Receiver for Windows 4.2

2015-02-03 18:25:19 UTC

Contents

Receiver for Windows 4.2 5

- About this release 6
- System requirements 11
- Install 18
  - Install and uninstall Receiver for Windows manually 20
  - Configure and install Receiver for Windows using command-line parameters 22
  - Deploy Receiver using Active Directory and sample startup scripts 29
    - Use the per-user sample startup scripts 31
  - Deploy Receiver from Receiver for Web 32
  - Deploy Receiver from a Web Interface logon screen 33
- Configure 34
  - Configure application delivery 35
  - Configure Shortcut Only mode 38
    - Using the Group Policy Object template to configure shortcuts 40
    - Registry keys for shortcuts customization 41
    - Configuring shortcuts based on StoreFront account settings 48
  - Configure your XenDesktop environment 50
    - Configure USB support for XenDesktop and XenApp connections 51
      - How USB support works 53
      - Mass storage devices 54
      - USB device classes allowed by default 55
      - USB device classes denied by default 57
      - Update the list of USB devices available for remoting 58
      - Configure Bloomberg keyboards 59
    - To prevent the Desktop Viewer window from dimming 60
    - To configure settings for multiple users and devices 61
  - Configure StoreFront 62
  - Configure Receiver with the Group Policy Object template 63
  - Provide users with account information 65

Optimize the Receiver environment 67
    Reduce application launch time 68
    Map client devices 71
        Map client drives to host-side drive letters 72
        HDX Plug and Play USB device redirection 73
        To map a client COM port to a server COM port 74
    Support DNS name resolution 75
    Use proxy servers with XenDesktop connections 76
Improve the user experience 77
    Client-side microphone input 78
    Multi-monitor support 79
    Printer setting overrides on devices 81
    Keyboard shortcuts 82
    Receiver support for 32-bit color icons 83
    Enabling Desktop Viewer 84
    Keyboard input in Desktop Viewer sessions 85
    Connect to virtual desktops 86
Secure your connections 87
    Configure domain pass-through authentication 88
    To enable pass-through authentication when sites are not in Trusted Sites or Intranet zones 90
    Configure domain pass-through authentication with Kerberos 91
    Configure smart card authentication 94
    To enable certificate revocation list checking for improved security with Receiver 98
Secure Receiver communication 100
    Connect with NetScaler Gateway 101
    Connect with Access Gateway Enterprise Edition 102
    Connect with Secure Gateway 103
    Connect through a firewall 104
    Enforce trust relations 105
    Elevation level and wfcrun32.exe 106
    Connect Receiver through a proxy server 107
    Connect with Secure Sockets Layer (SSL) Relay 108
        Connect with Citrix SSL Relay 109
            User device requirements 110
            To apply a different listening port number for all connections 111
            To apply a different listening port number to particular connections only 112

Configure and enable Receivers for TLS 113

Install root certificates on user devices 114

To configure Web Interface to use TLS for Receiver 115

To configure TLS support 116

To use the Group Policy template on Web Interface to meet FIPS 140 security requirements 117

To configure the Web Interface to use TLS when communicating with Citrix Receiver 118

To configure Citrix XenApp to use TLS when communicating with Citrix Receiver 119

To configure Citrix Receiver to use TLS when communicating with the server running the Web Interface 120

ICA File Signing to protect against application or desktop launches from untrusted servers 121

To select and distribute a digital signature certificate 123

Configure a Web browser and ICA file to enable single sign-on and manage secure connections to trusted servers... 124

To set client resource permissions.. 126

Receiver Desktop Lock 128

Receiver for Windows 4.2

Quick links

About Receiver for Windows 4.2	Configure
Issues fixed in this release	Optimize
System requirements and compatibility	Improve the user experience
License your product	Secure your connections
Install	Secure Receiver communications
Configure and install using command-line parameters	

About Receiver for Windows 4.2

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

What's new

Receiver for Windows 4.2 provides the following new features and enhancements.

- **Start menu integration and shortcut management.** Published apps are seamlessly integrated into the Start menu, or delivered as desktop shortcuts. This is a configurable option for the administrator, who can choose between offering apps integrated into the Start menu, as desktop shortcuts, or via the self-service interface. For more on moving applications to the Start menu, see Configure shortcut-only mode.
- **Enhanced user experience for Windows tablet and touch**
    - **True multi-touch remoting**. Users of touch-enabled Windows 8.1 devices can use multi-finger touch gestures, such as pinching to zoom in and out, in virtual apps and desktops that support touch.

      Note: Multi-touch remoting requires XenApp 7.0 or above, XenDesktop 7.0 or above, and is supported on Windows 7, 8, 8.1 and Windows 2012 R2 virtualized apps and desktops.
    - **Touch access to XenApp and XenDesktop**. Users of touch-enabled 8.1 devices can use basic gestures to work with applications which do not natively support touch. For example, single touch translates to a left mouse click, swipe up or down translates to mouse scroll up or down. Pinch and zoom are not supported.
    - **Updated Desktop Viewer toolbar**. Windows users can access helper functions, such as Ctrl+Alt+Del, and a virtual keyboard, from the Desktop Viewer toolbar, as well as Windows 8 shortcuts. The virtual keyboard button appears when there is no keyboard connected. Shortcuts gives you access to Start, Switch Apps, App Commands and Charms from Desktop Viewer toolbar.

- **Mobile SDK for Windows Apps**. Citrix Receiver for Windows 4.2 supports the Citrix Mobile SDK for Windows Apps v2, and Citrix Hosted MobileMail v3. For more information, see https://www.citrix.com/go/mobile-sdk-for-windows-apps.html and https://www.citrix.com/go/hosted-mobilemail.html. See the Mobile SDK for Windows Apps Receiver Features Matrix for the list of supported functions and enumerations.
- **Mandatory apps**. Administrators can make individual apps and sets of apps mandatory to users. There is no Remove option for users to unsubscribe to mandatory apps. Published apps in the Start menu and in desktop shortcuts are always mandatory and

cannot be removed by the user. For more on configuring mandatory apps, see Configure application delivery.

- **New Receiver Desktop lock**. A new Receiver Desktop Lock enables Receiver for Windows 4.2 to be used on locked-down thin clients and repurposed computers for access to virtual apps and desktops. Install the Receiver Desktop Lock (CitrixReceiverDesktopLock.MSI) to lock down the client. After installing the lock, the Home and Full Screen options cannot be accessed by the user from the Desktop Viewer toolbar. For more information on Receiver Desktop Lock, see Receiver Desktop Lock.
- **USB enhancements**
    - **USB plug-and-play**. Generic USB redirection, used for specialty USB devices, such as dictation equipment, is USB 3.0 ready in 7.6, enabling plug-n-play operation with Receiver for Windows. For more information on generic USB redirection, see Configure USB support for XenDesktop and XenApp connections.
    - **USB simplification**. In this release, the user interface for the Preferences dialog box and the Devices menu gives users more visibility and control over their connected devices.
    - **USB 3.0 redirection**. Receiver for Windows offers redirection of devices connected through USB 3.0 ports.

      Note: USB 3.0-specific features, such as SuperSpeed, are not available when using redirection.
    - **Device selection for seamless apps**. An updated Connection Center allows users to manage USB device connections for seamless apps, offering a native interaction experience.
- **Improved graphic performance**. Receiver for Windows now offers HD resolution H.264 video playback, enabling high-quality Windows Media video delivery to low-cost thin clients. H.264 decoding is improved for thin clients using multi-monitor configurations at higher screen resolutions.
- **UDP audio support**. Receiver for Windows uses native User Datagram Protocol (UDP) to support audio remoting through NetScaler Gateway.
- **Webcam switching**. Receiver for Windows users can choose between different webcams available on the client machine when working with video conferencing apps inside the XenDesktop or XenApp session.
- **Open the Connection Center from the system tray**. You can now right-click on the system tray in Citrix Receiver to quickly access the Connection Center, which displays all connections established from Citrix Receiver. In non-self service or start menu integration mode, you will see a Refresh button in the system tray.
- **Fast Connect Scripting API**. Provides APIs for Citrix partners to rapidly authenticate users to Citrix sessions or desktops. The latest version of Receiver for Windows supports Fast Connect 3 and previous versions.
- **SSON for bimodal domain pass-through**. Users can log on to their domain-joined client machine using either domain credentials or smart card and go straight to Receiver for Web or StoreFront via Receiver for Windows. Previously, users had an additional step of choosing between authentication modes before proceeding to Receiver.

- **Smart card SSON for non-domain devices**. A simplified logon procedure for users with smart cards means only one PIN authentication is required. For the administrator, the advantage is that only one StoreFront server has to be configured. Previously, a StoreFront server had to be configured for each authentication type (smart card and user name with password logon).
- **Session pre-launch feature enabled by default**. The session prelaunch feature is enabled by default when you install the Single Sign-on (SSO) component. Previously, this feature was enabled by editing registry keys or during installation.
- **Disabled use of SSL v3**. To prevent a new attack, such as "POODLE" ,against the SSLv3 protocol, this version of Receiver for Windows disables its use. See CTX200238.

  Important: You must ensure that TLS 1.0 is enabled.
- **Enhanced installation logging**. Install, uninstall, and upgrade histories are preserved in a consistent location for improved troubleshooting and issue resolution. The log location is at %TEMP%\ CTXReceiverInstallLogs for each user.
- **Deprecated features**. Merchandising Server can no longer be used for updating Receiver, as it has reached End of Maintenance. In addition, configuring Receiver to check for updates from citrix.com is not supported.

Fixed issues

For fixed issues, see Citrix Receiver 4.x - Issues Fixed in This Release.

Important: If you are using XenApp or XenDesktop 7.6, consider installing the VDA hotfix available at CTX141702, CTX141703 and CTX141704. This hotfix solves issues with audio after session reconnect, graphics responsiveness, image quality, and screen corruption in some situations.

Known issues

- It is not currently possible to enable apps in the Start menu or as Desktop short cuts on a **per app** basis. [#529321]

- Citrix Receiver for Windows 3.4 (13.4.400) can be upgraded to Citrix Receiver for Windows 4.2 only. To upgrade from 3.4 (13.4.400) to other 4.x versions, 13.4.400 must be uninstalled first.

- References to SSL may still be visible on field labels in the user interface, for example **TLS/SSL data encryption and server identification**. These will be updated in a future release.

- The language bar does not appear on the logon screen of the desktop lock client. The workaround is to use the floating language bar. [#502678]

- The Shortcut options present in the Citrix Desktop Viewer are not working when the session is opened in windowed mode. [#510529]

- The **Learn more** link in the Devices tab under Preferences should link to a user help page, which includes the following text:

  When you display your devices in the Citrix Receiver Preferences dialog box, Citrix Receiver chooses which devices to show on the Devices tab of the Preferences dialog box. If your device is not listed, click Refresh. This ensures that your device appears and is available for you to use with your hosted desktop and application. [#486294]

- The desktop viewer alert message during disconnect is not applicable for anonymous user sessions. This is by design. [#481561]

- Receiver for Windows does not install on a Windows 2012 R2 machine with a User (non-admin) account. [#492508]

- The same webcam selection preferences will be used for multiple Virtual Desktop Agents (VDAs) if the user has multiple VDAs with the same host name belonging to different domains.[#497489]

- When installing the VDA, CitrixReceiver.exe ignores the Custom Path. [#487849]

- System tray notifications can sometimes be seen in desktop lock mode. [#488620]

- The virtual keyboard does not appear automatically for the Terminal server VDA. The workaround is to open the virtual keyboard using the icon on the Desktop Viewer toolbar or for apps, from the virtual keyboard icon on the task bar. [#502774]

- If the webcam selection preference is set to "Automatic" and the PreferredWebcam registry entry is set on the client machine, then the webcam set by PreferredWebcam registry key will be given preference. This is by design. [#494785]

- The audio quality is lower than expected when remoting a USB headset (Logitech USB H340) over generic USB. This is by design. Audio optimization is not performed in USB redirection. This will be considered as an enhancement for a future release. [#469670]

- Slow app enumeration. [#492154] There are two workarounds for this:

1. If the user has enabled `RemoveappsOnLogoff` and `RemoveAppsonExit`, and is experiencing delays in app enumeration at every logon, then the following workaround configuration should reduce the delay.

    a. Reg add HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"

    b. Reg add HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"
    HKCU has preference over HKLM.

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

    a. On a machine, create stub executables for all of the apps. The easiest way to do this is to add all the applications to the machine via Windows Receiver, and it will generate the executables.

    b. Harvest the stub executables from %APPDATA%\Citrix\SelfService. You only need the **.exe** files.

    c. Copy the executables to a network share. For example \\ShareOne\ReceiverStubs

    d. Now for each client machine that is to be locked down, set the following registry keys

        - Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs"

        - Reg add HKLM\Software\Citrix\Dazzle /v CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"

        It is also possible to set these on HKCU if you prefer. HKCU has preference over HKLM.

    e. Exit and Restart Receiver to test.

    Note: HKLM paths are HKLM\Software\Citrix\Dazzle on 32-bit. HKLM paths are HKLM\Software\Wow6432Node\Citrix\Dazzle on 64-bit machines.

- A silent install of Receiver on a Windows 8 computer waits indefinitely (although Receiver installs successfully). To work around this issue, do not use the -wait parameter on the PowerShell command line. [#354627]

- If a user with an older Online plug-in installed connects to a Receiver for Web site from Internet Explorer 10, the plug-in is not upgraded to the latest Receiver for Windows version. To work around this issue, use a different supported browser or uninstall the Online plug-in. [#393929]

- Pinch and zoom gestures are not working on applications remoted through pre-7.0 versions of XenApp and XenDesktop, or on XenApp and XenDesktop version 7.0 or later on Window 2008 R2. [#517877]

- An error is displayed when launching a session in Receiver for Windows 4.2 on Windows XP Embedded thin client. [#514459]

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 8.1, 32-bit and 64-bit editions (including Embedded Edition)
- Windows 8, 32-bit and 64-bit editions (including Embedded Edition)
- Windows 7, 32-bit and 64-bit editions (including Embedded Edition)
- Windows Vista, 32-bit and 64-bit editions
- Windows Thin PC.

  Does not support the Self-Service Plug-in. For more information, see Configure and install Receiver for Windows using command-line parameters.
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2, 64-bit edition
- Windows Server 2008, 32-bit and 64-bit editions
- Windows Server 2003, 32-bit and 64-bit editions

Note: Windows XP (Embedded Edition) is not currently supported (see Known Issues). Support for Windows XP ended April 8, 2014 when Microsoft ended extended support for Windows XP.

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

Touch-enabled devices

Receiver for Windows 4.2 can be used on Windows 7 and 8.1 touch-enabled laptops, tablets, and monitors with XenApp and XenDesktop 7 or later, and with Windows 7, 8 and 2012 Virtual Desktop Agents.

Citrix Servers

- XenApp (any of the following products):
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5, Feature Pack 2, for Windows Server 2008 R2
  - Citrix XenApp 6.5, Feature Pack 1, for Windows Server 2008 R2
  - 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 4, feature pack 2, for Unix operating systems
- XenDesktop (any of the following products):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
  - XenDesktop 5.6, Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
  - XenDesktop 5
- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
- You can use Receiver for Windows 4.2 browser-based access in conjunction with StoreFront Receiver for Web and Web Interface, with - or without - the NetScaler Gateway plug-in.

  StoreFront:

  - StoreFront 2.6 (recommended), 2.5 and 2.1

    Provides direct access to StoreFront stores.

  - StoreFront configured with a Receiver for Web site

    Provides access to StoreFront stores from a web browser. For the limitations of this deployment, refer to "Important considerations" in Receiver for Web sites.

Web Interface in conjunction with the NetScaler VPN client:

  - Web Interface 5.4 for Windows web sites.

    Provides access to virtual desktops and apps from a Web browser.

  - Web Interface 5.4 for Windows with XenApp Services or XenDesktop Services sites
- Ways to deploy Receiver to users:
  - Enable users to download from receiver.citrix.com, then configure using an email or services address in conjunction with StoreFront.
  - Offer to install from Citrix Receiver for Web site (configured with StoreFront).
  - Offer to install Receiver from Citrix Web Interface 5.4.
  - Deploy using Active Directory (AD) Group Policy Objects (GPOs).
  - Deploy using Microsoft System Center 2012 Configuration Manager.

Browser

- Internet Explorer

  Connections to Receiver for Web or to Web Interface support the 32-bit mode of Internet Explorer. For the Internet Explorer versions supported, see StoreFront system requirements and Web Interface system requirements.
- Mozilla Firefox 18.*x* (minimum supported version)
- Google Chrome 21 or 20 (requires StoreFront)

Connectivity

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

- For LAN connections:
  - StoreFront using StoreFront services or Receiver for Web sites
  - Web Interface 5.4 for Windows, using Web Interface or XenApp Services sites

  For information about domain-joined and non-domain-joined devices, refer to the XenDesktop 7 documentation.
- For secure remote or local connections:
  - Citrix NetScaler Gateway 10.5
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway Enterprise Edition 10

- Citrix Access Gateway Enterprise Edition 9.*x*
- Citrix Access Gateway VPX

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

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

Note: References to NetScaler Gateway in this topic also apply to Access Gateway, unless otherwise indicated.

About secure connections and certificates

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

Private (self-signed) certificates

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

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

Installing root certificates on user devices

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

Wildcard certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. Receiver for Windows supports wildcard certificates, however they should only be used in accordance with your organization's security policy. In practice, alternatives to wildcard certificates, such as a certificate containing the list of server names within the Subject Alternative Name (SAN) extension, could be considered. Such certificates can be issued by both private and public certificate authorities.

Intermediate certificates and the NetScaler Gateway

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

Authentication

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

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

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

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

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

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

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

Upgrades

Receiver for Windows 4.x can be used to upgrade Receiver for Windows 3.x as well as Citrix online plug-in 12.x. For information more information on upgrading, see Considerations when upgrading.

Other

- **.NET Framework requirements**
    - .NET 3.5 Service Pack 1 is required by the Self-Service Plug-in, which allows users to subscribe to and launch desktops and applications from the Receiver window or from a command line. For more information, see Configure and install Receiver for Windows using command-line parameters.
    - The .NET 2.0 Service Pack 1 and Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package are required to ensure that the Receiver icon displays correctly. The Microsoft Visual C++ 2005 Service Pack 1 package is included with .NET 2.0 Service Pack 1, .NET 3.5, and .NET 3.5 Service Pack 1; it is also available separately.
    - For XenDesktop connections: To use the Desktop Viewer, .NET 2.0 Service Pack 1 or later is required. This version is required because, if Internet access is not available, certificate revocation checks slow down connection startup times. The checks can be turned off and startup times improved with this version of the Framework but not with .NET 2.0.
- For information about using Receiver with Microsoft Lync Server 2013 and the Microsoft Lync 2013 VDI Plug-in for Windows, see XenDesktop, XenApp and Citrix Receiver Support for Microsoft Lync 2013 VDI Plug-in.
- **Supported connection methods and network transports:**
    - TCP/IP+HTTP

      > **Important:** If stores are configured in StoreFront with a Transport type of HTTP, you must add the following key value to the registry key HKLM\Software\[Wow6432Node\]Citrix\AuthManager: ConnectionSecurityMode=Any.

      See CTX 134341 for additional values, which may be required.

      > **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.
    - TLS+HTTPS

Install 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 NetScaler Gateway (or Access Gateway) or StoreFront Server associated with the email address and then prompts the user to log on and continue the installation. This feature is referred to as "email-based account discovery."

    Note: A first-time user is one who does not have Receiver installed on the device.
  - Email-based account discovery for a first-time user does not apply if Receiver is downloaded from a location other than Citrix.com (such as a Receiver for Web site).
  - If your site requires configuration of Receiver, use an alternate deployment method.
- Automatically from Receiver for Web or from a Web Interface logon screen.
  - A first-time Receiver user can set up an account by entering a server URL or downloading a provisioning (CR) file.
- Using an Electronic Software Distribution (ESD) tool
  - A first-time Receiver user must enter a server URL or open a provisioning file to set up an account.

Refer also to Configure and install Receiver for Windows using command-line parameters, Install and uninstall Receiver for Windows manually, and Deploy Receiver using Active Directory and sample startup scripts.

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

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

Manual Upgrade to Receiver for Windows 4.2

Important: If the Citrix Lync Optimization Pack is installed on the endpoint device it must be uninstalled first and then reinstalled after upgrading Citrix Receiver for Windows. Refer to CTX200340 for additional details.

For deployments with StoreFront:

- Best practice for BYOD (Bring Your Own Device) users is to configure the latest versions of NetScaler Gateway and StoreFront as described in the documentation for those products in 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 providing a provisioning file, inform users to enter the URL of NetScaler Gateway (or Access Gateway Enterprise Edition). Or, if you configured email-based account discovery as described in the StoreFront documentation, inform users to enter their email address.
- Another method is to configure a Receiver for Web site as described in the StoreFront documentation and complete the configuration described in Deploy Receiver from Receiver for Web. Inform users how to upgrade Receiver, access the Receiver for Web site, and download the provisioning file from Receiver for Web (click the user name and click Activate).

For deployments with Web Interface

- Upgrade your Web Interface site with Receiver for Windows 4.2 and complete the configuration described in Deploy 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

Important: The process for configuring pass-through authentication (single sign-on) changed for Receiver for Windows 4.x. For information, refer to the /includeSSON description in Configure and install Receiver for Windows using command-line parameters.

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

To upgrade the Online plug-in (full) configured for PNA or Citrix Receiver (Enterprise) to Receiver for Windows 4.x (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 4.x provides Web-based access to Citrix Receiver.

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

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

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. For command line installation parameters and space requirements, see Configure and install Receiver for Windows using command-line parameters.

When you cancel the installation before completion, some components might be installed. In that case, remove Receiver with the Windows Programs and Features utility (Add/Remove Programs).

> **Important:** The process for configuring pass-through authentication (single sign-on) changed for Receiver for Windows 4.x. For information, refer to the /includeSSON description in Configure and install 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

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

Note: Do not use this method if Citrix Receiver Updater was used to install Receiver.

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 Programs and Features, the 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 with Programs and Features.

Auto-repair occurs if there is a problem with Receiver; however, there is no Repair option in Programs and Features for Receiver. 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 Server 2012/2008, Windows 8, Windows 7, Windows Vista

    C:\ProgramData\Citrix\Citrix Receiver\

  - Operating system: Windows 2003 and Windows XP

    C:\Documents and Settings\All Users\Application Data\Citrix\Citrix Receiver\

- If installed per user:
  - Operating system: Windows Server 2012/2008, Windows 8, Windows 7, Windows Vista

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

  - Operating system: Windows 2003 and Windows XP

    %USERPROFILE%\Local Settings\Application Data\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. To remove the 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.

Configure and install Receiver for Windows using command-line parameters

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.

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.

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

CitrixReceiver.exe [***Options***]

The options are:

- /? or /help displays usage information.
- /noreboot suppresses reboot during UI installations. This option is not necessary for silent installs. If you suppress reboot prompts, any USB devices which are in a suspended state when Receiver installs will not be recognized by Receiver until after the user device is restarted.
- /silent disables the error and progress dialogs to run a completely silent installation. See also: /noreboot.
- /includeSSON installs single sign-on (pass-through) authentication. This option is required for smart card single sign on.

  The related option, ENABLE_SSON, is enabled when /includeSSON is on the command line. If you use ADDLOCAL= to specify features and you want to install single sign on, you must also specify the value SSON.

  To enable pass-through authentication for a user device, you must install Receiver with local administrator rights from a command line that has the option /includeSSON. On the user device, you must also enable these policies located in Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication:

  Local user name and password

  Enable pass-through authentication

  Allow pass-through authentication for all ICA (might be needed, depending on the Web Interface configuration and security settings)

After the changes are completed, restart the user device. For more information, refer to How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication.

> **Note:** Smart card, Kerberos and Local user name and password policies are inter-dependent.The order of configuration is important. We recommend to first disable unwanted policies, and then enable the policies you require. Carefully validate the result.

- *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 most of the Receiver software will be installed. The default value is C:\Program Files\Citrix\Receiver. The following Receiver components are installed in the C:\Program Files\Citrix path: Authentication Manager, Receiver, and the Self-Service plug-in.

    If you use this option and specify an *Installation directory*, you must install RIInstaller.msi in the *Installation directory*\Receiver directory and the other .msi files in the *Installation directory*.

  - 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*[,...] Installs one or more of the specified components. When specifying multiple parameters, separate each parameter with a comma and without spaces. The names are case sensitive. If you do not specify this parameter, all components are installed by default.

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

    ReceiverInside – Installs the Receiver experience. (Required component for Receiver operation.)

    ICA_Client – Installs the standard Receiver. (Required component for Receiver operation.)

    SSON – Installs single sign on. Requires administrator rights.

    AM – Installs the Authentication Manager.

    SELFSERVICE - Installs the Self-Service Plug-in. The AM value must be specified on the command line and .NET 3.5 Service Pack 1 must be installed on the user device. The Self-Service Plug-in is not available for Windows Thin PC devices, which do not support .NET 3.5.

For information on scripting the Self-Service Plug-in (SSP), and a list of parameters available in Receiver for Windows 4.2 and later, see http://support.citrix.com/article/CTX200337.

The Self-Service Plug-in allows users to access virtual desktops and applications from the Receiver window or from a command line, as described in later in this section in *To launch a virtual desktop or application from a command line*. If the Self-Service Plug-in is not installed, users must access virtual desktops and applications from a web page.

USB – Installs USB support. Requires administrator rights.

DesktopViewer – Installs the Desktop Viewer.

Flash – Installs HDX media stream for Flash.

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

- 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.) Defaults to S.

  N – Never allow users to add or remove their own store.

  S – Allow users to add or remove secure stores only (configured with HTTPS).

  A – Allow users to add or remove both secure stores (HTTPS) and non-secure stores (HTTP). Not applicable if Receiver is installed per user.

  You can also control this feature by updating the registry key HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore.

  Note: Only secure (HTTPS) stores are allowed by default and are recommended for production environments. For test environments, you can use HTTP store connections through the following configuration:

  1. Set HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore to A to allow users to add non-secure stores.

  2. Set HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd to A to allow users to save their passwords for non-secure stores.

  3. To enable the addition of a store that is configured in StoreFront with a TransportType of HTTP, add to HKLM\Software\[Wow6432Node\]Citrix\AuthManager the value ConnectionSecurityMode (REG_SZ type) and set it to Any.

  4. Exit and restart Receiver.
- 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.

  N – Never allow users to save their passwords.

  S – Allow users to save passwords for secure stores only (configured with HTTPS).

A – Allow users to save passwords for both secure stores (HTTPS) and non-secure stores (HTTP).

You can also control this feature by updating the registry key HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd.

Note: The following registry key must be added manually if AllowSavePwd does not work.

Key for 32bit OS client: HKLM\Software\Citrix\AuthManager

Key for 64bit OS client: HKLM\Software\wow6432node\Citrix\AuthManager

Name: SavePasswordMode

Type: REG_SZ

Value: never - Never allow users to save their passwords. secureonly - Allow users to save passwords for secure stores only (configured with HTTPS). always - Allow users to save passwords for both secure stores (HTTPS) and non-secure stores (HTTP).

- ENABLE_SSON={Yes | No} – The default value is Yes. Enables single sign on when /includeSSON is also specified. This property is required for smart card single sign on. Note that users must log off and log back on to their devices after an installation with single sign-on authentication enabled. Requires administrator rights.

  Important: If you disable single sign-on authentication, users must reinstall Receiver if you later enable it.

- AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry } – The default value is Prompt, which prompts the user to choose a certificate from a list. Change this property to choose the default certificate (per the smart card provider) or the certificate with the latest expiry date. If there are no valid logon certificates, the user is notified, and given the option to use an alternate logon method if available.

  You can also control this feature by updating the registry key HKCU or HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }. Values defined in HKCU take precedence over values in HKLM to best assist the user in selecting a certificate.

- AM_SMARTCARDPINENTRY=CSP – By default, the PIN prompts presented to users are provided by Receiver rather than the smart card Cryptographic Service Provider (CSP). Receiver prompts users to enter a PIN when required and then passes the PIN to the smart card CSP. Specify this property to use the CSP components to manage the PIN entry, including the prompt for a PIN.

  You can also control this feature with the registry key HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP.

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

- 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 to deliver Microsoft Office applications to users running Windows 7.

- ENABLEPRELAUNCH={False | True} - The default value is False. For information about session pre-launch, refer to Reduce application launch time.

- STARTMENUDIR=*Text string* – By default, applications appear under Start > All Programs. You can specify the relative path under the programs folder to contain the shortcuts to subscribed applications. For example, to place shortcuts under Start > All Programs > Receiver, specify STARTMENUDIR=\Receiver\. Users can change the folder name or move the folder at any time.

  You can also control this feature through a registry key: Create the entry REG_SZ for StartMenuDir and give it the value "\RelativePath". Location:

  HKLM\Software\[Wow6432Node\]Citrix\Dazzle

  HKCU\Software\Citrix\Dazzle

  For applications published through XenApp with a Client applications folder (also referred to as a Program Neighborhood folder) specified, you can specify that the client applications folder is to be appended to the shortcuts path as follows: Create the entry REG_SZ for UseCategoryAsStartMenuPath and give it the value "true". Use the same registry locations as noted above.

  Examples: If Client applications folder is \Office, UseCategoryAsStartMenuPath is true, and no StartMenuDir is specified, shortcuts are placed under Start > All Programs > Office. If Client applications folder is \Office, UseCategoryAsStartMenuPath is true, and StartMenuDir is \Receiver, shortcuts are placed under Start > All Programs > Receiver > Office.

  Changes made to these settings have no impact on shortcuts that are already created. To move shortcuts, you must uninstall and re-install the applications.

- STORE*x*="*storename*;http[s]://*servername.domain*/*IISLocation*/discovery;[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/*store*/discovery". To obtain the URL, export a provisioning file from StoreFront, open it in notepad and copy the URL from the `<Address>` element.

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

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

- ALLOW_CLIENTHOSTEDAPPSURL=1 - Enables the URL redirection feature on user devices. Requires administrator rights. Requires that Receiver is installed for All Users. For information about URL redirection, refer to Local App Access and its sub-topics in the XenDesktop 7 documentation.
- SELFSERVICEMODE={False | True} - The default value is True. When the administrator sets the SelfServiceMode flag to false, the user no longer has access to the self service Receiver user interface. Instead, they can access subscribed apps from the Start menu and via desktop shortcuts - known as "shortcut-only mode". See Configure Shortcut Only mode for more information.
- DESKTOPDIR=Dir_Name. Brings all shortcuts into a single folder. CategoryPath is supported for desktop shortcuts.

  Note: DESKTOPDIR requires the `PutShortcutsOnDesktop` key to be set to True. See Configure Shortcut Only for more information.

To display an installation complete dialog during unattended installs

For unattended installs of CitrixReceiver.exe, an Add Account dialog appears before the installation completes for a first-time user. The Add Account dialog requires that a user enter an email or server address to complete the installation. To replace the Add Account dialog with one that appears when installation completes and gives the user the option to set up an account, add the following key value to the registry key HKCU\Software\Citrix\Receiver: EnableFTU=0.

Add that same registry key to machine-wide policies if multiple users log on to the same machine.

Note: If a common store has not been defined by the STOREx argument above, or by a Group Policy Object, then users who have not previously logged on to a computer where Receiver is installed, may see the Add Account dialog. To suppress this dialog, create a REG_DWORD value EnableFTU in the key HKLM\Software\Citrix\Receiver and set the value to `0`.

To troubleshoot installation

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

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

Examples of a command-line installation

To install all components silently and specify two application stores:

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

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

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

To launch a virtual desktop or application from a command line

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

Deploy 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. For general information about startup scripts, refer to Microsoft documentation.

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 Configure and install Receiver for Windows using command-line parameters.

To add the per-computer startup scripts

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

To deploy 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.

Use the per-user sample startup scripts

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

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

To set up the per-user startup scripts

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

To deploy 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.

Deploy 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 Receiver for Web sites in the StoreFront documentation.

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 Configure Receiver for Web sites using the configuration files in the StoreFront documentation.

Deploy Receiver from a Web Interface logon screen

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

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 website. 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, refer to Configuring Client Deployment in 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 websites.

   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.

Configure

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

- Configure application delivery and your XenDesktop environment. To provide remote users with secure access to their virtual desktops and applications, configure NetScaler Gateway or Access Gateway.
- Use a Group Policy Object template file to customize Receiver. Configure rules for routing, proxy servers, remote user devices, and more.
- Provide users with account information. Provide users with the information they need to set up access to accounts hosting their virtual desktops and applications. In some environments, users must manually set up access to those accounts.

Configure application delivery

When delivering applications with XenDesktop or XenApp, consider the following options to enhance the experience for users when they access their applications through StoreFront stores. For information about delivering applications using XenDesktop 7, refer to Create a Delivery Group application in the XenDesktop 7 documentation.

- Include meaningful descriptions for applications in a Delivery Group. Descriptions are visible to Receiver users.
- Append keywords to the descriptions you provide for delivery group applications:
    - To make an individual app mandatory, so that it cannot be removed from Receiver for Windows, append the string KEYWORDS:Mandatory to the application description. There is no Remove option for users to unsubscribe to mandatory apps.
    - To automatically subscribe all users of a store to an application, append the string KEYWORDS:Auto to the description. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
    - To advertise applications to users or to make commonly used applications easier to find by listing them in the Receiver Featured list, append the string KEYWORDS:Featured to the application description.
    - To specify that a locally installed application should be used instead of an application available in Receiver, append the string KEYWORDS:prefer="*pattern*". This feature is referred to as Local App Access.

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

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

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

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

        - prefer="*ApplicationName*"

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

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

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

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

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

- prefer=”\\Folder1\Folder2\\...\\ApplicationName”

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

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

"\Microsoft Word"	\Microsoft Word 2010	No

For information about other keywords, refer to "Additional recommendations" in Optimize the user experience in the StoreFront documentation.

Configure Shortcut Only mode

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

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

Users and administrators can use a number of registry settings to customize the way shortcuts are set up. See Registry keys for shortcuts customization.

Working with shortcuts

- Users cannot remove apps. All apps are mandatory when working with the `SelfServiceMode` flag set to `false` (shortcut-only mode). If the user removes a shortcut icon from the desktop, the icon comes back when the user selects Refresh from the Receiver system tray icon.
- Users can configure only one store. The Account and Preferences options are not available. This is to prevent the user from configuring additional stores. The administrator can give a user special privileges to add more than one account using the Group Policy Object template, or by manually adding a registry key (HideEditStoresDialog) on the client machine. When the administrator gives a user this privilege, the user has a Preferences option in the system tray icon, where they can add and remove accounts.
- Users cannot remove apps via the Windows Control Panel.
- You can add desktop shortcuts via a customizable registry setting. Desktop shortcuts are not added by default. After you make any changes to the registry settings, Receiver must be restarted.
- Shortcuts are created in the Start menu with a category path as the default, `UseCategoryAsStartMenuPath`.
- You can add a flag `[/DESKTOPDIR="Dir_name"]` during installation to bring all shortcuts into a single folder. `CategoryPath` is supported for desktop shortcuts.
- Auto Re-install Modified Apps is a feature which can be enabled via the registry key `AutoReInstallModifiedApps`. When AutoReInstallModifiedApps is enabled, any changes to attributes of published apps and desktops on the server are reflected on the client machine. When AutoReInstallModifiedApps is disabled, apps and desktop attributes are not updated and shortcuts are not re-stored on refresh if deleted on the client. By default this AutoReInstallModifiedApps is enabled. See Registry keys for

shortcuts customization.

Using the Group Policy Object template to configure shortcuts

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

1. Open the Local Group Policy Editor by running the command `gpedit.msc` locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add, browse to the Receiver Configuration folder and then select icaclient.adm.
5. Select Open to add the template and then Close to the return to the Group Policy Editor.
6. In the Group Policy Editor, got to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Self Service. **Note:** The icaclient.adm template is available on the User Configuration after it has been added to the Computer Configuration.
7. Select Manage SelfServiceMode to enable or disable the self service Receiver user interface.
8. Choose Manage App Shortcut to enable or disable:
    - Shortcuts on Desktop
    - Shortcuts in Start menu
    - Desktop Directory
    - Start menu Directory
    - Category path for Shortcuts
    - Remove apps on logoff
    - Remove apps on exit
9. Choose Allow users to Add/Remove account to give users privileges to add or remove more than one account.

Registry keys for shortcuts customization

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

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

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

Registry keys for 32-bit machines

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

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

AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	True in SelfServiceMode, and False in NonSelfServiceMode	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle

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

Registry keys for 64-bit machines

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

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

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

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

Configuring shortcuts based on StoreFront account settings

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

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

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

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

The section ends with the `</account>` tag.
Before the end of the account section, in the first properties section:

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

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

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

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

An extended example for this section is:

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

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

Configure your XenDesktop environment

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

Configure USB support for XenDesktop and XenApp connections

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

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

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

- Keyboards
- Mice
- Smart cards

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

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

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

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

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

- Bluetooth dongles
- Integrated network interface cards
- USB hubs

- USB graphics adaptors
- Audio devices
- Mass storage devices

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

For instructions on automatically redirecting specific USB devices, see CTX123015.

How USB support works

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

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

Mass storage devices

For mass storage devices only, in addition to USB support, remote access is available through client drive mapping, which you configure through the Citrix Receiver policy Remoting client devices > Client drive mapping. When this policy is applied, the drives on the user device are automatically mapped to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders with mapped drive letters.

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

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

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

USB device classes allowed by default

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

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

- Audio (Class 01). Includes audio input devices (microphones), audio output devices, and MIDI controllers. Modern audio devices generally use isochronous transfers, which is supported by XenDesktop 4 or later. Audio (Class01) is not applicable to XenApp because these devices are not available for remoting in XenApp using USB support.

  Note: Some specialty devices (for example, VOIP phones) require additional configuration. For 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. Mass Storage (Class 08) is not applicable to XenApp because these devices are not available for remoting in XenApp using USB support. Known subclasses include:
  - 01 Limited flash devices
  - 02 Typically CD/DVD devices (ATAPI/MMC-2)
  - 03 Typically tape devices (QIC-157)

  - 04 Typically floppy disk drives (UFI)
  - 05 Typically floppy disk drives (SFF-8070i)
  - 06 Most mass storage devices use this variant of SCSI

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

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

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

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

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

USB device classes denied by default

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

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

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

  The default USB policy does not allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). This is because most keyboards and mice are handled appropriately without USB support and it is normally necessary to use these devices locally as well remotely when connecting to a virtual desktop.
- USB Hubs (Class 09). USB hubs allow extra devices to be connected to the local computer. It is not necessary to access these devices remotely.
- Smart Card (Class 0b). Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card-equivalent chip.

  Smart card readers are accessed using smart card remoting and do not require USB support.
- Wireless Controller (Class e0). Some of these devices may be providing critical network access, or connecting critical peripherals, such as Bluetooth keyboards or mice.

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

Update the list of USB devices available for remoting

You can update the range of USB devices available for remoting to desktops by editing the 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/.

Configure Bloomberg keyboards

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

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

To turn Bloomberg keyboard support on or off

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

1. Locate the following key in the registry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Do one of the following:

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

To prevent the Desktop Viewer window from dimming

If users have multiple Desktop Viewer windows, by default the desktops that are not active are dimmed. If users need to view multiple desktops simultaneously, this can make the information on them unreadable. You can disable the default behavior and prevent the Desktop Viewer window from dimming by editing the Registry.

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

1. On the user device, create a REG_DWORD entry called DisableDimming in one of the following keys, depending on whether you want to prevent dimming for the current user of the device or the device itself. An entry already exists if the Desktop Viewer has been used on the device:

   - 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 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.

Configure StoreFront

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

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

To configure StoreFront

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

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

Configure Receiver with the Group Policy Object template

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 user 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.

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.

Manage a list of StoreFront accounts

These steps shows you how to use a policy setting in the icaclient.adm file to manage a list of StoreFront accounts.

In the icaclient.adm file:

1. Enable the key, HKLM\Software\Policies\Citrix\Receiver\Sites.
2. Enter a list of StoreFront accounts. For each entry, enter the following information, delimited by a semi-colon:
   - Store name. The name that the user sees for this store.
   - Store URL. The url for the store.

- Store enabled state. Set to On or Off.
- Store description. The description that the user sees for this store.

Example: `SalesStore;https://sales.example.com/Citrix/Store/discovery;On;Store for Sales staff`

Provide users with account information

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

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

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

Configure 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 NetScaler Gateway or Access Gateway, or StoreFront Server associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access virtual desktops and applications.

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

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

To configure NetScaler Gateway, see Connecting to StoreFront by using email-based discovery in the NetScaler Gateway documentation.

Provide users with provisioning files

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

- You can use StoreFront to create provisioning files containing connection details for accounts. Make these files available to your users to enable them to configure Receiver automatically. After installing Receiver, 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, refer to To export store provisioning files for users in the StoreFront documentation.

Provide users with account information to enter manually

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

- For connections to a StoreFront store, provide the URL for that server. For example: https://servername.company.com

  For web interface deployments, provide the URL for the XenApp Services site.

- For connections through NetScaler Gateway, first determine whether user should see all configured stores or just the store that has remote access enabled for a particular NetScaler Gateway.

  - To present all configured stores: Provide users with the NetScaler Gateway fully-qualified domain name.

  - To limit access to a particular store: Provide users with the NetScaler Gateway fully-qualified domain name and the store name in the form:

    NetScalerGatewayFQDN?MyStoreName

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

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

To manage accounts, a Receiver user opens the Receiver home page, clicks ▼, and then clicks Accounts.

Optimize the Receiver environment

You can optimize the environment in which Receiver operates for your users.

- Reduce application launch time
- Facilitate the connection of devices to published resources
- Support DNS name resolution
- Use proxy servers with XenDesktop connections
- Provide support for NDS users
- Use Receiver with XenApp for UNIX
- Enable access to anonymous applications

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

Reduce application launch time

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

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

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

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

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

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

The registry locations are:

HKLM\Software\[Wow6432Node\]Citrix\Dazzle

HKCU\Software\Citrix\Dazzle

There are two types of pre-launch:

- **Just-in-time pre-launch**. Pre-Launch starts immediately after the user's credentials are authenticated whether or not it is a high-traffic period. Typically used for normal traffic periods. A user can trigger just-in-time pre-launch by restarting Receiver.

- **Scheduled pre-launch**. Pre-launch starts at a scheduled time. Scheduled pre-launch starts only when the user device is already running and authenticated. If those two conditions are not met when the scheduled pre-launch time arrives, a session does not launch. To spread network and server load, the session launches within a window of when it is scheduled. For example, if the scheduled pre-launch is scheduled for 1:45 p.m., the session actually launches between 1:15 p.m. and 1:45 p.m. Typically used for high-traffic periods.

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

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

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

HKLM registry values

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

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

Name: UserOverride

Values:

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

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

Name: State

Values:

0 - Disable pre-launch.

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

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

Name: Schedule

Value:

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

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

HKCU registry values

`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch`

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

Map client devices

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

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

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

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

Turn off user device mappings

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

Redirect client folders

Client folder redirection changes the way client-side files are accessible on the host-side session. When you enable only client drive mapping on the server, client-side full volumes are automatically mapped to the sessions as Universal Naming Convention (UNC) links. When you enable client folder redirection on the server and the user configures it on the user device, the portion of the local volume specified by the user is redirected.

Only the user-specified folders appear as UNC links inside sessions instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session. For more information, including how to configure client folder redirection for user devices, see the XenDesktop 7 documentation.

Map client drives to host-side drive letters

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

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

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

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

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

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

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

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

HDX Plug and Play USB device redirection

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

Important: If you prohibit Plug and Play USB device redirection in a server policy, the user cannot override that policy setting.

A user can set permissions in Receiver to always allow or reject device redirection or to be prompted each time a device is connected. The setting affects only devices plugged in after the user changes the setting.

To map a client COM port to a server COM port

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

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

1. For XenDesktop 7 deployments, enable the Client COM port redirection policy setting.
2. Log on to Receiver.
3. At a command prompt, type: net use com*x*: \\client\comz: where *x* is the number of the COM port on the server (ports 1 through 9 are available for mapping) and *z* is the number of the client COM port you want to map.
4. To confirm the operation, type: net use at a command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports. To use this COM port in a virtual desktop or application, install your user device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session. Use this mapped COM port as you would a COM port on the user device.

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

Support 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 user devices

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

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

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

Use 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.

Improve the user experience

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

- Client-side microphone input
- Multi-monitor support
- Printer setting overrides on devices
- Keyboard shortcuts
- Receiver support for 32-bit color icons
- Enabling Desktop Viewer
- Keyboard input in Desktop Viewer sessions
- Connect to virtual desktops

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.

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

You can use up to eight monitors with Receiver.

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

Sessions can span multiple monitors in two ways:

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

  XenDesktop: To display the Desktop Viewer window across any rectangular subset of monitors, resize the window across any part of those monitors and press 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 desktop is displayed across the same monitors. Multiple virtual desktops can be displayed on one device provided the monitor arrangement is rectangular. If the primary monitor on the device is used by the XenDesktop session, it becomes the primary monitor in the session. Otherwise, the numerically lowest monitor in the session becomes the primary monitor.

To enable multi-monitor support, ensure the following:

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

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

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

Printer setting overrides on devices

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

To override the printer settings on the user device

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

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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Experience > Keyboard shortcuts.
7. From the Action menu, choose Properties, select Enabled, and choose the desired options.

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.

Enabling Desktop Viewer

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

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

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

Keyboard input in Desktop Viewer sessions

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

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

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

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

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

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

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

Connect to virtual desktops

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

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

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

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

Secure 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 smart card authentication, certificate revocation list checking, and Kerberos pass-through authentication.

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

Configure domain pass-through authentication

This topic shows you how to enable domain pass-through authentication for Citrix Receiver with XenDesktop or XenApp.

Note: In this example, the Receiver installation, application of computer policy, and the configuration of a trusted site on the client operating system are done manually. Once a Group Policy Object (GPO) template is built, you can apply it to any domain client machine where Receiver has been installed.

1. Install Citrix Receiver 4.2 with the /includeSSON switch.
    a. Install one or more StoreFront stores. You can complete this step later. Installing StoreFront stores is not a prerequisite for setting up domain pass-through authentication. For information on the syntax for adding one or more StoreFront stores, see Configure and install Receiver for Windows using command-line parameters.
    b. Check to see that pass-through authentication is enabled by starting Citrix Receiver and then confirm that the **ssonsvr.exe** process is running.
2. Add the ICA Client GPO Administrative Template to the Local Computer Policy on the user's local machine and/or in the VDA desktop gold image:
    a. Open **gpedic.msc**.

        Note: The Group Policy Editor snap-in, gpedic.msc, is available with Professional, Enterprise and Ultimate editions of Windows 7 and Windows 8.
    b. Right-click Computer Configuration > Administrative Templates and then select Add/Remote Templates.
    c. Add the **C:\Program Files\Citrix\ICA Client\Configuration\icaclient.adm** template.
3. Enable the following Local Computer GPO on the user's local machine and/or in the VDA desktop gold image:
    a. Choose Local user name password.
    b. Select Enabled.
    c. Select Enable pass-through authentication.
    d. Select Allow pass-through authentication for all ICA connections.
    e. Click OK.
    f. Reboot the VDA desktop gold image.
4. Log on the Delivery Controller(s), then open Windows PowerShell and execute the following commands to enable the Delivery Controller to trust XML requests sent from StoreFront.

   a. If not already loaded, load the Citrix cmdlets by typing `asnp Citrix*.` (be sure to include the period after Citrix*).

   b. Press Enter.

   c. Then type `Add-PSSnapin citrix.broker.admin.v2` and press Enter.

   d. Then type `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True` and press Enter.

   e. Close PowerShell.

5. Open Internet Explorer on the local machine and/or in the VDA desktop gold image.

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

   Note: You can also add the StoreFront server to the Trusted Sites using a Microsoft GPO. The GPO is called Zone Assignment List, and you can find it in Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page.

7. Log off, and log back on to Receiver.

When Citrix Receiver opens, if the current user is logged on to the domain, the user's credentials are passed through to StoreFront and enumerate apps and desktops within Citrix Receiver, as well as the user's Start menu. When the user clicks an icon, Receiver passes through the user's domain credentials to the Delivery Controller and the app or desktop opens.

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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password.
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.

Configure domain pass-through authentication with Kerberos

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

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

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

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

1. The Receiver single sign-on service captures the smart card PIN.
2. Receiver uses IWA (Kerberos) to authenticate the user to StoreFront. StoreFront then provides Receiver with information about available virtual desktops and apps.

   Note: You do not have to use Kerberos authentication for this step. Enabling Kerberos on Receiver is only needed to avoid an extra PIN prompt. If you do not use Kerberos authentication, Receiver authenticates to StoreFront using the smart card credentials.
3. The HDX engine (previously referred to as the ICA client) passes the smart card PIN to XenDesktop or XenApp to log the user on to the Windows session. XenDesktop or XenApp then deliver the requested resources.

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

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

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

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

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

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

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

- /includeSSON

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

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

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

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

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

To apply the settings, restart Receiver on the user device.

To configure StoreFront:

- In the default.ica file located on the StoreFront server, set `DisableCtrlAltDel to false`.

  Note: This step is not required if all client machines are running Receiver for Windows 4.2 or above.

- When you configure the authentication service on the StoreFront server, select the Domain pass-through check box. That setting enables Integrated Windows Authentication. You do not need to select the Smart card check box unless you also have non domain joined clients connecting to Storefront with smart cards.

For more information about using smart cards with StoreFront, refer to Configure the authentication service in the StoreFront documentation.

Configure smart card authentication

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

- **Pass-through authentication (single sign-on) -** Pass-through authentication captures smart card credentials when users log on to Receiver. Receiver uses the captured credentials as follows:

  - Users of domain-joined devices who log on to Receiver with smart card credentials can start virtual desktops and applications without needing to re-authenticate.

  - Users of non-domain-joined devices who log on to Receiver with smart card credentials must enter their credentials again to start a virtual desktop or application.

  Pass-through authentication requires StoreFront and Receiver configuration.

- **Bimodal authentication -** Bimodal authentication offers users a choice between using a smart card and entering their user name and password. This feature is useful if the smart card cannot be used (for example, the user has left it at home or the logon certificate has expired). Dedicated stores must be set up per site to allow this, using the `DisableCtrlAltDel` method set to `False` to allow smart cards. Bimodal authentication requires StoreFront configuration. If NetScaler Gateway is present in the solution, is also requires configuration.

  Bimodal authentication also now gives the StoreFront administrator the opportunity to offer the end user both user name and password and smart card authentication to the same store by selecting them in the StoreFront Console. See StoreFront documentation.

- **Multiple certificates -** Multiple certificates can be available for a single smart card and if multiple smart cards are in use. When a user inserts a smart card into a card reader, the certificates are available to all applications running on the user device, including Receiver. To change how certificates are selected, configure Receiver.

- **Client certificate authentication -** Client certificate authentication requires NetScaler Gateway/Access Gateway and StoreFront configuration.

  - For access to StoreFront resources through NetScaler Gateway/Access Gateway, users might have to re-authenticate after removing a smart card.

  - When the NetScaler Gateway/Access Gateway SSL configuration is set to mandatory client certificate authentication, operation is more secure. However mandatory client certificate authentication is not compatible with bimodal authentication.

- **Double hop sessions -** If a double-hop is required, a further connection is established between Receiver and the user's virtual desktop. Deployments supporting double hops are described in the XenDesktop documentation.

- **Smart card-enabled applications -** Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office, allow users to digitally sign or encrypt documents available in virtual desktop or application sessions.

Prerequisites

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

Limitations

- Certificates must be stored on a smart card, not the user device.
- Receiver for Windows does not save the user certificate choice, but can store the PIN when configured. The PIN is only cached in non-paged memory for the duration of the user session and is not stored to disk at any point.
- Receiver for Windows does not reconnect sessions when a smart card is inserted.
- When configured for smart card authentication, Receiver for Windows does not support virtual private network (VPN) single-sign on or session pre-launch. To use VPN tunnels with smart card authentication, users must install the NetScaler Gateway Plug-in and log on through a web page, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the NetScaler Gateway Plug-in is not available for smart card users.
- Receiver for Windows Updater communications with citrix.com and the Merchandising Server is not compatible with smart card authentication on NetScaler Gateway.

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

To enable single sign-on for smart card authentication

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

- ENABLE_SSON=Yes

  Single sign-on is another term for pass-through authentication. Enabling this setting prevents Receiver from displaying a second prompt for a PIN.

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

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

  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

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

- `/includeSSON` installs single sign-on (pass-through) authentication. Enables credential caching and the use of pass-through domain-based authentication.
- If the user is logging on to the endpoint with a different method to smart card for Receiver authentication (for example, user name and password), the command line is:

  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No

  This prevents the credentials being captured at log on time and allows Receiver to store the PIN when logging on to Receiver.
- Go to Policy > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Authentication > Local user name and password.

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

To configure StoreFront:

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

For more information about using smart cards with StoreFront, refer to Configure the authentication service in the StoreFront documentation.

To enable user devices for smart card use

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

To change how certificates are selected

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

A valid certificate must have all of these characteristics:

- The current time of the clock on the local computer is within the certificate validity period.

- The Subject public key must use the RSA algorithm and have a key length of 1024, 2048, or 4096 bits.
- Key Usage must contain Digital Signature.
- Subject Alternative Name must contain the User Principal Name (UPN).
- Enhanced Key Usage must contain Smart Card Logon and Client Authentication, or All Key Usages.
- One of the Certificate Authorities on the certificate's issuer chain must match one of the permitted Distinguished Names (DN) sent by the server in the TLS handshake.

Change how certificates are selected by using either of the following methods:

- On the Receiver command line, specify the option AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }.

  Prompt is the default. For SmartCardDefault or LatestExpiry, if multiple certificates meet the criteria, Receiver prompts the user to choose a certificate.

- Add the following key value to the registry key HKCU or HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }.

  Values defined in HKCU take precedence over values in HKLM to best assist the user in selecting a certificate.

To use CSP PIN prompts

By default, the PIN prompts presented to users are provided by Receiver rather than the smart card Cryptographic Service Provider (CSP). Receiver prompts users to enter a PIN when required and then passes the PIN to the smart card CSP. If your site or smart card has more stringent security requirements, such as to disallow caching the PIN per-process or per-session, you can configure Receiver to instead use the CSP components to manage the PIN entry, including the prompt for a PIN.

Change how PIN entry is handled by using either of the following methods:

- On the Receiver command line, specify the option AM_SMARTCARDPINENTRY=CSP.
- Add the following key value to the registry key HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP.

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 TLS connection 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.

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

8. From the CRL verification drop-down menu, select one of the options.

   - Disabled. No certificate revocation list checking is performed.

   - Only check locally stored CRLs. CRLs that were installed or downloaded previously are used in certificate validation. Connection fails if the certificate is revoked.

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

- Retrieve CRLs from network. CRLs from the relevant certificate issuers are checked. Connection fails if the certificate is revoked.

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

Secure Receiver communication

To secure the communication between XenDesktop sites or XenApp server farms and Receiver, you can integrate your Receiver connections using security technologies such as the following:

- Citrix NetScaler Gateway or Access Gateway. For information, refer to topics in this section as well as the NetScaler Gateway, Access Gateway, and StoreFront documentation.

  Note: Citrix recommends using NetScaler Gateway to secure communications between StoreFront servers and user devices.
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using 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.
- For XenApp or Web Interface deployments only; not applicable to XenDesktop 7: A SOCKS proxy server or secure proxy server (also known as *security proxy server*, HTTPS proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Receiver and servers. Receiver supports SOCKS and secure proxy protocols.
- For XenApp or Web Interface deployments only; not applicable to XenDesktop 7: SSL Relay solutions with Transport Layer Security (TLS) protocols.

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 NetScaler Gateway

To enable remote users to connect through NetScaler Gateway, configure NetScaler Gateway to work with StoreFront.

- For StoreFront deployments: Allow connections from internal or remote users to StoreFront through NetScaler Gateway by integrating NetScaler Gateway and StoreFront. This deployment allows users to connect to StoreFront to access virtual desktops and applications. Users connect through Receiver.

For information about configuring these connections, refer to Integrating NetScaler Gateway with XenMobile App Edition and the other topics under that node in Citrix eDocs. Information about the settings required for Receiver for Windows are in the following topics:

- Configuring Session Policies and Profiles for XenMobile App Edition
- Creating the Session Profile for Receiver for XenMobile App Edition
- Configuring Custom Clientless Access Policies for Receiver

To enable remote users to connect through NetScaler Gateway to your Web Interface deployment, configure NetScaler Gateway to work with Web Interface, as described in Providing Access to Published Applications and Virtual Desktops Through the Web Interface and its sub-topics in Citrix eDocs.

Connect with Access Gateway Enterprise Edition

To enable remote users to connect through Access Gateway, configure Access Gateway to work with StoreFront and AppController (a component of CloudGateway).

- For StoreFront deployments: Allow connections from internal or remote users to StoreFront through Access Gateway by integrating Access Gateway and StoreFront. This deployment allows users to connect to StoreFront to access virtual desktops and applications. Users connect through Receiver.
- For AppController deployments: Allow connections from remote users to AppController by integrating Access Gateway and AppController. This deployment allows users to connect to AppController to obtain their web and Software as a Service (SaaS) apps and provides ShareFile Enterprise services to Receiver users. Users connect through either Receiver or the Access Gateway Plug-in.

For information about configuring these connections, refer to Integrating Access Gateway with CloudGateway and the other topics under that node in Citrix eDocs. Information about the settings required for Receiver for Windows are in the following topics:

- Configuring Session Policies and Profiles for CloudGateway
- Creating the Session Profile for Receiver for CloudGateway Enterprise
- Creating the Session Profile for Receiver for CloudGateway Express
- Configuring Custom Clientless Access Policies for Receiver

To enable remote users to connect through Access Gateway to your Web Interface deployment, configure Access Gateway to work with Web Interface, as described in Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface and its sub-topics in Citrix eDocs.

Connect 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*.

Connect 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.

Enforce 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 TLS) is directed to a trusted zone on the server.

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

To enable trusted server configuration

If you are changing this on a local computer, close all 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network Routing > Configure trusted server configuration.
8. From the Action menu, choose Properties and select Enabled.

Elevation level and wfcrun32.exe

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

Example 1:

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

Example 2:

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

Connect 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.

Connect with Secure Sockets Layer (SSL) Relay

This topic does not apply to XenDesktop 7.

You can integrate Receiver with the Secure Sockets Layer (SSL) Relay service. Receiver supports TLS protocols. Receiver for Windows 4.2 supports TLS 1.0 only.

- TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

Connect with Citrix SSL Relay

This topic does not apply to XenDesktop 7.

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

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

You can use Citrix SSL Relay to secure communications:

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

For information about configuring SSL Relay to secure your installation, refer to the XenApp documentation.

User device requirements

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

- The user device supports 128-bit encryption
- The user device has a root certificate installed that can verify the signature of the Certificate Authority on the server certificate
- 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. From the Action menu, choose Properties, select Enabled, and type a new port number in the Allowed SSL servers text box in the following format: *server:SSL relay port number* where *SSL relay port number* is the number of the listening port. You can use a wildcard to specify multiple servers. For example, *.Test.com:*SSL relay port number* matches all connections to Test.com through the specified port.

To apply a different listening port number to particular connections only

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

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

   Note: If you already added the 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.

7. From the Action menu, choose Properties, select Enabled, and type a comma-separated list of trusted servers and the new port number in the Allowed SSL servers text box in the following format: *servername:SSL relay port number*,*servername:SSL relay port number* where *SSL relay port number* is the number of the listening port. You can specify a comma-separated list of specific *trusted* SSL servers similar to this example:

   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444

   which translates into the following in an example appsrv.ini file: [Word]
   SSLProxyHost=csghq.Test.com:443

   [Excel]

   SSLProxyHost=csghq.Test.com:444

   [Notepad]

   SSLProxyHost=fred.Test.com:443

Configure and enable Receivers for TLS

This topic does not apply to XenDesktop 7.

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 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.

Install root certificates on user devices

To use TLS to secure communications between a 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 TLS for Receiver

1. To use 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.

7. From the Action menu, choose Properties, select Enabled, and from the drop-down menus, select the TLS settings.

   - Set TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Receiver connects using TLS encryption.
   - 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.

7. From the Action menu, choose Properties, select Enabled, and from the drop-down menus, select the correct settings.

   - Set TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Receiver tries to connect using TLS encryption.
   - Set SSL ciphersuite to Government.
   - Set CRL verification to Require CRLs for connection.

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

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

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

You can configure Receiver to use 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 Install root certificates on 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 TLS.
4. Click Update to apply the change.
5. Enable TLS in the user device browser. For more information, see the online Help for the browser.

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

This topic applies only to deployments with Web Interface using Administrative Templates.

The ICA File Signing feature helps protect users from unauthorized application or desktop launches. Citrix Receiver 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. In the Group Policy Editor, go to Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver and navigate to Enable ICA File Signing.
7. If you choose Enabled, you can add signing certificate thumbprints to the white list of trusted certificate thumbprints or remove signing certificate thumbprints from the

white list by clicking Show and using the Show Contents screen. You can copy and paste the signing certificate thumbprints from the signing certificate properties. Use the Policy drop-down menu to select Only allow signed launches (more secure) or Prompt user on unsigned launches (less secure).

Option	Description
Only allow signed launches (more secure)	Allows only properly signed application or desktop launches from a trusted server. The user sees a Security Warning message in 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.

Configure a Web browser and ICA file to enable single sign-on and manage secure connections to trusted servers

This topic applies only to deployments using Web Interface.

To use Single sign-on (SSO) and to manage secure connections to trusted servers, add the Citrix server's site address to the Local intranet or Trusted sites zones in Internet Explorer under Tools > Internet Options > Security on the user device. The address can include the wildcard (*) formats supported by the Internet Security Manager (ISM) or be as specific as *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

Launch SSO or use secure connections with a Web site

Add the exact address of the Web Interface site in the sites zone.

Example Web site addresses

https://my.company.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

XenDesktop connections with Desktop Viewer

Add the address in the form *desktop://Desktop Group Name*. If the desktop group name contains spaces, replace each space with -20.

Custom ICA entry formats

Use one of the following formats in the ICA file for the Citrix server site address. Use the same format to add it to the Local intranet or Trusted sites zones in Internet Explorer under Tools > Internet Options > Security on the user device:

Example of ICA file HttpBrowserAddress entry

HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080

Examples of ICA file XenApp server address entries

If the ICA file contains only the XenApp server **Address** field, use one of the following entry formats:

icas://10.20.30.40:1494

icas://my.xenapp-server.company.com

ica://10.20.30.40

To set client resource permissions

This topic applies only to deployments using Web Interface.

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

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

Note: Due to 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 Interface site to the trusted site list

1. From the Internet Explorer Tools menu, choose Internet Options > Security.
2. Select the Trusted sites icon and click the Sites button.
3. In the Add this website to the zone text field, type the URL to your Web Interface site and click Add.
4. Download the registry settings from http://support.citrix.com/article/CTX133565 and make any registry changes. Use SsonRegUpx86.reg for Win32 user devices and SsonRegUpx64.reg for Win64 user devices.
5. Log off and then log on to the user device.

To change client resource permissions in the registry

1. Download the registry settings from http://support.citrix.com/article/CTX133565 and import the settings on each user device. Use SsonRegUpx86.reg for Win32 user devices and SsonRegUpx64.reg for Win64 user devices.

2. In the registry editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust and in the appropriate regions, change the default value to the required access values for any of the following resources:

Resource key	Resource description
FileSecurityPermission	Client drives
MicrophoneAndWebcamSecurityPermission	Microphones and webcams
ScannerAndDigitalCameraSecurityPermission	USB and other devices

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

Receiver Desktop Lock

You can use the Receiver Desktop Lock when users do not need to interact with the local desktop. Users can still use the Desktop Viewer (if enabled), however it has only the required set of options on the toolbar: Ctrl+Alt+Del, Preferences, Devices, and Disconnect.

The Receiver Desktop Lock works on domain-joined machines, which are SSON-enabled (Single Sign-On) and store configured. It does not support PNA sites. Previous versions of Desktop Lock are not supported when you upgrade to Receiver for Windows 4.2.

You must install Citrix Receiver for Windows with the `/includeSSON` flag. You must configure the store and single sign-on, either using the adm file or cmdline option.

Then, install the Receiver Desktop Lock as an administrator using the CitrixReceiverDesktopLock.MSI available at citrix.com/downloads.

System requirements for Citrix Receiver Desktop Lock

- Supported on Windows 7 (including Embedded Edition), Windows 7 Thin PC, Windows 8, and Windows 8.1.
- Connects to StoreFront through native protocols only.
- Domain-joined end points only.
- User devices must be connected to a local area network (LAN) or wide area network (WAN).

Note: Windows XP (Embedded Edition) is not currently supported. See Known Issues. Support for Windows XP ended on April 8, 2014, when Microsoft ended extended support for Windows XP.

Local App Access

Caution: Enabling Local App Access may permit local desktop access, unless a full lock down has been applied with the Group Policy Object template, or a similar policy. See Configure Local App Access and URL redirection in XenApp and XenDesktop for more information.

Working with Receiver Desktop Lock

- You can use Receiver Desktop Lock with the following Receiver for Windows features:
  - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013 plug-in, and local app access
  - Domain, two-factor, or smart card authentication only
- Disconnecting the Receiver Desktop Lock session logs out the end device.
- Flash redirection is disabled on Windows 8 and later versions. Flash redirection is enabled on Windows 7.

- The Desktop Viewer is optimized for Receiver Desktop Lock with no Home, Restore, Maximize, and Display properties.
- Ctrl+Alt+Del is available on the Viewer toolbar.
- Most windows shortcut keys are passed to the remote session, with the exception of Windows+L. For details, see Passing Windows shortcut keys to the remote session.
- Ctrl+F1 triggers Ctrl+Alt+Del when you disable the connection or Desktop Viewer for desktop connections.

To install Receiver Desktop Lock

This procedure installs Receiver for Windows so that virtual desktops appear using Receiver Desktop Lock. For deployments that use smart cards, see To configure smart cards for use with devices running Receiver Desktop Lock.

1. Log on using a local administrator account.
2. At a command prompt, run the following command (located in the Citrix Receiver and Plug-ins > Windows > Receiver folder on the installation media).

   For Receiver for Windows 4.2:

   CitrixReceiver.exe
       /includeSSON
   STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"

   For command details, see the Receiver for Windows install documentation at Configure and install Receiver for Windows using command-line parameters.
3. In the same folder on the installation media, double-click CitrixReceiverDesktopLock.MSI . The Desktop Lock wizard opens. Follow the prompts.
4. When the installation completes, restart the user device. If you have permission to access a desktop and you log on as a domain user, the device appears using Receiver Desktop Lock.

To allow administration of the user device after installation, the account used to install CitrixReceiverDesktopLock.msi is excluded from the replacement shell. If that account is later deleted, you will not be able to log on and administer the device.

To run a **silent install** of Receiver Desktop Lock, use the following command line: `msiexec /i CitrixReceiverDesktopLock.msi /qn`

To configure Receiver Desktop Lock

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

Using Active Directory policies, prevent users from hibernating virtual desktops.

Use the same administrator account to configure Receiver Desktop Lock as you did to install it.

- Ensure that the icaclient.adm and icaclient_usb.adm files are loaded into Group Policy (where the policies appear in Computer Configuration or User Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components). The .adm files are located in %Program Files%\Citrix\ICA Client\Configuration\.
- USB preferences - When a user plugs in a USB device, that device is automatically remoted to the virtual desktop; no user interaction is required. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.
  - Enable the USB policy rule.
  - In Citrix Receiver > Remoting client devices > Generic USB Remoting, enable and configure the Existing USB Devices, 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).
- Drive mapping - In Citrix Receiver > Remoting client devices, enable and configure the Client drive mapping policy.
- Microphone - In Citrix Receiver > Remoting client devices, enable and configure the Client microphone policy.

To configure smart cards for use with devices running Receiver Desktop Lock

1. Configure StoreFront.
   a. Configure the XML Service to use DNS Address Resolution for Kerberos support.
   b. Configure StoreFront sites for HTTPS access, create a server certificate signed by your domain certificate authority, and add HTTPS binding to the default website.
   c. Ensure pass-through with smart card is enabled (enabled by default).
   d. Enable Kerberos.
   e. Enable Kerberos and Pass-through with smart card.
   f. Enable Anonymous access on the IIS Default Web Site and use Integrated Windows Authentication.
   g. Ensure the IIS Default Web Site does not require SSL and ignores client certificates.
2. Use the Group Policy Management Console to configure Local Computer Policies on the user device.
   a. Import the icaclient.adm template from %Program Files%\Citrix\ICA Client\Configuration\.
   b. Expand Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication.
   c. Enable Smart card authentication.
   d. Enable Local user name and password.
3. Configure the user device before installing Receiver Desktop Lock.
   a. Add the URL for the Delivery Controller to the Windows Internet Explorer Trusted Sites list.
   b. Add the URL for the first Delivery Group to the Internet Explorer Trusted Sites list in the form desktop://*delivery-group-name*.
   c. Enable Internet Explorer to use automatic logon for Trusted Sites.

When Receiver Desktop Lock is installed on the user device, a consistent smart card removal policy is enforced. For example, if the Windows smart card removal policy is set to Force logoff for the desktop, the user must log off from the user device as well, regardless of the Windows smart card removal policy set on it. This ensures that the user device is not left in an inconsistent state. This applies only to user devices with the Receiver Desktop Lock.

To remove Receiver Desktop Lock

Be sure to remove both of the components listed below.

1. Log on with the same local administrator account that was used to install and configure Receiver Desktop Lock.
2. From the Windows feature for removing or changing programs:
    - Remove Citrix Receiver Desktop Lock.
    - Remove Citrix Receiver.

Passing Windows shortcut keys to the remote session

Most windows shortcut keys are passed to the remote session. This section highlights some of the common ones.

Windows

- Win+D - Minimize all windows on the desktop.
- Alt+Tab - Change active window.
- Ctrl+Alt+Delete - via Ctrl+F1 and the Desktop Viewer
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+All Character keys

Windows 8

- Win+C - Open charms.
- Win+Q - Search charm.
- Win+H - Share charm.
- Win+K - Devices charm.
- Win+I - Settings charm.
- Win+Q - Search apps.
- Win+W - Search settings.
- Win+F - Search files.

Windows 8 apps

- Win+Z - Get to app options.
- Win+. - Snap app to the left.

- Win+Shift+. - Snap app to the right.
- Ctrl+Tab - Cycle through app history.
- Alt+F4 - Close an app.

Desktop

- Win+D - Open desktop.
- Win+, - Peek at desktop.
- Win+B - Back to desktop.

Other

- Win+U - Open Ease of Access Center.
- Ctrl+Esc - Start screen.
- Win+Enter - Open Windows Narrator.
- Win+X - Open system utility settings menu.
- Win+PrintScrn - Take a screen shot and save to pictures.
- Win+Tab - Open switch list.
- Win+T - Preview open windows in taskbar.