Citrix Receiver for Windows 4.1 and 4.0

Oct 21, 2015

About this Release

System Requirements

Install

Configure

Optimize

User experience

Connect to virtual desktops

Secure your connections

Configure smart card authentication

To enable certificate revocation list checking for improved security with Receiver

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

Configure domain pass-through authentication with Kerberos

Secure Receiver communication

Connect with NetScaler Gateway

Connect with Access Gateway Enterprise Edition

Connect with Secure Gateway

Connect through a firewall

Enforce trust relations

Elevation level and wfcrun32.exe

Connect Receiver through a proxy server

Connect with Secure Sockets Layer Relay

Configure and enable Receivers for SSL and TLS

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

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

To set client resource permissions

About this release

Oct 21, 2015

Citrix Receiver for Windows provides users with secure, self-service access to virtual desktops and apps provided by XenDesktop and XenApp. Receiver also provides on-demand access to Windows, Web, and Software as a Service (SaaS) apps. Users can access apps through stores managed by Citrix StoreFront or legacy web pages managed by Web Interface.

What's new

Receiver for Windows 4.1.200 contains fixes associated with the use of the Microsoft Lync 2013 VDI Plug-in for Windows, along with fixes included in Receiver for Windows 4.0, 4.0.1, 4.1, 4.1.2, and 4.1.100. Receiver for Windows also contains new fixes in HDX MediaStream, printing, server farm administration, session connection, system exceptions, and user experience. See CTX138197 for details on all these fixed issues.

Citrix Receiver for Windows 4.1 adds support for Windows 8.1 and Windows Server 2012 R2 and includes bug fixes, described in Citrix Receiver 4.x - Issues Fixed in This Release.

Citrix Receiver for Windows 4.0 provides the following new features and enhancements.

- **Support for XenDesktop 7 features –** Receiver supports the many enhancements provided by XenDesktop 7, including Windows Media client-side content fetching, multicast support, client folder redirection, Local App Access, and support for IPv6 connections.
- **Support for StoreFront 2.0 features –** Receiver supports the many enhancements provided by StoreFront 2.0, including smart card authentication and support for IPv6 connections.
- **Integrated Smart card authentication –** Receiver now provides integrated smart card authentication for StoreFront connections, including support for:
  - Pass-through authentication (single sign-on). Users of domain-joined devices enter their smart card credentials to log on to Receiver. They can then start virtual desktops and apps without needing to re-enter credentials.
  - Bimodal authentication. Users can log on with a smart card or enter their user name and password. This enables a user to log on even if a certificate has expired or the user does not have the smart card.
  - Multiple certificates. When users insert a smart card into a card reader, Receiver chooses the certificates needed and can use multiple certificates from one or more cards.
  - Double hop sessions. Users can start a virtual desktop and then use Receiver on that virtual desktop to start an application from a different delivery group.
  - Smart card-enabled apps. Users can digitally sign or encrypt documents in a virtual desktop or app session.

  For more information, refer to Configure smart card authentication. For information about system requirements, planning smart card deployments, and an overview to the configuration required for all related Citrix components, refer to the latest XenDesktop and StoreFront documentation.

- **User experience improvements –**
  - Receiver now displays a notification when installation of an update completes.
  - When the session reliability policy is in effect, Receiver dims apps when the connection to the server is lost.
- **H.264 decoding –** When used XenDesktop 7, Receiver provides improved performance of rich and professional graphics apps on WAN networks.
- **Support for HDX Insight –** HDX Insight is the integration of EdgeSight network analysis and EdgeSight performance management with Director. With this support now in Receiver, XenDesktop administrators can check performance metrics related to the health of this component. No configuration of this feature is required.

- **COM port and LPT port mapping change –** In XenDesktop 7 deployments, COM port and LPT port mapping are disabled by default. Use the port redirection policies to enable mapping.

Fixed issues in 4.1

Fixed issues in 4.0

Citrix Receiver for Windows 4.1, 4.0 Fixed Issues

Oct 21, 2015

Receiver for Windows 4.1.200

Compared to: Citrix Receiver for Windows 4.1.100

Receiver for Windows 4.1.200 contains all fixes that were included in Receiver for Windows 4.0, 4.0.1, 4.1, and 4.1.2, 4.1.100, plus the following, new fixes:

HDX MediaStream Flash Redirection

- Browsing certain Web sites with HDX MediaStream Flash Redirection enabled can cause Internet Explorer to become unresponsive.

  To enable this fix, you must also install VDA/HDX Mediastream for Flash Fix #LA4151 and set the following registry key on the VDA/XenApp server:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: SupportedUrlHeads
  Type: REG_MULTI_SZ
  Data: <*each value on a separate line, null separated*>
  http://
  https://
  file://

  [From RcvrForWin4.1_14.1.200][#LA5255]

- Disabling Flash intelligent fallback in a session can cause Internet Explorer to become unresponsive.

  [From RcvrForWin4.1_14.1.200][#LA5404]

Printing

- The Citrix Printer Driver (UPD) does not print barcode fonts. The font appears as blank spaces or random characters when printing documents with the Citrix Printer Driver (cpviewer.exe) or a barcode printer.

  [From RcvrForWin4.1_14.1.200][#LC0141]

Server/Farm Administration

- If the "File redirection bandwidth limit" and "Overall session bandwidth limit" policies are set, the session might exit

unexpectedly.

In order to address the issue, you must install both a server and a receiver update that contains Fix #LA5925, and then set the following registry key on the server:

- Create the following registry key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  Name: DisableHighThroughput
  Type: DWORD
  Value: 1
- Change the following registry key::
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  Name: MaxNetCommands
  Type: DWORD
  Value: Set to a smaller value

[From RcvrForWin4.1_14.1.200][#LA5925]

Session/Connection

- If the network connection to a VDA is disconnected and then reconnected, clicking with the mouse fails.

  [From RcvrForWin4.1_14.1.200][#LA5743]

- COM port redirection can fail with the following error message:

  "Error in OpenPort: Comport 'COM4'"

  [From RcvrForWin4.1_14.1.200][#LC0434]

- When an endpoint connected to a VDA resumes from the sleep state, the mouse and the keyboard no longer work in the VDA session.

  [From RcvrForWin4.1_14.1.200][#LC0085]

- The windows session running in the foreground might unexpectedly lose the foreground focus.

  [From RcvrForWin4.1_14.1.200][#LA5489]

System Exceptions

- Playing a video in a media player in a pass-through session can cause the session to exit unexpectedly.

  [From RcvrForWin4.1_14.1.200][#LC0553]

User Experience

- Full-screen seamless applications do not move smoothly, can be jittery and show the desktop background on the borders when moved around.

  [From RcvrForWin4.1_14.1.200][#LC0696]

- On wireless networks, the session window can temporarily turn a solid gray.

  [From RcvrForWin4.1_14.1.200][#LC0530]

- In user session governed by a policy that sets the session sound quality to **High sound quality; lowest performance** (**Advanced Configuration** > **Properties** > **Client devices** > **Resources** > **Audio** > **Sound quality** > **High sound quality; lowest performance**), no sound is audible.

  [From RcvrForWin4.1_14.1.200][#LC0329]

- When looping a multimedia file in an RDS desktop session, the audio and video streams stop after the file is looping for an hour or longer.

  [From RcvrForWin4.1_14.1.200][#LC0641]

- Session pre-launch works only the first time Receiver for Windows is launched, not once it has been configured.

  [From RcvrForWin4.1_14.1.200][#LC0701]

Receiver for Windows 4.1.100

Compared to: Citrix Receiver for Windows 4.1

Receiver for Windows 4.1.100 contains all fixes that were included in Receiver for Windows 4.0, 4.0.1, 4.1, and 4.1.2, plus the following, new fixes:

HDX 3D Pro

- After a few hours of usage, the wfica32.exe process can consume 100% of the CPU when using HDX 3D Pro with the H264 codec and text tracking disabled.

  [From RcvrForWin4.1_14.1.100][#LA5554]

HDX MediaStream

- Attempts to view streaming videos by using a published web browser, such as Internet Explorer, might not work due to a failure in HDX MediaStream Flash Redirection.

  To enable the fix, set the following registry keys:

- *On 32-bit Windows*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  Name: FallbackIfFlashNotExist
  Type: REG_DWORD
  Data: 0
- *On 64-bit Windows*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  Name: FallbackIfFlashNotExist
  Type: REG_DWORD
  Data: 0

[From RcvrForWin4.1_14.1.100][#LA5278]

- With HDX Mediastream for Flash Version 1.0 (First Generation Flash Redirection) enabled, Microsoft Internet Explorer might exit unexpectedly while Adobe Flash Player 11.8 or later is installed.

  [From RcvrForWin4.1_14.1.100][#LA5421]

HDX Plug and Play

- after installing Receiver for Windows 4.0 on Windows XP SP3, USB ports on the docking station can no longer be redirected.

  [From RcvrForWin4.1_14.1.100][#LA4582]

HDX RealTime

- HDX RealTime Webcam Video Compression redirection might fail to support Quarter Video Graphics Array (QVGA) display resolution (320x240) and can cause the wfica32.exe process to exit unexpectedly.

  [From RcvrForWin4.1_14.1.100][#LA5232]

Installing, Uninstalling, Upgrading

- When upgrading to a newer version of Receiver for Windows without being connected to the Internet, the previous version is not completely uninstalled and the installation of the newer version fails.

  [From RcvrForWin4.1_14.1.100][#LA4896]

Printing

- This fix addresses an issue where duplex printing fails when the Universal Printer driver is configured and has to be done manually instead.

  [From RcvrForWin4.1_14.1.100][#261552]

- Attempts to print an HTML document using Internet Explorer 9 can result in garbled output in the Citrix Print Viewer (cpviewer.exe) and the printout for certain type of fonts.

  [From RcvrForWin4.1_14.1.100][#LA3962]

Server/Farm Administration

- If the StoreFront is configured with an unauthenticated store, Account Discovery might fail when using Receiver for

Windows.

[From RcvrForWin4.1_14.1.100][#LC0004]

- This feature enhancement supports auto creation of shortcuts for preferred applications by using a prefer template directory. For these applications, in addition to the existing prefer rules, the Self Service Plug-in searches for the shortcuts in the prefer template directory. If it matches the prefer rules, it copies shortcut to the user's start menu.

  By default, this directory is one of the following:

  - %systemdrive%:\Program Files\Citrix\shortcuts
  - %systemdrive%:\Program Files (x86)\Citrix\shortcuts for per user device installation and
  - %systemdrive%:\Users\<user name>\AppData\Local\Citrix\SelfService\shortcuts for per user installation.

  The default prefer template directory location can be specified in the registry.

  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle or HKEY_CURRENT_USER\Software\Citrix\Dazzle
  Name: PreferTemplateDirectory
  Type: REG_SZ
  Data: any path (for example, "%systemroot%:\Shortcuts")

  If the application is subsequently unsubscribed or removed from the store, the shortcut that was copied from the preferred directory is deleted.

  [From RcvrForWin4.1_14.1.100][#LC0005]

Session/Connection

- When using Citrix Receiver within a virtual desktop session, attempts to launch XenApp published applications fail and the following error message appears:

  "This version of Citrix Receiver does not support selected encryption. Please contact your administrator. [Error 1029: Invalid DLL load]."

  [From RcvrForWin4.1_14.1.100][#LA4743]

- With Receiver for Windows 13.4 Cumulative Update 2, when seamless application has focus, the input language on the language bar changes when pressing Alt + Tab to switch active windows.

  [From RcvrForWin4.1_14.1.100][#LA4963]

- With the "Group similar taskbar buttons" option selected on Taskbar and Start Menu Properties on a Windows XP system, launching applications might be slow.

  [From RcvrForWin4.1_14.1.100][#LA4191]

- After upgrading from Version 12.2 of the Citrix online plug-in to Version 3.x of Citrix Receiver for Windows, proxy connections to external Web sites might fail to launch with NTLM proxy authentication enabled.

  [From RcvrForWin4.1_14.1.100][#LA3781]

- If the user device does not have a connected webcam, attempts to start a published instance of Microsoft Lync 2010 might result in the application connecting and disconnecting several times before establishing a final connection and starting the application. This can occur if you install an application that installs a webcam when no other webcams are

installed, such as the Motorola Bluetooth package.

[From RcvrForWin4.1_14.1.100][#LA4867]

- When starting a published application or a desktop, Kerberos authentication might not work when using pass-through authentication on an IPv4 network. This release fixes the issue for IPv4 networks only.

  [From RcvrForWin4.1_14.1.100][#LA5026]

- This fix addresses audio/video issues related to the Microsoft Lync 2013 VDI Plug-in for Windows. It improves the user experience for Lync users. For more information, see Knowledge Center article CTX138408.

  [From RcvrForWin4.1_14.1.100][#LA5314]

- If the CANcaseXL USB network adapter is redirected into a virtual desktop, it appears to malfunction in Windows Device Manager. This USB device does not support the Citrix USB redirection driver. The VDA requires installation of Fix #LA5022 in order to work properly.

  [From RcvrForWin4.1_14.1.100][#LA5022]

- This fix reworks Fix #LA1257, which fails to fully address the following issue:

  With the Desktop Viewer disabled, a full-screen client session does not adjust the screen resolution of the Virtual Desktop Agent in response to a change in screen resolution on the endpoint.

  [From RcvrForWin4.1_14.1.100][#LA4000]

- When connectivity to a XenDesktop session is lost for an amount of time that exceeds the Session Reliability timeout, DesktopViewer remains onscreen indefinitely. The session itself disappears, as expected, from the Connection Center after the Session Reliability timeout.

  [From RcvrForWin4.1_14.1.100][#LA4856]

System Exceptions

- The wfica32.exe process can exit unexpectedly and the following error message appears:

  "Citrix HDX Engine has encountered a problem and needs to close."

  [From RcvrForWin4.1_14.1.100][#LA3964]

- The wfica32.exe process can exit unexpectedly and the following error message appears:

  "Citrix HDX Engine has encountered a problem and needs to close."

  [From RcvrForWin4.1_14.1.100][#LA4695]

- The wfica32.exe process might exit unexpectedly when starting a pass-through session from the XenApp 6.5 desktop to a XenApp 4.5 published application.

  [From RcvrForWin4.1_14.1.100][#LA5193]

- If the Multi-Stream policy is enabled, applications can become unresponsive when accessing the COM port.

  [From RcvrForWin4.1_14.1.100][#LA5543]

- In double-hop scenarios, launching Microsoft Outlook or Communicator can cause Receiver for Windows to exit unexpectedly.

  [From RcvrForWin4.1_14.1.100][#LA4813]

User Experience

- When connecting or reconnecting to a session hosted on XenApp for Unix, no screen updates occur for 90 seconds.

  [From RcvrForWin4.1_14.1.100][#LA5244]

User Interface

- A change introduced in Version 12.1 of the online plug-in introduced a delay in the appearance of the connection progress bar for seamless connections. However, for sessions connecting to slower servers, this behavior is not always desirable. This enhancement introduces support for the following registry key that allows you to configure the duration of the delay:

  On 32-bit Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: NotificationDelay
  Type: REG_DWORD
  Data: <*Delay, in milliseconds*>

  On 64-bit Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Name: NotificationDelay
  Type: REG_DWORD
  Data: <*Delay, in milliseconds*>

  [From RcvrForWin4.1_14.1.100][#LA0678]

- After changing the desktop color scheme from the default color blue to other colors, such as Olive Green or Silver (**Desktop** > **Properties** > **Appearance tab** > **Color scheme**), the text and the background color of Self-service Plug-in become identical, making it impossible to read menu items.

  [From RcvrForWin4.1_14.1.100][#LA5121]

Miscellaneous

- When using email-based discovery, if the SRV record created on the DNS side includes a port other than 443, the Receiver ignores the port specified in the SRV record and continues to connect to the Access/NetScaler Gateway URL using port 443.

  [From RcvrForWin4.1_14.1.100][#LA4491]

Receiver for Windows 4.1.2

Compared to: Citrix Receiver for Windows 4.1

Receiver for Windows 4.1.2 contains all fixes that were included in Receiver for Windows 4.0, 4.0.1, and 4.1, plus the

following, new fixes:

Microsoft Lync 2013 VDI Plug-in	Installing, Uninstalling, Upgrading

Microsoft Lync 2013 VDI Plug-in

- Video does not appear after you move the Lync conversation window to a second monitor.

  [#LA5314, #399447]

- When you move a Whiteboard presentation window to another user, the other user's video does not display in your conversation window.

  [#LA5314, #399465]

- Receiver can exit unexpectedly in multi-party video calls or when a video conference ends.

  [#LA5314, #426035]

- On some client devices, video is intermittently unavailable in video calls in full-screen VDA mode.

  [#LA5314, #418675]

- Video distortion can occur if you move a video conference window.

  [#LA5314, #419898]

Installing, Uninstalling, Upgrading

- When upgrading to a newer version of Receiver for Windows without being connected to the Internet, the previous version is not completely uninstalled and the installation of the newer version fails.

  [#LA4896]

Receiver for Windows 4.1

Compared to: Citrix Receiver for Windows 4.0.1

Receiver for Windows 4.1 contains all fixes that were included in Receiver for Windows 4.0 and 4.0.1, plus the following, new fixes:

HDX MediaStream Flash Redirection	Printing
HDX MediaStream Windows Media Redirection	Session/Connection
HDX Plug and Play	System Exceptions
Installing, Uninstalling, Upgrading	User Experience
Keyboard	User Interface

Local App Access | Miscellaneous

Logon/Authentication

HDX MediaStream Flash Redirection

- When playing several multimedia files in rapid succession on http://www.youtube.com/ with HDX MediaStream Flash Redirection enabled, the PseudoContainer2.exe process might exit unexpectedly.

  [#LA3846

HDX MediaStream Windows Media Redirection

- In Version 3.4 of Receiver for Windows with HDX MediaStream Windows Media Redirection enabled, a delay of up to ten seconds can be observed before a multimedia file starts to stream.

  [#LA4141]

HDX Plug and Play

- Clicking Devices within the Desktop Viewer to select a USB device to be remoted using HDX Plug-n-Play USB Device Redirection can cause the Desktop Viewer to become unresponsive.

  [#LA3348]

Installing, Uninstalling, Upgrading

- Attempts by non-administrative users to upgrade the Receiver for Windows might result in the partial installation of the receiver if the receiver was installed by an administrator.

  With this fix, a non-administrative user attempting to upgrade a receiver installed by an administrator receives an error message and the installation process is terminated.

  [#LA3425]

Keyboard

- When using version 3.3. of the Receiver for Windows, pressing the Alt key can cause the key to remain in a down state. As a result, pressing the "E" key subsequently can invoke Windows Explorer.

  [#LA3288]

- When clicking the Desktop Viewer toolbar with the Windows key pressed in full-screen mode, the key might remain in a down state. As a result, pressing the "E" key subsequently invokes Windows Explorer.

  [#LA3349]

- This fix addresses an issue that can cause the state of the Caps Lock, Num Lock, and/or Scroll Lock keys to be out of sync in an ICA session. This fix introduces a new parameter that allows you to force the synchronization of the keyboard LED state between the client and the server. To enable this option, add the entry "KeyboardForceLEDUpdate = On" to

the [WFClient] section of the appsrv.ini file in the local user profile location or of the default.ica file in the corresponding Web Interface site.

[#LA3682]

- This fix addresses an LED synchronization issue that can cause the state of the Caps Lock, Num Lock, and/or Scroll Lock keys to be out of sync between the client and server.

  [#LA4293]

Local App Access

- With Local App Access enabled, clicking the Desktop Viewer causes the client local taskbar to appear needlessly.

  [#LA3049]

Logon/Authentication

- Pass-through authentication might fail to work after installing XenDesktop 7 VDA on Windows Server 2008 R2. The issue occurs because the ssonsvr.exe process fails to start.

  [#LA4685]

Printing

- When sending multiple Adobe Acrobat print jobs to a session printer, random pages or entire print jobs can be lost.

  [#LA3643]

- Session printer enumeration can take an excessive amount of time.

  [#LA3951]

Session/Connection

- When a client device is in the sleep or hibernation state for an extended period of time with an active XenDesktop session running, upon resuming, the session might fail to reconnect as expected and become stuck in a reconnection phase requiring the session window to be manually closed.

  This fix addresses the issue so that upon resuming the client device, the session window closes as expected when reconnection fails.

  [#LA2748]

- When launching a published application in seamless mode, the progress bar window remains in the background.

  To enable the fix, set the following registry keys on the client-side:

  - *For Windows 32-bit systems:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Name: ForegroundProgressBar
    Type: DWORD
    Data: 1
  - *For Windows 64-bit systems:*

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
Name: ForegroundProgressBar
Type: DWORD
Data: 1

[#LA3491]

- Receiver with Desktop Lock presents a gray screen each time there is a hardware failure or if the VM is forcefully shut down from the hypervisor.

  [#LA3499]

- With Taskbar Grouping enabled on the client device, TaskbarGrpXpVista.dll - within wfica32.exe - unnecessarily queries the client device for information about published applications running in the session. For example, when running a published instance of cmd.exe, TaskbarGrpXpVista.dll queries C:\windows\system32\cmd.exe for information about the executable. In scenarios where the published application is running from the remote share, this can cause undesirable bandwidth consumption.

  [#LA3661]

- With a GPO setting in place to prevent taskbar grouping, clicking taskbar icons on Windows XP and Vista client devices fails to switch focus to the associated windows.

  [#LA3889]

- The Receiver can become unresponsive when you click the Devices button of the Desktop Viewer toolbar while the "Citrix Receiver – Device Access" dialog box is displayed. This dialog box appears if the device access preference is configured to "Ask me each time" instead of the default "Do nothing."

  [#LA3899]

- The Desktop Viewer (CDViewer.exe) and wfica32.exe processes might exit unexpectedly while reconnecting to a virtual desktop session.

  [#LA3944]

- With this fix, the IsReconnectInProgress() API is integrated to Citrix Fast Connect 2.0. The feature determines whether the reconnect process is in progress or not while the Auto Client Reconnect feature is enabled.

  [#LA4080]

- This fix allows pass-through applications to be reconnected and enables Workspace Control for pass-through applications.

  To enable the fix, you must set the following registry keys:

  To enable Workspace Control in pass-through mode:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PNAgent
  Name: ForceEnableWSC
  Type: DWORD
  Data = 1

To enable pass-through applications to be reconnected:

HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
Name: BypassPassThruMode
Type: DWORD
Data = 1

Note: This fix works only under the following conditions:

- The two or more connection hops cannot occur within the same XenApp Services site or farm. In other words, the endpoint Receiver can connect to a XenDesktop VDA published on XenApp Services Site A, and then the pass-through client on that VDA can connect to a published application or desktop on a *different* XenApp Services site, Site B.
- The second connection hop must be to a XenApp terminal session; it cannot be to a XenDesktop VDA.

[#LA4206]

- When using remote assistance software in a desktop that is published to be an odd (non-even) percentage of the client screen (for example, 95%), the remote assistance session might appear to be distorted.

  [#LA4313]

- This compatibility enhancement extends support for HDX Plug and Play USB device redirection to additional USB devices.

  [#LA4335]

- A deadlock in wfcrun32.exe can prevent new sessions from launching successfully.

  [#LA4344]

- Attempts to connect to XenApp servers using the Citrix Quick Launch tool or static ICA files that specify "HTTPBrowserAddress=ServerName_Or_IP:Port" (for example: "HTTPBrowserAddress=192.168.1.10:8080") can fail.

  [#LA4585]

System Exceptions

- The wfica32.exe process can exit unexpectedly and the following error message appears:

  "Citrix HDX Engine has encountered a problem and needs to close."

  [#LA3412]

- The wfica32.exe process might experience an access violation and exit unexpectedly.

  [#LA3639]

- The wfica32.exe process might exit unexpectedly.

  [#LA4208]

User Experience

- This fix eliminates the unnecessary appearance of logon prompts when Receiver 4.0 is used with StoreFront.

[#LA4652]

User Interface

- Application launches fail if there is a mismatch between the application name and the display name of the published application.

  [#LA3891]

Miscellaneous

- This release includes the latest version of the SSLSDK - Version 12.1.13.

  [#LA3804]

- This fix improves the functionality of the TerminateUser function of Receiver for Windows in some deployments.

  [#LA3881]

Receiver for Windows 4.0.1

Compared to: Citrix Receiver for Windows 4.0

Receiver for Windows 4.0.1 contains all fixes that were included in Receiver for Windows 4.0, plus the following, new fixes:

- This fix eliminates the unnecessary appearance of logon prompts when Receiver 4.0 is used with StoreFront.

  [#LA4652]

Receiver for Windows 4.0

Compared to: Citrix Receiver for Windows 3.4

Receiver for Windows 4.0 contains the following fixes compared to Citrix Receiver for Windows 3.4:

HDX MediaStream Flash Redirection

- Moving a video window offscreen in whole or in part while a video file is rendering can leave a dark area on the screen.

The dark area remains even after moving the video window back.

[#LA0599]

- **Important**: Before applying this fix on a client device, see Knowledge Center article CTX126817 for important information about how the Dynamic Blacklist feature might affect client-side Flash redirection.

  In scenarios where the *Enable server-side content fetching* policy is enabled on the server and the *Flash server-side content fetching URL list* setting is configured for the Flash Redirection policy on the client, attempts to play Flash content fail if the URL to the content contains multibyte/unicode characters such as those common in Asian languages

  To enable this fix in its entirety, you must install both a client hotfix that contains Fix #LA1621 and:

  - *For XenApp*: an HDX Flash hotfix that contains Fix #LA1621
  - *For XenDesktop*: a Virtual Desktop Agent hotfix that contains Fix #LA1621

  Note: This fix also requires the corresponding language code pages to be installed on both the client and the server. The code pages are installed by default by the Windows operating system. For example, the Japanese distribution of Windows 7 installs the Japanese code pages by default. However, if you are using a URL with Japanese characters on an English distribution of Windows 7, the Japanese code pages must be installed explicitly. This applies to both the client and the server because the URLs are transferred from the client to the server when server-side content fetching is enabled.

  [#LA1621]

- Certain user interactions with Flash content, such as clicking buttons, can cause Pseudocontainer2.exe to exit unexpectedly.

  [#LA1948]

- Client-side content redirection can fail for certain types of Flash content and revert to server-side rendering, including cases where:

  1. Flash content tries to download another Flash file that does not exist or cannot be located
  2. Flash content created by Adobe Captive fails some logic checks of the client-side content redirection feature
  3. Flash content causes the client-side content redirection feature to remote unsupported interfaces to the server
  4. The client attempts to fetch Flash content even if its URL is configured in the ServerContentFetching URL blacklist

  To enable this fix, you must install both an HDX Flash and a Receiver for Windows hotfix that contains Fix #LA2198. To enable this fix for issue #1 above, you must also set the following registry key on the client:

  - *On 32-bit Windows:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Type: REG_DWORD
    Data: 0
  - *On 64-bit Windows:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Type: REG_DWORD
    Data: 0

  [#LA2198]

- When switching the focus from the Flash window (- a child window of a Web browser running seamless window) to a local window and switching the focus back to the address bar of the seamless browser window, attempts to type in the browser's address bar can fail.

  [#LA2685]

- Important: Before applying this fix on a client device, see Knowledge Center article CTX126817 for important information about how the Dynamic Blacklist feature might affect client-side Flash redirection.

  The HDX MediaStream Flash Redirection feature might fail to work on Dailymotion videos (http://www.dailymotion.com) with an error. The issue occurs when the client and server are located in different geographical locations.

  To enable this fix, you must create the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client
  Name: DisableRegionFiltering
  Type: REG_DWORD
  Data: 1

  [#LA3134]

HDX Plug and Play

- This feature enhancement modifies the default USB Redirection behavior as follows:
  - When the Desktop Viewer is enabled, users can manually redirect USB devices.
  - When the Desktop Viewer is not enabled, USB devices are automatically redirected.

  [#LA0108]

- After failed attempts to map certain USB devices into a virtual desktop session, the devices disappear from the Device Manager until you restart the endpoint.

  [#LA0954]

- Clicking Devices within the Desktop Viewer to select a USB device to be remoted using HDX Plug-n-Play USB Device Redirection can cause the Desktop Viewer to become unresponsive.

  [#LA3348]

Installing, Uninstalling, Upgrading

- After upgrading to Receiver 3.*x*, users cannot launch published applications and the following error message appears:

  "This version of Citrix Receiver does not support selected encryption. Please contact your administrator. Error 1046: The Virtual Driver is not loaded."

  [#LA3120]

Keyboard

- Minimizing a virtual desktop session by clicking Home on the Desktop Viewer can intermittently cause the Tab key to stop working on the endpoint until the session is disconnected.

[#LA2925]

- As of Version 3.0 of the Receiver for Windows, the KeyboardTimer setting value set at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\LockdownProfiles\All Regions\Lockdown\Virtual Channels\Keyboard no longer works. This fix reinstates the functionality.

  [#LA2949]

- This fix addresses an issue that can cause the state of the Caps Lock, Num Lock, and/or Scroll Lock keys to be out of sync between the client and the server in pass-through sessions running in the foreground.

  [#LA3288]

- This fix addresses an issue that can cause the state of the Caps Lock, Num Lock, and/or Scroll Lock keys to be out of sync between the client and the server in pass-through sessions running in the background.

  [#LA3310]

Printing

- Clicking **Local Printer Settings** on the **Client Settings** tab a a UPD printer's **Properties** sheet and then closing the settings dialog box can cause the **Properties** sheet to become unresponsive.

  [#259485]

Seamless Windows

- When using the Connection Center or the Web Interface to log off from a seamless session with unsaved data, a black window appears with the following message:

  "Programs still need to close" - with the two options - "Force Logoff" or "Cancel." The "Cancel" option does not work.

  After installing this fix, the Cancel option works as designed. After utilizing the Cancel button, Citrix recommends that you save your data and then log out of the session to prevent further performance delays.

  [#LA0318]

Session/Connection

- After disconnecting and reconnecting to a virtual desktop session, attempts to record audio from within the session can fail. To enable this fix in its entirety, you must install both a server and a client hotfix that contains Fix #LA0821.

  [#LA0821]

- The time required for file transfers in a client session can be slower than in an RDP session.

  To enable this fix in its entirety, you must install both a server and a client hotfix that contains Fix #LA1263.

  [#LA1263]

- Under certain conditions, changing the resolution of a virtual desktop session before the session disconnects unexpectedly, such as due to a network outage, can cause the session resolution to be different than expected after you reconnect.

[#LA1377]

- Serial port barcode scanners cannot process labels the label's data size exceeds 512 bytes. To enable this fix, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: CommBufferSize
  Type: REG_DWORD
  Data: Range of 512 (minimum) and 2048 (maximum value)

  [#LA1695]

- Disabling the Network List Service and/or the Network Location Awareness service as described in Knowledge Center article CTX131577 causes Version 12.3 of the online plug-in to lose connectivity.

  [#LA2024]

- Attempts to launch a seamless application published to a UNC path over a low bandwidth connection can take more than two minutes to complete.

  [#LA2170]

- Invoking the input method of a seamless session by clicking Ctrl + Shift can change the client-side local input method as well. To prevent this issue, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: Showlocallanguagebar
  Type: REG_DWORD
  Data: 1 *<to show the local language bar>*; 0 *<to hide the local language bar>*

  [#LA2180]

- When Auto Client Redirection is enabled, after choosing Hibernate, reconnection attempts might fail when the client is automatically closed.

  With this fix, the system can be suspended or sent into Hibernation mode with the USB device redirection, and can be auto-reconnected after the system returns from Standby mode.

  [#LA3061]

- Published applications might fail to launch if ICA compression is set to "OFF" for Citrix Receiver for Windows 3.x at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP Compress=Off.

  [#LA3072]

- In a multi-monitor environment, the Desktop Viewer toolbar might no longer be visible while switching the display to a secondary monitor in full-screen mode.

  [#LA3083]

- In dual-monitor configurations connected to a Virtual Desktop Agent and where the primary monitor is a laptop, turning the laptop display off and back on causes the session to subsequently display only on the primary monitor.

[#LA3202]

- When using Version 3.3 of the Cumulative Update 1 or Version 3.4 of the Receiver for Windows on a Windows XP workstation running Internet Explorer 8, the initial application might fail to launch from the Web Interface.

  [#LA3234]

- Both console and XenDesktop sessions can become unresponsive (Stuck on "Welcome" screen) when attempting to reconnect to a disconnected virtual desktop session using the Receiver for Linux. The issue occurs when the WDDM driver is enabled on the Virtual Desktop Agent and another virtual desktop session is running within the session.

  [#LA3241]

- Version 3.4 of the Receiver for Windows might fail to start if the client's "Regional and Language Options" for Windows 7 is set to "Kazakh (Kazakhstan)."

  [#LA3517]

System Exceptions

- The wfica32.exe process can exit unexpectedly in environments where EdgeSight for Load testing is deployed.

  [#LA0289]

- The wfcrun.exe process can exit unexpectedly in environments where HP LoadRunner is deployed.

  [#LA0859]

- With the audio policy set to high definition sound, the wfica32.exe process can exit unexpectedly when playing random sample sound files in the Sound control panel of a published desktop.

  [#LA1000]

- Version 12.3 of the online plug-in might exit unexpectedly while disconnecting a session from a Web Interface site with a Microsoft Excel 2007 spreadsheet open.

  [#LA2274]

- With Local App Access enabled, connection attempts to a Virtual Desktop Agent can fail if a legal notice is configured for the Virtual Desktop Agent.

  [#LA2351]

- The Pnamain.exe process can exit unexpectedly when reconnecting to a session.

  [#LA2704]

- Sessions running on single-monitor, aero-enabled Windows client devices can disconnect unexpectedly. The issue can occur when a preview, as part of the Dynamic Window Preview feature, is sent to the client; at that time, a twi3.dll thread can terminate the Winlogon.exe process, which in turn causes the session to disconnect.

  To resolve this issue in its entirety, you must install both a XenApp and a Receiver hotfix that contains Fix #LA2858.

  [#LA2858]

- The wfica32.exe process might exit unexpectedly. The issue occurs due to an invalid memory dereference.

  [#LA2860]

- While printing in certain double-hop scenarios, the following error message appears and the Wfica32.exe process exits unexpectedly: "Citrix HDX Engine was stopped working." The issue is caused by port names that exceed 260 characters in length.

  To address this issue, you must install both a server and a Receiver hotfix that contains Fix #LA3009 (XA650R01W2K8R2X64056; RcvrForWin3.3_13.3.104, or their replacement hotfixes).

  [#LA3009]

- Citrix Receiver can spawn multiple instances of the selfserviceplugin.exe process, causing the system to run out of memory.

  [#LA3460]

- The Desktop Viewer might exit unexpectedly during logoff.

  [#LA3567]

- PNMain.exe can exit unexpectedly when using the online plug-in as the pass-through client.

  [#LA0785]

User Experience

- When using USB redirection, a USB SpaceMouse device might disappear from a virtual desktop session after a few hours of use.

  [#LA2256]

- This feature enhancement for Version 3.4 of the Receiver for Windows allows you to suppress the following authentication message for VPN logins that appears when the user switches between network connections.

  To suppress the message, create the following registry key:

  - *On 32-bit Windows*:
    HKEY_CURRENT_USER\Software\Citrix\Receiver
    Name: AutoSecureConnection
    Type: REG_DWORD
    Value: 0 (disables the VPN prompt)
  - *On 64-bit Windows*:
    HKEY_CURRENT_USER\Software\Wow6432Node\Citrix\Receiver
    Name: AutoSecureConnection
    Type: REG_DWORD
    Value: 0 (disables the VPN prompt)

  [#LA3772]

User Interface

- This fix modifies the Korean translation of the "Home Desktop" icon title on the Desktop Viewer toolbar to be more

specific.

[#232198]

- When clicking **Cancel** in the authentication dialog box that appears when running a desktop group shortcut on an endpoint, the following, inaccurate and misleading error message appears:

  "The application or desktop could not be launched. Check your network connection.

  [#259081]

- In a maximized session window, the Desktop Viewer toolbar can fail to paint properly if you click **Connect** in the USBMultiInsertDialogue dialog box *after* the Session Connection screen disappears.

  [#260390]

- The Client Drive Mapping Help topic of icaclient.adm incorrectly states that policies will not override user selections. Policies do override user selections.

  [#LA0398]

- With certain custom applications, Speed Screen Latency Reduction's local text echo edit box displays a black bar while typing.

  [#LA0544]

- The welcome and/or completion messages after first successful delivery from Merchandising Server fail to appear.

  [#LA2277]

- The icon for Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO) in the notification area of the Windows taskbar can disappear unexpectedly when launching a published application.

  [#LA3190]

- The local taskbar is inaccessible if set to autohide and then moved from its default location to the top, left, or right side of the screen.

  [#LA3400]

Miscellaneous

- When playing UDP audio streams, the handle count of the wfica32.exe process can increase significantly.

  [#LA3094]

- This fix removes a limitation to just one Program Neighborhood Web Interface 5.4 site in Receiver for Web 3.3.

  [#LA3142]

Citrix Receiver for Windows 4 Known Issues

Oct 21, 2015

Known issues

This section contains:

- Installation and upgrade issues
- General issues
- Known issues - Desktop connections
- Microsoft Lync 2013 VDI Plug-in issues

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

Installation and upgrade issues

- During upgrades of Receiver for Windows 3.4 from citrix.com, pending updates such as to plug-ins might not complete. To work around this issue, manually upgrade Receiver. [#396558]
- Upgrades to Receiver for Windows 3.3 from citrix.com do not work. To work around this issue, handle the upgrades manually. [#393294]
- Receiver for Windows does not properly install on a Windows 8 computer if .NET 3.5 is not installed. When you install Receiver for Windows on such computers, the Receiver installer prompts you to download and install .NET 3.5. After completing the .NET installation, the Receiver installation starts but does not complete. To complete the installation, use Programs and Features to uninstall Receiver and then reinstall it. [#352779]
- During installation of Receiver on a Windows 8 computer that does not have .NET 3.5 installed or enabled, if you cancel the prompt to install .NET 3.5 and then attempt to uninstall Receiver, the uninstallation fails. To complete the uninstallation, install or enable .NET 3.5 on the computer and then uninstall Receiver. To enable .NET 3.5 on a Windows 8 computer, go to Control Panel > Programs and Features > Turn Windows Features On or Off and select .Net Framework 3.5. [#354996]
- When installing the Receiver package onto a Windows 8 client using the Merchandising Server, the Receiver icon does not display in the task bar. To work around this issue, restart the user's machine. Alternatively, launch Receiver from the folder in which Receiver.exe is located. [#381529]
- 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]
- When Merchandising Server is used to install Receiver on a Windows 8 device, the Receiver icon might not display in the task bar. To work around this issue, launch Receiver from the folder where it is installed. [#381529]
- In an environment with App Controller 2.0 deployed, Receiver does not indicate that a user is logged on: The Receiver menu includes the Log On command and the user name does not appear in the Receiver window. All other features of the Receiver window work as expected. To avoid this issue, upgrade to App Controller 2.5 before users upgrade Receiver. [#353789]
- For deployments with Merchandising Server, you must upgrade to Receiver Updater for Windows 3.4 to enable Receiver to be uninstalled. In addition, let users know how to respond to the prompt after restarting Receiver. That is, a user must click Postpone. Receiver is not uninstalled if a user clicks Restart. [#346341]
- 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]

- If a user uninstalls a plug-in using the Control Panel and restarts the computer, the plug-in continues to display in the list that appears when you right-click the Receiver icon, click About, and then expand Advanced. This issue occurs only when Receiver is installed from Citrix.com or your own download site. [#320277]
- Plug-in updates on Windows XP, 64-bit edition, fail. To work around this issue, install the hotfix available from http://support.microsoft.com/kb/968730/en-us. [#328081]
- Before installing Receiver for Windows on a Windows XP Embedded thin client device, increase the RAM disk limit of the device to 100 MB. [#266384]

General issues

- For unsupported features, see Citrix Receiver feature matrix.
- The smart card authentication dialog box may lose focus, preventing the user from authenticating while trying to start an application through Receiver. This occurs when single sign-on is not enabled. If this happens, the user should restart the session. To prevent this issue, set TWISeamlessFlag to 1 in the following registry key: [#379878]
  For 32-bit machines: HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

  For 64-bit machines: HKEY_LOCAL_MACHINE\Software\ Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

- A SaaS app with an icon that is larger than 48x48 cannot be subscribed in Receiver. [#353794]
- After a user clicks Update in the About dialog box and then expands Advanced, the Reset Receiver link is no longer visible. To work around this issue, close and reopen the About dialog box. [#383110]
- After using the Receiver Reset command on a Windows 2008 R2 machine, Receiver cannot be launched from the Start menu and the Open command no longer appears in the Receiver menu. To work around this issue, restart Receiver after resetting it. (To reset Receiver, right-click the Receiver icon, choose About, expand Advanced, and then click Reset Receiver.) [#355092]
- When configured with multiple stores, Receiver might confuse the gateways required to connect to a store. This results in incorrect apps being available to users. Work around: Configure only one store. [#263165]
- Receiver can experience issues with automatic reconnection under the following conditions: Receiver is connected to a Web Interface site and the default.ica file contains the entry SessionReliabilityTTL=60. To work around this issue, edit the default.ica file and either remove the SessionReliabilityTTL entry (to use the default value of 180) or change the entry to SessionReliabilityTTL=180. [#373506]
- When a user starts apps provided by a Web Interface connection, Connection Center does not enumerate the sessions. [#261177]
- After a user starts a virtual app that is filtered for Access Gateway, other virtual apps do not launch. [#263003]
- For Windows 8 devices that support Touch Keyboards, you must enable the local Input Method Editor (IME) for Asian languages so users can input characters in virtual applications. To do that, run the following command from a command prompt: [#350071]
  For 32-bit computers: %PROGRAMFILES%/Citrix/ICA client/wfica32 /localime:on

  For 64-bit computers: %PROGRAMFILES(X86)%/Citrix/ICA client/wfica32 /localime:on

- If the Traditional Chinese, Korean, or Russian version of Receiver is integrated with Access Gateway Standard Edition, the Receiver log on screen displays in English because of an Access Gateway Standard Edition language limitation. [#263442]
- Disabling Certificate Revocation List (CRL) checking in Internet Options on the user device overrides the CertificateRevocationCheck registry setting for Receiver. This means users may be able to access websites that do not

have valid certificates. As a workaround, ensure that the Check server revocation option located at Settings > Control Panel > Internet Options > Advanced is enabled. [#32682]

- Receiver does not support the VPN keyword in Access Gateway ClientChoices mode. [#274828]
- If the VPN keyword is removed from an app after a user subscribes to it, Receiver continues to attempt an Access Gateway connection for the app. Workaround: Have the user unsubscribe and then re-subscribe to the app. That action will remove the VPN keyword from Receiver. [#298387]
- The Receiver icon is displayed instead of an app icon in the task bar when a user starts an app that was published with XenApp 5.0 and earlier versions. [#310366]
- When using Internet Explorer to open a Microsoft Office document in Edit mode from SharePoint, Microsoft Office might display the message, “Access denied.” Workaround: Go to the SharePoint site and check out the document, edit it, and check the file back in to SharePoint. [#258725]

Desktop connections

- Loss of video is experienced if files are being played with a published version of Windows Media Player through a virtual desktop session, and the Desktop Viewer window is changed from full-screen to window mode. As a workaround, minimize and restore the Media Player window, and then pause and resume the app (or stop and restart it). [#246230]
- You cannot log off normally from Windows XP 32-bit virtual desktops if you start (but do not log on to) the Receiver in the desktop session. If the Receiver logon dialog box is not completed, you cannot log off from the desktop. To work around the issue, complete the logon dialog box or close it. This issue is not observed on other virtual desktop operating systems. [#246516]
- The Desktop Viewer Devices menu may not close when the user clicks the Devices icon. It also may remain open after its corresponding dialog box closes. If this occurs, click the Devices icon again. [#262202]
- Windows Media Player, when displayed in the non-primary monitor of a two-monitor Windows user device, may not work as expected. Due to an issue with the DirectX video mixing renderer filter VMR-9, the screen is black and there is no sound, although the player's progress bar advances. To correct this issue, edit the registry on the user device from which the XenDesktop connection is launched. In the HKEY_CURRENT_USER\Software\Citrix subkey, create the HdxMediaStream key. Name the key DisableVMRSupport. Set the type as REG_DWORD. Give the key the value 3. [#262852]

Microsoft Lync 2013 VDI Plug-in issues

- After a virtual desktop session reconnects, the VDI log on dialog box does not appear and Lync in the virtual environment is no longer paired with the Lync VDI plug-in. To work around this issue, sign off and then sign back on to Lync. [#399459]
- If the virtual desktop session is disconnected during a Lync video call, the session does not disconnect the call and the Lync conversation window becomes unresponsive if you close it. [#399464]
- Mouse pointer movement is not visible in the Lync conversation window of a user who has shared their virtual desktop. [#399442]
- Video does not appear after you move the Lync conversation window to a second monitor. [#399447]
- When you move a Whiteboard presentation window to another user, the video from the other user does not display in your conversation window. [#399465]
- When a Lync call starts, Receiver reduces the volume on the device. Use the device audio controls to increase the volume. [#401519]

For more information, see XenDesktop 7, XenApp 6.x and Citrix Receiver 4.0 Support for Microsoft Lync 2013 VDI Plug-in.

System requirements

Oct 19, 2016

Device

Operating system

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

- For Receiver for Windows 4.1 only: 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 XP Professional SP3, 32-bit edition, and Windows XP Professional SP2, 64-bit edition (including Embedded Edition)
  Support for Windows XP ends April 8, 2014 when Microsoft ends extended support for Windows XP. Support for Windows XP Embedded will continue.
- Windows Vista, 32-bit and 64-bit editions
- Windows Thin PC
  Does not support the Self-Service Plug-in. For more information, see Configure and install Receiver for Windows using command-line parameters.
- For Receiver for Windows 4.1 only: Windows Server 2012 R2, 64-bit edition
- Windows Server 2012, 64-bit edition
- 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

Hardware

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

Server

- XenApp (any of the following products):
  - Citrix XenApp 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 4, Feature Pack 1 or 2, for UNIX operating systems
- XenDesktop (any of the following products):
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
  - XenDesktop 5.6 Feature Pack 1

    - XenDesktop 5.6
    - XenDesktop 5.5
    - XenDesktop 5
    - XenDesktop 4
- Citrix VDI-in-a-Box
    - VDI-in-a-Box 5.3
    - VDI-in-a-Box 5.2
    - VDI-in-a-Box 5.1
- Citrix Receiver can access virtual desktops and apps using StoreFront, App Controller, and Web Interface.
  StoreFront:
    - StoreFront 2.6 (recommended), 2.5 or 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.

  App Controller 9.0 and 2.10:

  Provides access to Web and Software as a Service (SaaS) apps. Also provides ShareFile account provisioning and single sign-on. App Controller is a component of XenMobile App Edition.

  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 legacy XenApp Services or XenDesktop Services sites.
- To deploy Receiver:
    - Citrix Receiver for Web site (configured with StoreFront)
    - Citrix Merchandising Server 2.x
    - Citrix Web Interface 5.4
    - 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-SSL connections through any one of the following configurations.

- For LAN connections:
    - StoreFront using StoreFront services or Receiver for Web sites
      Single sign-on to Web and SaaS apps published through App Controller requires StoreFront.

- Web Interface 5.4 for Windows, using Web Interface sites or legacy XenApp Services or XenDesktop 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 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPX
  - Citrix Access Gateway 5.0 (for use with Web Interface only)
  - Citrix Secure Gateway 3.x (for use with Web Interface only)

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

  For information about the 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 SSL certificates

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

When securing remote connections using SSL, Receiver verifies the authenticity of the remote gateway's SSL certificate against a local store of trusted root certificate authorities. Receiver automatically recognizes commercially issued certificates (such as VeriSign and Thawte) provided the root certificate for the certificate authority exists in the local keystore.

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 Configure and enable Receivers for SSL and TLS.

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.

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:

- Domain (not available for connections from NetScaler Gateway)
- Domain pass-through
  Receiver for Web sites do not support domain pass-through authentication. Not available for connections from NetScaler Gateway.
- Security token*
- Two-factor (domain plus security token)*
- SMS*
- Smart card (requires StoreFront 2.1 or 2.0)
- User certificate* (can be used alone or with other authentication methods)

* 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 App Controller, Receiver supports the following authentication methods:

- Domain
- Security token*
- Two-factor (domain plus security token)*
- SMS*

* Available only in 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.)

- Domain
- Domain pass-through (available only for connections through a web browser)
- Security token*
- Two-factor (domain plus security token)*
- SMS*
- Smart card
- User certificate* (can be used alone or with other authentication methods)

* 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

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

Availability of Receiver for Windows 4.0 features

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

Other

- **Compatible plug-ins**
  For a list of compatible plug-ins, see To manage Citrix Receiver updates.

- **.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 7, XenApp 6.x and Citrix Receiver 4.0 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.
    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.
  - SSL/TLS+HTTPS

- Previous versions of the Presentation Server Client/Online Plug-in and the current icaclient.adm file. Previous versions of the Presentation Server Client and Online Plug-in are not compatible with the Receiver for Windows 4.0 icaclient.adm file.

Install Receiver for Windows

Dec 24, 2014

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), StoreFront Server, or the App Controller virtual appliance associated with the email address and then prompts the user to log on and continue the installation. This feature is referred to as "email-based account discovery."
    Note: A first-time user is one who does not have Receiver installed on the device.
  - Email-based account discovery for a first-time user does not apply if Receiver is downloaded from a location other than Citrix.com (such as a Receiver for Web site) or if Receiver Updater for Windows is installed.
  - Receiver users can manually check for updates from the Receiver interface.
  - If your site requires configuration of Receiver, use an alternate deployment method.
- Automatically from 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 file.
  - XenDesktop 7 does not support Web Interface.
- 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.
  - You can use Merchandising Server or other methods to provide updates.
    If you are using email-based or URL-based account discovery for account setup, you can use Merchandising Server to add stores to Receiver. However, do not use Merchandising Server to deliver the same stores that are provided through email-based or URL-based account discovery.

Refer also to Configure and install Receiver for Windows using command-line parameters, Install and uninstall Receiver for Windows manually, and Deliver 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.

Upgrade to Receiver for Windows 4.0

Note: Sites that use legacy VDAs do not need to upgrade and should continue to use Receiver Enterprise.
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 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.
  If you also use App Controller (2.5 or higher), you can configure it to send an email to Receiver users that has a provisioning file attached. The provisioning file contains the settings that Receiver needs to connect to App Controller.
- 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 (not supported for XenDesktop 7)

- If you are using App Controller, configure the connectors as described in Configuring Additional Parameters in Application Connectors and its sub-topic in the App Controller documentation.
- Upgrade your Web Interface site with Receiver for Windows 4.0 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.

Disable automatic updates for pooled desktops

This section applies to updates obtained from the Merchandising Server.

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

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

1. Follow the instructions in
   — To use Merchandising Server to install and set up Citrix Receiver for Windows on a shared XenDesktop image
   in the Merchandising Server documentation.
2. Set the following registry key on the master image:
   Caution: Editing the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
   On 32-bit machines:

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

   On 64-bit machines:

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

Install and uninstall Receiver for Windows manually

Aug 17, 2015

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

If Citrix Receiver Updater was used to install Receiver, you can use Updater to uninstall Receiver. If Citrix Receiver Updater was not used to install Receiver, you can uninstall Receiver with the Windows Programs and Features utility (Add/Remove Programs).

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

Dec 09, 2014

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.

- 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 a list of the command-line parameters available for the Self-Service Plug-in, refer to http://support.citrix.com/article/CTX138514.

  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.

- 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.

- STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On | Off];[storedescription]"[STOREy="..."] – 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.

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.

To troubleshoot installation

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

CtxInstall-ICAWebWrapper.log

TrolleyExpress-20090807-123456.log

Examples of a command-line installation

To install all components silently and specify two application stores:

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

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

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

To launch a virtual desktop or application from a command line

The Self-Service Plug-in 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.

Deliver Receiver using Active Directory and sample startup scripts

May 08, 2015

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.

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.

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.

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.

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

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.

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.

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

Aug 12, 2015

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 Receiver for Windows

May 08, 2015

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.
- Configure StoreFront and App Controller. To make resources available to users, create stores that enumerate and aggregate resources from XenDesktop sites, XenApp farms, and App Controller.
- 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

Nov 04, 2013

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 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 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

KEYWORDS:prefer=	Shortcut under Programs	Matches?
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 USB support for XenDesktop connections

May 08, 2015

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

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

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

- Keyboards
- Mice
- Smart cards

Note: Specialist USB devices (for example, Bloomberg keyboards and 3D mice) can be configured to use USB support. For information on configuring Bloomberg keyboards, see 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. For example, a user may have a network interface card attached to the system board by internal USB. Remoting this would not be appropriate. The following types of USB device are not supported by default for use in a XenDesktop session:

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

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

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

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

For desktops accessed through the Desktop Viewer, when a user plugs in a USB device, a dialog box appears asking the user if they want that device remoted to the virtual desktop. The user can decide which USB devices are remoted to the virtual desktop by selecting devices from the list each time they connect. Alternatively, the user can configure USB support so that all USB devices plugged in both before and/or during a session are automatically remoted to the virtual desktop that is in focus.

Mass storage devices

For mass storage devices only, in addition to USB support, remote access is available through client drive mapping, which you configure through the Citrix 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 Plug-n-Play devices
Enabled by default	Yes	Yes
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, if the user clicks Safely Remove Hardware in the notification area

If both USB Plug-n-Play 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 sessions after additional configuration. These are noted below.

- Audio (Class 01). Includes audio input devices (microphones), audio output devices, and MIDI controllers. Modern audio devices generally use isochronous transfers, which is supported by XenDesktop 4 or later.
  Note: Some specialty devices (for example, VOIP phones) require additional configuration. For instructions on this, see CTX123015.
- Physical Interface Devices(Class 05). These devices are similar to Human Interface Devices (HIDs), but generally provide "real-time" input or feedback and include force feedback joysticks, motion platforms, and force feedback exoskeletons.
- Still Imaging (Class 06). Includes digital cameras and scanners. Digital cameras often support the still imaging class which uses the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP) to transfer images to a computer or other peripheral. Cameras may also appear as mass storage devices and it may be possible to configure a camera to use either class, through setup menus provided by the camera itself.
  Note that if a camera appears as a mass storage device, client drive mapping is used and USB support is not required.
- Printers (Class 07). In general most printers are included in this class, although some use vendor-specific protocols (class ff). Multi-function printers may have an internal hub or be composite devices. In both cases the printing element generally uses the Printers class and the scanning or fax element uses another class; for example, Still Imaging.
  Printers normally work appropriately without USB support.

  Note: This class of device (in particular printers with scanning functions) requires additional configuration. For instructions

on this, see CTX123015.

- Mass Storage (Class 08). The most common mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There are a wide variety of devices with internal storage that also present a mass storage interface; these include media players, digital cameras, and mobile phones. Known subclasses include:
  - 01 Limited flash devices
  - 02 Typically CD/DVD devices (ATAPI/MMC-2)
  - 03 Typically tape devices (QIC-157)
  - 04 Typically floppy disk drives (UFI)
  - 05 Typically floppy disk drives (SFF-8070i)
  - 06 Most mass storage devices use this variant of SCSI

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

  Important: Some viruses are known to propagate actively using all types of mass storage. Carefully consider whether or not there is a business need to permit the use of mass storage devices, either through client drive mapping or USB support.
- Content Security (Class 0d). Content security devices enforce content protection, typically for licensing or digital rights management. This class includes dongles.
- Video (Class 0e). The video class covers devices that are used to manipulate video or video-related material, such as webcams, digital camcorders, analog video converters, some television tuners, and some digital cameras that support video streaming.
  Note: Most video streaming devices use isochronous transfers, which is supported by XenDesktop 4 or later. Some video devices (for example webcams with motion detection) require additional configuration. For instructions on this, see CTX123015.
- Personal Healthcare (Class 0f). These devices include personal healthcare devices such as blood pressure sensors, heart rate monitors, pedometers, pill monitors, and spirometers.
- Application and Vendor Specific (Classes fe and ff). Many devices use vendor specific protocols or protocols not standardized by the USB consortium, and these usually appear as vendor-specific (class ff).

USB device classes denied by default

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

- Communications and CDC Control (Classes 02 and 0a). The default USB policy does not allow these devices, because one of them may be providing the connection to the virtual desktop itself.
- Human Interface Devices (Class 03). Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are keyboards, mice, pointing devices, graphic tablets, sensors, game controllers, buttons, and control functions.
  Subclass 01 is known as the "boot interface" class and is used for keyboards and mice.

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

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

- Wireless Controller (Class e0). Some of these devices may be providing critical network access, or connecting critical peripherals such as Bluetooth keyboards or mice.
  The default USB policy does not allow these devices. However, there may be particular devices it is appropriate to provide access to using USB support.

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 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

Mar 30, 2011

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

Jan 23, 2012

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 and App Controller

Nov 04, 2013

Citrix StoreFront authenticates users to XenDesktop, XenApp, App Controller, 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.
2. Configure stores for App Controller just as you would for applications delivered by XenDesktop or XenApp. No special configuration is needed for Receiver. For more information, refer to Configure stores in the StoreFront documentation.

To configure App Controller

App Controller, a component of XenMobile App Edition, securely delivers enterprise Web and Software-as-a-Service (SaaS) applications, native iOS applications, and integrated ShareFile-based data to Receiver users.

If you use email-based account discovery, Receiver determines the App Controller associated with a user's email address.

If you do not use email-based account discovery, provide users with a provisioning file that configures Receiver with the connection settings for App Controller. From the App Controller console, you can email a provisioning file (.cr) to users. For more information, refer to Connecting Users to Citrix Receiver in the App Controller documentation.

Alternatively, if you configure a Receiver for Web site, users can obtain a Receiver provisioning file from that site by clicking Activate in Receiver.

Configure Receiver with the Group Policy Object template

Jun 19, 2013

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.

Provide users with account information

Dec 03, 2013

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, StoreFront Server, or App Controller virtual appliance associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access 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 and App Controller provide provisioning files that users can open to connect to stores and App Controller.

- 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.

- You can configure App Controller to send Receiver users an email that has a provisioning file attached. The provisioning file contains the settings that Receiver needs to connect to App Controller. For more information, refer to Downloading the Receiver Configuration File in the App Controller 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 or App Controller, provide the URL for that server. For example: https://servername.company.com
  For legacy 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

Apr 30, 2013

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

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

May 17, 2013

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.

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

May 08, 2015

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.

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.

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.

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

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

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

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

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

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

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 the XenDesktop or XenApp documentation in eDocs.

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.

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 comx: \\client\com:
   where x is the number of the client COM port you want to map.
4. To confirm the operation, type:
   net use

   at a command promt. 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

Jun 19, 2013

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.

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

Apr 13, 2015

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

May 01, 2013

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
- Provide virtual desktops to Receiver users
- Keyboard input in Desktop Viewer sessions
- Connect to virtual desktops

Client-side microphone input

May 01, 2013

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

Jun 19, 2013

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

May 01, 2013

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

Dec 03, 2012

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

May 08, 2013

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.

Provide virtual desktops to Receiver users

Oct 18, 2013

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

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

Note: Your users must use Citrix Receiver to change the screen resolution on their virtual desktops. They cannot change Screen Resolution using Windows Control Panel.
For more information about Desktop Lock, supported only for CitrixReceiverEnterprise.exe, refer to the XenDesktop 7 documentation in eDocs.

Keyboard input in Desktop Viewer sessions

Jul 25, 2013

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

Oct 12, 2012

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

May 01, 2013

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 smart card authentication

Oct 30, 2013

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). Bimodal authentication requires StoreFront and NetScaler Gateway configuration.
- **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 it 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 PIN or certificate choice.
- 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.

- Direct smart card authentication to App Controller is not supported. However, you can deploy App Controller behind StoreFront to use the StoreFront certificate authentication service. Web apps that use client certificate authentication require separate smart card prompts for the browser to create its own SSL connection.
- 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 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\

To configure StoreFront:

- In the default.ica file located on the StoreFront server, set Set DisableCtrlAltDel to false.
- When you Configure the authentication service on the StoreFront server, select the Domain pass-through check box and leave the Smart card check box cleared.
  For more information about using smart cards with StoreFront, refer to Configure the authentication service in the StoreFront documentation.

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.

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 SSL 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.

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.

Enable certificate revocation list checking for improved security with Receiver

May 08, 2015

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

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

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

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Configuration folder for the Receiver (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. 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.

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

May 08, 2015

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

Nov 20, 2013

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.

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 `Set DisableCtrlAltDel to false`.
- 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.

Secure Receiver communication

May 01, 2013

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, or SSL tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Receiver and servers. Receiver supports SOCKS and secure proxy protocols.
- For XenApp or Web Interface deployments only; not applicable to XenDesktop 7: SSL Relay solutions with Secure Sockets Layer (SSL) and 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

Jun 01, 2013

To enable remote users to connect through NetScaler Gateway, configure NetScaler Gateway to work with StoreFront and App Controller (a component of XenMobile App Edition).

- 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 App Controller deployments: Allow connections from remote users to App Controller by integrating NetScaler Gateway and App Controller. This deployment allows users to connect to App Controller 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 NetScaler Gateway Plug-in.

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

May 01, 2013

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

Oct 12, 2012

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

Oct 12, 2012

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

May 03, 2013

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

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

When trusted server configuration is enabled, 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.)

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

To enable trusted server configuration

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

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.
   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.
2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the Action menu, choose Add/Remove Templates.
4. Choose Add and browse to the Receiver Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select Open to add the template and then Close to return to the Group Policy Editor.
6. Expand the Administrative Templates folder under the User Configuration node.
7. 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

May 01, 2013

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

Jan 02, 2013

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 Relay

May 08, 2015

This section does not apply to XenDesktop 7.

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

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

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

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

You can use Citrix SSL Relay to secure communications:

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

For information about configuring SSL Relay to secure your installation, refer to Configuring SSL/TLS Between Servers and Clients in the XenApp documentation.

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.

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.

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 SSL and TLS

May 08, 2015

This topic does not apply to XenDesktop 7.

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

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

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

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

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

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

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

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

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

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

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

1. To use SSL/TLS to encrypt application enumeration and launch data passed between Receiver and the server running the Web Interface, configure the appropriate settings using the Web Interface. You must include the computer name of the XenApp server that is hosting the SSL certificate.
2. To use secure HTTP (HTTPS) to encrypt the configuration information passed between Receiver and the server running the Web Interface, enter the server URL in the format https://servername. In the Windows notification area, right-click the Receiver icon and choose Preferences.
3. Right-click the Online Plug-in entry in the Plug-in Status and choose Change Server.

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.
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 SSL/TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Receiver connects using TLS encryption. If a connection using TLS fails, Receiver connects using SSL.
   - Set SSL cipher suite to Detect version to have Receiver negotiate a suitable cipher suite from the Government and Commercial cipher suits. You can restrict the cipher suites to either Government or Commercial.
   - Set CRL verification to Require CRLs for connection requiring Receiver to try to retrieve Certificate Revocation Lists (CRLs) from the relevant certificate issuers.

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

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

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

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

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

1. From the Citrix management console for the XenApp server, open the Properties dialog box for the application you want to secure.
2. Select Advanced > Client options and ensure that you select Enable SSL and TLS protocols.
3. Repeat these steps for each application you want to secure.

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

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

Ensure that a valid root certificate is installed on the user device.

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

Install root certificates on user devices

Oct 12, 2012

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

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

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

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

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

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

To configure Web Interface to use SSL/TLS for Receiver

Feb 22, 2012

1. To use SSL/TLS to encrypt application enumeration and launch data passed between Receiver and the server running the Web Interface, configure the appropriate settings using the Web Interface. You must include the computer name of the XenApp server that is hosting the SSL certificate.
2. To use secure HTTP (HTTPS) to encrypt the configuration information passed between Receiver and the server running the Web Interface, enter the server URL in the format https://servername. In the Windows notification area, right-click the Receiver icon and choose Preferences.
3. Right-click the Online Plug-in entry in the Plug-in Status and choose Change Server.

To configure TLS support

Dec 03, 2012

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 SSL/TLS Version to TLS or Detect all to enable TLS. If Detect all is selected, Receiver connects using TLS encryption. If a connection using TLS fails, Receiver connects using SSL.
   - Set SSL cipher suite to Detect version to have Receiver negotiate a suitable cipher suite from the Government and Commercial cipher suits. You can restrict the cipher suites to either Government or Commercial.
   - Set CRL verification to Require CRLs for connection requiring Receiver to try to retrieve Certificate Revocation Lists (CRLs) from the relevant certificate issuers.

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

Dec 03, 2012

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

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

Mar 18, 2011

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

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

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

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

Mar 18, 2011

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

1. From the Citrix management console for the XenApp server, open the Properties dialog box for the application you want to secure.
2. Select Advanced > Client options and ensure that you select Enable SSL and TLS protocols.
3. Repeat these steps for each application you want to secure.

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

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

May 02, 2013

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

Ensure that a valid root certificate is installed on the user device. For more information, see 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 SSL/TLS.
4. Click Update to apply the change.
5. Enable SSL/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

May 08, 2015

This topic applies only to deployments with Web Interface using legacy 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).

Option	Description

When selecting a digital signature certificate, Citrix recommends you choose from this prioritized list:

1. Buy a code-signing certificate or SSL signing certificate from a public Certificate Authority (CA).
2. If your enterprise has a private CA, create a code-signing certificate or SSL signing certificate using the private CA.
3. Use an existing SSL certificate, such as the Web Interface server certificate.
4. Create a new root CA certificate and distribute it to user devices using GPO or manual installation.

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

Dec 02, 2012

This topic applies only to deployments using Web Interface.

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

The same format must be used in both the ICA file and the sites entries. For example, if you use a fully qualified domain name (FQDN) in the ICA file, you must use an FQDN in the sites zone entry. XenDesktop connections use only a desktop group name format.

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

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

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

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

Sep 16, 2013

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.

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.

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
PdaSecurityPermission	PDA devices
ScannerAndDigitalCameraSecurityPermission	USB and other devices

Value	Description
0	No Access
1	Read-only access

Value	Description
2	Full access
3	Prompt user for access