Citrix Receiver for Linux 13.10

Contents

What's new

April 16, 2019

What's new in 13.10

Logging enhancements

Logging enhancements feature is an extension of Better logging. Logging support is being introduced for the Connection Center, Graphics (thinwire), and End User Experience Monitoring (EUEM) modules. This enhancement helps users troubleshoot, and - in cases of complicated issues - facilitate the support team's job by using detailed logs.

For information about enabling logging, see Enabling logging.

Cryptographic update

This feature is an important change to the secure communication protocol. Cipher suites with the prefix **TLS_RSA_** do not offer **forward secrecy**. These cipher suites are now generally deprecated by the industry. However, to support backward compatibility with older versions of XenApp and XenDesktop, Citrix Workspace App for Linux has an option to enable these cipher suites. For more information, see Configuring deprecated cipher suites.

Multi-monitor layout persistence

This feature lets you save the position of a desktop session, and then relaunch it in the same position. This feature avoids the overhead of repositioning sessions at every launch. It empowers you to dynamically adjust and save the layout information across endpoints, thus optimizing the end user experience in multi-monitor environments. For more information, see Configuring multi-monitor layout persistence.

SoC SDK update

Customers who use the SoC SDK might be required to update the plug-ins for H.264-based session graphics.

V3 Authentication Protocol

"V3" authentication indicates the third major definition of a logon protocol to NetScaler Gateway that is supported by Citrix Workspace App for Linux.

V3 is the standard logon protocol for NetScaler Gateway in combination with the "N-Factor" authentication policy framework that makes authentication steps and the associated credential collection forms completely configurable. Native Citrix Workspace App can support this protocol by building on the Forms logon support already implemented for StoreFront. The web logon page for NetScaler Gateway and Traffic Manager virtual servers also consume this protocol using code shared with Citrix Workspace App for Linux.

For more information, see SAML Authentication and Knowledge Center article NetScaler Authentication.

What's new in 13.9.1

Citrix Workspace App for Linux now includes GStreamer 1.0 files. These files are not available in the Citrix Workspace App for Linux 13.9 packages.

What's new in 13.9

Browser content redirection

Redirects the contents of a web browser to a client device and creates a corresponding browser embedded within Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or Flash video content. Browser content redirection is supported on the x86, x64, and ARM hard float (armhf) platforms.

For more information, see Browse content redirection and Browser content redirection policy settings in XenApp and XenDesktop documentation.

Better logging

The Citrix Workspace App for Linux build can now generate and send logs through syslog. This feature allows the handling of messages to be controlled based on their level and origin. Logging support is being introduced for the Connection Sequence (WD, PD, TD, Proxy) and Printing components. This helps users troubleshoot, and - in cases of complicated issues - facilitate the support team's job by using the detailed logs available. The log output is similar to the current debugging mode.

The logging parameters, log level, log file, log method (sequence, multi-sequential, cycle), and the module to be logged can be configured using configuration files. For information, see Enabling logging.

Support for Citrix Ready workspace hub

Citrix Ready workspace hub provides a secure connection to authorized apps and data. With this release, Citrix Workspace App for Linux enhances the implementation for workspace hub plug-in, which enables support for the Citrix HDX RealTime Optimization Pack and dual monitors connected to a workspace hub.

Fixed issues

November 14, 2018

Citrix Workspace for Linux 13.10

The following issues have been fixed since Version 13.9.1:

Seamless Windows

- When accessing published applications using Citrix Workspace in seamless mode, the applications might be published as an Applications Group with a tag restriction. As a result, this error message appears on XenApp and XenDesktop 7.15 Long Term Service Release (LTSR) Cumulative Update 1 (CU1).
  "The X Request 55.0 caused error: "9: BadDrawable (Invalid Pixmap or Window Parameter)"." [#LC9437]

Session/Connection

- The Automatic Proxy Detection feature might not work with Citrix Workspace app. As a result, the application does not start and this error message appears:
  "Cannot connect to "0.0.0.129 - Application Name." [#LC8101]
- When you start a user session in full-screen mode that is running on two different monitors, disconnecting one monitor can result in the following error message:
  "11: BadAlloc (insufficient resources for operation)" [#LC8522]

- When using Citrix Workspace app, the Automatically move pointer to the default button in a dialog box option might not work when it is enabled on the VDA. [#LC8845]
- When you start applications using Citrix Workspace app, this error message might appear: "BadWindow (invalid Window parameter)" [#LC9447]
- When you perform certain operations such as logging on or client drive mapping transfers, the user sessions that are connected through NetScaler might disconnect when using Citrix Workspace app. [#LC9574]
- The StoreFront store has two Delivery Controllers with one of them in an offline state. When you use the storebrowse –killdaemon or the storebrowse -K command, the most recently used set of credentials that is stored in the SSO cache might not be removed. As a result, storebrowse can still authenticate to the Delivery Controller without asking for credentials. [#LC9611]
- When you attempt to start a Citrix Workspace app session from the .tar file, an error occurs. Duplicate entries (LocaleKeyMapping=*,SuperMetaToWinKeys=* & RightSuperMetaToWinKey=*) might be found in "All_Regions.ini" at "linuxx64-13.x.tar\linuxx64\linuxx64\linuxx64.cor\config\usertemplate [#LC9765]

User Experience

- When you open a published Microsoft PowerPoint presentation slide in full-screen mode on an Ubuntu client, certain sections of the slides might be missing or be offset. [#LC8734]
- When you start a desktop session in a dual-monitor setup using Citrix Workspace app, the Windows taskbar might appear as a white screen. [#LC9021]

Citrix Workspace for Linux 13.9.x

The following issues have been fixed since Version 13.8:

Server/Site Administration

- When using the "storebrowse –killdaemon" command, you might directly log on to a session using the credentials that are stored in the cache, resulting in an invalid user. Instead, the user name and password prompt must appear for the current user. The issue occurs when the "storebrowse –killdaemon" command does not clear the cached credentials of the StoreFront Server since the last logon of the user. [#LC8707]

Session/Connection

- Attempts to record audio by using an input device in a VDA for Server OS might fail when using Citrix Workspace app. [#LC8072]
- Attempts to connect to published applications or desktops might fail when using TLS 1.0 and TLS 1.2. [#LC8122]
- Attempts to maximize published applications that are running on a Xubuntu operating system might fail. The issue occurs when you span the taskbar through multiple monitors. [#LC8436]

Citrix Workspace for Linux 13.8

The following issues have been fixed since Version 13.7:

Printing

- When printing a document, Citrix Workspace app redirects the print job to the default printer, regardless of the printer selected. [#LC8221]

Server/Site Administration

- When using the "storebrowse –killdaemon" command, you might directly log on to a session using the credentials that are stored in the cache, resulting in an invalid user. Instead, the user name and password prompt must appear for the current user. The issue occurs when the "storebrowse –killdaemon" command does not clear the cached credentials of the StoreFront Server since the last logon of the user. [#LC8707]

Session/Connection

- When using Citrix Workspace with Cisco VXME plug-ins, Microsoft Windows Server might disconnect while starting a session. [#LC8496]

Smart Cards

- In a double-hop scenario, attempts to access a smart card might fail when using Citrix Workspace app. The following error message appears:

  "No valid certificates were found on this smart card."

  [#LC7424]

Citrix Workspace for Linux 13.7

This release does not fix any customer reported issues.

Citrix Workspace for Linux 13.6

The following issues have been fixed since Version 13.5:

Printing

- Citrix Workspace app might complete the initial print job, but subsequent attempts to print in the same session can fail. [#LC7913]

Session/Connection

- With “Proxy Auto Configuration” enabled, attempts to start an application can result in a seg-fault error in wfica. [#LC8179]

Keyboard

- After upgrading to Citrix Workspace App for Linux 13.5, keyboard input might not work within a client session. [#LC7591]

Session/Connection

- The following error message might appear when using Citrix Workspace app:

  “The X Request 139.27 caused error: “8: BadMatch (invalid parameter attributes)”.”

  [#LC6682]

- The following error message might appear when using Citrix Workspace app:

  “The X Request 24.0 caused error: “5: BadAtom (invalid Atom parameter)”.”

  [#LC6733]

Citrix Workspace for Linux 13.5

The following issues have been fixed since Version 13.4:

HDX MediaStream Flash Redirection**

- If you resize a Microsoft Internet Explorer window with HDX MediaStream Flash Redirection enabled, websites with Flash content might fail to resize to fit the modified Internet Explorer window. [#LC6126]

Session/Connection

- When you play a media clip within the desktop session on an HP Thin Client, Windows Media Player might generate the following error message:

  "Windows Media Player encountered a problem while playing the file."

  In certain scenarios, a blank or a black window can appear.

  [#LC5508]

- The drop-down menus of published applications might disappear immediately after appearing when started from Citrix Workspace app. [#LC5574]
- When you start a session and then cancel the connection progress bar, the wfica process might send a SIGTERM to all processes within its process group. The processes can exit unexpectedly while sharing the process group. [#LC5858]
- In a multi-monitor environment, when a seamless application is running on the second monitor, switching between workspaces in Gnome 3 can cause the seamless application to render incorrectly. The issue occurs when "workspaces-only-on-primary" is enabled on Gnome 3. [#LC5897]
- The keyboard shortcut "Ctrl+Alt+Del" in the Desktop Viewer toolbar might not work in Linux VDA sessions. [#LC6164]
- When you attempt to start an application by clicking the corresponding desktop icon, the application might fail to start. [#LC6285]
- Attempts to start a session that is enabled with H.264 encoding support on a Linux VDA can result in a segfault error in wfica. [#LC6603]

System Exceptions

- Attempts to connect to certain XenApp or XenDesktop sites can cause AuthManagerDaemon to exit unexpectedly. [#LC6166]

User Experience

- When you start a seamless application that contains multiple child windows, you might not be able to move certain child windows. Additionally, you might not be able to change focus to these windows. [#LC4342]
- When you log off from a local desktop with the self-service credentials dialog open, further attempts to log on to self-service can fail and self-service might never progress to the authentication dialog box. [#LC4939]
- When you start Microsoft Excel in seamless mode, the keyboard focus sometimes does not move to the “Find” window in the application. [#LC5964]

User Interface

- The “Sametime” icons might not appear in the notification area when using Citrix Workspace app. [#LC3956]
- When you move the Microsoft Lync chat window to a new position, the window might not redraw completely. [#LC5583]
- Attempts to move the “Find” window in Microsoft Excel started in seamless mode might fail. [#LC5963]
- When minimizing a child window (for example, the main window of Spy++ is the parent window and the window for detecting specified windows is the child window), the size of the minimized title bar might appear to be smaller. [#LC6210]

Citrix Workspace for Linux 13.4

The following issues have been fixed since Version 13.3:

Client Device Issues

- With client drive mapping enabled, mapped drives occasionally take longer than expected to access. [#LC3930]

Enhancement

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

> Note: This feature is available only in sessions running on XenApp or XenDesktop 7.8. It is disabled by default.

- To enable the feature:*

  In the file $HOME/.ICAClient/wfclient.ini, in the section [WFClient], add the entry RelativeMouse=1.
  This enables the feature but keeps it inactive until you activate it.

- To activate the feature:

  Type - Ctrl/F12.
  Once the feature is enabled, type Ctrl/F12 again to synchronize the server pointer position with the client. The server and client pointer positions are not synchronized when using Relative Mouse.

- To deactivate the feature:

  Type Ctrl-Shift/F12.
  The feature is also switched off when a session window loses focus.

  * Alternatively, consider using the following values for RelativeMouse:

  RelativeMouse=2 Enables the feature and activates it whenever a session window gains focus.
  RelativeMouse=3 Enables, activates, and keeps the feature activated always.

  To change the keyboard commands, add settings like:

  RelativemouseOnChar=F11
  RelativeMouseOnShift=Shift
  RelativemouseOffChar=F11
  RelativeMouseOffShift=Shift

  The supported values for RelativemouseOnChar and RelativemouseOffChar are listed under [Hotkey Keys] in the config/module.ini file in the Citrix Workspace App for Linux installation tree. The values for RelativeMouseOnShift and RelativeMouseOffShift set the modifier keys to be used and are listed under the [Hotkey Shift States] heading. [#LC5000]

Logon/Authentication

- Version 13.3 of the Citrix Workspace app fails to pass certain command line parameters, including the -clearpassword option, to older versions of XenApp. As a result, users' attempts to log on can be unsuccessful. [#LC4594]

Session/Connection

- Attempts to start a user session in full-screen mode using the "-span" command line option might fail. [#LC3394]
- After resizing the secondary monitor in a dual-monitor configuration, the Windows taskbar can fail to revert to the original location. [#LC3856]
- A segfault error in wfica can cause sessions to disconnect or become unresponsive during screen updates that result from activities such as highlighting or scrolling. [#LC3947]
- When reconnecting to a disconnected, multiple-monitor session on Ubuntu 14.04, the session window appears on only one monitor instead of all. [#LC4181]
- Attempts to connect to an anonymous store might fail with the following error messages:

  "NoWebUIAuth 0" and "Cannot complete your request"

  [#LC4270]
- Attempts to start a published desktop can fail when using an SSL proxy host such as SSL Relay. [#LC4739]
- A published instance of Internet Explorer might lose focus and duplicate when a pop-up window appears in the original browser window. [#LC5066]

Smart Cards

- When using a smart card with pnabrowse, the PIN cannot be passed to the VDA and the authentication might fail. The session is started but the logon screen appears. [#LC4241]

System Exceptions

- After playing media with Windows Media Player on an ARM hf based Linux client, sessions disconnect. [#LC4625]

User Experience

- Microphone audio quality in sessions running on XenApp and XenDesktop 7.6 can be poor. [#LC3124]
- In ARM hf implementations, the taskbar occasionally does not flash to indicate the presence of new Lync 2010 messages. [#LC3688]
- After unlocking a user session in a dual-monitor setup, minimized windows might not get restored to the correct position and appear to be unresponsive. [#LC3984]

- When you start an application on a Gnome 3 desktop and maximize the application, the position of the mouse cursor might be offset by the distance of the Gnome 3 top bar. [#LC4738]
- Webcam redirection occasionally does not work in sessions running on Version 7.6 VDAs. [#LC4751]

User Interface

- The Copy and Paste function occasionally fails between server and server, and server and user device. [#LC4157]
- The mouse cursor disappears when playing full screen video and does not return to view until the video is no longer full screen. [#LC4428]
- A segment fault error can occur when certain third-party published applications spawn a dialog box. The cursor is no longer visible when you attempt to reconnect to the unexpectedly closed application. [#LC4955]

Citrix Workspace for Linux 13.3

The following issues have been fixed since Version 13.2:

Session/Connection

- After restoring a maximized seamless window, certain parts of the desktop fail to refresh automatically. This only occurs in some desktop environments, such as Ubuntu 12.04 Unity 2D. [#LC0602]
- When using the parameter “ProxyType=Secure,” a segmentation fault can occur. [#LC3396]
- Attempts to copy and paste content from a published application to a local application can cause the ICA engine component (wfica) process to close unexpectedly with a segmentation fault. [#LC3480]
- In some instances, the cached application list can get out of sync. [#556245]

System Exceptions

- Sometimes, smart card authentication causes a session to exit unexpectedly. [#582550]

User Experience

- With this fix, the Russian time zone information can be updated in Citrix Workspace App for Linux.

  To enable this fix:

  - For XenApp 6.5, you must install a minimum of Hotfix Rollup Pack 5 or subsequent Rollup Pack hotfixes to redirect all time zones correctly.
  - For the XenApp and XenDesktop 7.6 server operating system VDA, you must install Hotfix ICATS760WX64014.
  - If the server operating system is Windows Server 2008 R2 Service Pack 1, you must install Microsoft hotfix KB2870165 on the server.
  - Update both the server and user device operating systems to apply the latest time zone information.
  - Install Microsoft hotfix KB2998527 for Windows and then update the time zone data for Linux.

  [#LC1971]

User Interface

- The icons of published applications might not appear correctly on the taskbar. [#LC3405]
- Icons in seamless sessions might not appear on the taskbar while using ARM hard float (armhf) platforms. [#LC4051]
- An inaccurate dependency message is displayed when starting selfservice after installing Citrix Workspace app with a tar.gz distribution package on Fedora 21. [#582071]

Citrix Workspace for Linux 13.2

The following issues have been fixed since Version 13.1:

HDX Plug and Play

- The webcam might not be compatible with Citrix GoToMeeting and Cisco WebEx when using the HDX RealTime Optimization Pack (Linux) for Microsoft Lync 2010. To enable this fix in its entirety, you must install both a Citrix Workspace hotfix and an HDX RealTime Optimization Pack (Linux) for Microsoft Lync 2010 hotfix that contains Fix #LA0339.

> **Note**: After installing this fix, if you start Microsoft Lync in a VDA session while a Citrix GoToMeeting or Cisco WebEx video conference is running, the webcam might stop working. If this happens, stop and restart the camera from within the video conference. [#LC0339]

Logon/Authentication

- When users log on with smart card by using the Unicon user interface, users cannot enumerate or start applications if the smart card contains more than two certificates and if only one of them is an authentication certificate. If the smart card contains one client certificate for authentication, users can enumerate and start applications, however, the following error message always appears: “Cert Client Authentication OID info set, but unexpected value:…” [#LC2098]

Server/Farm Administration

- If connections with Citrix Workspace App for Linux go through a virtual private network (VPN) interface, Citrix Workspace app fails when starting a published application. [#LC1284]
- If running the command “ctx_rehash” to install a root or intermediate certificate on the user device, creating the correct hash or link might fail with the error message “Error adding store:AM_ERROR_HTTP_SERVER_CERTIFICATE_NOT_TRUSTED[65150].” When this occurs, Citrix Workspace cannot use the certificate and attempts to add a store fail. [#LC1513]
- With this fix, if the user adds a store by running the command “$ICAROOT/util/storebrowse –addstore < store URL>” or by using the Self-Service Plug-in and if the “discovery” parameter is not included in the URL, then the “discovery” parameter is appended to the URL automatically. [#LC1517]

Session/Connection

- When maximizing a window of a published Microsoft Office application in seamless mode, the window becomes maximized, but its contents can be offset and the left and top frames might not be drawn. [#LC0118]
- In a multi-monitor environment, if the second monitor is rotated or has a different resolution, when starting a published application in seamless mode and then maximizing the window, the server does not show the maximized window and the window is unusable.

  To enable the fix, in the file $HOME/.ICAClient/wfclient.ini, in the section [WFClient], add the entry “TWIAvoidFullScreenWhenMaximized =True.”

  [#LC0354]

- In a multi-monitor environment, if a published application window in seamless mode is maximized and restored several times, on occasion, a gray colored background might appear in the second monitor instead of the application window. [#LC0355]
- In a multi-monitor environment, resizing the window of a published application in seamless mode in the second monitor might fail while using client-side resize. [#LC0356]
- When switching between two published Remote Desktop (RDP) sessions in full-screen mode, such as mstsc1 and mstsc2, the connection bar is not updated correctly and shows mstsc2 as the primary window even after switching to mstsc1. [#LC0437]
- Attempts to start a session by using Citrix Workspace app can cause the session to disconnect when transferring data continuously through the Citrix Generic USB or Client drive redirection. [#LC0522]
- When trying to log on to the Web Interface by using the IP address, a segfault can occur and pnabrowse exits unexpectedly. [#LC0648]
- When switching between a published application and Microsoft SQL Server 2012 Management Studio, if users maximize both windows and then minimize the published application window only, the Microsoft SQL Server 2012 Management Studio window does not redraw correctly and a few portions of the window are not updated. [#LC0739]
- The window focus remains on the main window instead of switching to the dialog box. For example, when attempting to close a published Notepad with the modified content, a message appears to ask if you want to save the content. The message dialog box is not the active window. [#LC0952]
- Citrix Workspace app might close unexpectedly when copying an image from a published application to a local application. [#LC1017]
- Attempts to start a session by using Citrix Workspace app can fail through Citrix NetScaler Gateway. [#LC1103]
- A blank error window might appear when a user opens an application in a VDA session that needs the web camera, which is already in use by a local application. [#LC1135]
- When connecting to a XenDesktop 5.6 VDA and if the user device is connected to two monitors, there might be a display issue in the second monitor. In addition, when maximizing the window in the second monitor, the window might not expand completely on the screen. [#LC1148]
- When a session is started or resized, the frame buffer plug-in might not clear the screen. [#LC1515]
- Citrix Workspace app fails if an automatic proxy server URL is configured on the user device. The following syslog error appears in the log:

Ubuntu1204LTSi386 kernel: [xxxx.xxxxxx] wfica [xxxx] segfault at 2 ip bxxxxxxx sp bxxxxxxx error 4 in libproxy.so[bxxxxxxx+xxxx]

[#LC1584]

- When session reliability is enabled and if data is continuously transferred through the Citrix Generic USB, the existing session might disconnect. [#LC1588]
- The 64-bit version of Citrix Workspace app might fail to register the browser plug-in. [#LC1712]
- On systems with Fix #LC1127 installed, Citrix Workspace App for Linux 13.1.3 might become unresponsive when disconnecting from a desktop session that is published by XenDesktop. [#LC2365]
- When users log on with Citrix Workspace app and attempt to paste content within a hosted desktop published in XenApp 5.0, if users right-click and hover the mouse over the paste option, the session disconnects and a segmentation fault can occur. [#LC2467]
- When connected with Citrix Workspace App for Linux for Web, after downloading a StoreFront Services provisioning file (.cr) and then running the storebrowse command "./util/storebrowse -C /tmp/receiverconfig.cr," the "Add Service Record Add Store" dialog does not appear and the store is not created. [#LC2669]
- When using Citrix Workspace app 13.1, if users right-click an icon that is in the Windows notification area, the Citrix Workspace app session might become unresponsive and mouse and keyboard inputs do not work until the session is closed and then opened again. [#LC2824]

User Experience

- An error message might appear when scrolling through a large document in Citrix Workspace app. Users must respond to the error message to continue working within the session. [#LC1127]
- If the original screen resolution of a user device changes during a Citrix Workspace app session, the session does not retain the full-screen setting. As a result, the session size might change so that it does not match the current and original screen resolutions. [#LC1222]
- If the icon name contains a backward slash ("\"), application icons might not appear correctly in Citrix Workspace app. [#LC1364]
- Attempts to copy and paste content from Java applications to published applications might fail or the content from a previous clipboard gets pasted. The issue occurs when the Citrix Workspace app fails to synchronize the user device clipboard with the server clipboard information. [#LC1856]
- On a Hewlett-Packard thin device that uses the hardware decoder for H.264 graphics, in a VDA session and after starting an application in the session, attempts to copy and paste text in open

documents fails. Also, copying text fails from one application window to another application window that is running in a VDA. [#LC2985]

User Interface

- If StoreFront is configured with an aggregation group and if the application name contains a backward slash ("\"), starting applications in Citrix Workspace app might fail. The following error message appears:

  "Corrupt ICA file"

  [#LC1268]

Citrix Workspace for Linux 13.1

The following issues have been fixed since Version 13.0:

HDX MediaStream Windows Media Redirection

- The Citrix Workspace App for Linux 13.0 chooses Motion JPEG (MJPEG) output for the webcam even though YUYV output is available. [#LA5740]

HDX MediaStream Flash Redirection

- With HDX MediaStream for Flash enabled, reloading certain Flash videos in Internet Explorer might fail.[#LA4345]
- When playing a video on YouTube, audio and video might not play correctly in Internet Explorer. This occurs when users connect with Citrix Workspace App for Linux and HDX MediaStream Flash Redirection is enabled. [#LA5833]
- If HDX Flash redirection is enabled, selecting the video size control of YouTube can cause flash redirection to fall back to server side rendering. [#LA5834]

Keyboard

- Pressing key combinations that include the Alt, Shift, or CTRL keys can cause those keys to remain in a down state in a remote session. [#LA5730]

- This fix addresses the following issue with the interpretation of the Num Lock key state:

  When you move the mouse pointer out of a published application window and then back in, then press several keys on the numerical keypad while the Num Lock key is pressed, the first key pressed on the numerical pad does not appear in the session.

  [#LC0146]

Session/Connection

- With *Client clipboard redirection* enabled, copying and pasting files in a client session (for example, using seamless published Windows Explorer) might fail. [#LA5254]
- Published application windows without a taskbar entry fail to take input focus unless another published window exists for the same application. [#LA5617]
- When moving a seamless window, the window might not be redrawn correctly in certain scenarios.

  To enable this fix, in either of the files ~/.ICAClient/wfclient.ini file or config/All_Regions.ini add the entry "TWIRedrawAfterMove=TRUE" in the [WFClient] section.

  [#LA5669]
- This fix improves the file transfer rate in low latency environments. [#LA5725]
- The The Citrix Workspace App for Linux 13.0 chooses Motion JPEG (MJPEG) output for the webcam even though YUYV output is available. [#LA5742]
- DNS queries that return multiple responses for a single lookup - as is common in a round-robin configuration, can cause secure connection attempts to fail and the Citrix Workspace app to exit unexpectedly. [#LA5752]
- When restoring a window from maximization on the server, the local window is restored but the content of the window is not correct and there is a mouse offset. [#LA5926]
- If you move a published application window started in a seamless mode, the contents of the window might be corrupted. To fix this issue, do the following:
  - On the server, set the policy "View window contents while dragging" to "Prohibited."
  - On the user device, in the file "$HOME/wfclient.ini", locate the section [WFClient] and add the entries "TWICoordinateWinPosition=True" and "TWIRedrawAfterMove=True."

  [#LA5935]
- The display of sessions on 7.5 VDAs subject to a **Visual Display** policy where the **Visual quality** setting is set to a value other than the default (Medium) can be unresponsive from the moment they start. [#LC0043]

- Attempts to connect to published applications or desktops through the NetScaler Gateway can fail and the following error message appears:

  Cannot contact server for application <>.
  Server browser command contains an invalid parameter.
  The server name cannot be resolved.

  The issue occurs in scenarios where an extra Secure Ticket Authority is configured both for the NetScaler Gateway and for StoreFront.

  [#LC0059]

- When trying to authenticate to the Web Interface using a Kerberos ticket, a segfault can occur and pnabrowse exits unexpectedly. [#LC0065]
- When pressing Alt+Tab to browse among open windows and to bring up the Remote Desktop logon window, the window fails to take focus. [#LC0069]
- When the cursor is located within the boundaries of an application window, clicking Alt+Tab can fail to bring the window to the front. [#LC0070]
- Dragging a window in a desktop started by the Citrix Workspace app can leave a shadow behind. [#LA0128]
- This fix prevents the occasional appearance of an unexpected and unwarranted error message indicating a connectivity issue and presenting users with Exit and Retry options. [#LC0129]
- UDP audio can fail unexpectedly a few minutes into the session. [#LC0137]
- XenDesktop sessions might become unresponsive when transferring data over a serial port with Citrix Workspace App for Linux. [#LC0296]
- When users connect with Citrix Workspace App for Linux and the thin client HP t610 running on an HP ThinPro 4.4 operating system and if the time zone is set to GMT +8 in the following locations, the error message “Your current time zone is not recognized” appears:
  - Singapore
  - Brunei
  - Makassar
  - Kuala Lumpur
  - Kuching
  - Manila

  [#LC0299]

- When switching between Microsoft Word and the Microsoft Terminal Services Client (MSTSC) window, the content that appears in the windows can be corrupt. [#LC0308]
- The command pnabrowse -WT fails to end a desktop session.

To enable the fix, in the file $HOME/wfclient.ini, in the section [WFClient], add the entry "LogoffDesktopThroTWI=True."

[#LC0345]

- Attempts to interact with some drop-down boxes might fail when using Citrix Workspace app. [#LC0365]

Shadowing

- If the resolution of the Linux client is changed and a published application is started from the XenApp server by using Citrix Workspace App for Linux, the shadower might fail to refresh its display correctly while the session is shadowed from the management console. [#LA5165]

System Exceptions

- Citrix Workspace app might fail if you enable PersistentCacheSize. [#LC0528]

Miscellaneous

- Current tarball and RPM packages fail to integrate with GStreamer on recent Fedora, Red Hat, and CentOS AMD (x86_64) distributions. [#LA4212]
- If an x.509 Public Key Infrastructure (PKI) certificate with certain policy constraints is installed on NetScaler Gateway, starting an application by using Citrix Workspace App for Linux might fail with an SSL error 85.

  To start applications, you must set the following key in the All_Regions.ini file:
  [Network\SSL]
  EnableCertificatePolicyVerification=1

  [#LA5609]
- This feature enhancement adds support for SHA-2 certificates to Citrix Workspace App for Linux. [#LC0136]

Citrix Workspace for Linux 13.0

HDX MediaStream Windows Media Redirection

- With HDX RealTime enabled, the gst_read process can experience a slow memory leak over time as it redirects Web cam data. [#LA1933]

Keyboard

- When connecting from the Citrix Workspace App for Linux to a Windows 7 virtual desktop, the message “Caps Lock is on” on the Windows 7 logon screen might not reflect the accurate state of the Caps Lock key on the client until a character key is pressed. [#LA1784]
- When switching between local and published applications, the first key you press after pressing Ctrl is ignored or key other than the one you pressed can appear. [#LA3397]
- **Important**: Installing this fix on systems with Fix #LA1965 installed causes Fix #LA1965 to no longer work. Do not install this fix on systems where you installed and deem Fix #1965 necessary.

  Hotkeys, such as the Alt-Tab key combination, can fail to get passed through to the session and are instead interpreted by the client.

  From the description of Fix #LA1965:

  When connecting in non-seamless mode, the Citrix Workspace App for LINUX user might come across a gray screen flashing (for about one second) before a published desktop or application appears.

  [#LA3660]
- When a published application is configured to run a macro on one of the LED keys (Caps Lock, Num Lock, or Scroll Lock), pressing the key can cause the macro to run multiple times.

  To enable this fix, add the entry “BypassSetLED=True” to the [WFClient] section of the wfclient.ini file located in the ~/.ICAClient folder. If the ~/.ICAClient folder is not present, modify the /opt/Citrix/ICAClient/nls/en/wfclient.ini file instead.

  [#LA3825]
- When using the Japanese version of the Citrix Workspace app in a virtual desktop session, the state of the Caps Lock key on the IME bar can be incorrect while pressing the Shift+Eisu keys. [#LA4072]
- When using the Citrix Workspace app in a virtual desktop session with the Japanese IME installed and selected on the VDA, there can be inconsistencies between the state of the Caps Lock key on the IME bar and the endpoint while pressing the Shift+Eisu keys. [#LA4422]

Session/Connection

- In a multi-monitor environment, the Citrix Workspace app might set the size of a maximized window incorrectly in a secondary monitor. As a result, the window size can be larger than the monitor size. [#LA0663]

- When starting IBM Lotus Notes with any other published application (for example, Microsoft Excel), within a session attempts to open an attachment can cause the attachment window to be updated incorrectly, and appear on top of other windows. This can result in instances of other windows that appear as a black (or other background color) rectangle. [#LA1490]
- With time zone redirection enabled, the time as displayed and applied in the session might be accurate as designed. However, when attempting to open Date and Time on the Control Panel, the following error message appears:

  "Your current time zone is not recognized. Please select a valid time zone using the link below."

  [#LA1828]
- On systems with the IceWM window manager installed, the **-span o** command fails to span the session across two monitors. Instead, the session is shown on just one of the monitors. [#LA2178]
- Attempts to open a file whose name contains the 5C - Yen symbol (Shift-JIS encoded) from a client-side mapped USB device might fail. [#LA2183]
- This fix extends the SucConnTimeout setting so that it is honored not only by published applications but also by published desktops. As a result, multiple desktop starts wait for the number of seconds specified by the SucConnTimeout before proceeding.

  To modify the SucConnTimeout value:

  Edit the [WFClient] section of the ~/.ICAClient/wfclient.ini file as follows:

  ```
  [WFClient]
  Version=2

  SucConnTimeout=60
  KeyboardLayout=(User Profile)
  KeyboardMappingFile=automatic.kbd
  KeyboardDescription=Automatic (User Profile)
  ```

  If the ~/.ICAClient/ folder is not present in the user's home directory, modify the /opt/Citrix/ICAClient/nls/en/wfclient.ini file as shown above. The file will be copied into the ~/.ICAClient folder when the user connects for the first time. Also, you can add ApplySucConnTimeoutToDesktops=True to the same section as SucConnTimeout if required.

  [#LA2679]
- Attempts to start a published application from the Citrix Workspace app using domain credentials with Centrify might fail. [#LA3270]
- This enhancement allows the Citrix Workspace app to read and write to files on mapped client drives that use the XFS file system. [#LA3610]

- When switching from workspace A to workspace B and back to workspace A, the focus is not restored to the last window that had focus on that workspace.

  Note: This fix resolves the issue for KDE, Xfce, and Gnome desktop environments. It does not work for Unity desktops.

  [#LA3432]

- Using pnabrowse in a multiple domain environment might fail while using an alternate domain for user authentication. The issue occurs because the original code implementation separates user name and domain. As a result, using pnabrowse with an alternate domain does not work.

  For example, a user can be referenced as user1@this.company or as user1@this.local (where the primary domain is *this.company* and the alternate domain is *this.local*). This fix ensures that both of the following work:

  > ./pnabrowse -L desk -U user1 -D this.company -P company123 <*IP address*>
  >
  > ./pnabrowse -L desk -U user1@this.local -P company123 <*IP address*>

  [#LA3551]

- Custom virtual channels might fail to initialize after an automatic reconnect by Citrix Workspace App for Linux. [#LA3572]

- Even if the “Automatically move pointer to the default button in a dialog box” option (the feature that helps to move the mouse pointer to the default button when a dialog box is open) is enabled on the server, the feature might fail to work within a published application using Citrix Workspace app. [#LA4285]

- The right-hand edge and the lower portion of certain Java application windows (for example, jEdit) in seamless mode might fail to redraw properly when moved or restored.

  To enable the fix, add the entry “TWISetFocusBeforeRestore=True” in the [WFClient] section of the $HOME/.ICAClient/wfclient.ini file.

  [#LA4450]

- USB device redirection can be slow in Citrix Workspace App for Linux in NetScaler deployments. [#LA4549]

- When dragging a published application window (for example, Token 2) anywhere but by its title bar, the seamless application window might get minimized.

  To enable the fix, add the entry “TWIMoveResizeHideWindowType=2” to the [WFClient] section of the wfclient.ini file.

  [#LA4737]

System Exceptions

- Setting CommPollSize=On in module.ini can cause the wfica.exe process to exit unexpectedly. [#LA2155]
- Attempts to print from a Java based application in a published desktop can cause the Citrix Workspace app to exit unexpectedly. [#LA3321]
- The Citrix Workspace app can exit unexpectedly while pasting a large amount of data from the clipboard. [#LA3608]
- The Citrix Workspace app can exit unexpectedly. The issue can occur when a published application contains more than 50 Chinese language characters in the title bar. [#LA4119]

User Experience

- If you press the ALT key while dragging a published application window anywhere but by its title bar, the window contents do not move in unison with the window outline. Further, when you release the mouse button, the dragging motion just completed repeats. [#LA0837]
- The mouse pointer can be positioned in an incorrect location when maximizing the secondary monitor window. Menus and buttons might be incorrectly activated while hovering the mouse pointer over them. The issue occurs if the secondary monitor has a smaller vertical pixel resolution than the primary monitor.

  For example: Monitor 1 is set to 1920x1080 and Monitor 2 to 1280x1024 pixels. When you start a published application on Monitor 1 and then drag and maximize the application on Monitor 2, the mouse pointer might be positioned about one centimeter away from any target button. As a result, a tooltip pop-up can appear for the Maximize button when the pointer is a centimeter away from the button.

  [#LA2071]
- When a pop-up menu pertaining to a notification area icon of a seamless published application is dismissed, the area of the pop-up menu is not properly redrawn and a portion of the menu content is still visible. [#LA4139]

User Interface

- This enhancement to the pnabrowse utility allows for the display of higher resolution icons for published resources. [#LA1994]
- A taskbar entry named “Untitled Window” can appear when expanding a drop-down menu in a published application. [#LA3422]

Miscellaneous

- This is an enhancement that allows you to limit USB redirection from a given client on a per-user basis. To limit USB direction to a specific user, run the following commands on the client as a root user or administrator:

  1. Remove the setuid bit from the ctxusb binary:

     ```
     # chmod u-s /opt/Citrix/ICAClient/ctxusb
     ```

  2. Insert a USB device and locate the device in the file system using:

     ```
     # ls  - lR /dev/bus/usb
     ```

  3. Assign user permissions (for example, to user1), where /dev/bus/usb/001/041 is determined to be the USB device in Step 2:

     ```
     # chown user1 /dev/bus/usb/001/041
     ```

     [#LA1952]

- Integrating the GStreamer (a third-party application) with the Citrix Workspace App for Linux might fail for Version 12.04 of Ubuntu.

  [#LA2016]

- On 64-bit systems, for example the Ubuntu 64-bit distribution, the hdxcheck.sh script fails to locate the 32-bit versions of the following libraries - libpcsclite.so, libcrypto.so, libjpeg.so, libldapsdk.so, and libcap.so, resulting in the following warning messages:

  “Warning! - libpcsclite.so missing, check that the file exists.
  Warning! - libcrypto.so is not installed. This is required if you use NTLM proxies.
  Warning! - libjpeg.so is not installed! This is needed for Speedscreen Image and Browser Acceleration.
  Warning! - libldapsdk.so is not installed! This is only needed if you use Novell Netware Services.
  A compatible version of libcap could not be located!”

  The issue occurs because the script attempts to locate those libraries only under /user/lib. In 64-bit Linux distributions, the 32-bit versions of those libraries can be installed under /usr/lib/i386-linux-gnu or /lib/i386-linux-gnu/. With this fix, the script also attempts to locate the libraries under /lib. If the attempts are successful, the following messages appear instead of the warning messages:

  “Success! - Libpcsclite.so installed. Smartcard support enabled.
  Success! All OS dependencies found!
  A compatible version of libcap is installed!”

[#LA2204]

- This feature enhancement introduces support of the playbin2 open-source multimedia framework on the HP T510. To enable playbin2 support, you must set the following options in the All_Regions.ini file:

  SpeedScreenMMAClosePlayerOnEOS=True
  SpeedScreenMMAEnablePlaybin2=True

  [#LA2566]

- This fix addresses a number of issues found with #LA2566, a feature enhancement that introduces support of the playbin2 open-source multimedia framework on the HP T510. [#LA2757]

Known issues

February 20, 2019

Known issues in Citrix Receiver for Linux 13.10

The following known issues exist in this release:

- The StoreFront URL fails to be added if Citrix Receiver for Linux is installed in a custom localized path that contains one or more 4-byte characters.

  [RFLNX-613]

- When you upgrade Citrix Receiver, new settings cannot be added to the $HOME/.ICAClient/All_Regions.ini file. The issue occurs because a user's $HOME/.ICAClient/All_Regions.ini is created from a template on the user's first launch of a session. There is no attempt to modify the user's personal All_Regions.ini configuration on upgrade. This means that any new entries added to the All_Regions.ini template are not automatically added to an existing user's All_Regions.ini file, and new entries are blocked by default.

  As a workaround, if you have not modified the original $HOME/.ICAClient/All_Regions.ini, delete this file. Upgrading creates a new All_Regions.ini file. If you have modified this file, move it to a backup location. Make a connection to cause All_Regions.ini to be generated using the latest template. Then compare your version with the new $HOME/.ICAClient/All_Regions.ini file, using tools such as diff and meld, and bring across your personal configuration.

  [RFLNX-706]

- With HDX MediaStream Windows media redirection with GStreamer1.0 enabled, OpenGL can cause unexpected pop-up windows to appear on some platforms.

[RFLNX-949]

- With HDX MediaStream Windows media redirection with GStreamer1.4 or later enabled, in Fetch mode on the server side, some multimedia files (type MPG1, MPEG2, and H264) fail to play back.

  [RFLNX-952]

- On a device with CPU frequency scaling such as the Raspberry Pi, if you are experiencing stutters in audio or general performance issues, Citrix recommends that you set the scaling governor to performance mode. To see your current performance governor for each core, run the following command, where <c> is the core"

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  By default, this setting is an on-demand setting, and not always dynamic enough to provide the real-time performance you need.
  To set the scaling governor to performance mode, run the following command as root:

  echo performance > /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Repeat this command for each core <c>.

  [RFLNX-1003]

- The hardware-accelerated H264 decoder plug-in for the HDX Ready Pi does not operate correctly if you change the frame buffer resolution with the framebuffer_width and framebuffer_height parameters in the /boot/config.txt file. As a workaround, change the Pi's resolution with the hdmi_group and hdmi_mode parameters.

  [RFLNX-1049]

- Installing the tar.gz version of Citrix Receiver results in an invalid group error. The error occurs because the operating system does not have a group called "sys" and the following error message appears:

  "chgrp: invalid group: sys"

  As a workaround, run setupwfc with HOST_SYS_GROUP_NAME set to the desired group.

  HOST_SYS_GROUP_NAME=<group> ./setupwfc

  Then enter a group name for the installed files.

  [RFLNX-1377]

- Attempts to make a UDT connection fail if your network maximum transmission unit (MTU) is lower than 1500.

  As a workaround, reduce the size of the UDP packets generated. To do this, reduce the size of udtMSS sufficiently so that the generated UDP packets can be sent over your MTU network. For more information, see Knowledge Center article CTX224373.

[RFLNX-1390]

- The bandwidth estimate can fail to update with adaptive transport connections. The implications of this are misbehavior of any features that rely on an accurate read of the session bandwidth. For example:
  - Overall session throughput being lower than expected, or in the event of a change in network conditions after the session is established (reduction in available bandwidth), the client might try to send more data than the network can actually handle.
  - Incorrect or inappropriate encoded bit rate of H264 graphics.
  - Misbehavior of MediaStream transcoding feature.

[RFLNX-1408]

- Live streaming videos might not play in the overlay browser when using browser content redirection.
  Workaround: Install the latest version of WebKitGTK.

  [RFLNX-1589]

- User certificates and smart card authentication fail for Citrix Receiver for Linux when NetScaler Gateway is configured with SAML authentication.

  [RFLNX-2085], [RFLNX-2084]

- The pop-up message “Session layout saved successfully” is truncated when the session is in full-screen mode. This issues appears in the Japanese, French, and Spanish languages.

  [RFLNX-2114]

Known issues in Citrix Receiver for Linux 13.9.x

The following known issues exist in this release:

- The StoreFront URL fails to be added if Citrix Receiver for Linux is installed in a custom localized path that contains one or more 4-byte characters.

  [RFLNX-613]

- When you upgrade Citrix Receiver, new settings cannot be added to the $HOME/.ICAClient/All_Regions.ini file. The issue occurs because a user’s $HOME/.ICAClient/All_Regions.ini is created from a template on the user’s first launch of a session. There is no attempt to modify the user’s personal All_Regions.ini configuration on upgrade. This means that any new entries added to the All_Regions.ini template are not automatically added to an existing user’s All_Regions.ini file, and new entries are blocked by default.

  As a workaround, if you have not modified the original $HOME/.ICAClient/All_Regions.ini, delete this file. Upgrading creates a new All_Regions.ini file. If you have modified this file, move it to

a backup location. Make a connection to cause All_Regions.ini to be generated using the latest template. Then compare your version with the new $HOME/.ICAClient/All_Regions.ini file, using tools such as diff and meld, and bring across your personal configuration.

[RFLNX-706]

- With HDX MediaStream Windows media redirection with GStreamer1.0 enabled, OpenGL can cause unexpected pop-up windows to appear on some platforms.

  [RFLNX-949]

- With HDX MediaStream Windows media redirection with GStreamer1.4 or later enabled, in Fetch mode on the server side, some multimedia files (type MPG1, MPEG2, and H264) fail to play back.

  [RFLNX-952]

- On a device with CPU frequency scaling such as the Raspberry Pi, if you are experiencing stutters in audio or general performance issues, Citrix recommends that you set the scaling governor to performance mode. To see your current performance governor for each core, run the following command, where <c> is the core"

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  By default, this setting is an on-demand setting, and not always dynamic enough to provide the real-time performance you need.
  To set the scaling governor to performance mode, run the following command as root:

  echo performance > /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Repeat this command for each core <c>.

  [RFLNX-1003]

- The hardware-accelerated H264 decoder plug-in for the HDX Ready Pi does not operate correctly if you change the frame buffer resolution with the framebuffer_width and framebuffer_height parameters in the /boot/config.txt file. As a workaround, change the Pi's resolution with the hdmi_group and hdmi_mode parameters.

  [RFLNX-1049]

- Installing the tar.gz version of Citrix Receiver results in an invalid group error. The error occurs because the operating system does not have a group called "sys" and the following error message appears:

  "chgrp: invalid group: sys"

  As a workaround, run setupwfc with HOST_SYS_GROUP_NAME set to the desired group.

  HOST_SYS_GROUP_NAME=<group> ./setupwfc

  Then enter a group name for the installed files.

[RFLNX-1377]

- Attempts to make a UDT connection fail if your network maximum transmission unit (MTU) is lower than 1500.

  As a workaround, reduce the size of the UDP packets generated. To do this, reduce the size of udtMSS sufficiently so that the generated UDP packets can be sent over your MTU network. For more information, see Knowledge Center article CTX224373.

  [RFLNX-1390]

- The bandwidth estimate can fail to update with adaptive transport connections. The implications of this are misbehavior of any features that rely on an accurate read of the session bandwidth. For example:
  - Overall session throughput being lower than expected, or in the event of a change in network conditions after the session is established (reduction in available bandwidth), the client might try to send more data than the network can actually handle.
  - Incorrect or inappropriate encoded bit rate of H264 graphics.
  - Misbehavior of MediaStream transcoding feature.

[RFLNX-1408]

- Live streaming videos might not play in the overlay browser when using browser content redirection.
  Workaround: Install the latest version of WebKitGTK.

  [RFLNX-1589]

Known issues in Citrix Receiver for Linux 13.8

The following known issues exist in this release:

- The StoreFront URL fails to be added if Citrix Receiver for Linux is installed in a custom localized path that contains one or more 4-byte characters.

  [RFLNX-613]

- When you upgrade Citrix Receiver, new settings cannot be added to the $HOME/.ICAClient/All_Regions.ini file. The issue occurs because a user's $HOME/.ICAClient/All_Regions.ini is created from a template on the user's first launch of a session. There is no attempt to modify the user's personal All_Regions.ini configuration on upgrade. This means that any new entries added to the All_Regions.ini template are not automatically added to an existing user's All_Regions.ini file, and new entries are blocked by default.

  As a workaround, if you have not modified the original $HOME/.ICAClient/All_Regions.ini, delete this file. Upgrading creates a new All_Regions.ini file. If you have modified this file, move it to

a backup location. Make a connection to cause All_Regions.ini to be generated using the latest template. Then compare your version with the new $HOME/.ICAClient/All_Regions.ini file, using tools such as diff and meld, and bring across your personal configuration.

[RFLNX-706]

- With HDX MediaStream Windows media redirection with GStreamer1.0 enabled, OpenGL can cause unexpected pop-up windows to appear on some platforms.

  [RFLNX-949]

- With HDX MediaStream Windows media redirection with GStreamer1.4 or later enabled, in Fetch mode on the server side, some multimedia files (type MPG1, MPEG2, and H264) fail to play back.

  [RFLNX-952]

- On a device with CPU frequency scaling such as the Raspberry Pi, if you are experiencing stutters in audio or general performance issues, Citrix recommends that you set the scaling governor to performance mode. To see your current performance governor for each core, run the following command, where <c> is the core"

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  By default, this setting is an on-demand setting, and not always dynamic enough to provide the real-time performance you need.
  To set the scaling governor to performance mode, run the following command as root:

  echo performance > /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Repeat this command for each core <c>.

  [RFLNX-1003]

- The hardware-accelerated H264 decoder plug-in for the HDX Ready Pi does not operate correctly if you change the frame buffer resolution with the framebuffer_width and framebuffer_height parameters in the /boot/config.txt file. As a workaround, change the Pi's resolution with the hdmi_group and hdmi_mode parameters.

  [RFLNX-1049]

- Installing the tar.gz version of Citrix Receiver results in an invalid group error. The error occurs because the operating system does not have a group called "sys" and the following error message appears:

  "chgrp: invalid group: sys"

  As a workaround, run setupwfc with HOST_SYS_GROUP_NAME set to the desired group.

  HOST_SYS_GROUP_NAME=<group> ./setupwfc

  Then enter a group name for the installed files.

[RFLNX-1377]

- Attempts to make a UDT connection fail if your network maximum transmission unit (MTU) is lower than 1500.

  As a workaround, reduce the size of the UDP packets generated. To do this, reduce the size of udtMSS sufficiently so that the generated UDP packets can be sent over your MTU network. For more information, see Knowledge Center article CTX224373.

  [RFLNX-1390]

- The bandwidth estimate can fail to update with adaptive transport connections. The implications of this are misbehavior of any features that rely on an accurate read of the session bandwidth. For example:
  - Overall session throughput being lower than expected, or in the event of a change in network conditions after the session is established (reduction in available bandwidth), the client might try to send more data than the network can actually handle.
  - Incorrect or inappropriate encoded bit rate of H264 graphics.
  - Misbehavior of MediaStream transcoding feature.

[RFLNX-1408]

- The Citrix Receiver for Linux incorrectly reports to the VDA that the client address is the address of the server.

  [RFLNX-1735]

- Enlightened Data Transport (EDT) sessions can become unresponsive intermittently during logoff.

  [RFLNX-1740]

Known issues in Citrix Receiver for Linux 13.7

The following known issues exist in this release:

- The StoreFront URL fails to be added if Citrix Receiver for Linux is installed in a custom localized path that contains one or more 4-byte characters.

  [RFLNX-613]

- When you upgrade Citrix Receiver, new settings cannot be added to the $HOME/.ICAClient/All_Regions.ini file. The issue occurs because a user's $HOME/.ICAClient/All_Regions.ini is created from a template on the user's first launch of a session. There is no attempt to modify the user's personal All_Regions.ini configuration on upgrade. This means that any new entries added to the All_Regions.ini template are not automatically added to an existing user's All_Regions.ini file, and new entries are blocked by default.

As a workaround, if you have not modified the original $HOME/.ICAClient/All_Regions.ini, delete this file. Upgrading creates a new All_Regions.ini file. If you have modified this file, move it to a backup location. Make a connection to cause All_Regions.ini to be generated using the latest template. Then compare your version with the new $HOME/.ICAClient/All_Regions.ini file, using tools such as diff and meld, and bring across your personal configuration.

[RFLNX-706]

- With HDX MediaStream Windows media redirection with GStreamer1.0 enabled, OpenGL can cause unexpected pop-up windows to appear on some platforms.

  [RFLNX-949]

- With HDX MediaStream Windows media redirection with GStreamer1.4 or later enabled, in Fetch mode on the server side, some multimedia files (type MPG1, MPEG2, and H264) fail to play back.

  [RFLNX-952]

- On a device with CPU frequency scaling such as the Raspberry Pi, if you are experiencing stutters in audio or general performance issues, Citrix recommends that you set the scaling governor to performance mode. To see your current performance governor for each core, run the following command, where <c> is the core”

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  By default, this setting is an on-demand setting, and not always dynamic enough to provide the real-time performance you need.
  To set the scaling governor to performance mode, run the following command as root:

  echo performance > /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Repeat this command for each core <c>.

  [RFLNX-1003]

- The hardware-accelerated H264 decoder plug-in for the HDX Ready Pi does not operate correctly if you change the frame buffer resolution with the framebuffer_width and framebuffer_height parameters in the /boot/config.txt file. As a workaround, change the Pi’s resolution with the hdmi_group and hdmi_mode parameters.

  [RFLNX-1049]

- Installing the tar.gz version of Citrix Receiver results in an invalid group error. The error occurs because the operating system does not have a group called “sys” and the following error message appears:

  “chgrp: invalid group: sys”

  As a workaround, run setupwfc with HOST_SYS_GROUP_NAME set to the desired group.

  HOST_SYS_GROUP_NAME=<group> ./setupwfc

Then enter a group name for the installed files.

[RFLNX-1377]

- Attempts to make a UDT connection fail if your network maximum transmission unit (MTU) is lower than 1500.

  As a workaround, reduce the size of the UDP packets generated. To do this, reduce the size of udtMSS sufficiently so that the generated UDP packets can be sent over your MTU network. For more information, see Knowledge Center article CTX224373.

  [RFLNX-1390]

- The bandwidth estimate can fail to update with adaptive transport connections. The implications of this are misbehavior of any features that rely on an accurate read of the session bandwidth. For example:

  - Overall session throughput being lower than expected, or in the event of a change in network conditions after the session is established (reduction in available bandwidth), the client might try to send more data than the network can actually handle.
  - Incorrect or inappropriate encoded bit rate of H264 graphics.
  - Misbehavior of MediaStream transcoding feature.

[RFLNX-1408]

Known issues in Citrix Receiver for Linux 13.6

The following known issues exist in this release:

- The StoreFront URL fails to be added if Citrix Receiver for Linux is installed in a custom localized path that contains one or more 4-byte characters.

  [RFLNX-613]

- When you upgrade Citrix Receiver, new settings cannot be added to the $HOME/.ICAClient/All_Regions.ini file. The issue occurs because a user's $HOME/.ICAClient/All_Regions.ini is created from a template on the user's first launch of a session. There is no attempt to modify the user's personal All_Regions.ini configuration on upgrade. This means that any new entries added to the All_Regions.ini template are not automatically added to an existing user's All_Regions.ini file, and new entries are blocked by default.

  As a workaround, if you have not modified the original $HOME/.ICAClient/All_Regions.ini, delete this file. Upgrading creates a new All_Regions.ini file. If you have modified this file, move it to a backup location. Make a connection to cause All_Regions.ini to be generated using the latest template. Then compare your version with the new $HOME/.ICAClient/All_Regions.ini file, using tools such as diff and meld, and bring across your personal configuration.

[RFLNX-706]

- With HDX MediaStream Windows media redirection with GStreamer1.0 enabled, OpenGL can cause unexpected pop-up windows to appear on some platforms.

  [RFLNX-949]

- With HDX MediaStream Windows media redirection with GStreamer1.4 or later enabled, in Fetch mode on the server side, some multimedia files (type MPG1, MPEG2, and H264) fail to play back.

  [RFLNX-952]

- On a device with CPU frequency scaling such as the Raspberry Pi, if you are experiencing stutters in audio or general performance issues, Citrix recommends that you set the scaling governor to performance mode. To see your current performance governor for each core, run the following command, where <c> is the core"

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  By default, this setting is an on-demand setting, and not always dynamic enough to provide the real-time performance you need.
  To set the scaling governor to performance mode, run the following command as root:

  echo performance > /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Repeat this command for each core <c>.

  [RFLNX-1003]

- The hardware-accelerated H264 decoder plug-in for the HDX Ready Pi does not operate correctly if you change the frame buffer resolution with the framebuffer_width and framebuffer_height parameters in the /boot/config.txt file. As a workaround, change the Pi's resolution with the hdmi_group and hdmi_mode parameters.

  [RFLNX-1049]

- Installing the tar.gz version of Citrix Receiver results in an invalid group error. The error occurs because the operating system does not have a group called "sys" and the following error message appears:

  "chgrp: invalid group: sys"

  As a workaround, run setupwfc with HOST_SYS_GROUP_NAME set to the desired group.

  HOST_SYS_GROUP_NAME=<group> ./setupwfc

  Then enter a group name for the installed files.

  [RFLNX-1377]

- Attempts to make a UDT connection fail if your network maximum transmission unit (MTU) is lower than 1500.

As a workaround, reduce the size of the UDP packets generated. To do this, reduce the size of udtMSS sufficiently so that the generated UDP packets can be sent over your MTU network. For more information, see Knowledge Center article CTX224373.

[RFLNX-1390]

- The bandwidth estimate can fail to update with adaptive transport connections. The implications of this are misbehavior of any features that rely on an accurate read of the session bandwidth. For example:
  - Overall session throughput being lower than expected, or in the event of a change in network conditions after the session is established (reduction in available bandwidth), the client might try to send more data than the network can actually handle.
  - Incorrect or inappropriate encoded bit rate of H264 graphics.
  - Misbehavior of MediaStream transcoding feature.

[RFLNX-1408]

Known issues in Citrix Receiver for Linux 13.5

The following known issues have been observed in this release:

- The StoreFront URL fails to be added if Citrix Receiver for Linux is installed in a custom localized path that contains one or more 4-byte characters.

  [RFLNX-613]

- With HDX MediaStream Windows media redirection with GStreamer1.0 enabled, OpenGL can cause unexpected pop-up windows to appear on some platforms.

  [RFLNX-949]

- With HDX MediaStream Windows media redirection with GStreamer1.4 or later enabled, in Fetch mode on the server side, some multimedia files (type MPG1, MPEG2, and H264) fail to play back.

  [RFLNX-952]

- On a device with CPU frequency scaling such as the Raspberry Pi, if you are experiencing stutters in audio or general performance issues, Citrix recommends that you set the scaling governor to performance mode. To see your current performance governor for each core, run the following command, where <c> is the core”

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  By default, this setting is an on-demand setting, and not always dynamic enough to provide the real-time performance you need.
  To set the scaling governor to performance mode, run the following command as root:

echo performance > /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

Repeat this command for each core <c>.

[RFLNX-1003]

- The hardware-accelerated H264 decoder plug-in for the HDX Ready Pi does not operate correctly if you change the frame buffer resolution with the framebuffer_width and framebuffer_height parameters in the /boot/config.txt file. As a workaround, change the Pi's resolution with the hdmi_group and hdmi_mode parameters.

  [RFLNX-1049]

Known issues in Citrix Receiver for Linux 13.4

The following known issues have been observed in this release:

- Cannot reduce a fullscreen session to windowed mode using the Desktop Viewer toolbar when using the '-span o' argument to override the session window redirect.

  To resolve this issue, do not use the '-span o' option. Use a window manager with _NET_WM_FULLSCREEN_MONITORS support or disable Desktop Viewer instead.

  [#634855]

- The secondary session might not pop up when clicking its name under the Switch button on Desktop Viewer.

  [#648716]

- Receiver for Linux becomes unresponsive indefinitely when switching from X1 UI to Classic UI.

  If the self-service UI displays the error "NoWebUI 0," restart the self-service process to revert the self-service UI to normal.

  [#652810]

- Flash Redirection uses the wrong location with multi-monitor clients.

  When using Flash Redirection on a client with multiple monitors, Flash content can appear on the wrong monitor or off the screen. This can be avoided by ensuring the session is running on all available monitors before attempting to use the Flash Redirection feature.

  [#653550]

- Updating to this release can produce errors due to options dropped from All_Regions.ini.

  [#654826]

- HDX Webcam redirection is disabled for 45 seconds at startup.

To avoid this, add an entry to the [wfclient] section of ~/.ICAClient/wfclient.ini (or $ICAROOT/-config/module.ini) HDXRTMEWebCamLaunchDelayTime=0.

If you intend to use the RTME plug-in instead of HDX webcam redirection, do not change this value.

Known issues in Citrix Receiver for Linux 13.3

The following known issues have been observed in this release:

- Citrix Receiver does not recognize the PIV smartcard when starting a desktop for the first time.

  [#491235]

- Unclear error messages are displayed when Citrix Receiver cannot find the server immediately after it restarts.

  [#553886]

- An incorrect message dialog is displayed when the session reliability timer expires.

  [#556899]

- An error message (for example, “Unknown Error 1000047”) is displayed when connecting to the VDA with the SSLv3 protocol enabled.

  [#558641]

- A generic network error is displayed when connecting to a StoreFront server with the SSLv3 protocol enabled.

  [#558653]

- Changing SharedUserMode using storebrowse, -c SharedUserMode[=value], requires exact case matching using the value parameter. When using the value parameter for storebrowse, -c SharedUserMode[=value], you must specify an exact case match using “True” or “False.” No error message is displayed if an invalid value parameter is used. For example, -c SharedUserMode=True.

  [#559402]

- When connecting to a terminal server (for example, RDS) with only the SSLv3 protocol enabled the connection fails as expected but it might not fail with a SSL peer handshake failure.

  [#567407] one space using the space bar

- Generic USB webcam input fails on 64-bit systems.

  [#568556]

- The storebrowse –d command does not delete previously cleared cached store information created by self-service. This means that if the store is subsequently added the self-service UI loads from the previous cached state.

  [#569806]

- New TLS values are not applied for connections to the StoreFront server using selfservice/storebrowse when TLS values are changed after the EULA (license) has been accepted. Note that a running AuthManager does not read a changed TLS setting.

  [#570725]

- Connection Center doesn't support IPv6.

  [#571743]

- When specifying a negative value to an integer config entry such as TCPRecvBufferSize in $HOME/.ICAClient/All_Regions.ini, the value is erroneously passed to WFICA as a positive value. To resolve this issue, use $ICAROOT/config/module.ini to set a negative value for TCPRecvBufferSize.

  [#575474]

- GStreamer helper processes display a warning related to a GLIB threading issue.

  [#580753]one space using the space bar

- The ARMEL browser plug-in does not work at this release.

  [#588044]

- If you experience problems with time zones not correctly mapping with XenApp and XenDesktop 7.6 sessions, ensure that you have the hotfix referenced in CTX142640, and follow the steps for entry 7 [From ICATS760WX64014]. If that does not resolve the issue, try changing /etc/timezone (or /etc/localtime if /etc/timezone is not present) to be a symlink to a city name under /usr/share/zoneinfo/…

  If your time zone is still not supported, you might need to raise a support ticket to have a mapping added to the server.

  [#LC1061, #606648]

- In the Platform Optimization SDK, the plug-ins for non-X11 environments possess two issues:
  - Sessions to Windows servers for XenDesktop 7.x fail if session reliability is used.
  - Sessions with 16-bit color depth show video corruption.

These issues exist in both the SDL Library-based SDL_plugin and the raw kernel Framebuffer-based FB_plugin sample plug-in implementations. Any further plug-ins developed by the user can expect to suffer these same issues.

Known issues in Citrix Receiver for Linux 13.2.1

The following known issues have been observed in this release:

- The ARMEL browser plug-in (used for launching sessions from a web browser) fails to launch, preventing the user from launching a session. To resolve this, use the browser settings to disable the plug-in, which allows a fallback mechanism to take over.

  [#580782]

- When running on SLED 11sp3, launching storebrowse or selfservice from a terminal might cause several programs to produce errors saying "libidn.so.11: no version information available." This issue has little, if any, effect on the behavior of Citrix Receiver.

  [#582512]

- Flash redirection is not available on 64-bit clients. If this capability is important in your environment, contact the Citrix Product Management team or alternately use the support forums for additional guidance.

  [#582627]

- Receiver fails to add favorite applications when selecting Add to Favorites in the Details view. This issue occurs when running SuSE SLED 11sp3 without installing updates. To avoid this issue, ensure that the package libwebkit-1_0-2 is version 1.2.7-0.17.1 (or greater).

  [#585295]

- A third-party issue occurs in the EPEL 2.2.4 version of libwebkitgtk+. Citrix recommends using the EPEL (Extra Packages for Enterprise Linux) repository as a method for getting the GTK+2 version of libwebkitgtk on RedHat 7 and Centos 7. However, an issue with the provided EPEL version occurs when Japanese/Chinese characters are used in the hosted application names on the server. As a result, Receiver cannot ensure a proper method for securing a stable libwebkitgtk build on RedHat 7 and Centos 7 suitable for APAC characters.

  [#586967]

- On some platforms, installing the client from a tarball distribution might cause the system to hang after prompting you to integrate with KDE and GNOME. This issue occurs with the first time initialization of gstreamer-0.10. If you encounter this issue, end the installation process (using ctrl+c) and run the following command: one space using the space bargst-inspect-0.10 – gst-disable-registry-fork –version. After executing this command, you are able to re-run the tarball setup without experiencing a system hang.

  [#587640]

- In some Gnome desktop environments, a client might experience a crash when starting the Microsoft Remote Desktop app (Mstsc). This issue occurs after connecting to a remote desktop.

After inserting login credentials, the session cannot be closed gracefully by clicking the 'X' symbol (an error indicating that "A problem has occurred and the system can't recover.")

[#587922]

- Windows media player displays an error message stating "Windows Media Player encountered a problem while playing the file"; this error condition can be dismissed by closing the error message, then clicking the Play icon.

  [#588009]

- Windows Media Player on a Windows 7 desktop might fail to play audio/video when started from a 64-bit Receiver. This issue occurs due to a known issue with Ubuntu 14.04; expected GStreamer components are not being installed. See the section "Windows Media Player fails to play files in certain formats" in theTroubleshooting topic.

  [#588298]

- Windows Media Player fails to play files in certain formats.

Known issues in Citrix Receiver for Linux 13.2

The following known issues have been observed in this release:

- A new script was added that creates client-server file type associations. This script, ctx_app_bind, allows you to use a published application to open a specific file type. This script accepts either the name of the published app, either an example file or a MIME type, and optionally allows you to include a server name or URL.
  For example:

  ctx_app_bind example_file published_app_name server
  ctx_app_bind application/some-mime-name published_app_name

  Use the –p option to use pnabrowse rather than storebrowse for the session launch.

  Note: Citrix recommends using care when executing this script. It has not been tested against all possible OS environments.

  [#558649]

- If a user is unable to connect to the store, you can enable connection logs on Receiver to troubleshoot the nature of the problem. To enable the collection of connection logs in Receiver:

1. Edit the /opt/citrix/ICAClient/config/AuthManConfig.xml with the following parameters as a user with administrator privileges:

   <!– TracingEnabled - true, false –>

<key>TracingEnabled</key>
<value>true</value>
<!– LoggingMode - none, normal, verbose –>
<key>LoggingMode</key>
<value>verbose</value>

2. Halt the following processes: AuthManagerDaemon, selfservice, ServiceRecord, storebrowse.
3. Start Receiver and connect to the store.
4. Check the logs under $HOME/.ICAClient/logs.

HDX RealTime Webcam Video Compression requires:

```
- A Video4Linux compatible Webcam

- GStreamer 0.10.25 (or a later 0.10.x version), including the
    distribution's "plugins-good" package
```

[#559817]

- When using Linux Receiver X1 to remove an app, the app persists and when logging out and returning to the store.

  [#561719]

Known issues in Citrix Receiver for Linux 13.1

The following known issues have been observed in this release:

- You cannot disconnect or log off virtual desktops from Connection Center. The Disconnect button is unavailable and the Log off button does not work. To work around this issue, disconnect or log off from the desktop session, not Connection Center. This issue is not observed with virtual applications.

  [#423651, #424847]

- An error appears if a user opens the self-service UI to connect to the StoreFront store, and then closes the Receiver for Linux window when the Authentication Manager dialog box is open.

  [#430193]

- Receiver for Linux does not allow connection to a non-secure StoreFront store `http://`. Depending on the configuration of the store, the user will either receive an error message of the form, "Error: Cannot retrieve discovery document" [], or the initial connection will be made over HTTP, but further communications will switch to https. Alternatively, if you use the IP address for the hostname you might see errors referring to Citrix XenApp Services (formerly PNAgent).

Either explicitly use `https://` or do not prefix the server name with `http://` when entering the URL.

[#473027, #478667 and #492402]

- Receiver for Linux does not support logging on with a smart card that contains multiple authentication certificates.

  [#488614]

- If Receiver for Linux gives a segmentation fault when accessing smart cards, this might be due to a problem with the PKCS#11 library. You can check the library with the pkcs11-tool utility. The pkcs11-tool utility is part of the opensc package. An example test is:

  pkcs11-tool –module /usr/lib/libgtop11dotnet.so -

  If this also gives a segmentation fault, you must contact the supplier of the driver. You can also try a driver from another source for the same type of card. This problem has been seen with the Gemalto .NET driver included in Fedora 19 and Fedora 20.

  [#493172]

- Receiver for Linux supports multiple card readers; however only one smart card can be used at a time.

  [#494524]

- The host name of the Linux machine must be 20 characters or less for connections to work. This setting can be examined and set by using the hostname command. Any user can examine the hostname, but to set the hostname, you need to be the root user or have administrator privileges.

  [#494740]

- When working with XenDesktop in full screen mode in Receiver for Linux 13.x, the local screensaver might not activate. This is a third-party issue, and the behavior might vary depending on the client operating system.

  [#496398]

- If you insert the wrong smart card when trying to connect to a StoreFront store, you might see an error message such as “protocol error” or “Specified store not found,” which does not explain the issue.

  [#496904]

- On some low-performance devices in a full screen session, the logon process with smart card authentication might take longer than expected and a timeout occurs. You might be able to prevent this issue by disabling use of H264. To disable the use of H624, do the following:

  1. Open the wfclient.ini file.

2. Locate the “Thinwire3.0” section.
3. Add the entry “H264Enabled=False”.

This issue has been seen on a machine based on armhf (ARM hard float), without hardware accelerated H264.

[#497720]

- If a PNAgent server allows the user to change expired passwords by contacting the Domain controller directly, you can only do this with the MIT compatible version of the library, libkcpm.so. This is due to issues with the Heimdal compatible version. This restriction applies to x86, armel and x64 (which uses the x86 pnabrowse). It does not apply to armhf.

  [#498037]

- Receiver for Linux requires libpng12.so, however this is not normally available in the standard repositories for Fedora-based systems. In this case, please find a suitable RPM for your system on the internet. For openSUSE, libpng12.so is available, however it must be installed separately.

  [#501937]

- A hotfix for 12.1 added a pnabrowse exit code E_SSLSDK_PASSWORD_LOCKED with the value 220. This changed the exit code E_PASSWORD_EXPIRED to 239 from its documented value of 238. In 13.0, the value for E_SSLSDK_PASSWORD_LOCKED was changed to 240, restoring the correct value of E_PASSWORD_EXPIRED. However, the values listed by pnabrowse -errno still show the uncorrected meanings for values 220 to 240.

  [#502550]

Known issues in Citrix Receiver for Linux 13

The following known issues have been observed in this release:

Installation issues

- libxerces-c 3.1 is a required component for this release. However, it is not available in some Linux distributions that use RPM packaging. If this component is missing in your distribution, locate it on a suitable website and add it to your Linux system installation.

  [#384324]

- For platforms that cannot meet the libxerces or libwebkitgtk system requirement (or both requirements), you can install Receiver using the tarball package, or force the installation of the Debian or RPM packages, and use the browser-based Receiver for web to start connections. For example, you cannot install the RPM package on CentOS systems because it requires

libwebkitgtk-1.0.so.0, which is not available in those environments. To work around this issue, install the package with –nodeps or one space using the space bar–force, or use the Tarball package instead. Then launch a browser and enter the URL to your Receiver for web store.

[#426176]

- You can use the RPM package to install Receiver on the 32-bit version of OpenSUSE 13.1, but it fails at runtime. To work around this issue, download and install the following RPM package first, and repeat the installation: `ftp://rpmfind.net/linux/opensuse/factory/repo/oss/suse/i586/libpng12-0-1.2.50-7.3.i586.rpm`.

  [#429879]

- After installing Receiver from the 64-bit RPM package in a 64-bit Fedora 19.1 environment, you must perform additional steps before using pnabrowse or the client engine, wfica, to launch connections. (These steps do fix storebrowse and selfservice, which cannot be made to function due to limitations in the version of curl in this environment.) To work around this issue:

1. Install the 32-bit libpng12 package using the following command:

   yum install libpng12.i686

2. To minimize the number of audio errors, install the 32-bit ALSA plug-in using the following command:

   yum install alsa-plugins-pulseaudio.i686

3. To minimize the number of GtK errors, install the following packages using the following commands:

   yum install adwaita-gtk2-theme.i686
   yum install PackageKit-gtk3-module.i686
   yum install libcanberra-gtk2.i686

4. To allow connections to be started from Firefox, install the plug-in nspluginwrapper.i686 and register it with the web browser using the following commands:

   yum install nspluginwrapper.i686
   mozilla-plugin-config

[#429886]

General issues

- Resuming audio playback might be noisy. The noise is present only when the audio is paused and then restarted, not when it is first played. This has been observed with XenDesktop connections involving the Remote PC Access feature. There is no workaround for this issue.

  [#308772]

- Some media types only play on the user device if the appropriate codec is available on the server even though GStreamer should be able to connect directly to the source of the media and play it using the decoders on the device. There is no workaround for this issue.

  [#339394]

- On Ubuntu 12.04 with the Gnome 3 desktop, notification area icons for published applications do not integrate with the native desktop. Instead, they appear in a separate notification area window. There is no workaround for this issue.

  [#395140]

- Linux users cannot use their email addresses to set up StoreFront stores. Users should instead add the URL of the required stores using the Accounts page of the Preferences dialog box. You can alternatively provide a provisioning file with account information that is used to create a new account.

  [#395394]

- Proxy support for the selfservice and storebrowse commands is not available by default. To use a proxy server with a StoreFront server, set the http_proxy environment variable before starting either command. Use the following format for the environment variable:

  <server_name>.<domain>[:<port>]

  [#403729]

- Client-to-server content redirection (dropping published content on to a desktop icon) does not work with the self-service user interface. There is no workaround for this issue.

  [#403739]

- The Security-Enhanced Linux (SELinux) security module in RedHat Fedora can affect the operation of the Client Drive Mapping and USB Redirection features (on both XenApp and XenDesktop). If you require either or both of these features, disable SELinux before configuring them on the server.

  [#413554]

- The HDX MediaStream Flash Redirection feature has not been tested on the ARM hard float (armhf) platform because, in this release, Receiver does not work with Flash plug-ins on that platform.

  [#414253]

- If you configure a webcam frame rate that is not supported by the webcam, it defaults to a different value, which might be higher than expected.

  [#414576]

- If, in Receiver, you set a non-default resolution for a webcam, it does not stream video the first time you use it with Citrix GoToMeeting. The webcam appears to be active and gst_read is running, but no image is displayed. To work around this issue, stop and restart the webcam in GoToMeeting.

  [#414878]

- If window decorations are not present in the desktop environment (for example, in the LXDE environment with decorations disabled), you might not be able to close self-service dialog boxes.

  [#416689]

- With some versions of XenApp or XenDesktop, after starting a desktop or application, you cannot check the server name used for a connection because no server is listed in Connection Center. To work around this issue, click Properties. The server name is displayed in the Properties dialog.

  [#417114]

- If, while logging on to Receiver, you enter your credentials after a delay of about five minutes, the self-service user interface (UI) does not display your applications. To work around this issue, select Refresh Apps from the drop-down menu in the UI and re-enter your credentials.

  [#417564]

- An administrator who shadows a user's session might notice display errors if their screen is smaller than that of the user device. For example, scrollbars might not fit on to the administrator's screen, and regions of the user's screen might be inaccessible. There is no workaround for this issue. In addition, resizing the shadowed session from the administrator's machine can black out the session on the user device. To work around this issue, click the Restore button in the session window on the administrator's machine (not the user device).

  [#418672, #418690]

- The self-service user interface and associated StoreFront components (Authentication Manager and the Service Record daemon) are not supported on Fedora because of library incompatibilities. Receiver installs without errors but does not work after installation. To work around this issue, start Receiver through web Interface (a legacy component) or web Receiver.

  [#419662]

- When many applications or desktops are subscribed to, the self-service user interface (UI) includes a scrollbar. This disappears (as expected) when the UI is resized to show all the application and desktop icons. However, the scrollbar is not redisplayed when the UI is then reduced in size. This issue has been observed only on Ubuntu 13.04. To work around it, click the Refresh menu option, repeat the resizing operation a few times, or stop and restart Receiver.

  [#422520]

- The first time a connection is made, you might notice a delay that varies significantly depending on the network. A connection using 3G will likely be slower than a connection using ADSL.

  [#423663]

- When you enter an HTTPS store address in the self-service user interface (UI), the following error message is displayed if no certificate is present: "Your account cannot be added using this server address. Ensure you enter it correctly." This error is displayed if the address is correct but no certificate is present. To work around this issue, install a certificate.

  [#423757, #424674]

- You can apply a XenDesktop policy to raise the maximum frame rate in Receiver sessions above 30 frames per second (FPS). However, this value is not honored and the frame rate in the sessions never exceeds this value because it is limited by the flow control feature. This issue has been observed in XenDesktop 7 and 7.1. To work around this issue, disable flow control.

  [#423950]

- To switch accounts (and access desktops and applications from a different store), you use the Accounts menu in the self-service user interface. This might not be obvious to users.

  [#424027]

- If you use storebrowse in multiple locales that are not encoded as UTF-8, some of the text in the logon dialog box might be corrupt. For example, in a Spanish locale there is no text on the Log on button. To work around this issue, switch to a UTF-8 locale (for example, by creating a wrapper script around storebrowse, and the Service Record and Authentication Manager daemon executables).

  [#424052]

- You cannot disconnect or log off virtual desktops from Connection Center. The Disconnect button is unavailable and the Log off button does not work. To work around this issue, disconnect or log off from the desktop session, not Connection Center. This issue is not observed with virtual applications.

  [#424847]

- When storebrowse is used to start a session to a virtual desktop in a group in which all desktops are turned off, an exit status value of 255 EXEC_FAILED is displayed (sometimes after a delay), indicating that the start has failed. However, instead of failing, the desktop is in fact starting or registering and will be available soon. To work around this issue, advise users who encounter it to try starting the desktop again, or ensure any startup script does likewise.

  [#425076, #425103]

- In the Japanese and Simplified Chinese versions of Receiver, keyboard shortcuts do not work in some dialog boxes.

[#425275, #425278, #425281, #425332]

- In the German, French, and Spanish versions of Receiver running on the Ubuntu platform, keyboard shortcuts are not visible in some dialog boxes but they are functional.

  [#425282, #425285, #425289, #425294, #425339]

- In the German version of Receiver, duplicate keyboard shortcuts are present in some dialog boxes.

  [#425284, #425338]

- The openssl tool c_rehash is used to import and hash root certificates that are used to secure communications with StoreFront. Some versions of c_rehash do not correctly handle certificates that contain MS-DOS-style line endings. If the output from c_rehash does not generate symbolic links for your certificate, you might need to convert the line endings to UNIX format. You can do this using the following tr command line:

  tr -d '\r' < root_certificate_name.pem > new_root_certificate_name.pem

  Then, run the c_rehash script against the new root certificate created from this command.

  [#425775]

- On Debian platforms, the ctxusbd daemon does not restart when the system restarts, causing USB redirection to fail. This is because the init script, /etc/init.d/ctxusbd, contains a variable,###INIT_UDEV###, which must expand to udev. To work around this issue, edit /etc/init.d/ctxusbd as follows. You must have root permissions to do so:

  sed -ie's,###INIT_UDEV###,udev,g' /etc/init.d/ctxusbd

  Then, manually rerun insserv (again, with root permissions):

  /sbin/insserv /etc/init.d/ctxusbd

  This issue has only been observed on Debian platforms.

  [#425810]

- When connecting to Program Neighborhood Agent sites, absent or expired certificates might cause the Receiver user interface to flash, prompt the user repeatedly for credentials, or consume high CPU. To work around this issue, Citrix recommends installing your certificates properly and maintaining them regularly. The issue is not observed when connecting to StoreFront sites.

  [#425848]

- Icons in the self-service user interface might not be displayed when new users search for applications or desktops. To work around this issue, click Refresh Apps.

  [#426364]

- When using pnabrowse to connect to an HTTPS-secured Program Neighborhood Agent site on some Microsoft Server 2012 servers in armhf (hard float) environments, a generic error message is displayed and the connection fails. This issue is not fully defined but might be because the servers have a FQDN ending in .local, or because the key size specified in the Public Key field of the certificate on the servers is 2,048 Bits not 1,024 Bits. This issue does not occur with storebrowse and has only been observed in armhf environments.

  [#426420]

- If you log off from Receiver (by clicking Log Off in the self-service user interface) but then try to connect to a desktop or application, and cancel when prompted for your credentials, the message "Cannot process request" is displayed. You can ignore the message. You were successfully logged off.

  [#426424]

- A segmentation fault occurs, and Receiver fails, when you use the self-service user interface for the first time to connect to a Program Neighborhood Agent site, click Cancel in the logon dialog box, click Refresh Apps, and close the Receiver window. There is no workaround for this issue.

  [#426625]

- Multiple processes that call data store or load procedures at the same time can lead to data loss in files that are in memory (for example, StoreCache.xml). The last change to a given file is preserved; earlier changes are lost. There is no danger of file corruption.

  [#426692]

- If you remove and then add a store, the Accounts page of the Preferences dialog box does not show the new store until you close and reopen the dialog box.

  [#426735]

- With the Reconnect apps and desktops preference set to When I start or refresh apps and with a connection to a desktop or application in progress, selecting Refresh Apps from the Receiver menu makes the user interface unresponsive until the connection is established.

  [#426761]

- No error message is displayed when you try to add a store or gateway that is already listed in Receiver. There is no workaround for this issue, but no duplicate entries are created and the existing store or gateway continues to function correctly.

  [#427379]

- Menus in published applications disappear when they are clicked. This has been observed with maximized application windows in GNOME 3 desktop environments on Ubuntu 12.04 but not in Unity environments on Ubuntu 12.04.3.

  [#429686]

- Caution: A limitation in Windows means that the volume level of audio is maximized when a session automatically reconnects after a network outage. There is no workaround for this issue.

  [#430160]

- Receiver preferences only affect new or reconnected sessions, not disconnected ones. For example, you can start Citrix GoToMeeting from a virtual desktop and then disconnect from the desktop session (but not GoToMeeting). You can then select Use my microphone and webcam on the Mic & Webcam page of the Preferences dialog box, but this does not start the webcam in the GoToMeeting session. To work around this issue, close and restart the affected session (in the example, this is the GoToMeeting session).

  [#430692]

- If selfservice is run from a terminal, and the terminal is closed before selfservice is, the standard quit signal is sent to all foreground processes hosted by the terminal. Other Linux Receiver processes such as the Service Record and Authentication Manager daemons do not ignore this signal but selfservice does. This can make selfservice unresponsive because the processes on which it relies are ended. To work around this issue, start the daemons using storebrowse in one window, and then, in a second window, run selfservice. This lets you close the terminal window running selfservice but the daemons continue to operate in the background, and the user interface remains responsive.

  [#430697]

System requirements

March 5, 2019

Devices

- Linux kernel version 2.6.29 or later, with glibcxx 3.4.15 or later, glibc 2.11.3 or later, gtk 2.20.1 or later, libcap1 or libcap2, and udev support.
- For the self-service user interface (UI):
  - libwebkit or libwebkitgtk 1.0
  - libxml2 2.7.8
  - libxerces-c 3.1
- ALSA (libasound2), Speex, and Vorbis codec libraries.

- At least 55 MB of free disk space for the installed version of Receiver. And at least 110 MB if you expand the installation package on the disk. You can check the available disk space by typing the following command in a terminal window:

  ```
  df -k
  ```

- At least 1 GB RAM for system-on-a-chip (SoC) devices that use HDX MediaStream Flash Redirection.
- 256 color video display or higher.
- TCP/IP networking.

H.264

For x86 devices, processor speeds of at least 1.6 GHz display single-monitor sessions well at typical resolutions (for example, 1280 x 1024). If you use the HDX 3D Pro feature, a native hardware accelerated graphics driver and a minimum processor speed of 2 GHz are required.

For ARM devices, a hardware H.264 decoder is required for both general H.264 support and HDX 3D Pro. Performance also benefits from faster processor clock speeds.

HDX MediaStream Flash Redirection

For all HDX MediaStream Flash Redirection requirements, see CTX134786.

Citrix recommends testing with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes.

Customer Experience Improvement Program (CEIP) integration

To ensure that CEIP works properly, the following libraries are required:

- zlib 1.2.3.3
- libtar 1.2 and above
- libjson 7.6.1 or any latest version

HDX RealTime Webcam Video Compression

HDX RealTime Webcam Video Compression requires:

- A Video4Linux compatible Webcam

- GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package.

  Or

  GStreamer 1.0 (or a later 1.x version), including the distribution's "plugins-base," "plugins-good," "plugins-bad," "plugins-ugly," and "gstreamer-libav" packages.

HDX MediaStream Windows Media Redirection

HDX MediaStream Windows Media Redirection requires:

- GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package. In general, version 0.10.15 or later is sufficient for HDX MediaStream Windows Media Redirection.

  Or

  GStreamer 1.0 (or a later 1.x version), including the distribution's "plugins-base," "plugins-good," "plugins-bad," "plugins-ugly," and "gstreamer-libav" packages.

  > **Note:** If GStreamer is not included in your Linux distribution, you can download it from http://gstreamer.freedesktop.org. Use of certain codes (for example, those in "plugins-ugly") might require a license from the manufacturer of that technology. Consult with your corporate legal department to determine whether the codes you plan to use require extra licenses.

Browser content redirection

Browser content redirection requires:

- Linux operating system webkit2gtk version 2.16.6 and glibcxx 3.4.20 or later.

Philips SpeechMike

If you plan to use Philips SpeechMike devices with Receiver, you might need to install the relevant drivers on the user device. Visit the Philips web site for information and software downloads.

Smart card support

To configure smart card support in Citrix Receiver for Linux, you must have the StoreFront services site configured to allow smart card authentication.

> **Note:**
> Smart cards are not supported with the XenApp services site for Web Interface configurations (formerly known as Program Neighborhood Agent), or with the “legacy PNAgent” site that can be provided by a StoreFront server.

Citrix Receiver for Linux supports smart card readers that are compatible with PCSC-Lite and smart cards with PKCS#11 drivers for the appropriate Linux platform. By default, Receiver for Linux now locates opensc-pkcs11.so in one of the standard locations. To ensure that Receiver for Linux finds either opensc-pkcs11.so in a non-standard location or another PKCS#11 driver, store the location in a configuration file using the following steps:

1. Locate the configuration file: $ICAROOT/config/AuthManConfig.xml
2. Locate the line <key>PKCS11module</key> and add the driver location to the <value> element immediately following the line.

   Note: If you enter a file name for the driver location, Receiver navigates to that file in the$ICAROOT/PKCS#11 directory. Alternatively, you can use an absolute path beginning with “/.”

To configure the behavior of Citrix Receiver for Linux when a smart card is removed, update SmartCardRemovalAction in the configuration file using the following steps:

1. Locate the configuration file: $ICAROOT/config/AuthManConfig.xml
2. Locate the line <key>SmartCardRemovalAction</key> and add ‘noaction’ or ‘forcelogoff’ to the<value> element immediately following the line.

The default behavior is ‘noaction’. No action is taken to clear credentials stored and tokens generated with regards to the smart card on the removal on the smart card. The ‘forcelogoff’ action clears all credentials and tokens within StoreFront on the removal of the smart card.

Citrix Servers

- XenApp: All versions currently supported by Citrix. For more information, see the Citrix product matrix.
- XenDesktop: All versions currently supported by Citrix. For more information, see the Citrix product matrix.
- VDI-in-a-Box: All versions currently supported by Citrix. For more information, see the Citrix product matrix.
- You can use Citrix Receiver for Linux 1808 or later browser-based access with StoreFront Receiver for Web and Web Interface, with - or without - the NetScaler Gateway plug-in.

  StoreFront:

  - StoreFront 3.x, 2.6, 2.5 and 2.1

    Provides direct access to StoreFront stores.

  - StoreFront configured with a Citrix Receiver for Web site

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

  Web Interface 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 Linux with XenApp services or XenDesktop services sites

- Ways to deploy Citrix Receiver to users:
  - Enable users to download from receiver.citrix.com, then configure using an email or services address with StoreFront.
  - Offer to install from Citrix Receiver for Web site (configured with StoreFront).
  - Offer to install Receiver from Citrix Web Interface 5.4.

Browser

Citrix recommends that you use the latest version of Mozilla Firefox or Google Chrome.

> Note:
> For information on changes to Google Chrome NPAPI support, see Citrix blog article, Preparing for NPAPI being disabled by Google Chrome.

Connectivity

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

- For LAN connections:
  - StoreFront using StoreFront services or Citrix Receiver for Web sites
  - Web Interface 5.4 for Windows, using Web Interface or XenApp services sites
- For secure remote or local connections:
  - Citrix NetScaler Gateway 12.0
  - Citrix NetScaler Gateway 11.1
  - Citrix NetScaler Gateway 11.0
  - Citrix NetScaler Gateway 10.5

- Citrix NetScaler Gateway 10.1
- Citrix Access Gateway Enterprise Edition 10
- Citrix Access Gateway Enterprise Edition 9.x
- Citrix Access Gateway VPX

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

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

About secure connections and certificates

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

Private (self-signed) certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the user device to 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 key store), an untrusted certificate error appears. The root certificate must be installed in the client's certificate store.

Installing root certificates on user devices

For information about installing root certificates on user devices and configuring certificates on Web Interface, see Installing root certificates in Citrix Workspace app for Windows documentation.

Wildcard certificates

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

Intermediate certificates and the NetScaler Gateway

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

Joint Server Certificate Validation Policy

Citrix Receiver for Linux has a stricter validation policy for server certificates.

> **Important**
>
> Before installing this version of Citrix Receiver for Linux, confirm that the certificates at the server or gateway are correctly configured as described here. Connections may fail if:
>
> - the server or gateway configuration includes a wrong root certificate
> - the server or gateway configuration does not include all intermediate certificates
> - the server or gateway configuration includes an expired or otherwise invalid intermediate certificate
> - the server or gateway configuration includes a cross-signed intermediate certificate

When validating a server certificate, Citrix Receiver for Linux now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Receiver for Linux releases, it then also checks that the certificates are trusted. If the certificates are not all trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Receiver for Linux's connection to fail.

Suppose that a gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Receiver for Linux:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Example Root Certificate"

Then, Citrix Receiver for Linux checks that all these certificates are valid. Citrix Receiver for Linux also checks that it already trusts "Example Root Certificate." If Citrix Receiver for Linux does not trust "Example Root Certificate," the connection fails.

Important

- Some certificate authorities have more than one root certificate. If you require this stricter validation, make sure that your configuration uses the appropriate root certificate. For example, there are currently two certificates ("DigiCert"/"GTE CyberTrust Global Root," and "DigiCert Baltimore Root"/"Baltimore CyberTrust Root") that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available ("DigiCert Baltimore Root"/"Baltimore CyberTrust Root"). If you configure "GTE CyberTrust Global Root" at the gateway, Citrix Receiver for Linux connections on those user devices will fail. Consult the certificate authority's documentation to determine which root certificate should be used. Also note that root certificates eventually expire, as do all certificates.
- Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

Now suppose that a gateway is configured with these valid certificates. This configuration, omitting the root certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Then, Citrix Receiver for Linux uses these two certificates. It then searches for a root certificate on the user device. If it finds one that validates correctly, and is also trusted (such as "Example Root Certificate"), the connection succeeds. Otherwise, the connection fails. This configuration supplies the intermediate certificate that Citrix Receiver for Linux needs, but also allows Citrix Receiver for Linux to choose any valid, trusted, root certificate.

Now suppose that a gateway is configured with these certificates:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Wrong Root Certificate"

A web browser may ignore the wrong root certificate. However, Citrix Receiver for Linux will not ignore the wrong root certificate, and the connection will fail.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- "Example Server Certificate"
- "Example Intermediate Certificate 1"
- "Example Intermediate Certificate 2"

> **Important**
>
> - Some certificate authorities use a cross-signed intermediate certificate. This is intended for situations there is more than one root certificate, and an earlier root certificate is still in use at the same time as a later root certificate. In this case, there will be at least two intermediate certificates. For example, the earlier root certificate "Class 3 Public Primary Certification Authority" has the corresponding cross-signed intermediate certificate "VeriSign Class 3 Public Primary Certification Authority - G5." However, a corresponding later root certificate "VeriSign Class 3 Public Primary Certification Authority - G5" is also available, which replaces "Class 3 Public Primary Certification Authority." The later root certificate does not use a cross-signed intermediate certificate.
> - The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To). But the cross-signed intermediate certificate has a different Issuer name (Issued By). This distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such "Example Intermediate Certificate 2").

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Avoid configuring the gateway to use the cross-signed intermediate certificate, as it selects the earlier root certificate:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Example Cross-signed Intermediate Certificate" [not recommended]

It is not recommended to configure the gateway with only the server certificate:

- "Example Server Certificate"

In this case, if Citrix Receiver for Linux cannot locate all the intermediate certificates, the connection fails.

User requirements

Although you do not need to log on as a privileged (root) user to install the Citrix Receiver for Linux, USB support is enabled only if you are logged on as a privileged user when installing and configuring Receiver. Installations performed by non-privileged users will, however, enable users to access published resources using either StoreFront through one of the supported browsers or using Receiver's native UI.

Check whether your device meets the system requirements

Citrix provides a script, hdxcheck.sh, as part of the Receiver installation package. The script checks whether your device meets all of the system requirements to benefit from all of the functionality in Receiver for Linux. The script is located in the Utilities directory of the installation package.

To run the hdxcheck.sh script

1. Open a terminal window.
2. Type cd $ICAROOT/util and press ENTER to navigate to the Utilities directory of the installation package.
3. Type ./hdxcheck.sh to run the script.

Install and set up

February 20, 2019

The following packages are available for Citrix Receiver for Linux. You can access the packages from the download section of the Citrix website.

Package name	Contents
Debian packages (Ubuntu, Debian, Linux Mint etc.)	
icaclient_13.10.0.20_amd64.deb	Self-service support, 64-bit x86_64
icaclient_13.10.0.20_i386.deb	Self-service support, 32-bit x86
icaclient_13.10.0.20_armhf.deb	Self-service support, ARM HF
icaclientWeb_13.10.0.20_amd64.deb	Web Receiver only, 64-bit x86_64
icaclientWeb_13.10.0.20_i386.deb	Web Receiver only, 32-bit x86
icaclientWeb_13.10.0.20_armhf.deb	Web Receiver only, ARM HF
ctxusb_2.7.20_amd64.deb	USB package, 64-bit x86_64
ctxusb_2.7.20_i386.deb	USB package, 32-bit x86
ctxusb_2.7.20_armhf.deb	USB package, ARM HF
Redhat packages (Redhat, SUSE, Fedora etc.)	

Package name	Contents
ICAClient-rhel-13.10.0.20-0.x86_64.rpm	Self-service support, RedHat (including Linux VDA) based, 64-bit x86_64
ICAClient-rhel-13.10.0.20-0.i386.rpm	Self-service support, RedHat based, 32-bit x86
ICAClientWeb-rhel-13.10.0.20-0.x86_64.rpm	Web Receiver only, RedHat based, 64-bit x86_64
ICAClientWeb-rhel-13.10.0.20-0.i386.rpm	Web Receiver only, RedHat based, 32-bit x86
ICAClient-suse-13.10.0.20-0.x86_64.rpm	Self-service support, SUSE based, 64-bit x86_64
ICAClient-suse-13.10.0.20-0.i386.rpm	Self-service support, SUSE based, 32-bit x86
ICAClient-suse11sp3-13.10.0.20-0.x86_64.rpm	Self-service support, SUSE 11 sp3 (including Linux VDA) based, 64-bit x86_64
ICAClient-suse11sp3-13.10.0.20-0.i386.rpm	Self-service support, SUSE 11 sp3 based, 32-bit x86
ICAClientWeb-suse-13.10.0.20-0.x86_64.rpm	Web Receiver only, SUSE based, 64-bit x86_64
ICAClientWeb-suse-13.10.0.20-0.i386.rpm	Web Receiver only, SUSE based, 32-bit x86
ctxusb-2.7.20-1.x86_64.rpm	USB package, 64-bit x86_64
ctxusb-2.7.20-1.i386.rpm	USB package, 32-bit x86
Tarballs (Script install for any distribution)	
linuxx64-13.10.0.20.tar.gz	64-bit Intel
linuxx86-13.10.0.20.tar.gz	32-bit Intel
linuxarmhf-13.10.0.20.tar.gz	ARM HF

The difference between packages that offer support for Web Receiver and those packages that support self-service is that the latter packages include dependencies required for self-service in addition to those needed for the Web Receiver. Dependencies for self-service are a superset of those required for Web Receiver, but the files installed are identical.

If you require only Web Receiver support, or your distribution doesn't have the necessary packages to support self-service, install the Web Receiver only package.

> **Note**
>
> If your distribution allows, install Citrix Receiver from the Debian package or RPM package. These files are easier to use because they automatically install any required packages. If you want to

> control the installation location, install Citrix Receiver from the tarball package.
>
> Do not use both installation methods on the same machine. If you do, for example, if you install Citrix Receiver for Linux from a tarball package on a machine where Citrix Receiver for Linux was already installed from a Debian package, you are likely to see error messages and unwanted behaviors.

To install Citrix Receiver for Linux from a Debian package

If you are installing Receiver from the Debian package on Ubuntu, you might find it convenient to open the packages in the Ubuntu Software Center.

In the following instructions, replace
packagename with the name of the package that you are installing.

This procedure uses a command line and the native package manager for Ubuntu/Debian/Mint. You can also install the package by double-clicking the downloaded .deb package in a file browser. This typically starts a package manager that downloads any missing required software. If no package manager is available, Citrix recommends
gdebi, a command-line tool that performs this function.

To install the package using the command line

1. Log on as a privileged (root) user.
2. Open a terminal window.
3. Run the installation for the following three packages by typing **gdebi packagename.deb**. For example:
   - gdebi icaclient_13.9.1.6_amd64.deb
   - gdebi icaclientWeb_13.9.1.6_i386.deb
   - gdebi ctxusb_2.7.6_amd64.deb

   Note: To use dpkg in the above examples, replace “gdebi” with “dpkg -i.”

   A user must install the icaclient package or the icaclientWeb package. The ctxusb package is optional to support Generic USB Redirection.
4. If using dpkg, install any missing dependencies by typing sudo **apt-get -f install**.
5. Accept the EULA.

To install Citrix Receiver for Linux from an RPM package

If you are installing Citrix Receiver from the RPM package on SUSE, use the YaST or Zypper utility, not the RPM utility. The RPM utility does not download or install any necessary dependencies, it only installs the .rpm package. If the required dependencies are missing, you will receive an error.

Note: To follow an example of an installation using a RPM package, see the Citrix Blog article " Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop."

In the following instructions, replace
packagename with the name of the package that you are installing.

Note: If you receive an error indicating that the installation "… requires libwebkitgtk-1.0.so.0" on Red Hat based distributions (RHEL, CentOS, Fedora, etc.), add the EPEL repository (details can be found at https://fedoraproject.org/wiki/EPEL), which can provide the missing package, or switch to the Web variant of the package.

To set up the EPEL repository on Red Hat

1. Download the appropriate source RPM package from here:

   https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F

2. For example, for Red Hat Enterprise 7.x:

   yum localinstall epel-release-latest-7 .noarch.rpm

Tip: RPM Package Manager does not install any missing required software. To download and install the software, Citrix recommends using **zypper install <file name>** at a command line on OpenSUSE or **yum localinstall <filename>** on Fedora/Red Hat.

After setting up the EPEL repository, install Receiver from the RPM package

1. Log on as a privileged (root) user.
2. Run the installation for the following three packages by typing zypper in packagename.rpm.

   Note: A user must install the icaclient package or the icaclientWeb package. The ctxusb package is an optional to support Generic USB Redirection.

3. Open a terminal window.

   For SUSE installations:

   zypper in ICAClient-suse-13.9.1.6-0.x86_64.rpm

   zypper in ICAClient-suse-13.9.1.6-0.i386.rpm

   zypper in ctxusb-2.7.6-1.x86_64.rpm

   For Red Hat installations:

   yum localinstall ICAClient-rhel-13.9.1.6-0.i386.rpm

   yum localinstall ICAClientWeb-rhel-13.9.1.6-0.i386.rpm

   yum localinstall ctxusb-2.7.6-1.i386.rpm

4. Accept the EULA.

To install Citrix Receiver for Linux from a tarball package

Note: The tarball package does not do dependency checking or installation of dependencies. All system dependencies must be resolved separately.

1. Open a terminal window.
2. Decompress the .tar.gz file and extract the contents into an empty directory. For example, type: tar xvfz packagename.tar.gz.
3. Type **./setupwfc** and then press Enter to run the setup program.
4. Accept the default of 1 (to install the Receiver) and press Enter.
5. Type the path and name of the required installation directory and then press Enter, or press Enter to install Receiver in the default location.

   The default directory for privileged (root) user installations is /opt/Citrix/ICAClient.

   The default directory for non-privileged user installations is $HOME/ICAClient/platform. Platform is a system-generated identifier for the installed operating system. For example, $HOME-/ICAClient/linuxx86 for the Linux/x86 platform).

   Note: If you specify a non-default location, set it in $ICAROOT in $HOME/.profile or $HOME/.bash_profile.
6. When prompted to proceed, type y and then press Enter.
7. You can choose whether to integrate Receiver into your desktop environment. The installation creates a menu option from which users can start Receiver. Type **y** at the prompt to enable the integration.
8. If you have previously installed GStreamer, you can choose whether to integrate GStreamer with Receiver and so support HDX Mediastream Multimedia Acceleration. To integrate Receiver with GStreamer, type y at the prompt.

   Note: On some platforms, installing the client from a tarball distribution may cause the system to hang after prompting you to integrate with KDE and GNOME. This issue occurs with the first time initialization of gstreamer-0.10. If you encounter this issue, terminate the installation process (using ctrl+c) and run the command **gst-inspect-0.10 – gst-disable-registry-fork –version**. After executing this command, you can rerun the tarball setup without experiencing a system hang.
9. If you log on as a privileged user (root), choose to install USB support for XenDesktop and XenApp published VDI applications. Type y at the prompt to install USB support.

   Note: If you are not logged on as a privileged user (root), the following warning appears: “USB support cannot be installed by non-root users. Run the installer as root to access this install option.”

10. When the installation is complete, the main installation menu appears again. To exit from the setup program, type 3 and then press Enter.

Customize a Citrix Receiver for Linux installation

July 9, 2018

You can customize a configuration before installation by modifying the contents of the Citrix Receiver package and then repackaging the files. Your changes are included in every version installed using the modified package.

To customize a Citrix Receiver for Linux installation

1. Expand the Citrix Receiver package file into an empty directory. The package file is called platform.major.minor.release.build.tar.gz (for example, linuxx86.13.2.0.nnnnnn.tar.gz for the Linux/x86 platform).
2. Make the required changes to the Citrix Receiver package. For example, you might add a TLS root certificate to the package if you want to use a certificate from a Certificate Authority that is not part of the standard Receiver installation. To add a TLS root certificate to the package, see Install root certificates on user devices on the Citrix Product Documentation site.
   For more information about built-in certificates, see Configure and enable SSL and TLS on the Citrix Product Documentation site.
3. Open the PkgID file.
4. Add the following line to indicate that the package was modified: MODIFIED=traceinfo where traceinfo is information indicating who made the change and when. The exact format of this information is not important.
5. Save and close the file.
6. Open the package file list, platform/platform.psf (for example, linuxx86/linuxx86.psf for the Linux/x86 platform).
7. Update the package file list to reflect the changes you made to the package. If you do not update this file, errors can occur when installing your new package. Changes could include updating the size of any files you modified, or adding new lines for any files you added to the package. The columns in the package file list are:
   - File type
   - Relative path
   - Subpackage (which must always be set to cor)
   - Permissions
   - Owner

- Group
- Size

8. Save and close the file.
9. Use the tar command to rebuild Receiver package file, for example: tar czf ../newpackage.tar.gz * where newpackage is the name of the new Receiver package file.

Start Citrix Receiver for Linux

July 9, 2018

You can start Citrix Receiver either at a terminal prompt or from one of the supported desktop environments.

If Citrix Receiver was not installed in the default installation directory, ensure that the environment variable ICAROOT is set to point to the actual installation directory.

> **Tip**
>
> The following instruction does not apply to installations made from the Web packages, or where the tarball is used but where the requirements for self-service have not been met.

To start Citrix Receiver at a terminal prompt

At the terminal prompt, type /opt/Citrix/ICAClient/selfservice and press Enter (where /opt/Citrix/ICAClient is the directory in which you installed Citrix Receiver).

To start Citrix Receiver from the Linux desktop

You can start Citrix Receiver from a desktop environment for Linux by navigating to it using a file manager.

On some desktops, you can also start Citrix Receiver from a menu. Receiver is located in different menus depending on your Linux distribution.

Use Citrix Receiver for Linux as an ICA-to-X proxy

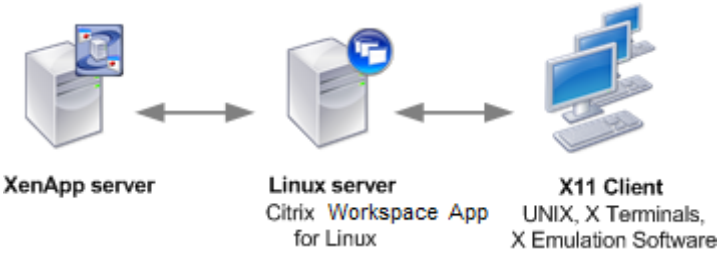
February 27, 2019

You can use a workstation running Citrix Receiver as a server and redirect the output to another X11-capable device. You might want to do this to deliver Microsoft Windows applications to X terminals or to UNIX workstations for which Citrix Receiver is not available.

> **Note**
>
> Citrix Receiver software is available for many X devices, and installing the software on these devices is the preferred solution in these cases. Running Citrix Receiver in this way, as an ICA-to-X proxy, is also referred to as server-side ICA.

When you run Citrix Receiver, you can think of it as an ICA-to-X11 converter that directs the X11 output to your local Linux desktop. However, you can redirect the output to another X11 display. You can run multiple copies of Citrix Receiver simultaneously on one system with each sending its output to a different device.

This graphic shows a system with Citrix Receiver for Linux set up as an ICA-to-X proxy:



To set up this type of system, you need a Linux server to act as the ICA-to-X11 proxy:

- If you have X terminals already, you can run Citrix Receiver on the Linux server that usually supplies the X applications to the X terminals.
- If you want to deploy UNIX workstations for which Citrix Receiver is not available, you need an extra server to act as the proxy. This can be a PC running Linux.

Supported features

Applications are supplied to the final device using X11, using the capabilities of the ICA protocol. By default, you can use drive mapping only to access the drives on the proxy. This is not a problem if you are using X terminals (which usually do not have local drives). If you are delivering applications to other UNIX workstations, you can either:

- NFS mount the local UNIX workstation on the workstation acting as the proxy, then point a client drive map at the NFS mount point on the proxy.
- Use an NFS-to-SMB proxy such as SAMBA, or an NFS client on the server such as Microsoft Services for UNIX.

Some features are not passed to the final device:

- USB redirection

- Smart card redirection
- COM port redirection
- Audio is not delivered to the X11 device, even if the server acting as a proxy supports audio.
- Client printers are not passed through to the X11 device. You access the UNIX printer from the server manually using LPD printing, or use a network printer.
- Redirection of multimedia input is not expected to work because it requires a webcam on the machine running Citrix Receiver, which is the server acting as a proxy. However, redirection of multimedia output works with GStreamer installed on the server acting as a proxy (untested).

To start Citrix Receiver with server-side ICA from an X terminal or a UNIX workstation

1. Use ssh or telnet to connect to the device acting as the proxy.
2. In a shell on the proxy device, set the **DISPLAY** environment variable to the local device. For example, in a C shell, type:

   ```
   setenv DISPLAY <local:0>
   ```

   Note: If you use the command ssh -X to connect to the device acting as the proxy, you do not need to set the
   DISPLAY environment variable.
3. At a command prompt on the local device, type xhost <proxy server name>
4. If Receiver is not installed in the default installation directory, ensure that the environment variable ICAROOT is set to point to the actual installation directory.
5. Locate the directory where Citrix Receiver is installed. At a command prompt, type selfservice &

Configure the Customer Experience Improvement Program (CEIP)

July 9, 2018

When you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous statistics and usage information are sent to Citrix to help Citrix improve the quality and performance of Citrix products. For more information about CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

By default, you are automatically enrolled in CEIP when you install Citrix Receiver for Linux. The first upload of data occurs approximately seven days after you install the Receiver. The data collected for active users is uploaded to the CIS server every seven days.

Registry setting that controls enrollment in CEIP:

- Location: <ICAROOT>/config/module.ini
- Section: CEIP
- Entry: EnableCeip
- Value: Enable (Default) / Disable

The following anonymous information is collected. The data does not contain any details that identify you as a customer. When EnableCeip is set to Disable, only the Receiver version information is collected.
Data point|Description
———-|———
Machine ID|Identifying the machine where data originates
Linux kernel version|String denoting the machine's kernel version
Linux OS name and version|String denoting the Linux OS name and version of the machine
Data collection date|Denoting the date when data capture is done
CPU model name|Denoting the CPU model of the client machine
System memory information|Collecting system memory information involving total RAM, free RAM, buffer RAM, shared RAM, total swap, free swap, and number of current processes
Monitor resolution|Fetching the monitor resolution of the client machine
Desktop environment|Fetching details on whether the current desktop environment being used in of type -XDG_CURRENT_DESKTOP or DESKTOP_SESSION
Browser version|Fetching information on the browser being used – firefox / chrome / and so on
USB devices information|Fetching information about USB ports available on the client system
Flash version|Fetching information on the Flash version being used
Locale version|Denoting the locale version
Language information|Mapping the keyboard and fetching this information
Schema information|Fetching Receiver schema information
Multimedia redirection|Boolean value denoting whether this feature is enabled
Webcam redirection|Boolean value denoting whether webcam redirection is enabled
Flash redirection|Boolean value denoting whether Flash redirection is enabled
MediaStream|Boolean value denoting whether media stream feature is enabled. This includes speed screen audio and video functionality.

Uninstall Citrix Receiver for Linux

July 9, 2018

This procedure has been tested with the tarball package. Remove the RPM and Debian packages using your operating system's standard tools.

The environment variable ICAROOT must be set to the installation directory of the client. The default

directory for non-privileged user installations is $HOME/ICAClient/platform. The platform variable is a system-generated identifier for the installed operating system. For example, $HOME/ICAClient/linuxx86 for the Linux/x86 platform. Privileged user installation defaults to /opt/Citrix/ICAClient.

1. Run the setup program by typing $ICAROOT/setupwfc and press Enter.
2. To remove the client, type 2 and press Enter.

> **Note**
>
> To uninstall Citrix Receiver for Linux, you must be logged in as the same user who performed the installation.

Connect

July 30, 2018

Citrix Workspace provides users with secure, self-service access to virtual desktops and applications, and on-demand access to Windows, web, and Software as a Service (SaaS) applications. Citrix StoreFront or legacy webpages created with Web Interface manage the user access.

To connect to resources using the Citrix Workspace UI

The Citrix Workspace app home page displays virtual desktops and applications that are available to users based on their account settings (that is, the server they connect to) and settings configured by Citrix XenDesktop or Citrix XenApp administrators. Using the Preferences > Accounts page, users can perform that configuration themselves by entering the URL of a StoreFront server or, if email-based account discovery is configured, by entering their email address.

> **Tip**
>
> If you use the same name for multiple stores on the StoreFront server, you avoid duplications by adding numbers. The names for such stores depend on the order in which they are added. For PNAgent, the store URL is displayed and uniquely identifies the store.

After connecting to a store, self-service shows the tabs: FAVORITES, DESKTOPS, and APPS. To launch a session, click the appropriate icon. To add an icon to FAVORITES, click the “Details” link next to the icon and select “Add To Favorites.”

Configure connection settings

You can configure some default settings for connections between Citrix Workspace App for Linux and XenApp and XenDesktop servers. You can also change those settings for individual connections, if

necessary.

The rest of this section contains procedures that support typical tasks performed by users of Citrix Workspace app. Although the tasks and responsibilities of administrators and users can overlap, the term "user" is employed in this section to distinguish typical user tasks from those typically performed by administrators.

- Connect to resources from a command line or browser
- Troubleshoot connections to resources
- Customize Citrix Workspace app using configuration files

Connect to resources from a command line or browser

March 5, 2019

You create connections to servers when you click on a desktop or application icon on the Receiver home page. In addition, you can open connections from a command line or from a web browser.

To create a connection to a Program Neighborhood or StoreFront server using a command line

As a prerequisite, ensure that the store is known to Citrix Receiver. If necessary, add it using the following command:

```
./util/storebrowse --addstore <store URL>
```

1. Obtain the unique ID of the desktop or application that you want to connect to. This is the first quoted string on a line acquired in one of the following commands:
   - List all of the desktops and applications on the server:

     ```
     ./util/storebrowse -E <store URL>
     ```

   - List the desktops and applications that you have subscribed to:

     ```
     ./util/storebrowse -S <store URL>
     ```

2. Run the following command to start the desktop or application:

   ```
   ./util/storebrowse -L <desktop or application ID> <store URL>
   ```

If you cannot connect to a server, your administrator might need to change the server location or SOCKS proxy details. For more information, see
Connect through a proxy server.

To create a connection from a web browser

Configuration for starting sessions from a web browser is typically carried out automatically during installation. Because of the wide variety of browsers and operating systems, some manual configuration can be required.

If you set up .mailcap and MIME files for Firefox, Mozilla, or Chrome manually, use the following file modifications so that .ica files start up the Receiver executable, wfica. To use other browsers, modify the browser configuration accordingly.

1. Run the following commands for non-administrator installation of Citrix Workspace app. The settings of ICAROOT might be changed if they are installed to a non-default location. You can test the result with the command "xdg-mime query default application/x-ica," which must return "wfica.desktop."

```
setenv ICAROOT=/opt/Citrix/ICAClient

xdg-icon-resource install --size 64  "$ICAROOT/icons/000\_Receiver
   \_64.png Citrix Workspace app"

xdg-mime default wfica.desktop application/x-ica

xdg-mime default new\_store.desktop application/vnd.citrix.
   receiver.configure
```

2. Create or extend the file /etc/xdg/mimeapps.list (for administrator installation) or $HOME/.local/share/applic (mimeapps.list). The file must start with [Default Applications], and follow by:

   application/x-ica=wfica.desktop;

   application/vnd.citrix.receiver.configure=new_store.desktop;

   You might need to configure Firefox on its Preferences/Applications setting page. For "Citrix ICA settings file content," select "Citrix Receiver Engine (default)" in the pull-down menu. Or select "Use other …" and then select the file /usr/share/applications/wfica.desktop (for an administrator installation of Receiver) or $HOME/.local/share/applications/wfica.desktop (for a non-administrator installation).

Troubleshoot connections to resources

July 30, 2018

Users can manage their active connections using the Connection Center. This feature is a useful productivity tool that enables users and administrators to troubleshoot slow or problematic connections. With Connection Center, users can manage connections by:

- Closing an application.
- Logging off a session. This step ends the session and closes any open applications.
- Disconnecting from a session. This step cuts the selected connection to the server without closing any open applications (unless the server is configured to close applications on disconnection).
- Viewing connection transport statistics.

To manage a connection

1. On the Citrix Workspace app menu, click Connection Center.

   The servers that are used are shown and, for each server, the active sessions are listed.

2. Do one of the following:

   - Select a server, and disconnect from it, log off from it, or view properties of it.
   - Select an application, and close the window it is displayed in.

Customize using configuration files

October 26, 2018

About the configuration files

To change advanced or less common settings, you can modify Receiver's configuration files. These configuration files are read each time wfica starts. You can update various files depending on the effect you want the changes to have.

If session sharing is enabled, an existing session might be used instead of a newly reconfigured one. This might cause the session to ignore changes you made in a configuration file.

Apply default to all Citrix Receiver users

If you want to change the default for all Citrix Receiver users, modify the module.ini configuration file in the $ICAROOT/config directory.

> **Note**
>
> You do not need to add an entry to All_Regions.ini for a configuration value to be read from module.ini, unless you want to allow other configuration files to override the value in module.ini. If an entry in All_Regions.ini sets a specific value, the value in module.ini is not used.

Apply changes to new Citrix Receiver users

If the $HOME/.ICAClient/wfclient.ini file does not exist, wfica creates it by copying $ICAROOT/config/wfclient.template. When you change this template file, the changes apply to all future new Citrix Receiver users.

Apply changes to all connections for particular users

If you want the changes to apply to all connections for a particular user, modify the wfclient.ini file in that user's $HOME/.ICAClient directory. The settings in this file apply to future connections for that user.

Validate configuration file entries

If you want to limit the values for entries in wfclient.ini, you can specify allowed options or ranges of options in All_Regions.ini. If you specify only one possible value, that value is used. $HOME/.ICAClient/All_Regsions.ini can only match or reduce the possible values set by $ICAROOT/config/All_Regions.ini, it cannot take away restrictions. See the All_Regions.ini file in the $ICAROOT/config directory for more information.

> **Note**
>
> If an entry appears in more than one configuration file, a value in wfclient.ini takes precedence over a value in module.ini.

About the parameters in the files

The parameters listed in each file are grouped into sections. Each section begins with a name in square brackets indicating parameters that belong together; for example, [ClientDrive] for parameters related to client drive mapping (CDM).

Defaults are automatically supplied for any missing parameters except where indicated. If a parameter is present but is not assigned a value, the default is automatically applied. For example, if InitialProgram is followed by an equal sign (=) but no value, the default (not to run a program after logging in) is applied.

Precedence

All_Regions.ini specifies which parameters can be set by other files. It can restrict values of parameters or set them exactly.

For any given connection, the files are checked in the following order:

1. All_Regions.ini. Values in this file override those in:
    - The connection's .ica file
    - wfclient.ini
2. module.ini. Values in this file are used if they have not been set in All_Regions.ini, the connection's .ica file, or wfclient.ini but they are not restricted by entries in All_Regions.ini.

If no value is found in any of these files, the default in the Receiver code is used.

> **Note**
>
> There are exceptions to this order of precedence. For example, the code reads some values specifically from wfclient.ini for security reasons, to ensure that they are not set by a server.

Configure Citrix XenApp (formerly PNAgent) connections using Web Interface

July 30, 2018

This topic applies only to deployments using either XenApp Services on Web Interface or "legacy PNAgent" on StoreFront.

Options such as selfservice, storebrowse, and pnabrowse enable users to connect to published resources (that is, published applications, and server desktops) through a server running a XenApp Services site. These programs can launch connections directly or can be used to create menu items through which users can access published resources. pnabrowse can also create desktop items for this purpose.

Customizable options for all users running Citrix XenApp on your network are defined in a configuration file, config.xml, which is stored on the Web Interface server. When a user starts one of these programs, it reads the configuration data from the server. After that, it updates its settings and user interface periodically, at intervals specified in the config.xml file.

> **Important**
>
> The config.xml file affects all connections defined by the XenApp Services site.

Publish content

A XenApp Services site may also publish a file, rather than an application or desktop. This process is referred to as publishing content, and allows pnabrowse to open the published file.

There is a limitation to the type of files that are recognized by Citrix Workspace App for Linux. For the system to recognize the file type of the published content and for users to view it through Citrix Workspace app, a published application must be associated with the file type of the published file. For example, to view a published Adobe PDF file using Citrix Workspace app, an application such as Adobe PDF Viewer must be published. Unless a suitable application is published, users cannot view the published content.

Optimize

April 16, 2019

By optimizing your environment you gain the best performance from Citrix Receiver and provide the best user experience. You can improve and optimize performance by:

- Mapping user devices
- Configuring USB support
- Bloomberg keyboard redirection
- Improving performance over low-bandwidth connections
- Improving multimedia performance
- Optimizing the performance of screen tiles
- Enabling logging
- Configuring multi-monitor layout persistence

Mapping user devices

Citrix Receiver supports client device mapping for connections to XenApp and XenDesktop servers. Client device mapping enables a remote application running on the server to access devices attached to the local user device. The applications and system resources appear to the user at the user device as if they are running locally. Ensure that client device mapping is supported on the server before using these features.

Note: The Security-Enhanced Linux (SELinux) security model can affect the operation of the Client Drive Mapping and USB Redirection features (on both XenApp and XenDesktop). If you require either or both of these features, disable SELinux before configuring them on the server.

Mapping client drives

Client drive mapping allows drive letters on the XenApp or XenDesktop server to be redirected to directories that exist on the local user device. For example, drive H in a Citrix user session can be mapped to a directory on the local user device running Receiver.

Client drive mapping can make any directory mounted on the local user device, including a CD-ROM, DVD, or a USB memory stick, available to the user during a session, provided the local user has permission to access it. When a server is configured to allow client drive mapping, users can access their locally stored files, work with them during their session, and then save them again either on a local drive or on a drive on the server.

Two types of drive mapping are available:

- Static client drive mapping enables administrators to map any part of a user device's file system to a specified drive letter on the server at logon. For example, it can be used to map all or part of a user's home directory or /tmp, and the mount points of hardware devices such as CD-ROMs, DVDs, or USB memory sticks.
- Dynamic client drive mapping monitors the directories in which hardware devices such as CD-ROMs, DVDs, and USB memory sticks are typically mounted on the user device. And any new ones that appear during a session are automatically mapped to the next available drive letter on the server.

When Citrix Receiver connects to XenApp or XenDesktop, client drive mappings are reestablished unless client device mapping is disabled. You can use policies to give you more control over how client device mapping is applied. For more information, see the XenApp and XenDesktop documentation.

Users can map drives using the Preferences dialog box.

Note: By default, enabling static client drive mapping also enables dynamic client drive mapping. To disable the latter but enable the former, set DynamicCDM to False in wfclient.ini.

Mapping client printers

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

- Print to all printing devices accessible from the user device
- Add printers

These settings, however, might not be the optimum in all environments. For example, the default setting that allows users to print to all printers accessible from the user device is the easiest to administer initially. But the default setting might create slower logon times in some environments. In this situation, you might want to limit the list of printers configured on the user device.

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

To limit the list of printers configured on the user device

1. Open the configuration file, wfclient.ini, in one of the following:
   - $HOME/.ICAClient directory to limit the printers for a single user
   - $ICAROOT/config directory to limit the printers for all Receiver users. All users in this case are those users who first use the selfservice program after the change.
2. In the [WFClient] section of the file type:

   ClientPrinterList=printer1:printer2:printer3

   Where printer1, printer2, and so on, are the names of the chosen printers. Separate printer name entries by a colon (:).
3. Save and close the file.

Mapping client printers on XenApp for Windows

The Citrix Receiver for Linux supports the Citrix PS Universal Printer Driver. So, usually no local configuration is required for users to print to network printers or printers that are attached locally to user devices. You might, however, manually map client printers on XenApp for Windows if, for example, the user device's printing software does not support the universal printer driver.

To map a local printer on a server

1. From Citrix Receiver, start a server connection and log on to a computer running XenApp.
2. On the Start menu, choose **Settings > Printers**.
3. On the File menu, choose **Add Printer**.

   The Add Printer wizard appears.
4. Use the wizard to add a network printer from the Client Network, Client domain. Usually this is a standard printer name, similar to those created by native Remote Desktop Services, such as "HP LaserJet 4 from client name in session 3."

   For more information about adding printers, see your Windows operating system documentation.

Mapping client printers on XenApp for UNIX

In a UNIX environment, printer drivers defined by Citrix Receiver are ignored. The printing system on the user device must be able to handle the print format generated by the application.

Before users can print to a client printer from Citrix XenApp for UNIX, printing must be enabled by the administrator. For more information, see the XenApp for UNIX section in the XenApp and XenDesktop documentation.

Mapping client audio

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

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

You configure client audio mapping using policies. For more information, see the XenApp and XenDesktop documentation.

Note: Client audio mapping is not supported when connecting to Citrix XenApp for UNIX.

To set a non-default audio device

The default audio device is typically the default ALSA device configured for your system. Use the following procedure to specify a different device:

1. Choose and open a configuration file according to which users you want your changes to affect. See Customize Receiver using configuration files for information about how updates to particular configuration files affect different users.
2. Add the following option, creating the section if necessary:

[ClientAudio]

AudioDevice = <device>

Where device information is located in the ALSA configuration file on your operating system.

Note: The location of this information is not standard across all Linux operating systems. Citrix recommends consulting your operating system documentation for more details about locating this information.

Configuring USB support

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 redirected to their virtual desktop. USB devices available for remoting include flash drives, smartphones, PDAs, printers, scanners, MP3 players, security devices, and tablets.

USB redirection requires either XenApp 7.6 (or later) or XenDesktop. XenApp does not support USB redirection of mass storage devices and requires special configuration to support audio devices. See XenApp 7.6 documentation for details.

Isochronous features in USB devices such as webcams, microphones, speakers, and headsets are supported in typical low latency/high speed LAN environments. But usually the standard audio or webcam redirection are more suitable.

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

- Keyboards
- Mice
- Smart cards
- Headsets
- Webcams

Note: Specialist USB devices (for example, Bloomberg keyboards and 3D mice) can be configured to use USB support. 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 might have a NIC 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 NICs
- USB hubs

To update the default list of USB devices available for remoting, edit the usb.conf file, located in $ICAROOT/. For more information, see the Update the list of USB devices available for remoting section.

To allow the remoting of USB devices to virtual desktops, enable the USB policy rule. For more information, see the XenApp and XenDesktop documentation.

How USB support works

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

For desktops accessed through desktop appliance mode, when a user plugs in a USB device, that device is automatically redirected to the virtual desktop. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.

The session window must have focus when the user plugs in the USB device for redirection to occur, unless desktop appliance mode is in use.

Mass storage devices

If a user disconnects from a virtual desktop when a USB mass storage device is still plugged in to the local desktop, that device is not redirected to the virtual desktop when the user reconnects. To ensure that the mass storage device is redirected to the virtual desktop, the user must remove and reinsert the device after reconnecting.

Note: If you insert a mass storage device into a Linux workstation that has been configured to deny remote support for USB mass storage devices, the device will not be accepted by the Receiver software. And a separate Linux file browser might open. Therefore, Citrix recommends that you pre-configure user devices with the **Browse removable media when inserted** setting cleared by default. On Debian-based devices, do this using the Debian menu bar by selecting **Desktop > Preferences > Removable Drives and Media**. And on the **Storage** tab, under **Removable Storage**, clear the **Browse removable media when inserted** check box.

Note: If the Client USB device redirection server policy is turned on, mass storage devices are always directed as USB devices even if client drive mapping is turned on.

Webcams

By default, optimum webcam performance is provided by HDX RealTime Webcam Video Compression. In some circumstances, however, you may require users to connect webcams using USB support. To do this, you must disable HDX RealTime Webcam Video Compression. For more information, see Video Conferencing with HDX RealTime Webcam Video Compression.

USB classes allowed by default

The following classes of USB device are allowed by the default USB policy rules:

- Audio (Class 01)

  Includes microphones, speakers, headsets, and MIDI controllers.

- Physical Interface (Class 05)

  These devices are similar to 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 might also appear as mass storage devices. And it might be possible to configure a camera to use either class, through setup menus provided by the camera itself.

  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 might 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.

- 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 is a wide variety of devices having internal storage which also presents 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. Consider carefully whether or not there is a business need to permit the use of mass storage devices, either through client drive mapping, or USB support. To reduce this risk, the server might be configured to prevent files being executed through client drive mapping.

- Content Security (Class 0d)

  Content security devices enforce content protection, typically for licensing or digital rights management. This class includes dongles.

- Personal Healthcare (Class 0f)

  These devices include personal healthcare devices such as blood pressure sensors, heart rate monitors, pedometers, pill monitors, and spirometers.

- Application and Vendor Specific (Classes fe and ff)

  Many devices use vendor specific protocols or protocols not standardized by the USB consortium, and these usually appear as vendor-specific (class ff).

USB device classes denied by default

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

- Communications and CDC Control (Classes 02 and 0a)

  Includes modems, ISDN adapters, network adapters, and some telephones and fax machines.

  The default USB policy does not allow these devices, because one of them might 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.

- 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.

  By default, optimum webcam performance is provided by HDX RealTime Webcam Video Compression.

- Wireless Controllers (Class e0)

  Includes a wide variety of wireless controllers, such as ultra wide band controllers and Bluetooth.

  Some of these devices might 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 might be particular devices it is appropriate to provide access to using USB support.

Updating the list of USB devices available for remoting

You can update the range of USB devices available for remoting to desktops by editing the list of default rules contained in the usb.conf file on the user device in $ICAROOT/.

You update the list by adding new policy rules to allow or deny USB devices not included in the default range. Rules created by an administrator in this way control which devices are offered to the server. The rules on the server control which of these to be accepted.

The default policy configuration for disallowed devices is:

DENY: class=09 # Hub devices

DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless Controllers

DENY: class=02 # Communications and CDC Control

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC Data

ALLOW: # Ultimate fallback: allow everything else

Creating USB policy rules

Tip: When creating policy rules, see the USB Class Codes, available from the USB web site at http://www.usb.org/. Policy rules in usb.conf on the user device take the format {ALLOW:|DENY:} followed by a set of expressions based on values for the following tags:

Tag	Description
VID	Vendor ID from the device descriptor
REL	Release ID from the device descriptor
PID	Product ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor
SubClass	SubClass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating policy rules, be aware of the following:

- Rules are case-insensitive.
- Rules might have an optional comment at the end, introduced by "#." A delimiter is not required and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- Whitespace used as a separator is ignored, but cannot appear in the middle of a number or identifier. For example, Deny: Class=08 SubClass=05 is a valid rule; Deny: Class=0 8 Sub Class=05 is not.
- Tags must use the matching operator "=." For example, VID=1230.

Example

The following example shows a section of the usb.conf file on the user device. For these rules to be implemented, the same set of rules must exist on the server.

ALLOW: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive

DENY: Class=08 SubClass=05 # Mass Storage Devices

DENY: Class=0D # All Security Devices

Configure start-up modes

Using desktop appliance mode, you can change how a virtual desktop handles previously attached USB devices. In the WfClient section in the file $ICAROOT/config/module.ini on each user device, set DesktopApplianceMode = Boolean as follows.

TRUE	Any USB devices that are already plugged in start-up provided the device is not disallowed with a Deny rule in the USB policies on either the server (registry entry) or the user device (policy rules configuration file).
FALSE	No USB devices start up.

Bloomberg keyboard redirection

The Bloomberg keyboard redirection can be performed through generic USB redirection.

To configure the Bloomberg v4 keyboard through Generic USB Redirection on the client side:

As a prerequisite, the policy should be enabled in Domain Delivery Controller (DDC).

1. Find the vid and pid of the Bloomberg keyboard. For example, in Debian and Ubuntu run the following command:

   ```
   lsusb
   ```

2. Go to $ICAROOT and edit the usb.conf file.
3. Add the following entry in the usb.conf file to allow the Bloomberg keyboard for USB redirection, and then save the file.

   ALLOW: vid=1188 pid=9545

4. Restart the ctxusbd daemon on the client. For example, in Debian and Ubuntu run the following command:

   ```
   systemctl restart ctxusbd
   ```

5. Launch a client session. Make sure the session has focus while plugging in the Bloomberg v4 keyboard for redirection.

Improving performance over low-bandwidth connections

Citrix recommends that you use the latest version of XenApp or XenDesktop on the server and Receiver on the user device.

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

- **Configure your Receiver connection** - Configuring your Receiver connections can reduce the bandwidth that ICA requires and improve performance
- **Change how Receiver is used** - Changing the way Receiver is used can also reduce the bandwidth required for a high-performance connection
- **Enable UDP audio** - This feature can maintain consistent latency on congested networks in Voice-over-IP (VoIP) connections
- **Use the latest versions of XenApp and Receiver for Linux** - Citrix continually enhances and improves performance with each release, and many performance features require the latest Receiver and server software

Configuring connections

On devices with limited processing power or where limited bandwidth is available, there is a trade-off between performance and functionality. Users and administrators can choose an acceptable mixture of rich functionality and interactive performance. Making one or more of these changes, often on the server not the user device, can reduce the bandwidth that a connection requires and can improve performance:

- **Enable SpeedScreen Latency Reduction** - SpeedScreen Latency Reduction improves performance over high latency connections by providing instant feedback to the user in response to typed data or mouse clicks. Use SpeedScreen Latency Reduction Manager to enable this feature on the server. By default, in Receiver, this is disabled for keyboard and only enabled for the mouse on high latency connections. See the Citrix Receiver for Linux OEM's Reference Guide.
- **Enable data compression** - Data compression reduces the amount of data transferred across the connection. This requires more processor resources to compress and decompress the data, but it can increase performance over low-bandwidth connections. Use Citrix Audio Quality and Image Compression policy settings to enable this feature.
- **Reduce the window size** - Change the window size to the minimum that is comfortable. On the XenApp Services site set the Session Options.
- **Reduce the number of colors** - Reduce the number of colors to 256. On the XenApp and XenDesktop Site, set the Session Options.
- **Reduce sound quality** - If audio mapping is enabled, reduce the sound quality to the minimum setting using the Citrix Audio quality policy setting.

Enabling UDP audio

UDP audio can improve the quality of phone calls made over the Internet. It uses User Datagram Protocol (UDP) instead of Transmission Control Protocol (TCP).

Note the following:

- UDP audio is not available in encrypted sessions (that is, those using TLS or ICA Encryption). In such sessions, audio transmission uses TCP.
- The ICA channel priority can affect UDP audio.

1. Set the following options in the ClientAudio section of module.ini:
   - Set EnableUDPAudio to True. By default, this is set to False, which disables UDP audio.
   - Specify the minimum and maximum port numbers for UDP audio traffic using UDPAudioPortLow and UDPAudioPortHigh respectively. By default, ports 16500 - 16509 are used.
2. Set client and server audio settings as follows so that the resultant audio is of a medium quality (that is, not high or low).

		Audio quality on client	Audio quality on client	Audio quality on client
		High	Medium	Low
Audio quality on server	High	High	Medium	Low
Audio quality on server	Medium	Medium	Medium	Low
Audio quality on server	Low	Low	Low	Low

Changing how Receiver is used

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

- **Avoid accessing large files using client drive mapping**. When you access a large file with client drive mapping, the file is transferred over the server connection. On slow connections, this might take a long time.
- **Avoid printing large documents on local printers**. When you print a document on a local printer, the print file is transferred over the server connection. On slow connections, this might take a long time.

- **Avoid playing multimedia content**. Playing multimedia content uses many bandwidth and can cause reduced performance.

Improving multimedia performance

The Receiver includes a broad set of technologies that provide a high-definition user experience for today's media-rich user environments. These improve the user experience when connecting to hosted applications and desktops, as follows:

- HDX MediaStream Windows Media Redirection
- HDX MediaStream Flash Redirection
- HDX RealTime Webcam Video Compression
- H.264 support

Configuring HDX Mediastream Windows Media Redirection

HDX Mediastream Windows Media Redirection overcomes the need for the high bandwidths required to provide multimedia capture and playback on virtual Windows desktops accessed from Linux user devices. Windows Media Redirection provides a mechanism for playing the media run-time files on the user device rather than on the server, thereby reducing the bandwidth requirements for playing multimedia files.

Windows Media Redirection improves the performance of Windows Media player and compatible players running on virtual Windows desktops. A wide range of file formats are supported, including:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAV sound files

Citrix Receiver includes a text-based translation table, MediaStreamingConfig.tbl, for translating Windows-specific media format GUIDs into MIME types GStreamer can use. You can update the translation table to do the following:

- Add previously unknown or unsupported media filters/file formats to the translation table
- Block problematic GUIDs to force fall-back to server-side rendering.
- Add more parameters to existing MIME strings to allow for troubleshooting of problematic formats by changing a stream's GStreamer parameters
- Manage and deploy custom configurations depending on the media file types supported by GStreamer on a user device.

With client-side fetching, you can also allow the user device to stream media directly from URLs of the form http://, <mms://>, or <rtsp://> rather than streaming the media through a Citrix server. The server is responsible for directing the user device to the media, and for sending control commands (including Play, Pause, Stop, Volume, Seek). But the server does not handle any media data. This feature requires advanced multimedia GStreamer libraries on the device.

To implement HDX MediaStream Windows Media Redirection

1. Install GStreamer 0.10, an open-source multimedia framework, on each user device that requires it. Typically, you install GStreamer before you install Citrix Receiver to allow the installation process to configure Citrix Receiver to use it.

   Most Linux distributions include GStreamer. Alternatively, you can download GStreamer from http://gstreamer.freedesktop.org.

2. To enable client-side fetching, install the required GStreamer protocol source *plugins* for the file types that users play on the device. You can verify that a plug-in is installed and operational using the gst-launch utility. If gst-launch can play the URL, the required plug-in is operational. For example, run gst-launch-0.10 playbin2 uri=http://example-source/file.wmv and check that the video plays correctly.

3. When installing Citrix Receiver on the device, select the GStreamer option if you are using the tarball script (this is done automatically for the .deb and .rpm packages).

Note about the client-side fetching feature:

- By default, this feature is enabled. You can disable it using the SpeedScreenMMACSFEnabled option in the Multimedia section of All-Regions.ini. With this option set to False, Windows Media Redirection is used for media processing.
- By default, all MediaStream features use the GStreamer playbin2 protocol. You can revert to the earlier playbin protocol for all MediaStream features except Client-Side Fetching, which continues to use playbin2, using the SpeedScreenMMAEnablePlaybin2 option in the Multimedia section of All-Regions.ini.
- Receiver does not recognize playlist files or stream configuration information files such as .asx or .nsc files. If possible, users must specify a standard URL that does not reference these file types. Use gst-launch to verify that a given URL is valid.

Note about GStreamer 1.0:

- By default, GStreamer 0.10 is used for HDX MediaStream Windows media redirection. GStreamer 1.0 is used only when GStreamer 0.10 is not available.
- If you want to use GStreamer 1.0, follow the instructions below:

1. Find the install directory of the GStreamer plug-ins. Depending on your distribution, the OS architecture, and the way you install GStreamer, the installation location of the plug-ins

varies. The typical installation path is /usr/lib/x86_64-linux-gnu/gstreamer-1.0 or $HOME/.local/share/gstreamer-1.0.

2. Find the install directory of Citrix Receiver for Linux. The default directory for privileged (root) user installations is /opt/Citrix/ICAClient. The default directory for non-privileged user installations is $HOME/ICAClient/platform (where platform can be linuxx64, for example). For more information, see Install and set up.
3. Install libgstflatstm1.0.so by making a symbolic link in the GStreamer plug-ins directory: ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so. This step might require elevated permissions, with sudo, for example.
4. Use gst_play1.0 as the player: ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play. This step might require elevated permissions, with sudo, for example.

- If you want to use GStreamer 1.0 in HDX RealTime Webcam Video Compression, use gst_read1.0 as the reader: ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

Configuring HDX MediaStream Flash Redirection

HDX MediaStream Flash Redirection enables Adobe Flash content to play locally on user devices, providing users with high definition audio and video playback, without increasing bandwidth requirements.

1. Ensure that your user device meets the feature requirements. For more information, see System requirements.
2. Add the following parameters to the [WFClient] section of wfclient.ini (for all connections made by a specific user) or the [Client Engine\Application Launching] section of All_Regions.ini (for all users of your environment):

HDXFlashUseFlashRemoting= Never Always

- Enables HDX Mediastream for Flash on the user device. By default, this is set to **Never** and users are presented with a dialog box asking them if they want to optimize Flash content when connecting to webpages containing that content.

HDXFlashEnableServerSideContentFetching=D Enabled

- Enables or disables server-side content fetching for Receiver. By default this is set to **Disabled**.

HDXFlashUseServerHttpCookie=Disabled Enabled

- Enables or disables HTTP cookie redirection. By default, this is set to **Disabled**.

HDXFlashEnableClientSideCaching=Disabled Enabled

- Enables or disables client-side caching for web content fetched by Receiver. By default, this is set to **Enabled**.
- **HDXFlashClientCacheSize= [25-250]**

  Defines the size of the client-side cache, in MB. This can be any size between 25 MB and 250 MB. When the size limit is reached, existing content in the cache is deleted to allow storage of new content. By default, this is set to **100**.

**HDXFlashServerSideContentC Temporary	NoCaching**

- Defines the type of caching used by Receiver for content fetched using server-side content fetching. By default, this is set to **Persistent**.

  Note: This parameter is required only if **HDXFlashEnableServerSideContentFetching** is set to **Enabled**.

3. Flash redirection is disabled by default. In /config/module.ini change FlashV2=Off to FlashV2=On to enable the feature.

Configure HDX RealTime webcam video compression

HDX RealTime provides a webcam video compression option to improve bandwidth efficiency during video conferencing, ensuring users experience optimal performance when using applications such as GoToMeeting with HD Faces, Skype for Business.

1. Ensure that your user device meets the feature requirements.
2. Ensure that the Multimedia virtual channel is enabled. To do this, open the module.ini configuration file, located in the $ICAROOT/config directory, and check that MultiMedia in the [ICA3.0] section is set to “On.”
3. Enable audio input by clicking Use my microphone and webcam on the Mic & Webcam page of the Preferences dialog.

Disable HDX RealTime webcam video compression

By default, optimum webcam performance is provided by HDX RealTime Webcam Video Compression. In some circumstances, however, you might require users to connect webcams using USB support. To do this, you must do the following:

- Disable HDX RealTime Webcam Video Compression
- Enable USB support for webcams

1. Add the following parameter to the [WFClient] section of the appropriate .ini file:

   HDXWebCamEnabled=Off

   For more information, see Customize Receiver using configuration files.

2. Open the usb.conf file, typically located at $ICAROOT/usb.conf.
3. Remove or comment out the following line:

   ```
   DENY: class=0e ## UVC (default via HDX RealTime Webcam Video Compression
   )
   ```

4. Save and close the file.

Configuring H.264 support

Receiver supports the display of H.264 graphics, including HDX 3D Pro graphics, that are served by XenDesktop 7. This support uses the deep compression codec feature, which is enabled by default. The feature provides better performance of rich and professional graphics applications on WAN networks compared with the existing JPEG codec.

Follow the instructions in this topic to disable the feature (and process graphics using the JPEG codec instead). You can also disable text tracking while still enabling deep compression codec support. This helps to reduce CPU costs while processing graphics that include complex images but relatively small amounts of text or non-critical text.

Important: To configure this feature, do not use any lossless setting in the XenDesktop Visual quality policy. If you do, H.264 encoding is disabled on the server and does not work in Receiver.

To disable deep compression codec support:

In wfclient.ini, set H264Enabled to False. This also disables text tracking.

To disable text tracking only

With deep compression codec support enabled, in wfclient.ini set TextTrackingEnabled to False.

Optimizing the performance of screen tiles

You can improve the way that JPEG-encoded screen tiles are processed using the direct-to-screen bitmap decoding, batch tile decoding, and deferred XSync features.

1. Ensure that your JPEG library supports these features.
2. In the Thinwire3.0 section of wfclient.ini, set DirectDecode and BatchDecode to True.

   Note: Enabling batch tile decoding also enables deferred XSync.

Enabling logging

To enable logging for Citrix Receiver for Linux:

1. Download the Citrix Receiver for Linux and install it on your Linux machine, setting the ICAROOT environment variable to the installation location.
2. For the Citrix Receiver for Linux, debug.ini is present in the configuration folder of ICAROOT. Create a symlink of this file at the $ICAROOT path by typing **> ln -s config/debug.ini debug.ini** from the command line.
3. Edit the debug.ini at $ICAROOT and add the required trace parameters under the [wfica] section.
4. Edit the $ICAROOT/config/module.ini file to add SyslogThreshold=7 at the end of the [WFClient] section. Doing so generates logs of all levels. To log only errors, set the SyslogThreshold to 3.
5. To get syslog traces, edit the syslog configuration file. Go to the /etc/rsyslog.conf file (or syslog.conf, depending on your Linux distribution) and make the following changes:

   To enable local logging from all facilities, ensure that the **$ModLoad imuxsock.so** line is uncommented at the beginning of the file.

   The next two changes in the configuration file are necessary for remote logging, but **not** required for local logging to syslog.

   Server-side configuration: Uncomment the following lines in the rsyslog.conf file of the syslog server:

   $ModLoad imtcp

   $InputTCPServerRun 10514

   Client-side configuration: Add the following line by replacing localhost with the IP of the remote server:
   ***.* @@localhost:10514**
6. Save your changes and then restart the syslog service by typing >**sudo service rsyslog restart** from the command line.

7. All syslog logs are saved at /var/log. To view or edit logs in this folder, you need sudo access. The logs are going to the user-all-drivers_proxy22.log file. You can configure the path and name of the log file by editing the following line under the RULES section in the rsyslog.cong file –

   user.* -/var/log/logfile_name.log

   You can edit the RULES section in the syslog configuration file. If the RULES section is not present in your syslog configuration file , you can add the RULES section from the sample rsyslog.conf file into your system syslog configuration file.

   Note: Every time you edit the rsyslog.conf file, you must restart the syslog service.

8. Launch the Receiver process (./selfservice at $ICAROOT) and after the session ends, you can find the log file at /var/log.
   By default, the logs are appended to the log file on subsequent launches. To track traces for each launch, edit the configuration file before each launch to change the logfile and restart the rsyslog service.

> **Note**
>
> To enable tracing, change the following parameters in the **$ICAROOT/debug.ini** file:
>
> - Connection Center Logging: under [conncenter] section, change “traceClasses” to “+TC_NCS”
> - Graphics (Thinwire) Logging: under [wfica] section, change “traceClasses” to “+TC_TW”
> - EUEM Logging: under [wfica] section, change “traceClasses” to “+TC_CLIB”
>
> To disable tracing, change “traceClasses” entries to null.
>
> For Example:
>
> [wfica]
>
> traceFlags =
>
> traceClasses =
>
> traceFeatures =
>
> traceFile = clb.log.$$
>
> traceBufferSize = 65536

Configuring multi-monitor layout persistence

This feature retains the session monitor layout information across endpoints. The session appears at the same monitor(s) as configured.

Prerequisite

This feature requires the following:

- StoreFront v3.15 or later.
- If .ICAClient is already present in the home folder of the current user:

  Delete All_Regions.ini file

  or

  To retain AllRegions.ini file, add the following lines at the end of the [Client Engine\Application Launching] section:

  SubscriptionUrl=

  PreferredWindowsBounds=

  PreferredMonitors=

  PreferredWindowState=

  SaveMultiMonitorPref=

If the .ICAClient folder is not present, it indicates a fresh install of the receiver. In that case the default setting for the feature is retained.

Examples of use cases

- Launch a session on any monitor in windowed mode and save the setting.
  When you relaunch the session, it appears in the same mode, on the same monitor, and in the same position.
- Launch a session on any monitor in full-screen mode and save the setting.
  When you relaunch the session, it appears in full-screen mode on the same monitor.
- Stretch and span a session in windowed mode across multiple monitors and then switch to full-screen mode. The session continues in full-screen across all monitors. When you relaunch the session, it appears in full-screen mode, spanning across all monitors.

> **Note**
>
> The layout is overwritten with every save, and the layout is saved only on the active StoreFront.
>
> If you launch multiple desktop sessions from the same StoreFront on different monitors, saving the layout in one session saves the layout information of all the sessions.

Configuring the save layout feature

To enable the save layout feature:

1. Install the StoreFront 3.15 or later version (equal or greater than v3.15.0.12) on a compatible Delivery Controller (DDC).
2. Download the build of Citrix Receiver for Linux 13.10 from the Downloads page and then install it on your Linux machine.
3. Set the ICAROOT environment variable to the install location.
4. Check whether the **All_Regions.ini** file is present in the **.ICAClient** folder. If so, delete it.
5. In the **$ICAROOT/config/All_Regions.ini** file, look for the field – **SaveMultiMonitorPref**. By default, the value of this field is "true" (meaning this feature is turned on). To toggle off this feature, set this field to false.
   If you make any changes to the value of **SaveMultiMonitorPref**, you must delete the **All_Regions.ini** file present in the **.ICAClient** folder to prevent value mismatches and a possible profile lockdown. Set or unset the **SaveMultiMonitorPref** flag before launching sessions.
6. Launch a new desktop session.
7. Click **Save Layout** on the desktop viewer toolbar to save the current session layout. A notification appears at the bottom right of the screen, indicating success.
   When you click Save layout, the icon greys out. This indicates that saving is in progress. When the layout is saved the icon appears normal.
   However, if the icon is grayed out for a long time, see Knowledge Center article CTX235895 for troubleshooting information.
8. Disconnect or log off the session.
   Relaunch the session. The session appears in the same mode, on the same monitor, and in the same position.

Limitations and unsupported scenarios

- Saving a layout for windowed mode session spanning across multiple monitors is not supported due to limitations with the Linux Display manager.
- Saving session information across monitors with varied resolution is not supported in this release and might result in unpredictable behavior.
- Customers deployments with multiple storefront

Using Citrix Virtual desktops on dual monitor

1. Select the desktop viewer and click the down arrow.
2. Select **Window**.

3. Drag the Citrix Virtual Desktops screen between the two monitors. Ensure that about half the screen is present in each monitor.
4. From the Citrix Virtual Desktop toolbar, select **Full-screen**.

   The screen extends to both the monitors.

Improving the user experience

March 5, 2019

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

Setting preferences

You can set preferences by clicking
Preferences on the Citrix Workspace app menu. You can control how desktops are displayed, connect to different applications and desktops, and manage file and device access.

To manage an account

To access desktops and applications, you need an account with XenDeskop or XenApp. Your IT help desk might ask you to add an account to Citrix Workspace for this purpose. Or they might ask you to use a different NetScaler Gateway or Access Gateway server for an existing account. You can also remove accounts from Citrix Workspace.

1. On the Accounts page of the Preferences dialog box, do one of the following:
   - To add an account, click Add. Your help desk may alternatively provide a provisioning file with account information that you can use to create an account.
   - To change details of a store that the account uses, such as the default gateway, click Edit.
   - To remove an account, click Remove.
2. Follow the on-screen prompts. You may be required to authenticate to the server.

To change how you see your desktops

This feature is not available with Citrix XenApp for UNIX sessions.

You can display desktops across the entire screen on your user device (full screen mode), which is the default, or in a separate window (windowed mode).

- On the General page of the Preferences dialog box, select a mode using the "**Display desktop in**" option.

Citrix Workspace app now has the **You can enable Desktop Viewer** toolbar functionality so it is possible dynamically modify the window configuration of your remote session from the original settings specified by the configuration mentioned here.

Desktop Viewer

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

Use the Desktop Viewer when users interact with their virtual desktop. The user's virtual desktop can be a published virtual desktop, or a shared or dedicated desktop. In this access scenario, the Desktop Viewer toolbar functionality allows the user to switch a session between windowed and full-screen session window, including multi-monitor support for the intersected monitors. Users can switch between desktop sessions and work with more than one desktop using multiple XenDesktop connections on the same user device. Buttons to minimize all desktop sessions, send the Ctrl+Alt+Del sequence, disconnect, and log off the session are provided to manage a user's session conveniently.

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

See the Linux OEM guide for advanced configuration entries to enable or disable Desktop Viewer or change the accessibility key sequence.

To reconnect sessions automatically

Citrix Workspace app can reconnect to desktops and applications that you become disconnected from (for example, if there is a network infrastructure issue):

- On the General page of the Preferences dialog box, select an option in Reconnect apps and desktops.

To control how local files are accessed

A virtual desktop or application may need to access files on your device. You can control the extent to which this happens.

1. On the File Access page of the Preferences dialog box, select a mapped drive and then one of the following options:

- Read and write - Allow the desktop or application to read and write to local files.
- Read only - Allow the desktop or application to read but not write to local files.
- No access - Do not allow the desktop or application to access local files.
- Ask me each time - Display a prompt each time the desktop or application needs to access local files.

2. If you selected one of the options that grants access to local files, you can additionally save time when browsing to locations on your user device. Click Add, specify the location, and select a drive to map to it.

To set up a microphone or webcam

You can change the way a virtual desktop or application accesses your local microphone or webcam:

On the Mic & Webcam page of the Preferences dialog box, select one of the following options:

- Use my microphone and webcam - Allow the microphone and webcam to be used by the desktop or application.
- Don’t use my microphone or webcam - Do not allow the microphone or webcam to be used by the desktop or application.

To set up Flash Player

You can choose how Flash content is displayed. This content is normally displayed in Flash Player and includes video, animation, and applications:

On the Flash page of the Preferences dialog box, select one of the following options:

- Optimize content - Improve playback quality at the risk of reducing security.
- Don’t optimize content - Provide basic playback quality without reducing security.
- Ask me each time - Prompt me each time Flash content is displayed.

Configuring ClearType font smoothing

ClearType font smoothing (also known as subpixel font rendering) improves the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing. You can turn this feature on or off. Or you specify the type of smoothing by editing the following setting in [WFClient] section of the appropriate configuration file:

FontSmoothingType = number

where number can take one of the following values:

Value	Behavior
0	The local preference on the device is used. This value is defined by the FontSmoothingTypePref setting.
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing

Both standard smoothing and ClearType smoothing can increase Citrix Workspace app's bandwidth requirements.

Important: The server can configure FontSmoothingType through the ICA file. This takes precedence over the value set in [WFClient]. If the server sets the value to 0, the local preference is determined by another setting in the [WFClient]:

FontSmoothingTypePref = number

where number can take one of the following values:

Value	Behavior
0	No smoothing
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing (default)

Configuring special folder redirection

In this context, there are only two special folders for each user:

- The user's Desktop folder
- The user's Documents folder (My Documents on Windows XP)

Special folder redirection enables you to specify the locations of a user's special folders so that these remain fixed across different server types and server farm configurations. It is important if, for example, a mobile user logs on to servers in different server farms. For static, desk-based workstations, where the user can log on to servers that reside in a single server farm, special folder redirection is rarely necessary.

To configure special folder redirection

A two-part procedure is as follows. First, you enable special folder redirection by making an entry in module.ini; then you specify the folder locations in the [WFClient] section, as described here:

1. Add the following text to module.ini (for example, $ICAROOT/config/module.ini):

   [ClientDrive]

   SFRAllowed = True

2. Add the following text to the [WFClient] section (for example, $HOME/.ICAClient/wfclient.ini):

   DocumentsFolder = documents

   DesktopFolder = desktop

   where documents and desktop are the UNIX filenames, including the full path, of the directories to use as the users Documents and Desktop folders respectively. For example:

   DesktopFolder = $HOME/.ICAClient/desktop

   - You can specify any component in the path as an environment variable, for example, $HOME.
   - Specify values for both parameters.
   - The directories you specify must be available through client device mapping. That is, the directory must be in the subtree of a mapped client device.
   - Use the drive letters C or higher.

Setting up server-client content redirection

Server-client content redirection enables administrators to specify that URLs in a published application are opened using a local application. For example, opening a link to a webpage while using Microsoft Outlook in a session opens the required file using the browser on the user device. Server-client content redirection enables administrators to allocate Citrix resources more efficiently, thereby providing users with better performance.

The following types of URL can be redirected:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Older Real Players)

If Citrix Workspace App for Linux does not have an appropriate application or cannot directly access the content, the URL is opened using the server application.

Server-client content redirection is configured on the server and enabled by default in Citrix Workspace app if the path includes RealPlayer and at least one of Firefox, Mozilla, or Netscape.

> **Note**
>
> For more information about RealPlayer for Linux, see http://www.real.com/resources/unix/.

To enable server-client content redirection if RealPlayer and a browser are not in the path

1. Open the configuration file wfclient.ini.
2. In the [Browser] section, modify the following settings:

   Path=path

   Command=command

   where path is the directory where the browser executable is located and command is the name of the executable used to handle redirected browser URLs, appended with the URL sent by the server. For example:

   $ICAROOT/nslaunch netscape,firefox,mozilla

   This setting specifies the following:

   - The nslaunch utility is run to push the URL into an existing browser window
   - Each browser in the list is tried in turn until content can be displayed successfully
3. In the [Player] section, modify the following settings:

   Path=path

   Command=command

   where path is the directory where the RealPlayer executable is located and command is the name of the executable used to handle the redirected multimedia URLs, appended with the URL sent by the server.
4. Save and close the file.

> **Note**
>
> For both Path settings, you need only specify the directory where the browser and RealPlayer executables reside. You do not need to specify the full path to the executables. For example, in the [Browser] section, Path might be set to /usr/X11R6/bin rather than /usr/X11R6/bin/netscape. In addition, you can specify multiple directory names as a colon-separated list. If these settings are not specified, the user's current $PATH is used.

To turn off server-client content redirection from Citrix Workspace

1. Open the configuration file module.ini.
2. Change the CREnabled setting to Off.
3. Save and close the file.

Controlling keyboard behavior

To generate a remote Ctrl+Alt+Delete key combination:

1. Decide which key combination creates the Ctrl+Alt+Delete combination on the remote virtual desktop.
2. In the WFClient section of the appropriate configuration file, configure UseCtrlAltEnd accordingly:
    - True means that Ctrl+Alt+End passes the Ctrl+Alt+Delete combination to the remote desktop.
    - False (default) means that Ctrl+Alt+Enter passes the Ctrl+Alt+Delete combination to the remote desktop.

Using xcapture

The Citrix Workspace app package includes a helper application, xcapture, to assist with the exchange of graphical data between the server clipboard and non-ICCCM-compliant X Windows applications on the X desktop. Users can use xcapture to:

- Capture dialog boxes or screen areas and copy them between the user device desktop (including non-ICCCM-compliant applications) and an application running in a connection window
- Copy graphics between a connection window and X graphics manipulation utilities xmag or xv

To start xcapture from the command line

At the command prompt, type /opt/Citrix/ICAClient/util/xcapture and press ENTER (where /opt/Citrix/ICAClient is the directory in which you installed Citrix Workspace app).

To copy from the user device desktop

1. From the xcapture dialog box, click From Screen. The cursor changes to a crosshair.
2. Choose from the following tasks:
    - Select a window. Move the cursor over the window you want to copy and click the middle mouse button.

- Select a region. Hold down the left mouse button and drag the cursor to select the area you want to copy.
- Cancel the selection. Click the right mouse button. While dragging, you can cancel the selection by clicking the right button before releasing the middle or left mouse button.

3. From the xcapture dialog box, click To ICA. The xcapture button changes color to show that it is processing the information.
4. When the transfer is complete, use the appropriate paste command in an application launched from the connection window.

To copy from xv to an application in a connection window

1. From xv, copy the information.
2. From the xcapture dialog box, click From XV and then click To ICA. The xcapture button changes color to show that it is processing the information.
3. When the transfer is complete, use the appropriate paste command in an application launched from the connection window.

To copy from an application in the connection window to xv

1. From the application in a connection window, copy the information.
2. From the xcapture dialog box, click From ICA and then click To XV. The xcapture button changes color to show that it is processing the information.
3. When the transfer is complete, paste the information into xv.

Reconnecting users automatically

This topic describes the HDX Broadcast auto-client reconnection feature. Citrix recommends that you use this feature with the HDX Broadcast session reliability feature.

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

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

By default, Citrix Workspace App for Linux waits 30 seconds before attempting to reconnect to a disconnected session and attempts to reconnect to that session three times.

When connecting through an AccessGateway, ACR is not available. To protect against network dropouts, ensure that Session Reliability is enabled both on the Server and Client, as well as configured on the AccessGateway.

For instructions on configuring HDX Broadcast auto-client reconnection, see your XenApp and XenDesktop documentation.

Ensure session reliability

This topic describes the HDX Broadcast session reliability feature, which is enabled by default.

With HDX Broadcast session reliability, users continue to see a published application's window if the connection to the application experiences an interruption. For example, wireless users entering a tunnel may lose their connection when they enter the tunnel and regain it when they emerge on the other side. During the downtime, all of the user's data, key presses, and other interactions are stored, and the application appears frozen. When the connection is re-established, these interactions are replayed into the application.

When auto-client reconnection and session reliability are configured, session reliability takes precedence if there is a connection problem. Session reliability attempts to re-establish a connection to the existing session. It might take up to 25 seconds to detect a connection problem. And then takes a configurable period (the default is 180 seconds) to attempt the reconnection. If session reliability fails to reconnect, then auto-client reconnect attempts to reconnect.

If HDX Broadcast session reliability is enabled, the default port used for session communication switches from 1494 to 2598.

Citrix Workspace users cannot override the server settings. For more information, see the XenApp and XenDesktop documentation.

> **Important**
>
> HDX Broadcast session reliability requires that another feature, Common Gateway Protocol, is enabled (using policy settings) on the server. Disabling Common Gateway Protocol also disables HDX Broadcast session reliability.

Relative Mouse

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

> **Note**
>
> This feature is available only in sessions running on XenApp or XenDesktop 7.8 (or later). It is disabled by default.

To enable the feature:

In the file $HOME/.ICAClient/wfclient.ini, in the section [WFClient], add the entry RelativeMouse=1.

This step enables the feature but keeps it inactive until you activate it.

> **Tip**
>
> Refer to the section Alternative Relative Mouse values for additional information about enabling relative mouse features.

To activate the feature:

Type Ctrl/F12.

After the feature is enabled, type Ctrl/F12 again to synchronize the server pointer position with the client. The server and client pointer positions are not synchronized when using Relative Mouse.

To deactivate the feature:

Type Ctrl-Shift/F12.

The feature is also switched off when a session window loses focus.

Alternative Relative Mouse values

Alternatively, consider using the following values for RelativeMouse:

- RelativeMouse=2 Enables the feature and activates it whenever a session window gains focus.
- RelativeMouse=3 Enables, activates, and keeps the feature activated always.
- RelativeMouse=4 Enables or disables the feature when the client-side mouse pointer is hidden or shown. This mode is suitable for automatically enabling or disabling relative mouse for first-person gaming-style application interfaces.

To change the keyboard commands, add settings like:

- RelativemouseOnChar=F11
- RelativeMouseOnShift=Shift
- RelativemouseOffChar=F11
- RelativeMouseOffShift=Shift

The supported values for **RelativemouseOnChar** and **RelativemouseOffChar** are listed under [Hotkey Keys] in the config/module.ini file in the Citrix Workspace app installation tree. The values for **RelativeMouseOnShift** and **RelativeMouseOffShift** set the modifier keys to be used and are listed under the [Hotkey Shift States] heading.

Secure

February 20, 2019

In this article:

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

- A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server, or TLS 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.
- Secure Gateway or SSL Relay solutions with Transport Layer Security (TLS) protocols. TLS versions 1.0 through 1.2 are supported.
- 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.

Connecting through a proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Receiver and your Citrix XenApp or Citrix XenDesktop deployment. Citrix Receiver supports the SOCKS protocol, along with the Secure Gateway and Citrix SSL Relay, the secure proxy protocol, and Windows NT Challenge/Response (NTLM) authentication.

The list of supported proxy types is restricted by the contents of Trusted_Regions.ini and Untrusted_Regions.ini to the Auto, None, and Wpad types. If you use the SOCKS, Secure or Script types, edit those files to add the additional types to the permitted list.

> **Note**
>
> To ensure a secure connection, enable TLS.

Connecting through a secure proxy server

Configuring connections to use the secure proxy protocol also enables support for Windows NT Challenge/Response (NTLM) authentication. If this protocol is available, it is detected and used at run time without any additional configuration.

> **Important**
>
> NTLM support requires that the OpenSSL library, libcrypto.so, is installed on the user device. This library is often included in Linux distributions, but can be downloaded from http://www.openssl.org/ if necessary in new window.

Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay

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

Connecting with the Secure Gateway

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

Citrix Receiver uses settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway. For information about configuring proxy server settings for Citrix Receiver, see the Web Interface documentation.

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. For more information, see the XenApp (Secure Gateway) documentation.

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

- The fully qualified domain name (FQDN) of the Secure Gateway server.
- The port number of the Secure Gateway server. 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 referred to as the domain name.

Connecting with Citrix SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the XenApp server for TLS-secured communication. When the SSL Relay receives a TLS connection, it decrypts the data before redirecting it to the server.

If you configure SSL Relay to listen on a port other than 443, you must specify the non-standard listening port number to Citrix Receiver.

You can use Citrix SSL Relay to secure communications:

- Between a TLS-enabled user device and a server
- With Web Interface, between the XenApp server and the web server

For information about configuring and using SSL Relay to secure your installation, see the XenApp documentation. For information about configuring the Web Interface to use TLS encryption, see the Web Interface documentation.

Configuring and enabling TLS

You can control the versions of the TLS protocol that can be negotiated by adding the following configuration options in the [WFClient] section:

- MinimumTLS=1.0
- MaximumTLS=1.2

These values are the default values, which are implemented in code. Adjust them as you require.

Note: These values are read whenever programs start. If you change them after starting selfservice or storebrowse, type: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse.**

Note: Citrix Receiver for Linux does not allow the use of the SSLv3 protocol.

Citrix Receiver for Linux supports DTLS 1.0 and TLS 1.0, 1.1 and 1.2, with the following cipher suites:

- RSA+AES256-SHA (RSA for key exchange, AES 256 for encryption, SHA-1 for digest)
- RSA+AES256-SHA256 (RSA for key exchange, AES 256 for encryption, SHA-256 for digest)
- RSA+AES128-SHA (RSA for key exchange, AES 128 for encryption, SHA-1 for digest)

- RSA+DES-CBC3-SHA (RSA for key exchange, Triple-DES for encryption, SHA-1 for digest)
- RSA+RC4128-MD5 (RSA for key exchange, RC4 128 for encryption, MD5 for digest)
- RSA+RC4128-SHA (RSA for key exchange, RC4 128 for encryption, SHA-1 for digest)
- RSA+AES128_GCM+SHA256 (RSA for key exchange, AES 128 for encryption, SHA-256 for digest)
- RSA+AES256_GCM+SHA384 (RSA for key exchange, AES 256 for encryption, SHA-384 for digest)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Elliptic curve Diffie–Hellman for key exchange, RSA for authentication, AES 256, and GCM SHA 384 for digest)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (Elliptic curve Diffie–Hellman for key exchange, RSA for authentication, AES 256, and CBC SHA 384 for digest)
- TLS_RSA_AES256_CBC_SHA256 (RSA for authentication, AES 256, and CBC SHA 256 for digest)

The effective encryption key size is as defined for that standard SSL/TLS cipher suite as named above:

- RC4 algorithm: 128 bits (stream cipher)
- Triple DES algorithm: 3x64 bits (effective size 3x56=168 bits) (block size 64 bits)
- AES algorithm: 128 bits or 256 bits (block size 128)
- For RSA key exchange and authentication the supported key lengths (modulus) range from 1,024 bits to 4,096 bits.
- For ECDH key exchange, the supported elliptic curves are NIST P-256 and NIST P-384 (256 bit and 384 bit key lengths).

To select the cipher suite set, add the following configuration option in the [WFClient] section:

- SSLCiphers=GOV

This value is the default value. Other recognized values are COM and ALL.
Note: As with the TLS version configuration, if you change this after starting selfservice or storebrowse you must type:
killall AuthManagerDaemon ServiceRecord selfservice storebrowse

Installing root certificates on user devices

To use TLS, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate. By default, Citrix Receiver supports the following certificates.

Certificate	Issuing Authority
Class4PCA_G2_v2.pem	VeriSign Trust Network
Class3PCA_G2_v2.pem	VeriSign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority

Certificate	Issuing Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

You are not required to obtain and install root certificates on the user device to use the certificates from these Certificate Authorities. However, if you choose to use a different Certificate Authority, you must obtain and install a root certificate from the Certificate Authority on each user device.

Citrix Receiver for Linux supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

Note: Receiver for Linux 13.0 uses
c_rehash from the local device. Version 13.1 and subsequent versions use the
ctx_rehash tool as described in the following steps.

Use a root certificate

If you authenticate a server certificate that was issued by a certificate authority and is not yet trusted by the user device, follow these instructions before adding a StoreFront store.

1. Obtain the root certificate in PEM format.
   Tip: If you cannot find a certificate in this format, use the openssl utility to convert a certificate in CRT format to a .pem file.
2. As the user who installed the package (usually root):
   a) Copy the file to $ICAROOT/keystore/cacerts.
   b) Run the following command:
   ```
   $ICAROOT/util/ctx_rehash
   ```

Use an intermediate certificate

If your StoreFront server is not able to provide the intermediate certificates that match the certificate it is using, or you install intermediate certificates to support smart card users, follow these steps before adding a StoreFront store.

1. Obtain one or more intermediate certificates separately in PEM format.
   Tip: If you cannot find a certificate in this format, use the openssl utility to convert a certificate in CRT format to a .pem file.
2. As the user who installed the package (usually root):
   a) Copy one or more files to $ICAROOT/keystore/intcerts.

b) Run the following command as the user who installed the package:
`$ICAROOT/util/ctx_rehash`

Enabling smart card support

Citrix Receiver for Linux supports various smart card readers. If smart card support is enabled for both the server and Receiver, you can use smart cards for the following purposes:

- Smart card logon authentication. Use smart cards to authenticate users to Citrix XenApp servers.
- Smart card application support. Enable smart card-aware published applications to access local smart card devices.

Smart card data is security sensitive and should be transmitted over a secure authenticated channel, such as TLS.

Smart card support has the following prerequisites:

- Your smart card readers and published applications must be PC/SC industry standard compliant.
- Install the appropriate driver for your smart card.
- Install the PC/SC Lite package.
- Install and run the pcscd Daemon, which provides middleware to access the smart card using PC/SC.
- On a 64-bit system, both 64-bit and 32-bit versions of the "libpscslite1" package must be present.

Important: If you are using the SunRay terminal with SunRay server software Version 2.0 or later, install the PC/SC SRCOM bypass package, available for download from http://www.sun.com/.

For more information about configuring smart card support on your servers, see the XenApp and XenDesktop documentation.

Connecting through NetScaler Gateway

Citrix NetScaler Gateway (formerly Access Gateway) secures connections to StoreFront stores, and lets administrators control, in a detailed way, user access to desktops and applications.

To connect to desktops and applications through NetScaler Gateway

1. Specify the NetScaler Gateway URL that your administrator provides. You can do this in one of these ways:

- The first time you use the self-service user interface, you are prompted to enter the URL in the Add Account dialog box
- When you later use the self-service user interface, enter the URL by clicking Preferences > Accounts > Add
- If you are establishing a connection with the storebrowse command, enter the URL at the command line

The URL specifies the gateway and, optionally, a specific store:

- To connect to the first store that Receiver finds, use a URL of the form https://gateway.company.com.
- To connect to a specific store, use a URL of the form https://gateway.company.com?<storename>. This dynamic URL is in a non-standard form; do not include = (the equals sign character) in the URL. If you are establishing a connection to a specific store with storebrowse, you might need quotation marks around the URL in the storebrowse command.

2. When prompted, connect to the store (through the gateway) using your user name, password, and security token. For more information on this step, see the NetScaler Gateway documentation.

   When authentication is complete, your desktops and applications are displayed.

Configuring deprecated cipher suites

Cipher suites with the prefix TLS_RSA_ do not offer forward secrecy. These cipher suites are now generally deprecated by the industry. However, to support backward compatibility with older versions of XenApp and XenDesktop, Receiver for Linux has an option to enable these cipher suites.

Flags have been created to allow the usage of deprecated cipher suites. In Receiver for Linux version 13.10, these flags are enabled by default, but they do not enforce deprecation for the cipher suites using the AES or 3DES algorithms by default. However, you can modify and use these flags to enforce the deprecation more strictly.

For better security, set the flag Enable_TLS_RSA_ to False.

Following is the list of deprecated cipher suites:

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Note**
>
> The last two cipher suites use the RC4 algorithm and are deprecated because they are insecure. You might also consider the TLS_RSA_3DES_CBC_EDE_SHA cipher suite to be deprecated. You can use flags to enforce all these deprecations.

For information on configuring DTLS v1.2, see Adaptive transport.

Prerequisite

To configure this feature on client, perform the following step:

If .ICAClient is already present in the home folder of the current user:

- Delete All_Regions.ini file

Or

- To retain AllRegions.ini file, add the following lines at the end of the [Network\SSL] section:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

If the .ICAClient folder is not present in the home folder of the current user, then it indicates a fresh install of the receiver. In that case, the default setting for the features is retained.

To configure deprecated cipher suites

1. Open the **$ICAROOT/config/All_Regions.ini** file.
2. Under the **Network\SSL** section, use the following three flags to enable or disable the deprecated cipher suites:
   - **Enable_TLS_RSA_**: By default, the flag Enable_TLS_RSA_ is set to True.
     Set the flag Enable_TLS_RSA_ to true to view the following cipher suites:
     - TLS_RSA_AES256_GCM_SHA384
     - TLS_RSA_AES128_GCM_SHA256
     - TLS_RSA_AES256_CBC_SHA256
     - TLS_RSA_AES256_CBC_SHA
     - TLS_RSA_AES128_CBC_SHA
     - TLS_RSA_3DES_CBC_EDE_SHA

> **Important**
>
> Set the flag Enable_TLS_RSA_ to true to use the other two cipher suites Enable_RC4-MD5 and Enable_RC4_128_SHA.

- **Enable_RC4-MD5**: By default, the flag Enable_RC4-MD5 is set to **False**.
  Set this flag to true to enable the RC4-MD5 cipher suite.
- **Enable_RC4_128_SHA**: By default, the flag Enable_RC4_128_SHA is set to **False**.
  Set this flag to true to enable the RC4_128_SHA cipher suite.

3. Save the file.

The following table lists the cipher suites in each set:

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open		FIPS				SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

> **Important**
>
> In the future, Citrix will be supporting only the following three cipher suites:
>
> - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS 1.2/DTLS 1.2, GOV/ALL
> - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS 1.2/DTLS 1.2 GOV/ALL
> - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – TLS 1.0/1.1/1.2, DTLS 1.0/1.2 COM/ALL
>
> **Note**
>
> All cipher suites above are FIPS- and SP800-52- compliant. The first two are allowed only for (D)TLS1.2 connections. See **Table 1 – Cipher suite support matrix** for a comprehensive representation of cipher suite supportability.

Troubleshoot

February 20, 2019

This article contains information to help administrators troubleshoot issues with Citrix Receiver for Linux.

Connection issues

You might encounter the following connection issues.

I cannot connect properly to a published resource or desktop session

If, when establishing a connection to a Windows server, a dialog box appears with the message "Connecting to server…" but no subsequent connection window appears, you might need to configure the server with a Client Access License (CAL). For more information about licensing, see Licensing.

I sometimes fail to connect when I try reconnecting to sessions

Sometimes reconnecting to a session with a higher color depth than that requested by Receiver causes the connection to fail. This is due to a lack of available memory on the server. If the reconnection fails, Receiver tries to use the original color depth. Otherwise, the server tries to start a new session with the requested color depth, leaving the original session in a disconnected state. However, the second connection might also fail if there is still a lack of available memory on the server.

I cannot connect to a server using its full Internet name

Citrix recommends that you configure DNS (Domain Name Server) on your network to enable you to resolve the names of servers to which you want to connect. If you do not have DNS configured, it may not be possible to resolve the server name to an IP address. Alternatively, you can specify the server by its IP address, rather than by its name. TLS connections require a fully qualified domain name, not an IP address.

I get a "Proxy detection failure" error message when connecting

If your connection is configured to use automatic proxy detection and you see a "Proxy detection failure: Javascript error" error message when trying to connect, copy the wpad.dat file into $ICAROOT/util. Run the following command, where hostname is the hostname of the server to which you are trying to connect:


```
cat wpad.dat | ./pacexec pac.js FindProxyForURL <http://hostname>
    hostname 2\>&1 | grep  “undeclared variable”
```

If you get no output, there is a serious issue with the wpad.dat file on the server that you need to investigate. However, if you see output such as “assignment to undeclared variable …” you can fix the problem. Open pac.js and for each variable listed in the output, add a line at the top of the file in the following format, where “…” is the variable name.

var …;

Sessions are very slow to start

If a session does not start until you move the mouse, there might be a problem with random number generation in the Linux kernel. As a workaround, run an entropy-generating daemon such as rngd (which is hardware-based) or haveged (from Magic Software).

Weak cipher-suites for SSL connections

When making a TLS connection, with the 13.7 release, the Receiver for Linux offers a more modern and restricted set of cipher suites by default.
If you are connecting to a server that requires an older cipher suite, set the configuration option SSL-Ciphers=ALL in the [WFClient] section of a configuration file.

When using the UDT protocol, I see the error message: Connection to “…” has been lost

The reason might be that the connection goes through a router with a Maximum Transmission Unit for UDT that is smaller than the default of 1,500 bytes. Try both:

- Uncomment the udtMSS entry in $ICAROOT/config/All_Regions.ini and in $HOME/.ICAClient/All_Regions.ini
- Set udtMSS=1000 in a configuration file

Connection errors

Connection errors might produce various different error dialogs. Examples are:

- Error in connection: A protocol error occurred while communicating with the Authentication Service
- The Authentication Service could not be contacted
- Your account cannot be added using this server address

Some problems might cause such errors, including:

- When the local computer and the remote computer cannot negotiate a common TLS protocol. For more information, see Configure and enable TLS.
- When the remote computer requires an older cipher suite for a TLS connection. In this case, you can set the configuration option SSLCiphers=ALL in the [WFClient] section of a configuration file and run **killall AuthManagerDaemon ServiceRecord selfservice storebrowse** before restarting the connection.
- When the remote computer requests a client certificate inappropriately. IIS should only "accept" or "require" certificates for "Citrix/Authentication/Certificate."
- Other problems.

Display issues

Why am I seeing Screen Tearing?

Screen tearing occurs when parts of two (or more) different frames appear on the screen at the same time, in horizontal blocks. This is most visible with large areas of fast changing content on screen. Although the data is captured at the VDA in a way that avoids tearing, and the data is passed to the client in a way that doesn't introduce tearing, X11 (the Linux/Unix graphics subsystem) does not provide a consistent way to draw to the screen in a way that prevents tearing.

To prevent screen tearing, Citrix recommends the standard approach which synchronizes application drawing with the drawing of the screen. That is, wait for vsvnc, to initiate the drawing of the next frame. There are some options when using Linux, depending on the graphics hardware you have on the client and what window manager you are using. These options are divided into two groups of solutions:

- X11 GPU settings
- Use a Composition Manager

X11 GPU Configuration

For Intel HD graphics, create a file in the xorg.conf.d called
20-intel.conf with the following contents:

Section "Device"

```
1 Identifier     "Intel Graphics"
2
3 Driver         "intel"
4
5 Option         "AccelMethod" "sna"
6
```



```
7  Option          "TearFree" "true"
```

EndSection

For Nvidia graphics, locate the file in the xorg.conf.d folder that contains the "MetaModes" Option for your configuration. For each comma separated MetaMode used add the following:

{ForceFullCompositionPipeline = On}

For example:

Option "MetaModes" "DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}"

Note: Different Linux distributions use different paths to xorg.conf.d, for example, /etc/X11/xorg.conf.d, or, /user/share/X11/xorg.conf.d.

Composition Managers

Use the following:

- Compiz (built into Ubuntu Unity). Install the "CompizConfig Settings Manager."

  Run "CompizConfig Settings Manager"

  Under "General->Composition," uncheck "Undirect Fullscreen Windows"

Note: "CompizConfig Settings Manager" should be used with caution, as incorrectly changing values can prevent the system from launching.

- Compton (an add-on utility). Refer to the man page/documentation for Compton for full details. For example, run the following command:

  compton –vsync opengl –vsync -aggressive

Incorrect keystrokes appear when I use the keyboard

If you are using a non-English language keyboard, the screen display may not match the keyboard input. In this case, you should specify the keyboard type and layout that you are using. For more information about specifying keyboards, see Control keyboard behavior.

I see excessive redrawing when moving seamless windows

Some window managers continuously report the new window position when moving a window, which can result in excessive redrawing. To fix this problem, switch the window manager to a mode that draws only window outlines when moving a window.

Icon compatibility

Receiver creates window icons that work with most window managers, but are not fully compatible with the X Inter-Client Communication Convention.

To provide full icon compatibility

1. Open the wfclient.ini configuration file.
2. Edit the following line in the [WFClient] section: UseIconWindow=True
3. Save and close the file.

I have cursor visibility problems

The cursor can be difficult to see if it is the same or similar in color to the background. You can fix this issue by forcing areas of the cursor to be black or white.

To change the color of the cursor

1. Open the wfclient.ini configuration file.
2. Add one of the following lines to the [WFClient] section:

   CursorStipple=ffff,ffff (to make the cursor black)

   CursorStipple=0,0 (to make the cursor white)
3. Save and close the file.

I experience color flashing on the screen

When you move the mouse into or out of a connection window, the colors in the non-focused window may start to flash. This issue is a known limitation when using the X Windows System with Pseudo-Color displays. If possible, use a higher color depth for the affected connection.

I experience rapid color changes with TrueColor displays

Users have the option of using 256 colors when connecting to a server. This option assumes that the video hardware has palette support to enable applications to change the palate colors to produce animated displays.

TrueColor displays have no facility to emulate the ability to produce animations by rapidly changing the palette. Software emulation of this facility is expensive both in terms of time and network traffic. To reduce this cost, Receiver buffers rapid palette changes, and updates the real palette only every few seconds.

Japanese characters display incorrectly on my screen

Receiver uses EUC-JP or UTF-8 character encoding for Japanese characters, while the server uses SJIS character encoding. Receiver does not translate between these character sets. This can cause problems displaying files that are saved on the server and viewed locally, or saved locally and viewed on the server. This issue also affects Japanese characters in parameters used in extended parameter passing.

I want to make a session that spans multiple monitors

Full-screen sessions span all monitors by default, but a command-line multi-monitor display control option, -span, is also available. It allows full-screen sessions to span multiple monitors.

Desktop viewer toolbar functionality allows you to switch a session between windowed and full screen session window, including multi-monitor support for the intersected monitors. For details, see Improving the user experience.

Important: -span has no effect on Seamless or normal windowed sessions (including those in maximized windows).

The - span option has the following format:
-span [h][o][a|mon1[,mon2[,mon3,mon4]]]

If h is specified, a list of monitors is printed on stdout. And if that is the whole option value, wfica then exits.

If o is specified, the session window has the override-redirect redirect attribute.

Caution: The use of this option value is not recommended. It is intended as a last resort, for use with uncooperative window managers. The session window is not visible to the window manager, does not have an icon, and cannot be restacked. It can be removed only by ending the session.

If a is specified, Receiver tries to create a session that covers all monitors.

Receiver assumes that the rest of the -span option value is a list of monitor numbers. A single value selects a specific monitor, two values select monitors at the top-left and bottom-right corners of the required area, four specify monitors at the top, bottom, left, and right edges of the area.

Assuming o was not specified, wfica uses the _NET_WM_FULLSCREEN_MONITORS message to request an appropriate window layout from the window manager, if it is supported. Otherwise, it uses size and position hints to request the desired layout.

The following command can be used to test for window manager support:
xprop -root | grep _NET_WM_FULLSCREEN_MONITORS

If there is no output, there is no support. If there is no support, you may need an override-redirect window. You can set up an override-redirect window using -span o.

To make a session that spans multiple monitors from the command line:

1. At a command prompt, type:

   /opt/Citrix/ICAClient/wfica -span h

   A list of the numbers of the monitors currently connected to the user device is printed to stdout and wfica exits.

2. Make a note of these monitor numbers.

3. At a command prompt, type:

   /opt/Citrix/ICAClient/wfica -span [w[,x[,y,z]]]

   where w, x, y, and z are monitor numbers obtained in step 1 above and the single value w, specifies a specific monitor, two values w and x specify monitors at the top-left and bottom-right corners of the required area, and four values w, x, y and z specify monitors at the top, bottom, left, and right edges of the area.

   Important: Define the WFICA_OPTS variable before starting selfservice or connecting to the Web interface through a browser. To do this, edit your profile file, normally found at $HOME/.bash_profile or $HOME/.profile, adding a line to define the WFICA_OPTS variable. For example:

   export WFICA_OPTS=”-span a”

   This change affects both XenApp and XenDesktop sessions.

   If you have started selfservice or storebrowse, remove processes they started in order for the new environment variable to take effect. Remove them with:

   killall AuthManagerDaemon ServiceRecord storebrowse

I cannot escape from a full-screen session to use local applications or another session

The reason is that the client-side system UI is hidden and the Keyboard Transparency feature disables the usual keyboard command, for example Alt+Tab, sending the command to the server instead.

As a workaround, use CTRL+F2 to turn off the Keyboard Transparency feature temporarily until the focus next returns to the session window. An alternative workaround is to set TransparentKeyPassthrough to No in $ICAROOT/config/module.ini. This disables the Keyboard Transparency feature. However you might have to override the ICA file by adding this setting in the All_regions.ini file.

Browser Issues

When I click on a link in a Windows session, the content appears in a local browser

Server-client content redirection is enabled in wfclient.ini. This causes a local application to run. To disable server-client content redirection, see Set up server-client content redirection.

When accessing published resources, my browser prompts me to save a file

Browsers other than Firefox and Chrome may require configuration before you can connect to a published resource. If you are connecting through the Web Interface, you may be able to access the Web Interface home page with the list of resources. However, when trying to access a resource by clicking an icon on the page, your browser prompts you to save the ICA file.

To configure a different browser for use with Web Interface

Details vary among browsers, but you can set up the MIME data types in the browser so that the $ICAROOT/wfica is executed as a helper application when the browser encounters data with the application/x-ica MIME type or an .ica file.

The installer does not support a specific browser

If you have problems using a specific web browser, set the environment variable BROWSER to specify the local path and name of the required browser before running setupwfc.

When I launch desktops or applications in Firefox, nothing happens

Try enabling the ICA plug-in.

The ICA plug-in is enabled in Firefox, however desktop and application sessions are not starting

Try disabling the ICA plug-in.

Other issues

You might also encounter the following issues.

I want to know if the server has instructed Receiver to close a session

You can use the *wfica* program to log when it has received a command to terminate the session from the server.

To record this information through the syslog system, add *SyslogThreshold* with the value 6 to the [WFClient] section of the configuration file. This enables the logging of messages that have a priority of LOG_INFO or higher. The default value for *SyslogThreshold* is 4 (=LOG_WARNING).

Similarly, to have *wfica,* send the information to standard error, and add *PrintLogThreshold* with the value 6 to the [WFClient] section. The default value for *PrintLogThreshold* is 0 (=LOG_EMERG).

Refer to your operating system's documentation for instructions on configuring your syslog system.

My configuration file settings no longer work

For each entry in wfclient.ini, there must be a corresponding entry in All_Regions.ini for the setting to take effect. In addition, for each entry in the [Thinwire3.0], [ClientDrive], and [TCP/IP] sections of wfclient.ini, there must be a corresponding entry in canonicalization.ini for the setting to take effect. See the All_Regions.ini and canonicalization.ini files in the $ICAROOT/config directory for more information.

I have problems running published applications that access a serial port

If a published application accesses a serial port, the application might fail (with or without an error message, depending on the application itself) if the port has been locked by another application. Under such circumstances, check that there are no applications that have either temporarily locked the serial port or have locked the serial port and exited without releasing it.

To overcome this problem, stop the application that is blocking the serial port. Regarding UUCP-style locks, there might be a lock file left behind after the application exits. The location of these lock files depends on the operating system used.

I cannot start Receiver

If Receiver does not start, the error message "Application default file could not be found or is out of date" appears. The reason might be that the environment variable ICAROOT is not defined correctly. This is a requirement if you installed Receiver to a non-default location. To overcome this problem, Citrix recommends that you do one of the following:

- Define ICAROOT as the installation directory.

To check that the ICAROOT environment variable is defined correctly, try starting Receiver from a terminal session. If the error message still appears, it is likely that the ICAROOT environment variable is not correctly defined.

- Reinstall Receiver to the default location. For more information about installing Receiver, see Install and set up.

  If Receiver was previously installed in the default location, remove the /opt/Citrix/ICAClient or $HOME/ICAClient/platform directory before reinstalling.

I want to find the Citrix CryptoKit (formerly SSLSDK) or OpenSSL version number

To confirm the version number of the Citrix SSLSDK or OpenSSL that you are running, you can use the following command:
strings libctxssl.so | grep “Citrix SSLSDK”

You can also run this command on AuthManagerDaemon or PrimaryAuthManager

My keyboard shortcuts do not function correctly

If your window manager uses the same key combinations to provide native functionality, your key combinations might not function correctly. For example, the KDE window manager uses the combinations from CTRL+SHIFT+F1 to CTRL+SHIFT+F4 to switch between desktops 13 to 16. If you experience this problem, try the following solutions:

- Translated mode on the keyboard maps a set of local key combinations to server-side key combinations. For example, by default in Translated mode, CTRL+SHIFT+F1 maps to the server-side key combination ALT+F1. To reconfigure this mapping to an alternative local key combination, update the following entry in the [WFClient] section of $HOME/.ICAClient/wfclient.ini. This maps the local key combination Alt+Ctrl+F1 to Alt+F1:
  - Change Hotkey1Shift=Ctrl+Shift to Hotkey1Shift=Alt+Ctrl.
- Direct mode on the keyboard sends all key combinations directly to the server. They are not processed locally. To configure Direct mode, in the [WFClient] section of $HOME/.ICAClient/wfclient.ini, set TransparentKeyPassthrough to Remote.
- Reconfigure the window manager so that it suppresses default keyboard combinations.

I want to enable a remote Croatian keyboard

This procedure ensures that ASCII characters are correctly sent to remote virtual desktops with Croatian keyboard layouts.

1. In the WFClient section of the appropriate configuration file, set UseEUKSforASCII to True.
2. Set UseEUKS to 2.

I want to use a Japanese keyboard on the client

To configure use of a Japanese keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Japanese (JIS)

I want to use an ABNT2 keyboard on the client

To configure use of an ABNT2 keyboard, update the following entry in the wfclient.ini configuration file:

KeyboardLayout=Brazilian (ABNT2)

Some keys on my local keyboard do not behave as expected

Choose the best-matching server layout from the list in $ICAROOT/config/module.ini.

Windows Media Player fails to play files in certain formats

Citrix Receiver might not have GStreamer plugins to handle a requested format. This normally causes the server to request a different format. Sometimes the initial check for a suitable plugin incorrectly indicates that one is present. This is normally detected and causes an error dialog to appear on the server indicating that Windows Media Player encountered a problem while playing the file. Retrying the file within the session typically works because the format is rejected by Citrix Receiver. And as a result, the server either requests another format or renders the media itself.

In a few situations, the fact that there is no suitable plugin is not detected and the file is not played correctly, despite the progress indicator moving as expected in Windows Media Player.

To avoid this error dialog or failure to play in future sessions:

1. Temporarily add the configuration option “SpeedScreenMMAVerbose=On” to the [WFClient] section of $Home/.ICAClient/wfclient.ini, for example.
2. Restart wfica from a self-service that has been started from a terminal.
3. Play a video that generates this error.
4. Note (in the tracing output) the mime-type associated with the missing plugin trace, or the mime-type that should be supported but does not play (for example, “video/x-h264..”).
5. Edit $ICAROOT/config/MediaStreamingConfig.tbl. On the line with the noted mime-type, insert a ‘?’ between the ‘:’ and the mime type. This disables the format.
6. Repeat steps 2 - 5 (above) for other media formats that produce this error condition.

7. Distribute this modified MediaStreamingConfig.tbl to other machines with the same set of GStreamer plugins.

Note: Alternately, after identifying the mime-type it may be possible to install a GStreamer plugin to decode it.

I want to configure a serial port setting

To configure a single serial port, add the following entries in the $ICAROOT/config/module.ini configuration file:

LastComPortNum=1

ComPort1=device

To configure two or more serial ports, add the following entries in the $ICAROOT/config/module.ini configuration file:

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Connection configuration errors

These errors might occur if you configured a connection entry incorrectly.

E_MISSING_INI_SECTION - Verify the configuration file: "…". The section "…" is missing in the configuration file.

The configuration file was incorrectly edited or is corrupt.

E_MISSING_INI_ENTRY - Verify the configuration file: "…". The section "…" must contain an entry "…".

The configuration file was incorrectly edited or is corrupt.

E_INI_VENDOR_RANGE - Verify the configuration file: "…". The X server vendor range "…" in the configuration file is invalid.

The X Server vendor information in the configuration file is corrupt. Contact Citrix.

wfclient.ini configuration errors

These errors might occur if you edited wfclient.ini incorrectly.

E_CANNOT_WRITE_FILE - Cannot write file: "…"

There was a problem saving the connection database; for example, no disk space.

E_CANNOT_CREATE_FILE - Cannot create file: "…"

There was a problem creating a connection database.

E_PNAGENT_FILE_UNREADABLE - Cannot read XenApp file "…": No such file or directory.

— Or —

Cannot read XenApp file "…": Permission denied.

You are trying to access a resource through a desktop item or menu, but the XenApp file for the resource is not available. Refresh the list of published resources by selecting **Application Refresh** on the **View** menu, and try to access the resource again. If the error persists, check the properties of the desktop icon or menu item, and the XenApp file to which the icon or item refers.

PAC file errors

These errors might occur if your deployment uses proxy auto-configuration (PAC) files to specify proxy configurations.

Proxy detection failure: Improper auto-configuration URL.

An address in the browser was specified with an invalid URL type. Valid types are http:// and https://, and other types are not supported. Change the address to a valid URL type and try again.

Proxy detection failure: .PAC script HTTP download failed: Connect failed.

Check if an incorrect name or address was entered. If so, fix the address and retry. If not, the server could be down. Retry later.

Proxy detection failure: .PAC script HTTP download failed: Path not found.

The requested PAC file is not on the server. Either change this on the server, or reconfigure the browser.

Proxy detection failure: .PAC script HTTP download failed.

The connection failed while downloading the PAC file. Reconnect and try again.

Proxy detection failure: Empty auto-configuration script.

The PAC file is empty. Either change this on the server, or reconfigure the browser.

Proxy detection failure: No JavaScript support.

The PAC executable or the pac.js text file is missing. Reinstall Receiver.

Proxy detection failure: JavaScript error.

The PAC file contains invalid JavaScript. Fix the PAC file on the server. Also see Connection issues.

Proxy detection failure: Improper result from proxy auto-configuration script.

A badly formed response was received from the server. Either fix this on the server, or reconfigure the browser.

Other errors

This topic contains a list of other common error messages you may see when using Receiver.

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting.

When running Receiver from the command line, this usually means the description given on the command line was not found in the appsrv.ini file.

E_BAD_OPTION - The option "…" is invalid.

Missing argument for option "…".

E_BAD_ARG - The option "…" has an invalid argument: "…".

Invalid argument specified for option "…".

E_INI_KEY_SYNTAX - The key "…" in the configuration file "…" is invalid.

The X Server vendor information in the configuration file is corrupt. Create a configuration file.

E_INI_VALUE_SYNTAX - The value "…" in the configuration file "…" is invalid.

The X Server vendor information in the configuration file is corrupt. Create a configuration file.

E_SERVER_NAMELOOKUP_FAILURE - Cannot connect to server "…".

The server name cannot be resolved.

Cannot write to one or more files: "…". Correct any disk full issues or permissions problems and try again.

Check for disk full issues, or permissions problems. If a problem is found and corrected, retry the operation that prompted the error message.

Server connection lost. Reconnect and try again. These files might be missing data: "…".

Reconnect and retry the operation that prompted the error.

Sending diagnostic information to Citrix Technical Support

If you are experiencing problems using Receiver, you may be asked to provide Technical Support with diagnostic information. This information assists this team in trying to diagnose the problem and offer assistance to rectify it.

To obtain diagnostic information about Receiver

1. In the installation directory, type util/lurdump. It is recommended that you do this while a session is open and, if possible, while the issue is occurring.

   A file is generated that contains detailed diagnostic information, including version details, the contents of Receiver's configuration files, and the values of various system variables.

2. Check the file for confidential information before sending it to Technical Support.

SDK and API

November 7, 2018

Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) provides support for writing server-side applications and client-side drivers for additional virtual channels using the ICA protocol. The server-side virtual channel applications are on XenApp or XenDesktop servers. This version of the SDK provides support for writing new virtual channels for Receiver for Linux. If you want to write virtual drivers for other client platforms, contact Citrix.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI is designed to make writing your own virtual channels easier.
- Working source code for several virtual channel sample programs that demonstrate programming techniques.
- The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

For more information on SDK, see Citrix Virtual Channel SDK for Citrix Receiver for Linux.

Command-line Reference and Parameters

For information on command-line reference and parameters, see Citrix Receiver for Linux Command Reference.

Platform Optimization SDK

As part of the HDX SoC initiative for Citrix Receiver for Linux, we have come up with the 'Platform optimization SDK' for enabling an ecosystem of low cost, low power, high performance devices with

innovative form factors.

The Platform Optimization SDK can be used by developers looking to improve the performance of Linux-based devices by allowing them to create plug-in extensions for the ICA engine component (wfica) of Citrix Receiver for Linux. Plugins are built as shareable libraries that are dynamically loaded by wfica. These plugins can help you optimize the performance of your Linux devices, enabling the following functions:

- Provide accelerated decoding of JPEG and H.264 data used to draw the session image
- Control the allocation of memory used to draw the session image
- Improve performance by taking control of the low-level drawing of the session image
- Provide graphics output and user input services for OS environments that do not support X11

For information, see Citrix Receiver for Linux - Platform Optimization SDK.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States