receiver provisioning files from those sites.

For more information, see the StoreFront documentation in Citrix eDocs.

Providing Users with Account Information to enter Manually

If providing users with account details to enter manually, ensure you distribute the following information to enable them to connect to their hosted and desktops successfully:

- The URL for the StoreFront store or XenApp Services site hosting resources; for example: https://servername.company.com

- For access using the Access Gateway, the Access Gateway address

  For more information about configuring the Access Gateway, see the Access Gateway documentation in Citrix eDocs.

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

To configure an account manually

When users launch Receiver for the first time, they have the option to set up a new account. To do this, they must enter the URL for the StoreFront store or XenApp Services site hosting resources. For access using the Access Gateway, they must enter the Access Gateway address.

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

To add, enable, disable, or remove an account, open the Receiver home page, click ⚙, and then click Accounts.

Optimizing the Receiver Environment

The ways you can optimize the environment in which your Receiver operates for your users include:

- Improving performance
- Improving performance over low bandwidth
- Facilitating the connection of devices to published resources
- Supporting DNS name resolution
- Using proxy servers with XenDesktop connections
- Providing support for NDS users
- Using Receiver with XenApp for UNIX

Improving Receiver Performance

You can improve Receiver performance by:

- Reconnecting Users Automatically
- Providing session reliability
- Improving Performance over Low-Bandwidth Connections

Reconnecting Users Automatically

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the HDX Broadcast auto-client reconnection feature, Receiver can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically.

When this feature is enabled on the server, users do not have to reconnect manually to continue working. Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts. If user authentication is required, a dialog box requesting credentials appears to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off.

You configure HDX Broadcast auto-client reconnect using policy settings on the server. For more information see the XenApp or XenDesktop documentation.

Providing HDX Broadcast Session Reliability

With the HDX Broadcast Session Reliability feature, users continue to see hosted application and desktop windows if the connection experiences an interruption. For example, wireless users entering a tunnel may lose their connection when they enter the tunnel and regain it when they emerge on the other side. During such interruptions, the session reliability feature enables the session window to remain displayed while the connection is being restored.

You can configure your system to display a warning dialog box to users when the connection is unavailable.

You configure HDX Broadcast Session Reliability using policy settings on the server. For more information see the XenApp or XenDesktop documentation.

Important: If HDX Broadcast Session Reliability is enabled, the default port used for session communication switches from 1494 to 2598.

Improving Performance over Low-Bandwidth Connections

Citrix recommends that you use the latest version of XenApp or XenDesktop on the server. Citrix continually enhances and improves performance with each release. Many performance features require the latest Receiver and server software to function.

If you are using a low-bandwidth connection, you can make a number of changes to your Receiver configuration and the way you use the Receiver to improve performance.

Changing Your Receiver Configuration

On devices with limited processing power or in circumstances where only limited bandwidth is available, there is a trade-off between performance and functionality. Receiver provides both user and administrator with the ability to choose an acceptable mixture of rich functionality and interactive performance. Making one or more of these changes on the server or user device can reduce the bandwidth your connection requires and improve performance:

- **Enable SpeedScreen Latency Reduction.** SpeedScreen Latency Reduction improves performance over high latency connections by providing instant feedback to the user in response to typed data or mouse clicks.

  User's side: icaclient.adm file.

  Server side: SpeedScreen Latency Reduction Manager.

- **Reduce the window size.** Change the window size to the minimum size you can comfortably use.

  User side: icaclient.adm file or use the Receiver icon in the notification area and choose Preferences and right-click the Online Plug-in entry in the Plug-in Status and choose Options > Session Options.

  Server side: XenApp services site > Session Options.

- **Reduce the number of colors.** Reduce the number of colors to 256.

  User side: icaclient.adm file or use the Receiver icon in the notification area and choose Preferences and right-click the Online Plug-in entry in the Plug-in Status and choose Options > Session Options.

  Server side: XenApp services site > Session Options.

- **Reduce sound quality.** If Receiver audio mapping is enabled, reduce the sound quality to the minimum setting.

  User's side: icaclient.adm file.

Server side: Citrix Audio quality policy setting.

Changing Receiver Use

ICA technology is highly optimized and typically does not have high CPU and bandwidth requirements. However, if you are using a very low-bandwidth connection, the following tasks can impact performance:

- **Accessing large files using client drive mapping.** When you access a large file with client drive mapping, the file is transferred over the ICA connection. On slow connections, this may take a long time.
- **Playing multimedia content.** Playing multimedia content uses a lot of bandwidth and can cause reduced performance.

Connecting User Devices and Published Resources

You can facilitate sessions and optimize the connection of your user devices to resources published in the server farm by:

- Configuring workspace control settings to provide continuity for roaming users
- Making scanning transparent for users
- Mapping client devices

Providing Continuity for Roaming Users

Workspace control lets desktops and 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 desktops and applications on each device.

Policies and client drive mappings change appropriately when you move to a new user device. Policies and mappings are applied according to the user device where you are currently logged on to the session. For example, if a health care worker logs off from a user device in the emergency room of a hospital and then logs on to a workstation in the hospital’s X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session as soon as the user logs on to the user device in the X-ray laboratory.

Workspace control is available only to users connecting to published resources with Citrix XenApp or through StoreFront, Receiver for Web, or the Web Interface.

Making Scanning Transparent for Users

If you enable HDX Plug-n-Play TWAIN image scanning device support, users can control client-attached TWAIN imaging devices transparently with applications that reside on the server farm. To use this feature, a TWAIN device must be attached to the user device and the associated 32-bit TWAIN driver must also be installed on the user device.

To enable or disable this feature, configure the Citrix policy Client TWAIN device redirection setting.

The following policy settings allow you to specify the maximum amount of bandwidth (in kilobits per second or as a percentage) and the compression level of images from client to server used for TWAIN redirection:

- TWAIN device redirection bandwidth limit
- TWAIN device redirection bandwidth limit percent
- TWAIN compression level

Mapping User Devices

The Receiver supports mapping devices on user devices so they are available from within a session. Users can:

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

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

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

Turning off User Device Mappings

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

Mapping Client Drives to XenApp Server Drive Letters

Client drive mapping allows drive letters on the XenApp server to be redirected to drives that exist on the client device. For example, drive H in a Citrix user session can be mapped to drive C of the local device running the plug-in.

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

Note that Client drive mapping is not supported when connecting to MetaFrame Server 1.0 for UNIX operating systems.

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

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

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

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

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

When a client device connects to a XenApp server, client mappings are reestablished unless automatic client device mapping is disabled. You can use the Terminal Services Configuration tool to configure automatic client device mapping for ICA connections and users. You can also use policies to give you more control over how client device mapping is applied. For more information about policies, see the XenApp documentation in Citrix eDocs.

HDX Plug-n-Play for USB Storage Devices

HDX Plug-n-Play for USB storage devices enables users to interact with USB mass storage devices connected to their user devices when connected to XenApp sessions. When HDX Plug-n-Play for USB storage devices is enabled, users can connect or disconnect a USB device from a session at any time, regardless of whether the session was started before or after the drive connection.

HDX Plug-n-Play for USB storage devices is enabled by default and can be disabled or enabled by editing the ICA\File Redirection - Client removable drives policy setting. For more information, see the XenApp documentation.

Supported Mass Storage Devices with XenApp

Mass storage devices, including USB thumbdrives, USB-attached hard drives, CD-DVD drives, and SD card readers are supported.

Not supported:

- U3 smart drives and devices with similar autorun behavior
- Explorer.exe published as a seamless application

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.

HDX Plug-n-Play USB Device Redirection for XenApp Connections

HDX Plug-n-Play USB Device Redirection on computers running Vista and Windows 7 enables dynamic redirection of media devices, including cameras, scanners, media players, and point of sale (POS) devices to the server. You or the user can restrict redirection of all or some of the devices. Edit policies on the server or apply group policies on the user device to configure the redirection settings. Three methods can enforce HDX Plug-n-Play USB device redirection policies:

- **Server side.** The administrator can enable or disable all device redirections for a specific user or user group using the Active Directory policies available in XenApp. The policy controls redirection of all devices and is not specific to a device. For more information, see the XenApp administration documentation.
- **Plug-in side.** The administrator can enable or disable all device redirection for a specific user or computer by using the group policy editor. There are two policy settings - the USB Plug-n-Play Devices policy setting controls redirection of all devices and the USB Point of Sale Devices policy setting controls POS devices only. If USB Plug-n-Play Devices allows devices to be redirected, you can use the USB Point of Sale Devices, which is a subset of USB Plug-n-Play Devices, to control only POS devices.
- **Plug-in side.** The user can allow or reject device redirection. When a device is going to be redirected, the permission set by the user in the Connection Center is applied (the setting applies to the current session). If the permission is set to Full Access, devices are always redirected. If the permission is set to No Access, devices are not redirected. If the permission is set to Ask Permission, a dialog box appears before redirection occurs requiring the user to make a selection. Depending on the answer, the device is redirected or not. If the user is prompted with any of the device security dialog boxes (for example, file security or audio security) and instructs the system to remember the decision, applications launched in subsequent ICA sessions load and use these settings.

  This setting affects only devices plugged in after the user changes the setting. Devices that are already plugged in when the user changes the setting are unaffected by the new setting.

  Important: If you prohibit Plug-n-Play USB device redirection in a server policy, the user cannot override that policy setting with the plug-in side policy.

Plug-in Group Policies

Access the plug-in policies using the Group Policy Editor available through gpedit.msc from the Start menu's Run dialog box. You can apply the policies to both users and computers. Two policies are available:

- USB Plug-n-Play Devices is the main policy that turns HDX Plug-n-Play USB device redirection on or off. Enabling redirection allows any Media Transfer Protocol (MTP), Picture Transfer Protocol (PTP), and Point of Sale (POS) device connected to the user device to be redirected in the session. The policy has three values: Not Configured, Enabled, and Disabled. The default is Not Configured, which allows redirection.

- USB Point of Sale Devices controls the redirection of POS devices and USB Plug-n-Play Devices must be Enabled to enable this policy. The policy can have three values: Not Configured, Enabled, and Disabled. The default is Not Configured, which allows redirection of POS devices.

Mapping Client Printers for More Efficiency

The Receiver support printing to network printers and printers that are attached locally to user devices. By default, unless you create policies to change this, XenApp lets users:

- Print to all printing devices accessible from the user device
- Add printers (but it does not retain settings configured for these printers or save them for the next session)

However, these settings might not be the optimum in all environments. For example, the default setting that allows users to print to all printers accessible from the user device is the easiest to administer initially, but might create slower logon times in some environments.

Likewise, your organization’s security policies might require that you prevent users from mapping local printing ports. To do so, configure the Citrix policy Auto connect client COM ports setting to Disabled.

To change default printing settings, configure policy settings on the server. For more information, see the XenApp administration topics.

To view mapped client printers

While connected to the XenApp server, from the Start menu, choose Printers in the Control Panel.

The Printers window displays the local printers mapped to the session. When connecting to servers running Citrix Presentation Server 4.0 or 4.5 or Citrix XenApp, by default the name of the printer takes the form:

printername (from *clientname*) in session *x*

where:

- *printername* is the name of the printer on the user device.
- *clientname* is the unique name given to the user device or the Web Interface.
- *x* is the SessionID of the user’s session on the server.

For example, printer01 (from computer01) in session 7

When connecting to servers running Presentation Server 3.0 or earlier, or when the Legacy printer name option from the Citrix policy Client printer names setting is enabled on the server, a different naming convention is used. The name of the printer takes the form:

Client/clientname#/printername

where:

- *clientname* is the unique name given to the user device during client setup.
- *printername* is the Windows printer name. Because the Windows printer name is used and not the port name, multiple printers can share a printer port without conflict.

For more information about printing, and about managing printing using policies, see the Citrix XenApp Administrator's documentation.

To map a client COM port to a server COM port

Client COM port mapping allows devices attached to the COM ports of the user device to be used during sessions on a XenApp server. These mappings can be used like any other network mappings.

Important: Client COM port mapping is not supported when connecting to MetaFrame Server 1.0 and 1.1 for UNIX Operating Systems.

You can map client COM ports at the command prompt. You can also control client COM port mapping from the Terminal Services Configuration tool or using policies. See the Citrix XenApp Administrator's documentation for more information about policies.

1. Start Receiver and log on to the XenApp server.
2. At a command prompt, type: net use com*x*: \\client\com*z*: where *x* is the number of the COM port on the server (ports 1 through 9 are available for mapping) and *z* is the number of the client COM port you want to map.
3. To confirm the operation, type: net use at a command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports. To use this COM port in a session on a XenApp server, install your device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session on the server. Use this mapped COM port as you would a COM port on the user device.

   Important: COM port mapping is not TAPI-compatible. TAPI devices cannot be mapped to client COM ports.

Mapping Client Audio to Play Sound on the User Device

Client audio mapping enables applications executing on the XenApp server to play sounds through Windows-compatible sound devices installed on the user device. You can set audio quality on a per-connection basis on the XenApp server and users can set it on their device. If the user device and server audio quality settings are different, the lower setting is used.

Client audio mapping can cause excessive load on servers and the network. The higher the audio quality, the more bandwidth is required to transfer the audio data. Higher quality audio also uses more server CPU to process.

Important: Client sound support mapping is not supported when connecting to Citrix XenApp for UNIX.

Associating User Device File Types with Published Applications

Receiver supports HDX Plug-n-Play content redirection. Functionally equivalent to extended parameter passing, content redirection allows you to enforce all underlying file type associations from the server, eliminating the need to configure extended parameter passing on individual user devices.

To associate file types on the user device with applications published on the server, configure Plug-n-Play content redirection on the server. For more information, see the XenApp administration topics.

Supporting DNS Name Resolution

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

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

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

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

To disable DNS name resolution for specific client devices

If you are using DNS name resolution in the server farm and are having problems with specific user devices, you can disable DNS name resolution for those devices.

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

1. Add a string registry key xmlAddressResolutionType to HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing.

2. Set the value to IPv4-Port.

3. Repeat for each user of the user devices.

Using Proxy Servers with XenDesktop Connections

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

Improving the User Experience

You can improve your users' experience with the following features:

- ClearType font smoothing
- Client-Side Microphone Input
- Multi-Monitor Support
- Printing Performance
- Printer Setting Overrides on Devices
- Keyboard shortcuts
- Receiver support for 32-bit color icons
- Providing Virtual Desktops to Receiver Users
- Keyboard Input in XenDesktop Sessions
- Connecting to Virtual Desktops

ClearType font smoothing

This topic does not apply to XenDesktop connections.

ClearType font smoothing (also known as Sub-pixel font rendering) improves the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing. ClearType font smoothing is set by default in Windows 8, Windows 7, and Windows Vista. Standard font smoothing is set by default in Windows XP.

If you enable ClearType font smoothing on the server, you are not forcing user devices to use ClearType font smoothing. You are enabling the server to support ClearType font smoothing on user devices that have it enabled locally and are using Receiver.

Receiver automatically detects the user device's font smoothing setting and sends it to the server. The session connects using this setting. When the session is disconnected or terminated, the server's setting reverts to its original setting.

Client-Side Microphone Input

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

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

Digital dictation support is available with Receiver. For information about configuring this feature, see the XenApp and XenDesktop documentation.

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

Multi-Monitor Support

Multiple monitors are fully supported by Receiver. As many as eight monitors are supported.

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

Sessions can span multiple monitors in two ways:

- Full screen mode, with multiple monitors shown inside the session; applications snap to monitors as they would locally.

  XenDesktop: If users access a desktop through the Citrix Desktop Lock, the desktop is displayed across all monitors. The primary monitor on the device becomes the primary monitor in the XenDesktop session. You can display the Desktop Viewer toolbar across any rectangular subset of monitors by resizing the window across any part of those monitors and pressing the Maximize button.

- Windowed mode, with one single monitor image for the session; applications do not snap to individual monitors.

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

To enable multi-monitor support, ensure the following:

- The user device must have a single video board that can support connections to more than one monitor or multiple video boards compatible with the Receiver on the appropriate platform.

- The user device operating system must be able to detect each of the monitors. On Windows platforms, to verify that this detection occurs, on the user device, view the Settings tab in the Display Settings dialog box and confirm that each monitor appears separately.

- After your monitors are detected:

  - **XenDesktop:** Configure the graphics memory limit using the Citrix Machine Policy setting Display memory limit.

  - **XenApp:** Depending on the version of the XenApp server you have installed:

    - Configure the graphics memory limit using the Citrix Computer Policy setting Display memory limit.

    - From the Citrix management console for the XenApp server, select the farm and in the task pane, select Modify Server Properties > Modify all properties >

Server Default > HDX Broadcast > Display (or Modify Server Properties > Modify all properties > Server Default > ICA > Display) and set the Maximum memory to use for each session's graphics.

Ensure the setting is large enough (in kilobytes) to provide sufficient graphic memory. If this setting is not high enough, the published resource is restricted to the subset of the monitors that fits within the size specified.

For information about calculating the session's graphic memory requirements for XenApp and XenDesktop, see ctx115637.

Printing Performance

Printing performance can play a vital role in your users' experiences. The printing configuration you create affects these aspects of the user's experience:

- User ease and comfort level
- Logon times
- Ability to print to a nearby printer when traveling or when moving between client devices in a building

You configure printer policy settings on the server.

User Ease and Comfort Level

In environments with novice users, consider changing the following potentially confusing default printing behaviors:

- **Printer names change at the start of each session.** When, by default, client printers are auto-created, the printer name is appended with the name of the user device and session. For example, auto-created client printers appear in the Print dialog box with a name like HP LaserJet 1018 (from *clientname*) in session 35.

  To resolve this problem, you can either reduce the number of printers auto-created or provision printers using another method. To control printer auto-creation, configure the Citrix policy setting Auto-create client printers and select one of the following options:

  - Do not auto-create client printers. Client printers are not auto-created.
  - Auto-create the client's default printer only. Only the client's default printer attached to or mapped from the client preconfigured in the Control Panel is auto-created in the session.
  - Auto-create local (non-network) client printers only. Any non-network printers attached to the client device preconfigured in the Control Panel are auto-created in the session.
  - Auto-create all client printers. All network printers and any printers attached to or mapped from the user device preconfigured in the Control Panel are auto-created in the session.
- If many printers are installed by default on user devices, your users might be confused by the large number of available printers. You can limit the printers that appear to them in sessions.
- **HDX Plug-n-Play Universal Printer uses a nonstandard printing dialog box.** If your users have trouble learning new features on their own, you might not want to use the Universal Printer as the default printer in a session. The user interface for this printer is slightly different from the standard Windows print dialog box.

Logon Times

The printing configuration you select can impact how long it takes users to start a session. When Receiver is configured to provision printers by creating them automatically at the beginning of each session, it increases the amount of time to build the session environment. In this case, Receiver has to rebuild every printer found on the user device. You can decrease logon time by specifying any of the following on the XenApp server:

- Auto-create only the Universal Printer. This is done automatically when you configure the Universal Printer.
- Auto-create only the default printer for the client device by using the Auto-create client printers policy setting.
- Do not auto-create any client printers through the Auto-create client printers policy setting and route print jobs to network printers by configuring the Session printers policy setting

Configuring Printers for Mobile Workers

If you have users who move among workstations in the same building (for example, in a hospital setting) or move among different offices, you might want to configure Proximity Printing. The Proximity Printing solution ensures that the closest printer is presented to the users in their sessions, even when they change user devices during a session.

Printer Setting Overrides on Devices

To improve printing performance, you can configure various printing policy settings on the server:

- Universal printing optimization defaults
- Universal printing EMF processing mode
- Universal printing image compression limit
- Universal printing print quality limit
- Printer driver mapping and compatibility
- Session printers

If you enabled Allow non-admins to modify these settings in the Universal printing optional defaults policy setting on the server, users on their user devices can override the Image Compression and Image and Font Caching options specified in that policy setting.

To override the printer settings on the user device

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

Keyboard shortcuts

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

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

   Note: If you already imported the icaclient 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 icaclient.adm.

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

6. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > User Experience > Keyboard shortcuts. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.

7. From the Action menu, choose Properties, select Enabled, and choose the desired options.

Receiver support for 32-bit color icons

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

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

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

Providing Virtual Desktops to Receiver Users

Different enterprises have different corporate needs, and your requirements for the way users access virtual desktops may vary from user to user, and as your corporate needs evolve. The user experience of connecting to virtual desktops and the extent of user involvement in configuring the connections depend on how you set up the Citrix Receiver for Windows. You have two options for providing users with access to virtual desktops: using the Desktop Viewer or the Citrix Desktop Lock.

Desktop Viewer

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

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

Citrix Desktop Lock

Use the Desktop Lock when users do not need to interact with the local desktop. In this access scenario, the Desktop Viewer is not available and the virtual desktop effectively replaces the local one, allowing the user to interact with the virtual desktop as if it is local. This provides the best user experience in a XenDesktop environment.

To decide which option best suits your deployment, consider how you want users to access and interact with virtual desktops.

To understand the user experience of connecting to desktops created with XenDesktop, consult the planning topics in the XenDesktop documentation in eDocs.

Keyboard Input in XenDesktop Sessions

Note the following about how keyboard combinations are processed in XenDesktop sessions:

- Windows logo key+L is directed to the local computer.
- CTRL+ALT+DELETE is directed to the local computer except in some cases if you use the Citrix Desktop Lock.
- Key presses that activate StickyKeys, FilterKeys, and ToggleKeys (Microsoft accessibility features) are normally directed to the local computer.
- As an accessibility feature of the Desktop Viewer, pressing CTRL+ALT+BREAK displays the Desktop Viewer toolbar buttons in a pop-up window.
- Windows key combinations (for example, CTRL+ESC and ALT+TAB) are directed according to the settings that your help desk has selected. For more information, see the table below.

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

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

The table shows the remoting behavior of other Windows key combinations. The behavior depends on whether a Desktop Viewer or a Desktop Lock session is used, and is controlled by the Local resources setting, available from the Session Options task on the XenDesktop site. XenApp settings are also shown for reference. For more information on configuring this setting, see the Web Interface documentation.

With Local resources set to	Desktop Viewer sessions have this behavior	Desktop Lock sessions have this behavior	XenApp (or disabled Desktop Viewer) sessions have this behavior
Full screen desktops only	Key combinations are sent to the remote, virtual desktop only if the Desktop Viewer window has focus and is maximized (full-screen).	Key combinations are always sent to the remote, virtual desktop.	Key combinations are sent to the remote XenApp server if the session is maximized (full-screen).

Remote desktop	Key combinations are sent to the remote, virtual desktop only if the Desktop Viewer window has focus.	Key combinations are always sent to the remote, virtual desktop.	Key combinations are sent to the remote XenApp server if the session or application has focus.
Local desktop	Key combinations are always kept on the local user device.	Key combinations are always kept on the local user device. Citrix does not recommend setting Local resources to Local desktop if the Desktop Lock is used.	Key combinations are always kept on the local user device.

Connecting to Virtual Desktops

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

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

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

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

Securing Your Connections

To maximize the security of your environment, the connections between Receiver and the resources you publish must be secured. You can configure various types of authentication for your Receiver software, including enabling certificate revocation list checking and using Security Support Provider Interface/Kerberos Pass-Through Authentication.

Windows NT Challenge/Response (NTLM) Support for Improved Security

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

To enable certificate revocation list checking for improved security with Receiver

When certificate revocation list (CRL) checking is enabled, Receiver checks whether or not the server's certificate is revoked. By forcing Receiver to check this, you can improve the cryptographic authentication of the server and the overall security of the SSL/TLS connections between a user device and a server.

You can enable several levels of CRL checking. For example, you can configure Receiver to check only its local certificate list or to check the local and network certificate lists. In addition, you can configure certificate checking to allow users to log on only if all CRLs are verified.

If you are making this change on a local computer, exit Receiver if it is running. Make sure all Receiver components, including the Connection Center, are closed.

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

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

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Configuration folder for the Receiver (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.
7. From the Action menu, choose Properties and select Enabled.
8. From the CRL verification drop-down menu, select one of the options.

   - Disabled. No certificate revocation list checking is performed.
   - Only check locally stored CRLs. CRLs that were installed or downloaded previously are used in certificate validation. Connection fails if the certificate is revoked.

- Require CRLs for connection. CRLs locally and from relevant certificate issuers on the network are checked. Connection fails if the certificate is revoked or not found.
- Retrieve CRLs from network. CRLs from the relevant certificate issuers are checked. Connection fails if the certificate is revoked.

If you do not set CRL verification, it defaults to Only check locally stored CRLs.

To enable pass-through authentication when sites are not in Trusted Sites or Intranet zones

Your users might require pass-through authentication to the server using their user logon credentials but cannot add sites to the Trusted Sites or Intranet zones. Enable this setting to allow pass-through authentication on all but Restricted sites.

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 icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Configuration folder for Receiver (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > User authentication > Local user name and password. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.
7. From the Local user name and password Properties menu, select Enabled, and then select the Enable pass-through authentication and Allow pass-through authentication for all ICA connections check boxes.

Using Security Support Provider Interface/Kerberos Pass-Through Authentication for Improved Security

This topic does not apply to XenDesktop connections.

Rather than sending user passwords over the network, Kerberos pass-through authentication leverages Kerberos authentication in combination with Security Support Provider Interface (SSPI) security exchange mechanisms. Kerberos is an industry-standard network authentication protocol built into Microsoft Windows operating systems.

Kerberos logon offers security-minded users or administrators the convenience of pass-through authentication combined with secret-key cryptography and data integrity provided by industry-standard network security solutions. With Kerberos logon, the Receiver does not need to handle the password and thus prevents Trojan horse-style attacks on the user device to gain access to users' passwords.

Users can log on to the user device with any authentication method; for example, a biometric authenticator such as a fingerprint reader, and still access published resources without further authentication.

System requirements. Kerberos works only between Receiver and servers that belong to the same or to trusted Windows 2000, Windows Server 2003, or Windows Server 2008 domains. Servers must also be *trusted for delegation*, an option you configure through the Active Directory Users and Computers management tool.

Kerberos logon is not available in the following circumstances:

- Connections configured with any of the following options in Remote Desktop Services (formerly known as Terminal Services) Configuration:
  - On the General tab, the Use standard Windows authentication option
  - On the Logon Settings tab, the Always use the following logon information option or the Always prompt for password option
- Connections you route through the Secure Gateway
- If the server requires smart card logon
- If the authenticated user account requires a smart card for interactive logon

Important: SSPI requires XML Service DNS address resolution to be enabled for the server farm, or reverse DNS resolution to be enabled for the Active Directory domain. For more information, see the Citrix XenApp administrator documentation.

Configuring Kerberos Authentication

Receiver, by default, is not configured to use Kerberos authentication when logging on to the server. You can set the Receiver configuration to use Kerberos with pass-through authentication or Kerberos with smart card pass-through authentication.

To use Kerberos authentication for your connections, you can either specify Kerberos using a command line installation or configure Receiver using the Group Policy Editor. See the Microsoft Group Policy documentation for more information about editing .adm files

To configure Kerberos with pass-through authentication

This topic does not apply to XenDesktop connections.

Use Kerberos with pass-through authentication if you want to use Kerberos with Receiver.

When Receiver configurations are set to use Kerberos with pass-through authentication, Receiver uses Kerberos authentication first and uses pass-through authentication if Kerberos fails.

The user cannot disable this Receiver configuration from the user interface.

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 icaclient 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 icaclient.adm.

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

6. From the Group Policy Editor, expand Administrative Templates, navigate through Citrix Components > Citrix Receiver > User authentication, double click Kerberos authentication and select Enabled. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.

7. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > User authentication > Local user name and password. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.

8. From the Action menu, choose Properties and select Enabled > Enable pass-through authentication.

To apply the setting, close and restart Receiver on the user device.

Securing Receiver Communication

To secure the communication between your server farm and Receiver, you can integrate your Receiver connections to the server farm with a range of security technologies, including:

- Citrix Access Gateway. For information about configuring Access Gateway with StoreFront, refer to the "Manage" topics in the StoreFront documentation in eDocs. For information about configuring Access Gateway or Secure Gateway with Web Interface, refer to topics in this section.

  Note: Citrix recommends using Access Gateway to secure communications between StoreFront servers and users' devices.

- A SOCKS proxy server or secure proxy server (also known as *security proxy server*, HTTPS proxy server, or SSL tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Receiver and servers. Receiver supports SOCKS and secure proxy protocols.

- SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Receiver through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

- Trusted server configuration.

Note: For information about increasing security in application streaming for desktops, see the Citrix Knowledge Base article *Enhancing Security in Application Streaming for Desktops*.

Receiver is compatible with and functions in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates are used. These templates are supported on the Microsoft Windows XP, Windows Vista, and Windows 7 platforms. Refer to the Windows XP, Windows Vista, and Windows 7 security guides available at http://technet.microsoft.com for more information about the templates and related settings.

Connect with Access Gateway Enterprise Edition

This topic summarizes how to configure Access Gateway with Receiver for Windows in a StoreFront or Web Interface deployment.

To integrate Access Gateway and StoreFront

To give users access to XenApp and XenDesktop published resources, configure Access Gateway for StoreFront, as summarized in this topic. For additional configuration, refer to *Integrating Access Gateway with CloudGateway* in the Access Gateway documentation.

To give users access to Web apps, refer to *Configuring Connections to Enterprise Web Applications Through Access Gateway* in the AppController documentation.

To configure Access Gateway for a StoreFront deployment

For more information about configuring Access Gateway for StoreFront connections, refer to topics about CloudGateway under *Integrate* in the Access Gateway documentation.

1. Configure authentication policies to authenticate users connecting to the Access Gateway by using the Access Gateway Plug-in. Bind each authentication policy to a virtual server.

    - If double-source authentication is required (such as RSA SecurID and Active Directory), security token authentication must be the primary authentication type. Domain authentication must be the secondary authentication type.

    - RSA SecurID uses a RADIUS server to enable token authentication.

    - Active Directory authentication can use either LDAP or RADIUS.

    Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. Create a session policy on the Access Gateway to identify that the connection is from Receiver. As you create the session policy, configure the following expression and select Match All Expressions as the operator for the expression:

    REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

    You can also configure a policy expression to distinguish the Receiver type:

    REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Windows/

> **Important:** If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway documentation.

3. Create a session profile for the Receiver connection to StoreFront and specify the following settings.

   a. If using double-source authentication, on the Security tab, set Default Authorization to Allow. For more information, refer to *Configuring Client Choices Options* in the Access Gateway documentation.

   b. On the Client Experience tab:

      - Next to Single Sign-on to Web Applications, click Override Global and then select the check box Single Sign-on to Web Applications.

      - Verify that Single Sign-on with Windows is not enabled. That setting is not compatible with the feature that provides single authentication to both VPN and clientless access.

      - Next to Clientless Access, click Override Global and then select On.

      - Next to Clientless Access URL Encoding, click Override Global and then select Clear.

      - If using double-source authentication, next to Credential Index, click Override Global, and then choose SECONDARY.

   c. On the Published Applications tab:

      - If using double-source authentication, next to ICA Proxy, click Override Global, and then select ON.

      - Next to Single Sign-on Domain, click Override Global, enter the domain name and then click Create. For example, enter *mydomain*.

      - In Web Interface Address, enter the Store Web address on which remote access is enabled for Access Gateway.

        For example, type https://*StorefrontFQDN*/Citrix/*StoreWebName*/ where *StorefrontFQDN* is the fully qualified domain name (FQDN) of Storefront and *StoreWebName* is the name of the store.

      - If using email-based discovery, configure the Account Services Address globally or for a session profile as described in *Connecting to StoreFront by Using Email-Based Discovery* in the Access Gateway documentation.

4. Bind the session policy to a virtual server.

To integrate Access Gateway and Web Interface

To give users browser-based access to XenApp and XenDesktop published resources, configure Access Gateway for Web Interface, as summarized in this topic. For additional configuration, refer to *Providing Access to Published Applications and Virtual Desktops* in the Access Gateway documentation.

To configure Access Gateway for a Web Interface deployment

For more information about configuring Access Gateway for Web Interface connections from a Web browser, refer to topics about Web Interface under *Integrate* in the Access Gateway documentation.

1. Configure authentication policies to authenticate users connecting to the Access Gateway by using the Access Gateway Plug-in. Bind each authentication policy to a virtual server.

   - If double-source authentication is required (such as RSA SecurID and Active Directory), security token authentication must be the primary authentication type. Domain authentication must be the secondary authentication type.

   - RSA SecurID uses a RADIUS server to enable token authentication.

   - Active Directory authentication can use either LDAP or RADIUS.

   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. Create a session policy on the Access Gateway to identify that the connection is from Receiver, allowing incoming XenApp connections from Receiver. As you create the session policy, configure the following expression and select Match All Expressions as the operator for the expression:

   REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

   Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway documentation.

3. Create a session profile for the Web Interface site and specify the following settings.

   a. If using double-source authentication, on the Security tab, set Default Authorization to Allow. For more information, refer to *Configuring Client Choices Options* in the Access Gateway documentation.

   b. On the Client Experience tab:

      - Next to Single Sign-on to Web Applications, click Override Global and then select the check box Single Sign-on to Web Applications.

      - If using double-source authentication, next to Credential Index, click Override Global, and then choose SECONDARY.

   c. On the Published Applications tab:

      - If using double-source authentication, next to ICA Proxy, click Override Global, and then select ON.

      - In Web Interface Address, click Override Global, and then enter the URL for the Web Interface site.

For example, enter https://*WIFQDN*/Citrix/XenApp or https://*WIFQDN*/Citrix/*CustomPathName* where *WIFQDN* is the fully qualified domain name (FQDN) of Web Interface and *CustomPathName* is the name of the Web Interface site.

For more information about creating a session profile, refer to the Access Gateway documentation.

4. Bind the session policy to a virtual server.

Connecting with Access Gateway 5.0

This topic applies only to deployments using the Web Interface.

Access Gateway setup requires that you configure a basic or a SmartAccess logon point on Access Gateway and use the Web address for the XenApp Services site.

Before you configure a logon point, install the Web Interface and verify that it is communicating with the network. When you configure a logon point, you must also configure at least one Secure Ticket Authority (STA) server and ICA Access Control in Access Gateway. For more information, expand Access Gateway 5.0 in eDocs, and locate the topic *To configure Access Gateway to use the Secure Ticket Authority*.

To configure the Access Gateway 5.0 appliance

1. Configure Authentication profiles to authenticate users connecting to the Access Gateway using the Receiver.

   - If double source authentication is required (such as Active Directory and RSA SecurID), Active Directory authentication must be the primary authentication type. RSA SecurID authentication must be the secondary authentication type.

   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.

   - You can configure Active Directory authentication on Access Controller. You can use Active Directory on the Access Gateway appliance by using either an LDAP or RADIUS authentication profile.

   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. To establish communication with XenApp servers and the Web Interface, configure the Access Gateway with STA servers and the ICA Access Control list on Access Gateway. For more information, see the Access Gateway section of eDocs.

3. Configure logon points on the Access Gateway. Configure the Access Gateway to allow incoming XenApp connections from the Receiver, and specify the location of your Web Interface site.

   a. In the Access Gateway Management Console, click Management.

   b. Under Access Control, click Logon Points > New.

   c. In the Logon Points Properties dialog box, in Name, type a unique name for the logon point.

   d. Select the Type:

      - For a Basic logon point, in the Web Interface field, type the fully qualified domain name (FQDN) of the Web Interface, such as `http://xenapp.domain.com/citrix/apps`. You cannot configure a SmartGroup with a basic logon point. Select the authentication type, or click Authenticate with the Web Interface.

        If you select Authenticate with the Web Interface, when users type the URL to Access Gateway and enter credentials, the credentials are passed to the Web Interface for authentication.

      - For a SmartGroup to use the settings in a SmartAccess logon point, you must select the logon point within the SmartGroup. Select the authentication profiles. If you configure a SmartAccess logon point, Access Gateway authenticates users. You cannot configure authentication by using the Web Interface.

        If you select Single Sign-on to Web Interface, users do not have to log on to the Web Interface after logging on to the Access Gateway. If not selected, users must log on to both the Access Gateway and Web Interface.

e. Under Applications and Desktops, click Secure Ticket Authority and add the STA details. Make sure the STA information is the same as the Web Interface site.

f. Finally, under Applications and Desktops, click XenApp or XenDesktop to add the ICA control list (required for Access Gateway 5.0). For more information, expand Access Gateway 5.0 in eDocs, and locate *To configure ICA Access Control*.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway section on *Configuring Intermediate Certificates*.

To configure Access Controller

1. Configure Authentication profiles to authenticate users connecting to the Access Gateway using the Receiver.

   - If double source authentication is required (such as Active Directory and RSA SecurID), Active Directory authentication must be the primary authentication type. RSA SecurID authentication must be the secondary authentication type.

   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.

   - You can configure Active Directory authentication on Access Controller. You can use Active Directory on the Access Gateway appliance by using either an LDAP or RADIUS authentication profile.

   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. To establish communication with XenApp servers and the Web Interface, configure Access Controller to recognize the servers. Configure Access Controller to allow incoming XenApp connections from the Receiver and specify the location of your Web Interface site.

   a. In the Deliver Services Console, expand Citrix Resources > Access Gateway, and then click the Access Controller on which you want to create the Web resource.

   b. Expand Resources, click Web Resources, and then under Common tasks, click Create Web resource. In the wizard, enter a unique name. On the New Web Address page, enter the Web address URL of the XenApp Web site.

   c. In **Application type**, select Citrix Web Interface and click the Enable Single Sign-on check box.

   d. After you click OK, click Publish for users in their list of resources , and then in Home page, enter the URL of the XenApp Web Site, such as `http://xenapp.domain.com/citrix/apps`, and finish the wizard.

   e. In the navigation pane, click Logon Points, click Create logon point, and in the wizard, enter a unique name, and select the type:

      - For a Basic logon point, in the Web Interface field, type the fully qualified domain name (FQDN) of the Web Interface, such as `http://xenapp.domain.com/citrix/apps`. Select the Home page, and then select the authentication profile. Leave the remaining options as default values, and click Enable this logon point check box at the end of the wizard.

      - For a SmartAccess logon point, on Select Home Page, select the Display the Web resource with the highest priority. Click Set Display Order, and move the Web Interface Web resource to the top.

        Select the Authentication Profiles for both authentication and group extraction. Leave the remaining options as default values, and click Enable this logon point check box at the end of the wizard.

   f. In the navigation pane, under Policies > Access Policies, select Create access policy and on the Select Resources page, expand Web Resources to select the Web

Interface web resource.

g. In Configure Policy Settings, select the settings, click Enable this policy to control this setting, and select Extended access, unless denied by another policy. Add the users allowed to access this resource and finish the wizard.

h. In the navigation pane, under Access Gateway appliances, select Edit Access Gateway appliance properties, click Secure Ticket Authority and add the STA details. Make sure the STA information is the same as the Web Interface site.

i. Finally, click ICA Access Control to add the ICA control list (required for Access Gateway 5.0). For more information, expand Access Gateway 5.0 in eDocs, and locate *To configure ICA Access Control* in the Access Controller documentation.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway section on *Configuring Intermediate Certificates*.

Connecting with Secure Gateway

This topic applies only to deployments using the Web Interface.

You can use the Secure Gateway in either *Normal* mode or *Relay* mode to provide a secure channel for communication between Receiver and the server. No Receiver configuration is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

Receiver uses settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway. See the topics for the Web Interface for information about configuring proxy server settings for Receiver.

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. See the topics for the Secure Gateway for more information about Relay mode.

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure Receiver to use:

- The fully qualified domain name (FQDN) of the Secure Gateway server.
- The port number of the Secure Gateway server. Note that Relay mode is not supported by Secure Gateway Version 2.0.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example: *my_computer.my_company.com* is an FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (my_company), and a top-level domain (com). The combination of intermediate and top-level domain (my_company.com) is generally referred to as the *domain name*.

Connecting Receiver through a Proxy Server

This topic applies only to deployments using Web Interface.

Proxy servers are used to limit access to and from your network, and to handle connections between Receivers and servers. Receiver supports SOCKS and secure proxy protocols.

When communicating with the server farm, Receiver uses proxy server settings that are configured remotely on the server running Receiver for Web or the Web Interface. For information about proxy server configuration, refer to StoreFront or Web Interface documentation.

In communicating with the Web server, Receiver uses the proxy server settings that are configured through the Internet settings of the default Web browser on the user device. You must configure the Internet settings of the default Web browser on the user device accordingly.

Connecting with Secure Sockets Layer Relay

You can integrate Receiver with the Secure Sockets Layer (SSL) Relay service. Receiver supports both SSL and TLS protocols.

- SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.
- TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, the certificates you use for SSL in your software installation will also work with TLS. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

Connecting with Citrix SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the XenApp server for SSL/TLS-secured communication. When the SSL Relay receives an SSL/TLS connection, it decrypts the data before redirecting it to the server, or, if the user selects SSL/TLS+HTTPS browsing, to the Citrix XML Service.

If you configure SSL Relay to listen on a port other than 443, you must specify the nonstandard listening port number to the plug-in.

You can use Citrix SSL Relay to secure communications:

- Between an SSL/TLS-enabled client and a server. Connections using SSL/TLS encryption are marked with a padlock icon in the Citrix Connection Center.
- With a server running the Web Interface, between the XenApp server and the Web server.

For information about configuring and using SSL Relay to secure your installation, see the Citrix XenApp administrator's documentation. For information about configuring the server running the Web Interface to use SSL/TLS encryption, see the Web Interface administrator's documentation.

User Device Requirements

In addition to the System Requirements, you also must ensure that:

- The user device supports 128-bit encryption
- The user device has a root certificate installed that can verify the signature of the Certificate Authority on the server certificate
- Receiver is aware of the TCP listening port number used by the SSL Relay service in the server farm
- Any service packs or upgrades that Microsoft recommends are applied

If you are using Internet Explorer and you are not certain about the encryption level of your system, visit the Microsoft Web site at http://www.microsoft.com to install a service pack that provides 128-bit encryption.

Important: Receiver supports certificate key lengths of up to 4096 bits. Ensure that the bit lengths of your Certificate Authority root and intermediate certificates, and those of your server certificates, do not exceed the bit length your Receiver supports or connection might fail.

To apply a different listening port number for all connections

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 imported the icaclient 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 icaclient.adm.

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

6. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.

7. From the Action menu, choose Properties, select Enabled, and type a new port number in the Allowed SSL servers text box in the following format: *server:SSL relay port number* where *SSL relay port number* is the number of the listening port. You can use a wildcard to specify multiple servers. For example, *.Test.com:*SSL relay port number* matches all connections to Test.com through the specified port.

To apply a different listening port number to particular connections only

If you are changing this on a local computer, close all Receiver components, including the Connection Center.

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

   Note: If you already added the icaclient 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 icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.
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

Connecting through a Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using a firewall in your deployment, Receiver must be able to communicate through the firewall with both the Web server and Citrix server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for user device to Web server communication. For Receiver to Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

If the firewall is configured for Network Address Translation (NAT), you can use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your XenApp or XenDesktop server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to Receiver. Receiver then connects to the server using the external address and port number. For more information, see the Web Interface documentation.

Configuring and Enabling Receivers for SSL and TLS

SSL and TLS are configured in the same way, use the same certificates, and are enabled simultaneously.

When SSL and TLS are enabled, each time you initiate a connection, Receiver tries to use TLS first and then tries SSL. If it cannot connect with SSL, the connection fails and an error message appears.

To force Receiver to connect with TLS, you must specify TLS on the Secure Gateway server or SSL Relay service. See the topics for the Secure Gateway or your SSL Relay service documentation for more information.

In addition, make sure the user device meets all system requirements.

To use SSL/TLS encryption for all Receiver communications, configure the user device, Receiver, and, if using Web Interface, the server running the Web Interface. For information about securing StoreFront communications, refer to topics under "Secure" in the StoreFront documentation in eDocs.

Installing Root Certificates on the User Devices

To use SSL/TLS to secure communications between a SSL/TLS-enabled Receiver and the server farm, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate.

Receiver supports the Certificate Authorities that are supported by the Windows operating system. The root certificates for these Certificate Authorities are installed with Windows and managed using Windows utilities. They are the same root certificates that are used by Microsoft Internet Explorer.

If you use your own Certificate Authority, you must obtain a root certificate from that Certificate Authority and install it on each user device. This root certificate is then used and trusted by both Microsoft Internet Explorer and Receiver.

You might be able to install the root certificate using other administration or deployment methods, such as:

- Using the Microsoft Internet Explorer Administration Kit (IEAK) Configuration Wizard and Profile Manager
- Using third-party deployment tools

Make sure that the certificates installed by your Windows operating system meet the security requirements for your organization or use the certificates issued by your organization’s Certificate Authority.

To configure Web Interface to use SSL/TLS for Receiver

1. To use SSL/TLS to encrypt application enumeration and launch data passed between Receiver and the server running the Web Interface, configure the appropriate settings using the Web Interface. You must include the computer name of the XenApp server that is hosting the SSL certificate.

2. To use secure HTTP (HTTPS) to encrypt the configuration information passed between Receiver and the server running the Web Interface, enter the server URL in the format https://*servername*. In the Windows notification area, right-click the Receiver icon and choose Preferences.

3. Right-click the Online Plug-in entry in the Plug-in Status and choose Change Server.

To configure TLS support

If you are changing this on a local computer, close all Receiver components, including the Connection Center.

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

   Note: If you already imported the icaclient 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 icaclient.adm.

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

6. From the Group Policy Editor, expand Administrative Templates and navigate through 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 SSL/TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Receiver connects using TLS encryption. If a connection using TLS fails, Receiver connects using SSL.
   - Set SSL cipher suite to Detect version to have Receiver 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 Receiver to try to retrieve Certificate Revocation Lists (CRLs) from the relevant certificate issuers.

To use the Group Policy template on Web Interface to meet FIPS 140 security requirements

If you are changing this on a local computer, close all Receiver 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 icaclient template 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 icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. From the Group Policy Editor, expand Administrative Templates and navigate through 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 SSL/TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Receiver tries to connect using TLS encryption. If a connection using TLS fails, Receiver tries to connect using SSL.
   - Set SSL ciphersuite to Government.
   - Set CRL verification to Require CRLs for connection.

To configure the Web Interface to use SSL/TLS when communicating with Citrix Receiver

When using the Web Interface, specify the computer name of the server hosting the SSL certificate. See the information about Web Interface for more details about using SSL/TLS to secure communications between Receiver and the Web server.

1. From the Configuration settings menu, select Server Settings.
2. Select Use SSL/TLS for communications between clients and the Web server.
3. Save your changes.

Selecting SSL/TLS changes all URLs to use HTTPS protocol.

To configure Citrix XenApp to use SSL/TLS when communicating with Citrix Receiver

You can configure the XenApp server to use SSL/TLS to secure the communications between Receiver and the server.

1. From the Citrix management console for the XenApp server, open the Properties dialog box for the application you want to secure.

2. Select Advanced > Client options and ensure that you select Enable SSL and TLS protocols.

3. Repeat these steps for each application you want to secure.

When using the Web Interface, specify the computer name of the server hosting the SSL certificate. See the information about Web Interface for more details about using SSL/TLS to secure communications between Receiver and the Web server.

To configure Citrix Receiver to use SSL/TLS when communicating with the server running the Web Interface

You can configure Receiver to use SSL/TLS to secure the communications between Receiver and the server running the Web Interface.

Ensure that a valid root certificate is installed on the user device. For more information, see Installing Root Certificates on the User Devices.

1. In the Windows notification area, right-click the Receiver icon and choose Preferences.
2. Right-click the Online Plug-in entry in the Plug-in Status and choose Change Server.
3. The Change Server screen displays the currently configured URL. Enter the server URL in the text box in the format https://*servername* to encrypt the configuration data using SSL/TLS.
4. Click Update to apply the change.
5. Enable SSL/TLS in the client device browser. For more information about enabling SSL/TLS in the browser, see the online Help for the browser.

ICA File Signing to Protect Against Application or Desktop Launches from Untrusted Servers

The ICA File Signing feature helps protect users from unauthorized application or desktop launches. Citrix Receiver 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 Receiver 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 Receiver 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 Receiver 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. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Enable ICA File Signing. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.

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 Receiver if an application or desktop launch has an invalid signature. The user cannot continue and the unauthorized launch is blocked.
Prompt user on unsigned launches (less secure)	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).

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.

Configuring a Web Browser and ICA File to Enable Single Sign-on and Manage Secure Connections to Trusted Servers

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 *protocoll*://*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

Launching SSO or Using Secure Connections with a web site

Add the exact address of the Receiver for Web or 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 Entry

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

To set client resource permissions

You can set client resource permissions using trusted and restricted site regions by:

- Adding the Receiver for Web or the Web Interface site to the Trusted Site list
- Making changes to new registry settings

Note: Due to enhancements to Receiver, the .ini procedure available in earlier versions of the plug-in/Receiver is replaced with these procedures.

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

To add the web 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 Receiver for Web or Web Interface site and click Add.
4. Download the registry settings from http://support.citrix.com/article/CTX124871.html 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

1. Download the registry settings from http://support.citrix.com/article/CTX124871.html 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
PdaSecurityPermission	PDA devices
ScannerAndDigitalCameraSecurityPermission	USB and other devices

Value	Description
0	No Access
1	Read-only access
2	Full access
3	Prompt user for access

Enforcing Trust Relations

Trusted server configuration is designed to identify and enforce trust relations involved in Receiver connections. This trust relationship increases the confidence of Receiver administrators and users in the integrity of data on user devices and prevents the malicious use of Receiver connections.

When this feature is enabled, Receivers can specify the requirements for trust and determine whether or not they trust a connection to the server. For example, a Receiver connecting to a certain address (such as https://*.citrix.com) with a specific connection type (such as SSL) is directed to a trusted zone on the server.

When trusted server configuration is enabled, XenApp servers or the Access Gateway must reside in a Windows Trusted Sites zone. (For step-by-step instructions about adding servers to the Windows Trusted Sites zone, see the Internet Explorer online help.)

If you connect using SSL, add the server name in the format https://CN, where CN is the Common Name shown on the SSL certificate. Otherwise, use the format that Receiver uses to connect; for example if Receiver connects using an IP address, add the server's IP address.

To enable trusted server configuration

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 imported the icaclient 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 icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. Expand the Administrative Templates folder under the User Configuration node.
7. From the Group Policy Editor, expand Administrative Templates and navigate through Citrix Components > Citrix Receiver > Network Routing > Configure trusted server configuration. In Windows 8, Windows 7, and Windows Server 2008, expand Administrative Templates and navigate through Classic Administrative Templates (ADM) > Citrix Components to the desired configuration option.
8. From the Action menu, choose Properties and select Enabled.

Elevation Level and wfcrun32.exe

When User Access Control (UAC) is enabled on devices running Windows 8, Windows 7, or Windows Vista, only processes at the same elevation/integrity level as wfcrun32.exe can launch published applications.

Example 1:

When wfcrun32.exe is running as a normal user (un-elevated), other processes such as Receiver must be running as a normal user to launch applications through wfcrun32.

Example 2:

When wfcrun32.exe is running in elevated mode, other processes such as Connection Center, Receiver, and third party applications using the ICA Client Object that are running in non-elevated mode cannot communicate with wfcrun32.exe.